# Safety management in process industries

## Part 1 – Standards

**Robert Martinez, Per Christian Juel, Per Fjelldalen**

**Industrial processes involve the control of huge energies, for example in the form of a red-hot steel furnace or a tank of poisonous chemicals. The malfunction or failure of a critical component can release a considerable destructive potential – putting humans and the environment at risk. Besides such worst-case scenarios, countless smaller incidents can cause local damage and disturbances affecting the productivity, reliability and reputation of the plant and its owners.**

**No system can be made completely failsafe. Instead, safety management must seek to minimize both the risk of incidents occurring, and the consequences of those incidents should they occur nevertheless. To achieve this, safety has to be omnipresent in the design and operation of all phases and aspects of the plant's lifecycle and operation. New standards and a clear safety-oriented approach to project management make this achievable.**

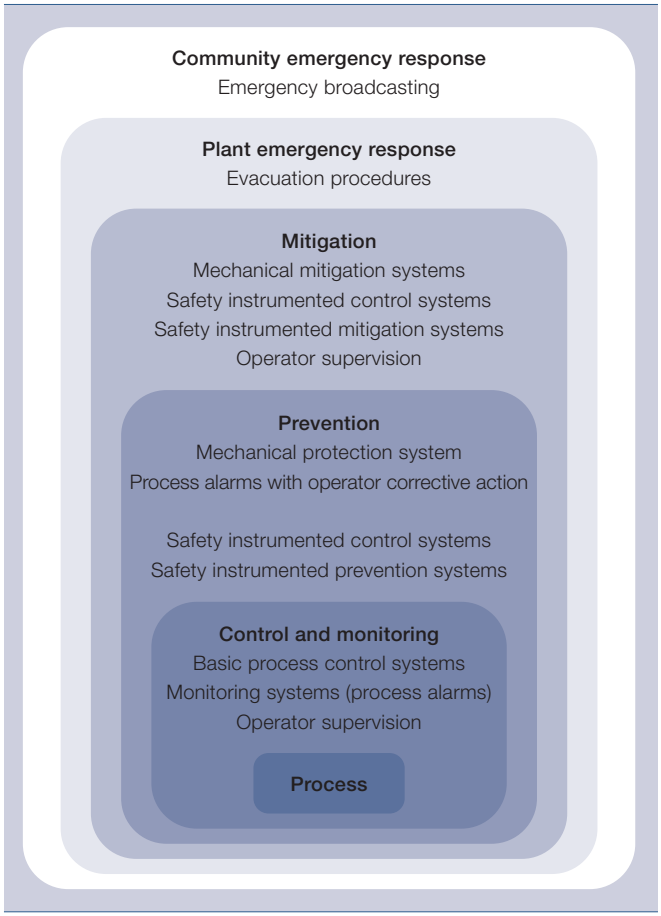
Most industrial activities imply a potential safety risk – to plant personnel, local communities or the environment. The enormous physical and chemical energies used in process industries constitute a major risk. The scale of these energies is evident to anyone who has stood next to a paper machine or peered into a foundry furnace. It is these high energies that distinguish process from manufacturing industries. Industrial accidents such as in Bhopal, India have raised public awareness to the need to contain the risks in process industries.

Each and every stage of a plant's lifecycle contributes to safety: specification of requirements, engineering, contracting, testing, training, operation, and maintenance. In many countries strict standards are imposed on automation component suppliers, system integrators and operators. Such standards reflect that there is more to safety than designing and installing safety equipment – safety is a way of thinking that must be applied throughout all phases of the plant's lifecycle.

Ensuring safety over such long time scales and across so many different teams and suppliers requires very strong management procedures. The new breed of safety regulations is often referred to as "safety management".

Operating companies have learned that safety management is a sound business practice: It protects their assets and contributes to continuity and quality in the production processes as well as taking into account the potential consequences of law suits and damage actions. Less tangible but still very important is the concern for the companies' image within the world community. The globalization of production has been followed by the globalization of media: companies must constantly demonstrate the same high level of safety wherever they have outsourced their production.

1 Safety lifecycle phases as defined in IEC-61511 Part 1.




### International standards for safety management

Over the past 10 years, the IEC (International Electrotechnical Commission) has led the effort to internationalize the requirements for safety related systems. In 1998, IEC published a generic standard for the design, manufacture and management of Electrical/ Electronic/ Programmable Electronics (E/E/PE) components for use in safety-related systems. IEC-61508 is today globally recognized and customers require that suppliers demonstrate the compliance of their instruments and control platforms.

A complementary standard, IEC-61511, was published in 2003. This standard applies to system integrators and operators in process industries. It must be complied to when entire safety and automation systems are delivered. Both standards focus on compliance throughout the product's lifecycle: project planning, product development, project execution, services and maintenance and decommissioning.

The American ISA sp84 standard, first published in 1997, is now harmonized with and corresponds to IEC-61511, which will soon replace the former. The third IEC standard in this series, IEC-62061, addresses safety in machin-

Table 1 Safety terms from IEC-61511.

| | |
|---|---|
| Basic Process Control System (BPCS) | The control system minus any safety equipment or software. |
| Diagnostic Coverage (DC) | Ratio of the detected failure rate to the total failure rate as detected by diagnostic tests. |
| Logic Solver | The controller unit with CPU |
| Programmable Electronic System (PES) | The control loop including sensors, logic solver and actuators. |
| Safety Integrity Level (SIL) | A number from 1 to 4 specifying target failure rates for safety instrumented functions. |
| Safety Instrumented Function (SIF) | A PES with a specified SIL for protection from a specific hazard. |
| Safety Instrumented System (SIS) | One or more SIFs working together. |

### 1 ABB Safety Jargon Buster

ABB's Safety Jargon Buster explains some of the terminology users are likely to encounter when purchasing or handling safety equipment and systems. The document is available as hyperlinked .pdf document from the ABB website: www.abb.com.

ery. This standard, which is of special interest to robotics, is currently under development and will eventually be harmonized with IEC-61508.

The IEC-61511 standard has three parts: Part 1 is "normative"; the legally binding text which can be difficult for non-experts to read without a grasp of the special safety vocabulary see textbox 1. The other two parts provide explanation and guidelines to Part 1.

The IEC is a standards-setting body only; companies seeking certification of their safety systems must approach a certification authority such as TÜV in Germany.

Each and every stage of a plant's lifecycle contributes to safety: specification of requirements, engineering, contracting, testing, training, operation, and maintenance.

**Safety planning and project management phase**

Part 1 of IEC-61511 divides the plant lifecycle into the phases shown in 1. Before project work can begin however, a comprehensive safety plan must be defined describing in detail how the entire lifecycle is to be managed. The competence level and role of each safety team member must also be documented. The safety plan describes the formal procedures to ensure that what is delivered conforms to the specification (verification) and to the intentions of the standard (validation).

**Safety hazard and risk assessment phase**

The main purpose of this phase is to ensure that hazards are identified and that their risk to their surroundings is quantified. The first step is the identification and characterization of the hazard associated with the process equipment, sometimes referred to as Hazard Analysis. HAZOP see textbox 2 is one of several methodologies recommended by IEC-61511. According to the vocabulary of IEC-61511, a hazard will only result in "risk" if it there is a corresponding loss of life or property or environmental damage. The scale of this loss is coded in the IEC standard "risk graph" scheme 2. Discrete values for the four parameters C, F, P, W are found in standard risk graph tables. The values of these parameters are estimated for each item of hazardous equipment. This approach results in a target Safety Integrity Level (SIL) which forms the basis for the next lifecycle phase: the design of the Safety Instrumented Function (SIF) which must reduce risk to a tolerable level. These tolerable levels are low but not zero; complete prevention can never by guaranteed.

**Safety function allocation and requirements phase**

New and essential in the IEC publications for safety related systems is the concept of considering a safety function as a whole. The programmable controller, the instrument(s) and the actuator(s) that form a function should not be considered in isolation but in their interaction and common functionality.

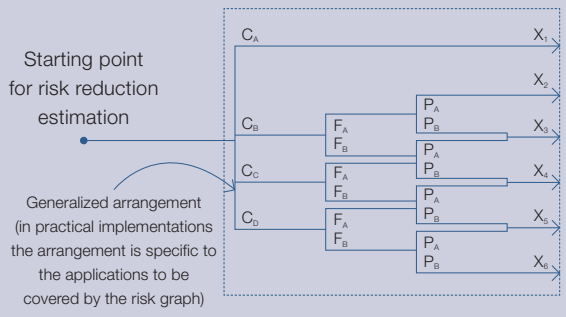
An SIF consists of three subsystems: the initiator (measurement) subsystem, the logic solver (controller) subsystem and the final element (actuator) subsystem. The subsystems must individually meet relevant IEC-61511 requirements. Reliability figures are calculated individually for each subsystem and summarized and verified to comply with the required reliability figure for the complete function.

The main purpose of this phase is the specification of an SIF with sufficient reliability to reduce the risk quantified in the previous phase. SIF reliability is classified as one of four possible SIL levels quantifying the reliability of the entire SIF loop. In the process industry SIL 1–3 are relevant. Normally, SIL-3 SIF represents less than 15 percent of the total SIF in a plant.

Over the past 10 years, the IEC has led the effort to internationalize the requirements for safety related systems.

The instrumented SIF need not absorb the entire required risk reduction. The standard recommends a Layer of Protection Analysis (LOPA) to evaluate other, non-instrumented means to reduce the risk to tolerable levels, such as mechanical pressure relief valves, containment walls etc. 3.

2 Risk graph scheme from IEC-61511.




| $W_3$ | $W_2$ | $W_1$ |
|---|---|---|
| a | --- | --- |
| 1 | a | --- |
| 2 | 1 | a |
| 3 | 2 | 1 |
| 4 | 3 | 2 |
| b | 4 | 3 |

C = Consequence parameter
F = Exposure time parameter
P = Probability of avoiding the hazardous event
W = In the absence of the SIF under consideration

--- = no safety requirements
a = no special safety requirements
b = A single SIF is not sufficent
1, 2, 3, 4 = Safety integrity level

## 2 HAZOP

HAZOP (Hazard and Operability Studies) is a methodology used for identifying potential hazards and operability problems in process plants.

Essentially, the procedure starts with a full description of a process. It questions every part of this description in a systematical and structured way to identify how possible deviations from the intended functionality can arise.

Table 2 Demand Mode of Operation.

| Safety integrity level (SIL) | Target average probability of failure on demand | Target risk reduction |
|---|---|---|
| 4 | $\geq 10^{-5}$ to $< 10^{-4}$ | > 10 000 to ≤ 100 000 |
| 3 | $\geq 10^{-4}$ to $< 10^{-3}$ | > 1 000 to ≤ 10 000 |
| 2 | $\geq 10^{-3}$ to $< 10^{-2}$ | > 100 to ≤ 1 000 |
| 1 | $\geq 10^{-2}$ to $< 10^{-1}$ | > 10 to ≤ 100 |

### Safety function design and engineering phases

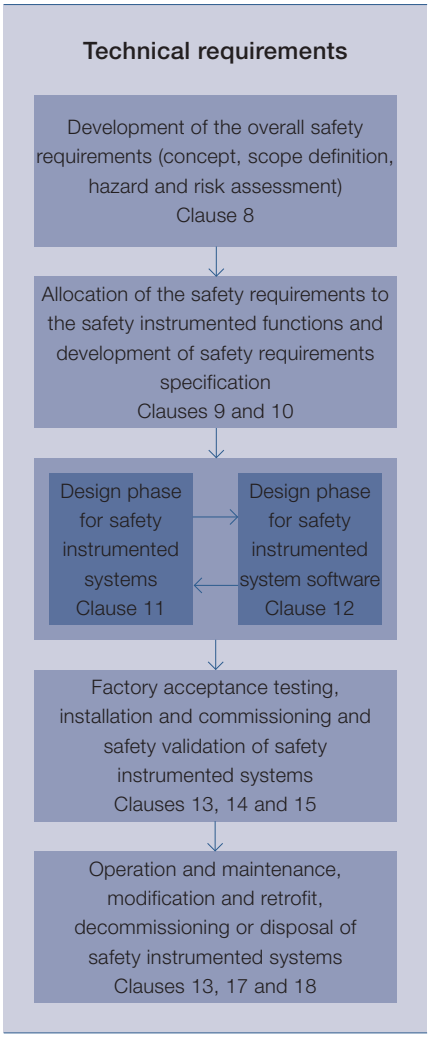
In the design phase, SIF is configured and instruments are specified with the necessary reliability (Probability of Failure on Demand, PFD). SIF loop design is an iterative process involving SIL reliability calculations for each design candidate. The main output of the design phase is the Safety Requirements Specification (SRS).

The mode of operation is determined by the form of the reliability calculations. There are two main operational modes for safety instrumented functions; low demand and continuous mode. Low demand is characterized by the requirement of not having more than one demand for the safety function per year. The SIL PFD values for this mode are shown in Table 2.

When designing a subsystem in a safety instrumented function several parameters must be considered:

- Safe Failure Fraction (SFF), the portion of the total amount of failures that can be considered safe by design or by diagnostic coverage.
- The fault tolerance indicates how many dangerous undetected failures can be tolerated before the integrity (SIL) degrades (eg, if only one single analog input channel is used for the safety instrumented function, the fault tolerance is zero).

3 Layers of protection from IEC-61511: Part 1.




Safety management must focus on the risks and safety aspects of all components and subsystems as well as their interaction throughout all phases of the plant's lifecycle.

Vendors of certified (IEC-61508) safety subsystem products must publish these parameters, which are vital to the configuration and verification of the whole SIF design. These parameters are the basis for the safety requirements specification for the engineering phase. In this phase, the SIF is implemented by software measures and detailed hardware design. Test specifications are defined for use in the subsequent installation and operation phases.

### Installation and operation phases

After delivery of the safety system the responsibility for safety management shifts from vendors (such as ABB) to their operating company customers. This article cannot cover these phases in detail, however some highlights of the safety requirements of these phases are:

- Pre-delivery validation testing should include loop, application and system tests: Simulation methods are recommended.
- Safety manuals and other documentation are required, as is training of operators and maintenance personnel.
- All safety-related incidents must be logged.
- All SIF sub-systems must be proof-tested at regular intervals, and the test results documented.
- Modifications must follow formal change and configuration management procedures.

### Conclusion and outlook

The combination of "safe" components does not automatically lead to a "safe" system. Rather, safety management must focus on the risks and safety aspects of all components and subsystems as well as their interaction throughout all phases of the plant's lifecycle. It must use certified methods to minimize the risk of the system as a whole. To make this possible, all teams and sub-suppliers must be involved in the safety process: from design and construction, through training and operations to decommissioning and disposal.

In the following article, ABB's application of the concepts and guidelines presented here are discussed.

**Robert Martinez**
**Per Christian Juel**
Corporate R&D
Billingstad, Norway
robert.martinez@no.abb.com,
per.c.juel@no.abb.com

**Per Fjelldalen**
ABB Process automation
Oslo, Norway
per.fjelldalen@no.abb.com