Safety Instrumented Systems

By Steve Gillespie BSc (hons), Dip I.T. (Open), GCGI (Eng), I. Eng, MIIE
Shell Global Solutions UK, Measurement, Instrumentation and Automation Business Group

Summary:

In an increasingly multidisciplinary engineering environment, and in the face of ever increasing system complexity, there is a growing need for all engineers and technicians involved in process engineering to be aware of the implications of designing and operating safety-related systems. This includes knowledge of the relevant safety standards. Safety Instrumented Systems play a vital role in providing the protective layer functionality in many industrial process and automation systems. This article describes the purpose of process safety-related systems in general and highlights best engineering practice in the design and implementation of typical safety instrumented systems, underpinned by the relevant standards.

The Need for Safety Instrumentation

Managing and equipping industrial plant with the right components and sub-systems for optimal operational efficiency and safety is a complex task. Safety Systems Engineering (SSE) describes a disciplined, systematic approach, which encompasses hazard identification, safety requirements specification, safety systems design and build, and systems operation and maintenance over the entire lifetime of plant. The foregoing activities form what has become known as the “safety Life-cycle” model, which is at the core of current and emerging safety related system standards.

Risk and Risk Reduction Methods

Safety can be defined as “freedom from unacceptable risk”. This definition is important because it highlights the fact that all industrial processes involve risk. Absolute safety, where risk is completely eliminated, can never be achieved; risk can only be reduced to an acceptable level. Therefore all risks should be dealt with on the ALARP basis, i.e. the target is to ensure that risk is reduced to As Low As Reasonably Practicable.

Safety Methods employed to protect against or mitigate harm/damage to personnel, plant and the environment, and reduce risk include:

- Changing the process or engineering design
- Increasing mechanical integrity of the system
- Improving the Basic Process Control System (BPCS)
- Developing detailed training and operational procedures
- Increasing the frequency of testing of critical system components
- Using a safety Instrumented System (SIS)
- Installing mitigating equipment

Figure 1 illustrates the above measures in terms of employing protective layers (equipment and/or administrative controls) to reduce risk to an acceptable level. The amount of risk reduction for each layer is dependent on the nature of the risk and the amount of risk reduction afforded by the applicable layer employed. Protective layers can be further classified as either Prevention or Mitigation layers. The former are put in place to stop hazardous occurrences and the latter are designed to reduce the consequences after hazardous events have occurred. In the case illustrated in figure 1, the protective layers are further sub-divided

into in-plant and external areas. Methods that provide layers of protection should be independent, reliable, auditable and designed specifically for the risk involved.

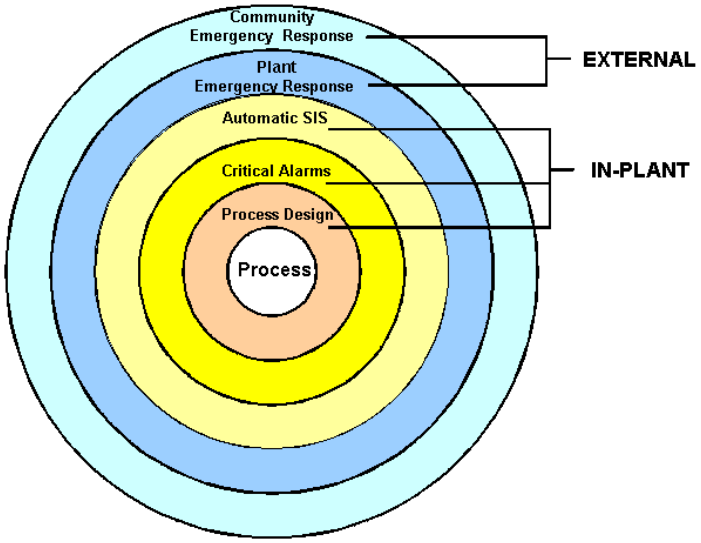

Figure 1 – Safety Protective layers

Hazards Analysis

Generally, the first step in determining the levels of protective layers required involves conducting a detailed hazard and risk analysis. In the process industries a Process Hazards Analysis (PHA) is generally undertaken, which may range from a screening analysis through to a complex Hazard and Operability (HAZOP) study, depending on the complexity of operations and severity of the risks involved. The latter involves a rigorous detailed process examination by a multi-disciplinary team comprising process, instrument, electrical and mechanical engineers, as well as safety specialists and management representatives. Detailed cause and effect scenarios are considered and risks quantified for all process functions and operations. If the study determines that the mechanical integrity of a process and the process control are insufficient to protect against the potential hazard, a SIS may be required. The remainder of this article will focus on SISs and the applicable standards to establish best practice.

Safety Instrumented Systems

A SIS is a system comprising sensors, logic solvers and actuators for the purposes of taking a process to a safe state when normal predetermined set points are exceeded, or safe operating conditions are violated. SISs are also called emergency shutdown (ESD) systems, safety shutdown (SSD) systems, and safety interlock systems. Although such systems may contain pneumatics, this article focuses on the more common electric, electronic, or programmable electronic systems.

Process Control Systems and SIS

As illustrated in figure 2, it is generally preferable that any protection system (including a SIS) be kept functionally separate from the BPCS in terms of its ability to operate independent of

the state of the BPCS. The operating equipment is also known as the Equipment Under Control (EUC). In essence, protection systems should be capable of functioning to protect the EUC when the process control system is in fault. Where separation is not possible because the safety functions are integral with the process control system (increasingly common in modern complex systems), all parts of the system that have safety-related functions should be regarded as a SIS for the purposes of safety integrity assessment.

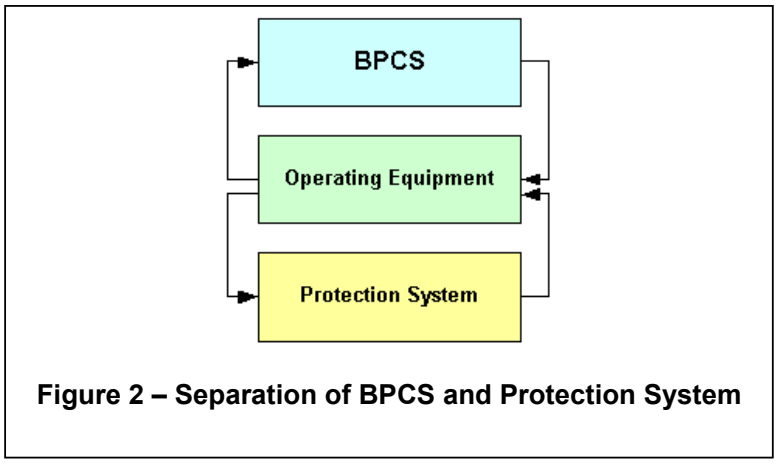

Figure 2 – Separation of BPCS and Protection System

Figure 3 shows the basic layout of a typical SIS (in this case controlling a shutdown valve as the final control element).

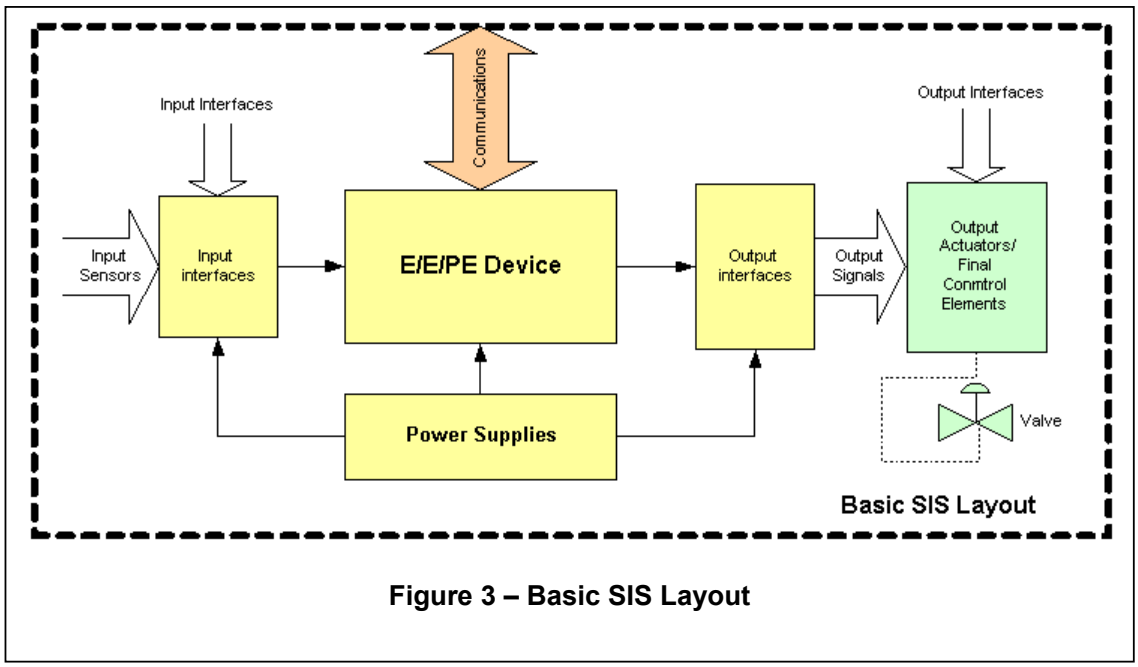

Figure 3 – Basic SIS Layout

The basic SIS layout comprises:

- Sensor(s) for signal input and power
- Input signal interfacing and processing
- Logic solver with associated communications and power
- Output signal processing, interfacing and power
- Actuators and valve(s) or switching devices to provide the final control element function.

The scope of a SIS encompasses all instrumentation and controls that are responsible for bringing a process to a safe state in the event of an unacceptable deviation or failure.

Standards – IEC 61508, IEC 61511 and ANSI/ISA S84

IEC 61508:*Functional Safety of Electrical, Electronic and Programmable Electronic Safety related Systems* [1] is a generic standard on which sector specific safety standards are to be based. For the process sector IEC61511 is in draft form and ANSI/ISA S84 [2] (the USA equivalent) is already published. The IEC61508 standard is fast becoming the European norm, and can apply to a range of Electrical/Electronic/Programmable Electronic (E/E/PES) safety-related systems including:

- Emergency Shut-Down (ESD) systems,
- Fire and gas systems,
- Turbine control,
- Gas burner management,
- Dynamic positioning
- Railway signalling systems,
- Machinery guarding & interlock systems.

IEC 61508 is a seven-part standard that provides specific guidelines on the functional safety of E/E/PES safety-related systems. Developed by the International Electrotechnical Commission (IEC, Geneva, Switzerland), the standard directs the disciplined management of all components of Safety Related Systems, from sensors and logic solvers, to the response function applications that will take the process to a safe state when predetermined variables are reached. The standard applies to the entire life cycle of the safety system, from initial concept, through specification, design, operation and use, to final decommissioning. Parts 1 to 3 of the standard provide guidance on the management, development, deployment, and operation of the E/E/PES system hardware and software. Parts 4 to 7 of the standard deal specifically with definitions, applications and additional related information.

The following provides an outline of each part of the standard with the relevant section headings summarised in table 1.

IEC 61508-1
Defines the overall safety lifecycle model. The standard employs qualitative or quantitative techniques to identify the process risk to the safety related system. These techniques focus on project management, quality assurance and configuration management.

IEC 61508-2
Provides objectives for the safety development of the E/E/PES. Software is further defined in part 3. However, it should be noted that part 2 maintains jurisdiction.

IEC 61508-3
Provides objectives for the safety development of the software residing in the E/E/PES.

IEC 61508-4
Contains definitions, abbreviations and terminology used in the safety process that must be adhered to in order to establish and maintain consistency.

IEC 61508-5
Provides the formal approach for determining the Safety Integrity Level (SIL) of the safety system (SIL is described later in this article).

IEC 61508-6
Provides specific guidelines for applying IEC 61508 parts 2 and 3.

IEC 61508-7
Provides details of the safety techniques and measures relevant to parts 2 and 3.

IEC 61508: Parts and Headings	
Part 1, December 1998	General requirements
Part 2, May 2000	Requirements for E/E/PE Safety Related Systems
Part 3, December 1998	Software requirements
Part 4, December 1998	Definitions and abbreviations
Part 5, December 1998	Examples of methods for determination of SIL
Part 6, April 2000	Guidelines on the application of IEC 61508-2 and 61508-3
Part 7, March 2000	Overview of techniques and measures

Table 1 – IEC 61508 Standard Parts and Headings

The Safety Life-Cycle Model

The core of IEC 61508 is the Safety Life-cycle model (figure 4), which specifies the structured and auditable management of safety related systems from first concept through to eventual de-commissioning.

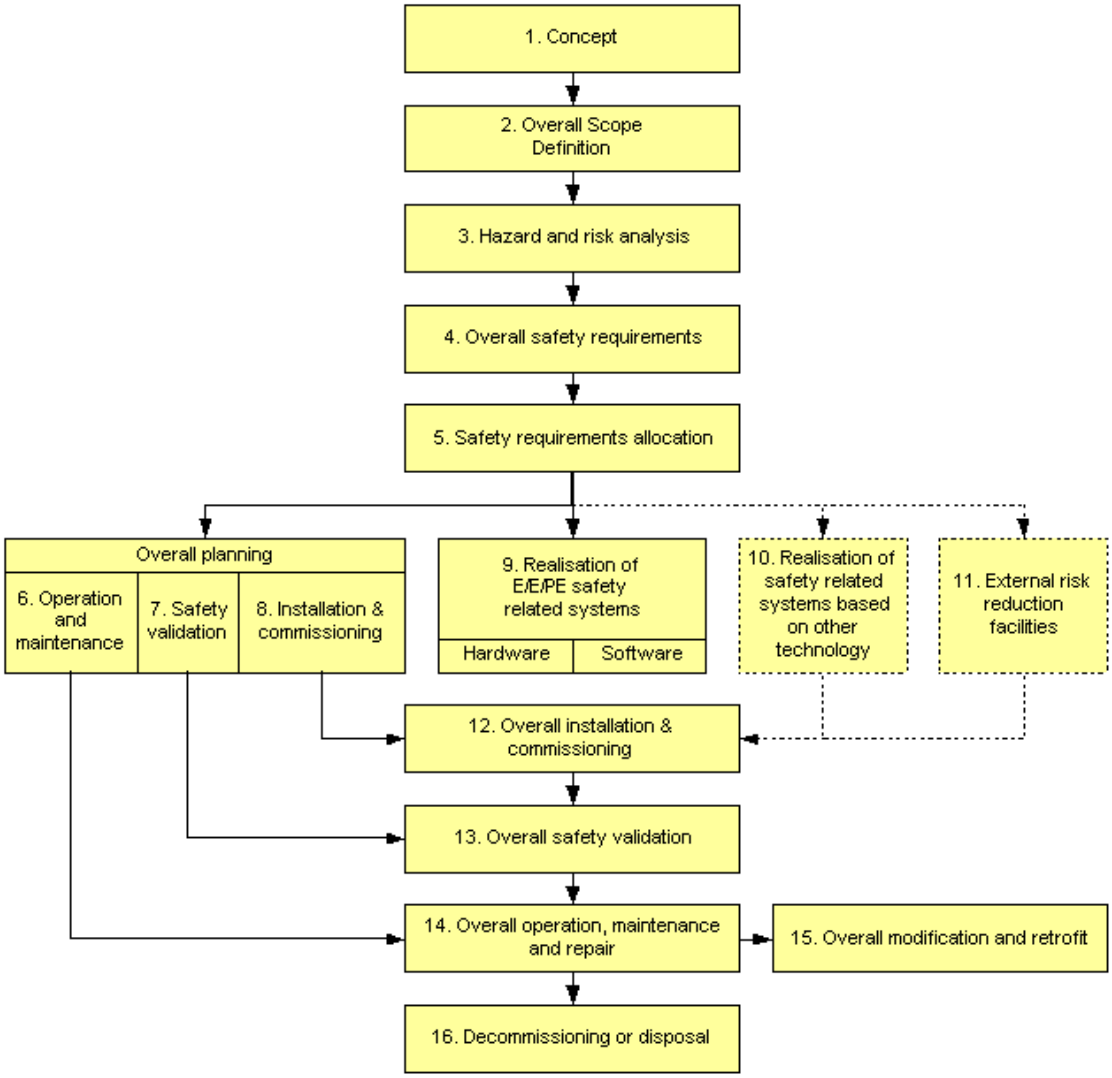

Figure 4 – IEC 61508 Life-Cycle Model

A detailed treatment of each part of the safety life cycle and how each step is carried out is beyond the scope of this article. However, a simplified sequential approach to developing safety-related systems is outlined below, followed by an example methodology for determining safety Integrity Level (SIL) for a SIS.

Simplified steps in developing the Safety-related System

1. Formulate the conceptual design of the process and define the overall scope
2. Identify process hazards and risks via a hazard analysis and risk assessment
3. Identity non-SIS layers of protection
4. Determine the need for additional protection i.e. a SIS

Where a SIS is identified as being required…

5. Determine the target SIL (using qualitative and/or quantitative methods)
6. Develop safety requirement specification (SRS)
7. Develop SIS conceptual designs to meet SRS
8. Develop detailed SIS design
9. Install the SIS
10. Perform Commissioning and pre-startup testing
11. Develop operation and maintenance procedures
12. Conduct pre-startup safety review
13. Carry out operation and maintenance of SIS
14. Record and re-assess any modification to SIS
15. Carry out decommissioning procedures at the end of the life of the SIS.

Safety Integrity Level (SIL) and Availability

Safety Integrity Level (SIL) is a statistical representation of the safety availability of an SIS at the time of process demand. It is at the heart of acceptable SIS design and includes the following factors:

- Device integrity
- Diagnostics
- Systematic and common cause failures
- Testing
- Operation
- Maintenance

The safety availability (i.e. proportion of time that the system is operational) of a SIS depends on:

- Failure rates and Failure modes of components
- Redundancy
- Voting scheme(s) adopted
- Testing frequency

When the hazards identification and risk assessment phase concludes that a SIS is required, the level of risk reduction afforded by the SIS and the target SIL have to be assigned. The effectiveness of a SIS as an independent protective layer is described in terms of the probability it will fail to perform its required function when it is called upon to do so. This is called its Probability of Failure on Demand (PFD). In practice, the average Probability of Failure on Demand (PFD_{avg}) is used. Table 2 shows the relationship between PFD_{avg}, required safety system Availability, Mean Time Between Failure (MTBF) and SIL.

SIL	Availability	PFD (avg)	MTBF
4	>99.99%	10^{-5} to $<10^{-4}$	100000 to 10000
3	99.9%	10^{-4} to $<10^{-3}$	10000 to 1000
2	99-99.9%	10^{-3} to $<10^{-2}$	1000 to 100
1	90-99%	10^{-2} to $<10^{-1}$	100 to 10

Table 2 – IEC 61508 SIL and related Measures
This is for low demand mode operation[1]

The assignment of a SIL is a corporate decision based on risk management and risk tolerance philosophy. IEC 61508 requires that the assignment of SIL be carefully performed and documented, and provides both qualitative and quantitative guidance tables.

Example SIL evaluation

IEC 61508 contains guidance on using both qualitative and quantitative methods to determine the SIL for a system based on risk frequency and consequence tables and graphs. This article will focus on a simple quantitative method as an illustrative example, and reference should be made to the actual standard for further details on alternative methods.

Assuming the hazards analysis and risk assessment phase reveals that overall risk reduction is required it may be determined that a SIS is necessary. It follows that the amount of risk reduction to be provided by the SIS must be determined and this will in turn determine the SIL level for the intended SIS. The following steps illustrate application of the general guidelines contained in IEC-61508:

1. Set the target Tolerable Risk level (Ft), where Ft is the risk frequency, often determined as hazardous event frequency x consequence of hazardous event expressed numerically

2. Calculate the present risk level (Fnp) for the EUC, which is the risk frequency with no protective functions present (or unprotected risk)

[1] IEC 61508 defines both low and high demand modes of operation. Low demand covers systems where the demand on the safety system is lower than once per year. High demand covers systems where the demand is greater than once per year or is continuous.

3. The ratio Fnp/Ft gives the Risk Reduction Factor (RRF) required to achieve the target tolerable risk

4. Determine the amount of RRF to be assigned to the SIS (RRF_{SIS}). The reciprocal of RRF_{SIS} gives the target average Probability of Failure on Demand (PFD_{avg}) the SIS must achieve.

5. Translate the PFD_{avg} value into a SIL value (using guidance tables)

Consider a system with EUC that has an unprotected risk frequency (Fnp) of 1 hazardous event per 5 years (Fnp = 0.2/year) with a consequence classified as “Critical”. Tables 3 and 4 show examples of guidance tables used for risk classification and class interpretation of accidents from IEC 61508-5.

Frequency	Catastrophic	Critical	Marginal	Negligible
	> 1 death	1 death or injuries	Minor injury	Production loss
1 per year	I	I	I	II
1 per 5 years	I	I	II	III
1 per 50 years	I	II	III	III
1 per 500 years	II	III	III	IV
1 per 5000 years	III	III	IV	IV
1 per 50000 years	IV	IV	IV	IV

Table 3 – Risk Classification of Accidents: Table B1 of IEC 61508-5
Suggested example adapted to hypothetical industry sector.

Risk Class	Interpretation
I	Intolerable risk
II	Undesirable risk, tolerable only if risk reduction is impracticable or if the costs are grossly disproportionate to the improvement gained
III	Tolerable risk if the costs of risk reduction would exceed the improvement gained
IV	Negligible risk

Table 4 – Risk Classification of Accidents: Table B2 of IEC 61508-5
Interpretation of risk classes

Using tables 3 and 4, the unprotected risk is determined as class I. The target is to reduce this risk to a tolerable risk of class III, i.e. 1 hazardous event per 500 to 5000 years.

If we consider the safest target, Ft = 1 hazardous event in 5000 years, this represents a frequency of 0.0002 events/year.

This gives a target risk reduction factor RRF of Fnp/Ft = 0.2/0.0002 = 1000

If there are no non-SIS protective layers assigned to the system, the SIS must fulfil the total RRF of 1000. So, in this case the total RRF = RRF_{SIS}.

Now $PFD_{avg} = 1/ RRF_{SIS} = 1/1000 = 0.001 = 1 \times 10^{-3}$

Using the SIL assignments in table 2, this gives a SIL target 2.

Summary

This has provided a brief introduction to safety-related systems with the focus on Safety Instrumented Systems. It is likely that IEC 61508 and emerging industry sector specific standards based on IEC 61508 (e.g. IEC 61511 for the process industry sector) will continue to gain momentum. All multidisciplinary engineers can benefit from awareness of the implications and applications of safety-related systems and these standards.

Training:

Safety Instrumentation & Shutdown Systems for Industry (Short Course) - IDC Technologies, web site – www.idc-online.com

Further Reading:

Safety Shutdown Systems – ISA, 1998, Gruhn and Cheddie

Out of Control – UK Health & Safety Executive Publication, 1995

Programmable Electronic Systems in Safety Related Applications: an Introductory Guide - Health & Safety Executive Publication

Functional Safety: A Straightforward Guide to IEC61508 and Related Standards - Butterworth-Heinemann Publications; D.J. Smith & K.G.L. Simpson

References:

[1] IEC 61508 Parts 1-7: 1998, *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems*, International Electrotechnical Commission, Geneva, Switzerland.

[2] ANSI/ISA Standard S84.01-1996, *Application of Safety Instrumented Systems to the Process Industries*, International Society for Measurement & Control, Research Triangle Park, NC, (1996)

Steve Gillespie is a measurement technologist with the Measurement, Instrumentation and Automation Business Group of Shell Global Solutions UK.