SIL MANUAL

SAFETY INSTRUMENTED SYSTEMS

DIGITAL PREVIEW

Plant Engineering and Maintenance
according to
IEC 61508 and IEC 61511

- Safety Integrity Levels
- Reliability and Probability of Failure on Demand
- Redundant System Architectures
- Risk Reduction
- Safety Requirements Specification
- IEC 61508 and IEC 61511 compendiums

gmi technology for safety

5th Edition

SAFETY INSTRUMENTED SYSTEMS

Manual for Plant Engineering and Maintenance

With reference to IEC61508 Ed. 2.0 “Functional safety of electrical/ electronic/programmable electronic safety-related systems” and IEC61511 Ed. 2.0 “Functional safety - Safety instrumented systems for the process industry sector”.

5th Edition

Authors

Basilio Abbamonte
Software Development and Quality Assurance Manager, GM International. (Retired)

Glisente Landrini
Former President and Managing Director, GM International.

Chapters 7; 8; 10
Tino Vande Capelle
Director Functional Safety Services, GM International.
FS Senior Expert and Trainer (TÜV Rheinland, # 0109/05, SIS).

gmi technology for safety

www.gminternational.com

ISBN: 978-88-942087-0-2
ISBN-A: 10.978.88942087 / 02
SIAE: 2017000345

Printed in Italy, March 2025

Introduction

GM International designs, manufactures and sells SIL2 and SIL 3 certified Intrinsically Safe Interfaces for use in Hazardous Locations, Safety Relays and Power Supplies that are intended to prevent accidents before they occur, thus reducing risk and enhancing safety in a very wide variety of applications.

This manual is a practical aid for the analysis, installation and maintenance of safety instrumented systems and associated components and will hopefully serve as a guide for understanding and implementing procedures into practical applications.

It represents an effort to share the results achieved in many years of research and experience in the field, with anyone willing to approach Safety Related Systems.

This manual is not intended for safety reliability specialists, but for the thousands of professionals employed in process industries who work with safety instrumented systems and who are expected to follow the appropriate industry standards.

Aren't the standards alone enough? The answer depends upon the knowledge and experience of the individual and the company.

The growing demand for experts in a critical sector like functional safety, underlies the urgency of a greater awareness and comprehension of all subjects presented herein.

Glisente Landrini
Former President of GM International

Index

Chapter 1 Presentation of IEC 61508, IEC 61511 and other safety related standards

Safety-related systems serve the function of protecting equipment and industrial processes where danger may occur in case of failure. These systems are not part of the process control system since their purpose is to bring the plant to a safe state in case of malfunctioning. Until a few years ago, these systems, for example ESD (Emergency Shut-Down), were being designed in compliance with the respective standards in force in the different countries, with no reference to a general normative.
This condition has changed with IEC 61508 and IEC 61511 which also introduce the following benefits for the final user:

- A more technical and scientific method in formulating requirements and specifications in the designing process.
- A more accurate definition of risk.
- A more valid designing of safety-related systems.
- An easier and wider demonstration of safety-related system's effectiveness.
- A far more cost-effective implementation of safety-related systems.
- An easier evaluation and effectiveness of maintenance operations.

The number of manufacturers of equipment complying with this standard is expected to grow. Information provided by the manufacturers allows the integration of their products into safety-related systems.

IEC 61508 is an international standard for the "functional safety" of electrical, electronic, and programmable electronics equipment. At present, in Europe, EN 61508 has been issued but not yet acknowledged as European Directive. This standard started in the mid 1980s when the International Electrotechnical Committee Advisory Committee of Safety (IEC ACOS) set up a task force to consider standardization issues raised by the use of a programmable electronic system (PES).Work began within IEC SC65A/Working Group 10 on a standard for PES used in safety-related systems. The group merged with Working Group 9 where a standard on software safety was in progress. The combined group treated safety as a system issue. IEC 61508 Brief history:

- 1985: Task Group set up to assess viability of developing a generic standard on PES's.
- Two working groups collaborate of developments of IEC standard that was to become IEC 61508 (draft IEC1508).
- 1998-2000: The parts of IEC 61508 (1-2-3-4-5-6-7) Edition 1 were published.
- 2005: PD IEC TR 61508-0 was published.
- "ENs" adopted in same year as the IEC publication dates.
- 2003: Revision of IEC 61508 /Edition 1 started.
- 2010: IEC 61508 / Edition 2 was published in April.

IEC 61508 (Functional Safety of electrical, electronic & programmable electronic safety-related systems) is divided into eight parts covering all safety lifecycle activities - concept - specifications - design - implementation - operation maintenance & modification.
Parts 1, 2, 3 are required for compliance (normative), the others are supporting information (informative) which provide further guidance information.

- Part 1 General requirements. (Normative)
- Part 2 Requirements for electrical/electronic/programmable electronic safety-related systems. (Normative)
- Part 3 Software requirements. (Normative)
- Part 4 Definitions and abbreviations. (Informative)
- Part 5 Examples of methods for the determination of safety integrity levels. (Informative)
- Part 6 Guidelines on the application of Parts 2 and 3. (Informative)
- Part 7 Overview of techniques and measures. (Informative)

Edition 2 has been approved in April 2010. The relationship between technical requirements presented in parts 1, 2 and 3 and the supporting information in parts 4 through 7 is shown in Figure 1, in the following page.

Although the standard has been criticized for the “extensive” documentation requirements and use of unproven “statistical” techniques, it represents a great step forward in many industries.

The standard focuses attention on risk-based safety-related systems design, which should result in far more cost-effective implementations. It also requires the attention to details that is vital to any safe system design. Because of these features and the large degree of international acceptance for a single set of documents, many consider the standard to be major advance for the technical world.

The experience of GM International on SIL 2 and SIL 3 hardware and software design, has shown how the suggested techniques in the standard are indeed a valid guidance for reducing “dangerous undetected failures” which is the correct path towards increasing safety integrity levels for any safety-related system.

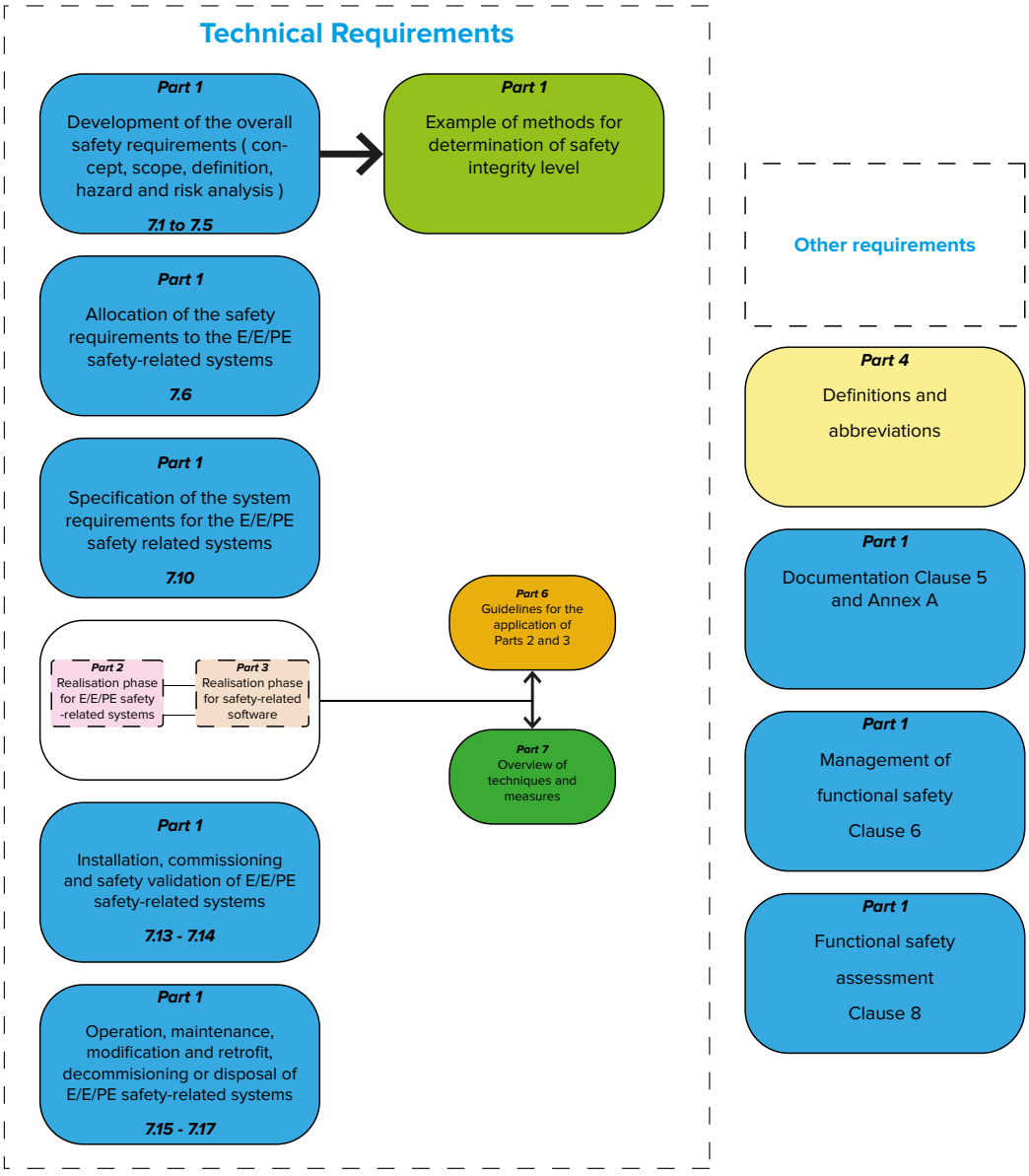

Figure 1, IEC 61508 requirements

1.1 Scope of IEC 61508

Safety can be primary, functional or derived. Primary safety deals with risks, such as electric discharges generated by an electric equipment. Functional safety depends on the measures of risk reduction adopted in the system or equipment under control (EUC). Derived safety deals with the indirect consequences of an EUC, which does not perform as expected, for example providing a drug with a wrong recipe which might kill instead of healing. The standard specifically refers to functional safety, however its principles can also be generally applied to other aspects of safety.

IEC 61508 is one of the main publications, on safety matters, of IEC (International Electrotechnical Commission) and involves many industries and applications, such as, for example, the PED directive (Pressured Equipment Directive) and protection method “b” for non-electrical equipment of ATEX (mechanic), as well as EN 50495 (Safety devices required for safe functioning of equipment with respect to explosion risks), in which, for the first time in ATEX standard, functional Safety Integrity Levels (SIL) are used as a protection system.

The main purpose of IEC 61508 is to provide the basis for the preparation of specific safety standards for plant and industrial sectors. A second scope of the standard is to help the development of safety-related systems E/E/PE (Electrical/Electronic/Programmable Electronic) where specific standards do not exist. Starting from 2002, two new specific standards directly referring to IEC 61508 were introduced: IEC 61511 for process control industries and IEC/EN 62061, EN ISO 13849-1 Safety of Machinery.

IEC 61508 covers safety-related systems when one or more of such systems incorporate electrical/electronic/programmable electronic devices. These devices can include anything from electrical relays and switches to Programmable Logic Controllers (PLCs) and all the way up to complicated computer-driven overall safety systems. The standard specifically covers possible hazards created when failures of safety functions performed by E/E/PE safety-related systems occur. The overall program to insure that a safety-related E/E/PE system brings about a safe state, when called upon to do so, is defined as “**functional safety**”.

IEC 61508 does not cover safety issues like electric shock, hazardous falls, long-term exposure to a toxic substance, etc.; these issues are covered by other standards like ATEX or similar. IEC 61508 also does not cover low safety E/E/PE systems where a single E/E/PE system is capable of providing the necessary risk reduction and the required safety integrity level of the E/E/PE system is less than SIL 1.
IEC 61508 is concerned with the E/E/PE safety-related systems whose failure could affect the safety of persons and/or the environment. However, it is recognized that the methods of IEC 61508 also may be applied to business loss and asset protection cases.

DIGITAL PREVIEW

If you want to request the full hard copy or to read the online full version scan the **QR-code** on the last page of this document.

Chapter 2 Prevention and mitigation layers for hazardous events

Accidents rarely have a single cause and are usually a combination of improbable events that people initially assumed as independent and unlikely to happen at the same time. A tragic example is the one occurred to a pesticide plant in Bhopal (India). It was December 3, 1984 and the unexpected leakage of more than 40 tons of methyl isocyanate (MIC) immediately killed almost 4000 people and caused illnesses and death to many thousands more.

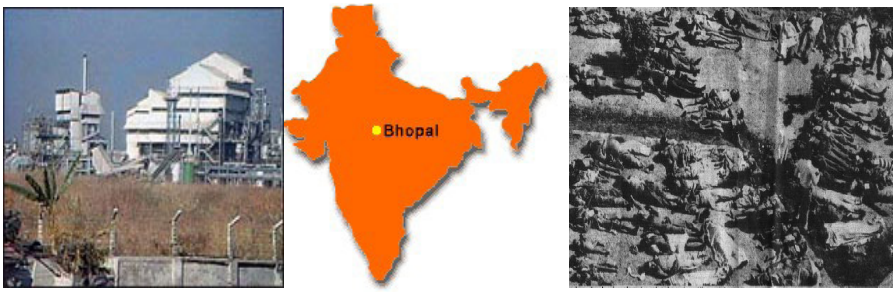

Figure 3, Bhopal Disaster. 1976 Union Carbide plant: 20 thousand deaths and almost 200 thousand injured

Although operative procedures prescribed the tank to be refrigerated at a temperature below 5°C, the alarm was set at 11°C. At that time, the refrigerating system was switched off due to bad economic conditions and the material was stored at the temperature of 20°C. The alarm set was therefore moved from 11°C to 20°C (**first cause**). The plant was in shutdown for maintenance. A worker was tasked to wash some clogged pipes and filters. Blind flanges were not installed as required by the procedures in case of cleaning of the pipes (**second cause**) and water leaked past the valves into the tank containing MIC. Temperature and pressure gauges indicated abnormal conditions but were ignored, because thought to be inaccurate (**third cause**). A vent scrubber, which could have neutralized the MIC release into the atmosphere, was not working because it was presumed not to be necessary while production was suspended (**fourth cause**). But the vent scrubber would not have been able to handle that size of dangerous release anyway (**fifth cause**). The flare tower, although insufficient for the task (**sixth cause**), could have burned off part of the material, but it was out of service for maintenance (**seventh cause**). The material could have been vented to nearby tanks, but the gauges erroneously showed them as partially filled (**eight cause**). A water curtain was available to neutralize a release in the atmosphere, but the MIC was vented from a stack that was 33 meters above

the ground level, too high to be reached by the water curtain. Workers became aware of the MIC release because of the irritation to their eyes and throats. Their complaints to the management, at that time, were ignored. Workers panicked and fled ignoring the availability of 4 buses that were intended for emergency evacuation of the employees. The plant supervisor could not find his oxygen mask and broke a leg while trying to climb over the boundary fence. When the plant manager was later informed of the accident he did not believe the fact, by stating that the gas release could not be from his plant, nothing could ever happen to the plant, especially a MIC release, because the plant was not in operation.

Investigations of several industrial accidents proved that many of them happen during an interruption of production while an operator was trying to maintain or restart production. In each case, the company's safety procedures were violated or jeopardized.

The best and most redundant safety layers can be defeated by poor or conflicting management practices. If all prevention layers are effective (e.g. strong and solid), failures cannot spread from one to another. In reality, these layers are not strong and solid, but more like Swiss cheese. The holes are caused by flaws in management, design specifications, engineering, operations, procedures, improperly performed maintenance, and other errors. Not only there are holes in each layer, but these holes are constantly moving, increasing, ad decreasing, as well as appearing and disappearing. It is clear that if these "holes" line up properly, a failure can propagate through all layers causing a hazardous event. Supposing these holes are not present, the SIL levels (PFDavg) of each layer can be multiplied. This means that three SIL 1 layers could lead to SIL 3. Unfortunately this is just theory, due to the imperfections mentioned above. However, increasing the level of the three layers (SIL 2 and SIL 3), makes the achieving of a SIL 3 global level much more probable.

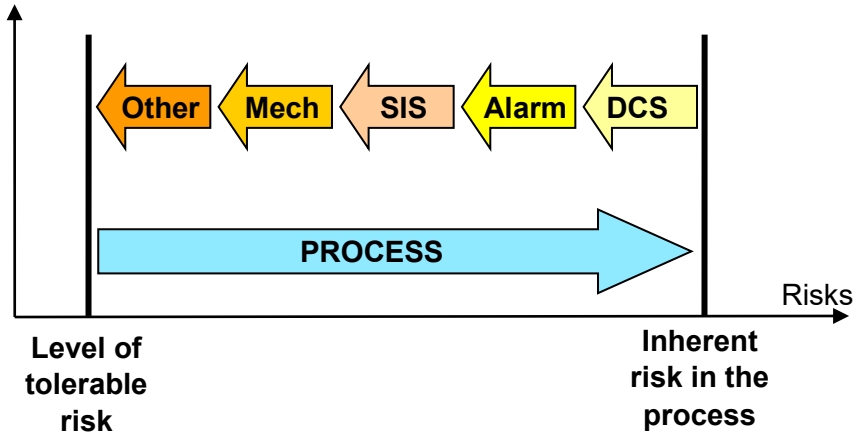

Figure 4, Risk reduction with several prevention layers

As already seen, risk is a function of the probability (or **frequency**) of a hazardous event and of its severity (or **consequence**). In an industrial plant the various layers are planned to reduce one or the other. Prevention layers are used to reduce the probability of the hazardous event, while mitigation layers are implemented to reduce the damaging consequences of an already happened hazardous event. In an industrial plant, there are usually four prevention and four mitigation layers. In this chapter ten layers are specified (5 for prevention + 5 for mitigation). This is not relevant if not for a better comprehension and identification of the functions of the different layers.

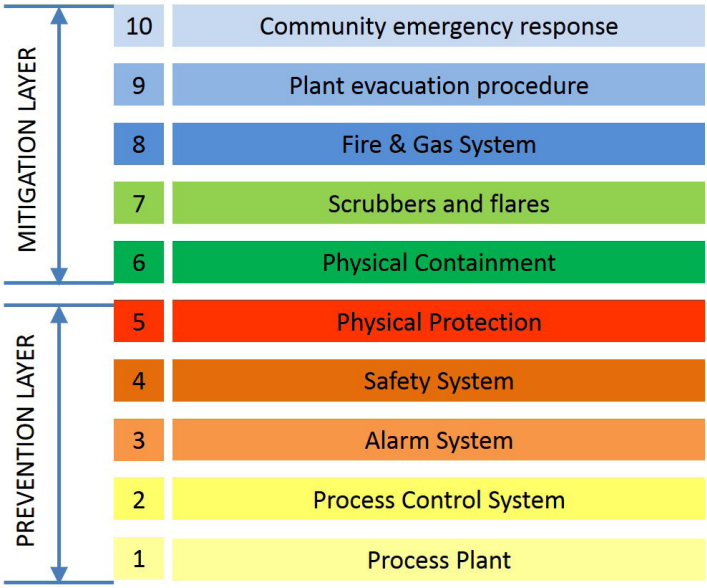

Figure 5, Prevention and mitigation layers of the hazardous event

2.1 Plants and processes in their environmental context

Industrial plants and processes must always be designed taking safety issues into consideration. This is why HAZOP (Hazard and Operability studies) or other safety reviews, such as fault tree analysis and various checklists, what-if, etc., should always be performed. Trevor Kletz [1] points out that: “time is usually better spent looking for all the sources of hazard, than in quantifying with even greater precision those we have already found”. In the NASA space program almost 35% of actual in-flight malfunctions had not been identified during the analysis. The main requirement of an industrial process is to be safe, not forgetting the rule that “what is not there cannot be damaged”, which means that it is important to make the process as simple as possible. Safe processes and systems may be more expensive, but offer greater advantages to the final user throughout the life of the plant. Risk reduction may result in a simplification and therefore in a reduction of costs.

For example, the problem of children remaining trapped and suffocated while playing in refrigerators has lead the industry to the use of magnetic latches, which, a part from being much safer, are simpler and less expensive.

Figure 6, Refinery

Layer 1 takes into consideration all processes, plants and activities which may generate hazardous situations. All these represent the environmental context to which each safety matter refers to.

Arguments which are taken in to evaluation are:

- Area's classification
- Stocking plants
- Production plants
- Storage plants
- Hot fluid plants
- Cold fluid plants
- Electric plants
- Auxiliary fluid plants.
- Organizational structure of the layer.

Teams of expert engineers working on this layer are:

- Team Leader
- Project Engineer
- Quality Assurance Engineer
- Machinery Engineer
- Mechanical Engineer

1. Trevor Kletz, D. Sc., F. Eng., member of HSE and process safety consultant, has published more than one hundred papers and nine books on loss of prevention and process safety.

DIGITAL PREVIEW

If you want to request the full hard copy or to read the online full version scan the **QR-code** on the last page of this document.

Chapter 3 Basic concepts for a better comprehension of safety standards

Some fundamental concepts for understanding safety related argumentations are presented here to ease the comprehension of Part 6 of IEC 61508, which concerns guidelines on the application of Part 2 and 3.
Some of these concepts are used in the previous Parts of IEC 61508 and for this reason, they are here recalled.
This chapter is not a complete and exhaustive presentation of all the treated subjects, but rather a manual, to "refresh" some specific arguments, or basic equations for the calculation of MTBF, PFDavg, SFF, SIL levels, etc.
Other subjects like HAZOP, FMEDA, etc., are presented at Chapter 5.

3.1 Reliability and Unreliability

3.1.1 Reliability

Reliability is a measure of success and is defined by engineers as:
"The probability that a component part, equipment, or system will satisfactorily perform its intended function when required to do so, under given circumstances, such as design limits, environmental conditions, limitations as to operating time, and frequency and thoroughness of maintenance for a specified period of time".

This definition includes four important aspects:

- The device's "intended function" must be known.
- "When the device is required to function" must be judged.
- "Satisfactory performance" must be determined.
- "Specified design limits" must be known.

All four aspects must be addressed when defining a situation to be a success or a failure.

The first aspect concerns the clear definition of what the device is asked to do, and nothing else.
The second aspect concerns the requested operability: when it will be requested to do so, not in another moment or in any moment but "on demand".
The third aspect deals with the evaluation of what the device has to do with good performances, in order to honor the demand in an acceptable way.
The forth aspect regards operability conditions in which the device works,
e.g. design limits, temperature limits, etc.

The four aspects together define the terms in which reliability is evaluated.
Reliability is valid for those conditions and not for others.
If conditions change, reliability can change too.
Mathematically, reliability (R) is:
“The probability that a device will be successful in the time interval from time 0 to time t”.

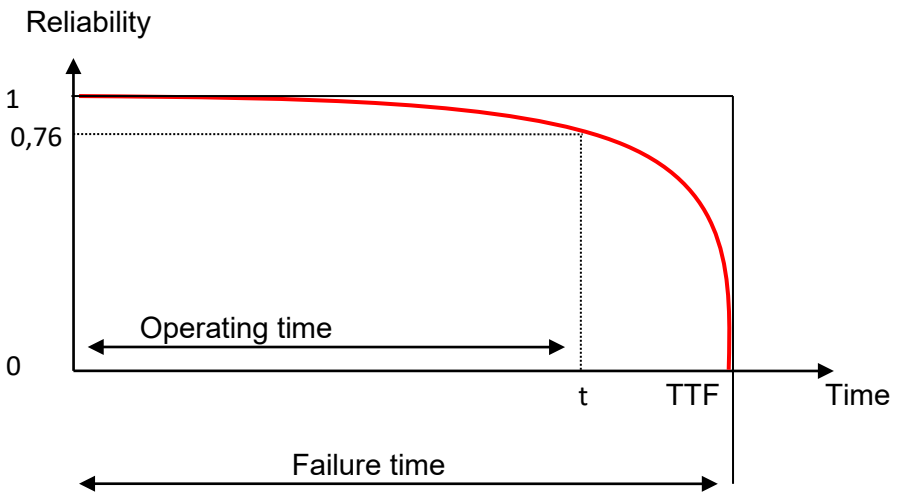

Figure 13, Reliability Figure of a device

Reliability equals the probability that TTF, failure time, is greater than t, operating time interval. The graph in Figure 13 shows device reliability as a function of time. Increasing the time interval from 0 to TTF (estimated failure time, or TTF -Time To Fail, where the device is estimated to fail with probability close to 100%) reliability changes from 1 to 0.
At time t probability will be 76%; in other words, operability without failure from 0 to t is 0.76. Calculating reliabilities for a time t greater than TTF has no meaning.

> ***Example***
> *A newly manufactured and successfully tested washing machine operates properly when put into service at time t = 0 (success = 1).*
> *Since the machine will eventually fail, the probability of success for an infinite time interval is zero. Thus, all reliability functions start at a unitary probability and decrease to a probability of zero (failure).*

Note 1
Reliability is a function of operating time. A statement such as “System reliability is 0.95” is meaningless because the time interval is unknown. The statement “Reliability equals 0.98 for a mission time of 10,000 hrs” instead, makes perfect sense.

Note 2
The reliability function graph indicated in Figure 13 is just a simple example. Reliability functions considered in this manual assume an exponential decay of failure probability, similar to those indicated below Figure 14, where the concept of TTF, as defined limit value, is not applicable because mathematically a reliability equal to zero is never reached. This family of curves represents the reliability function characterized by a **constant failure rate**.

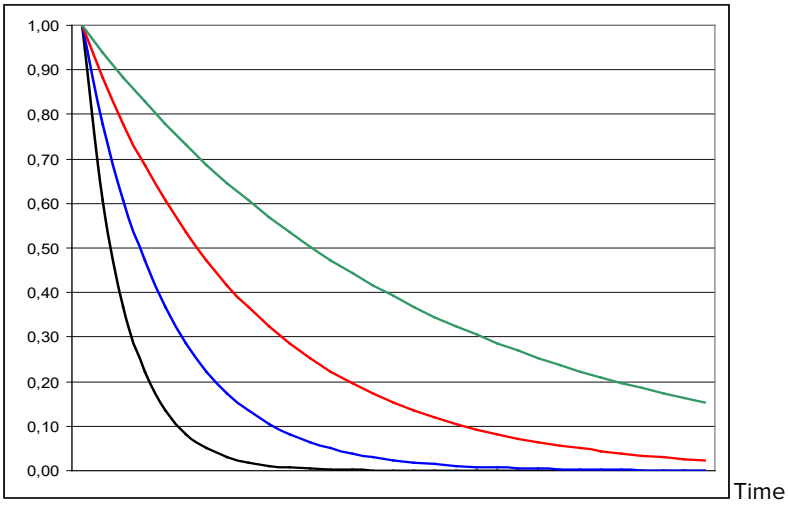

Figure 14, Device Reliability Function with exponential decay

These curves are represented mathematically by the general equation:

$$R(t) = e^{-\lambda t}$$

and have different values of λ (failure rate). They are defined at constant failure rate because the ratio between the calculated values at equal time intervals is constant:

$$\frac{R(t + \delta)}{R(t)} = f(\delta)$$

The ratio between two values of the function (the rate) depends on the time difference delta and not on the time in which the values are calculated.
In other words, being δ the value of the ratio, or rate, the time is constant.
This is better defined by the following equation:

$$\frac{e^{-\lambda(t+\delta)}}{e^{-\lambda t}} = e^{-\lambda\delta}$$

in which the ratio does not depend on the time but on the value of interval δ.

Note
It is useful to remind that representing the function of this family in a graph with logarithmic scale for values and linear scale for time, the functions will be straight.
Reliability is an important measure for those devices which are not repairable, like airplanes. Washing machines or industrial control systems are repairable and MTTF (Mean time to failure) is more likely to be used instead.

3.1.2 Unreliability

Unreliability is the measure of failure; it is defined as "the probability that a device will fail in the time interval from 0 to t".

Unreliability U(t) = 1 – Reliability (t)

It starts with probability zero and increases up to probability one.

> ***Example***
> *A controller has a reliability of 0,99 for a mission of 10,000 hrs.*
> *What is its unreliability for the same mission time?*
> *Unreliability = 1 – 0,99 = 0,01*

A property of exponential reliability curves is the constant failure rate for values of $\lambda << 1$.
Mathematically, unreliability is defined as:

$$U(t) = 1 - R(t) = 1 - e^{-\lambda t}$$

Applying Mc Laurin's expansion equation, unreliability can also be expressed by the following:

$$U(t) = 1 - \sum_{0}^{\infty} \frac{-(\lambda t)^n}{n!} = 1 - \left[1 - \frac{\lambda}{1!}t + \frac{\lambda^2}{2!}t^2 + \frac{\lambda^3}{3!}t^3 + \ldots\right]$$

To be noticed that terms beyond $\lambda 2$ are very small, and therefore the equation can be approximated to the easier:

$$U(t) = 1 - 1 + \lambda t = \lambda t$$

This can save calculation time, however remember that approximation degrades with higher values of failure rates and interval times. Further considerations can be made on the mean time to failure (MTTF). Supposing a number of n devices to be analyzed with known failure rates λ and a population of n units, after time t, the number of failed units is nF:
$n_F = n \times \lambda \times t$

DIGITAL PREVIEW

If you want to request the full hard copy or to read the online full version scan the **QR-code** on the last page of this document.

Chapter 4 Consequence Analysis of relevant accidents involving chemical substances

4.1 Analysis of risks from the release of chemical substances

Before conducting a consequence analysis of any hazardous event it is necessary to consider consequences which could derive from the release of chemical substances.

Figure 33 shows an event tree diagram for the release of hazardous chemicals, for a gas release and for a liquid/liquefied gas release.

If the release of a chemical substance occurs, consequences may result directly from the release event, as for example in BLEVE/Fireball[1], or physical explosions.

It is also possible to have only a release of chemical substances in the atmosphere, which may later cause damages depending on their chemical/physical properties.
Two possible consequences, coincident with the initial release event, are physical explosions and/or the BLEVEs with the resulting fireballs.

1. BLEVE: Boiling Liquid Expanding Vapor Explosion (see Section 4.2.4).

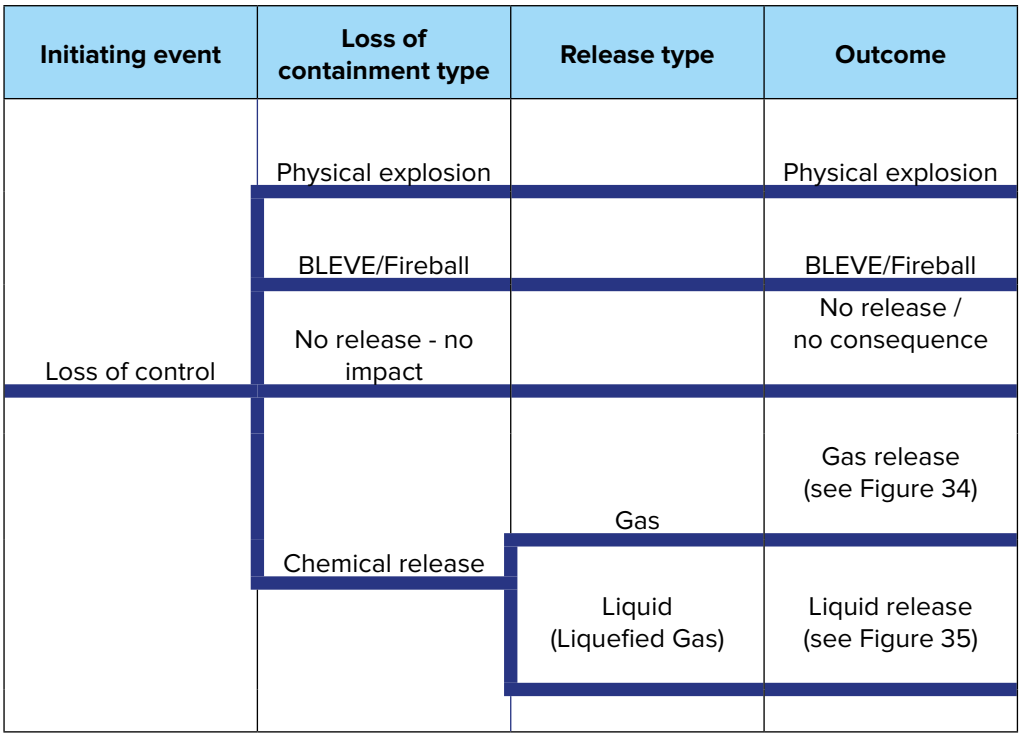

Figure 33, Event tree diagram for simplified loss of chemical containment

A pressure vessel, stimulated beyond its nominal designed pressure, can undergo a catastrophic failure creating a physical explosion.
Such event is euphemistically called by the media as an “energy release”.
If released substances as the result of a physical explosion are flammable, a fireball may also occur.

If the accident involves a flammable liquid spill, followed by ignition, with the resulting fire of the whole tank, a BLEVE/Fireball may occur.
If the loss of containment event does not cause a fire or an immediate explosion, the chemical substances contained in the process will be spread into the atmosphere.

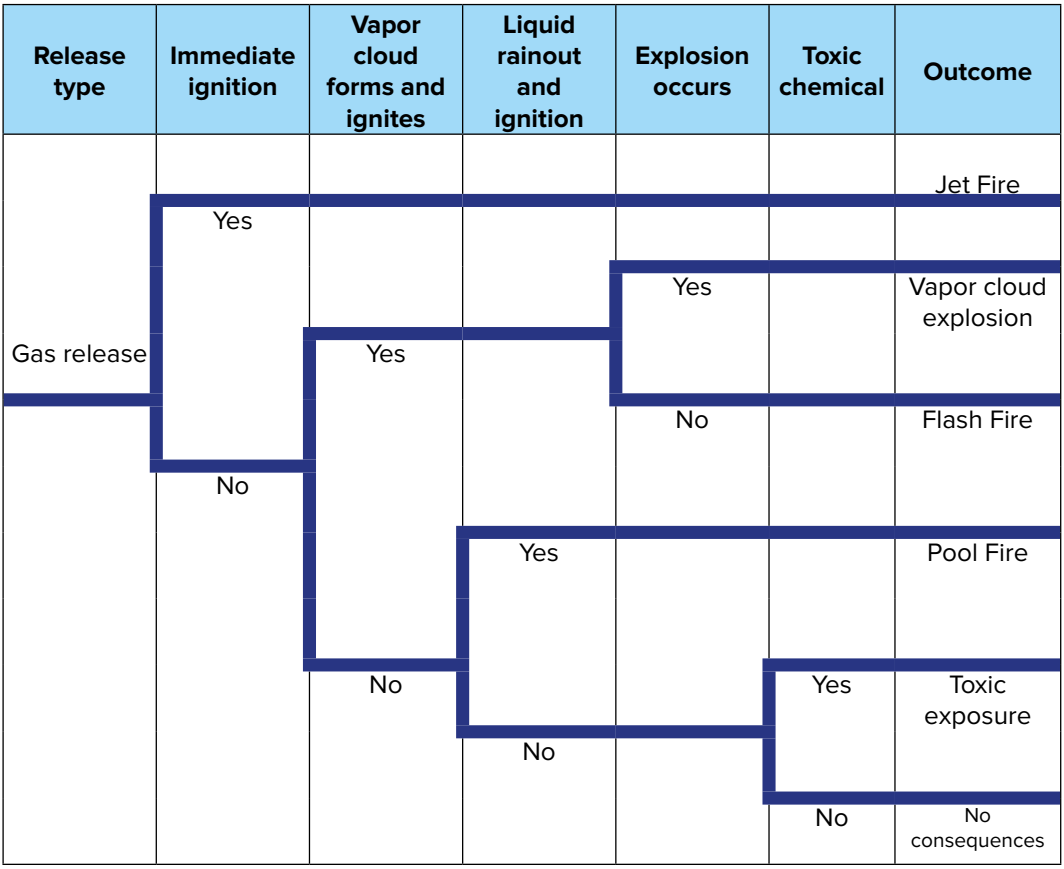

Figure 34, Event tree for gas release

The effects of this kind of release may be involved in a variety of effects depending on:

- Release conditions
- Thermodynamic conditions
- Release nature (liquid, gas, liquefied gas)

Consequences strongly depend on the conditions mentioned above and could have a large impact depending on possible incident outcomes.

If released substances are high pressure gas or liquids that instantly flash into a gas upon release, a jet fire ignition will occur if the gas is immediately ignited. In the absence of immediate ignition, a large vapor cloud may form. Delayed ignition of the vapor cloud may cause an explosion (VCE, Vapor Cloud Explosion) with the resulting blast overpressure and shock wave.

Depending on the characteristics of the released material and the surrounding environment, a vapor cloud may not result in an explosion after ignition.
In this case the cloud could burn in a slower laminar fashion, causing a flash fire which has a strong thermal effect, but does not cause a blast wave.

Differences between these two combustion modalities depend on the complex phenomenon of flame propagation velocity, which requires a specific modeling to predict with any accuracy.
Even if any ignition does not happen, the non-ignited toxic cloud of gas will spread and disperse, with risks for workers and nearby residents.
Non-ignited gas releases, and in some cases the combustion products of the ignited release, can have a detrimental effect on the surrounding environment.

Possible incident outcomes, as the result of a liquid or liquefied gas discharge, mostly depend on the behavior of the liquid upon release:
1) Immediate vaporization of liquid.
2) Rapid vaporization of the liquid with substantial formation of a liquid pool.
3) Slow or negligible vaporization with significant liquid pooling.

In case 1) the event tree shown in Figure 33 will unfold.
In cases 2) and 3) the event tree shown in Figure 34 better represents the possible outcomes of the release.

Figure 35 shows that the outcomes from a liquid release, with vapor cloud formation, are largely similar to the ones resulting from a release with direct formation of a vapor cloud.
The cloud formation can result from either rapid vaporization or slow evaporation of a pool. In the case where a pool of liquid is formed and ignited, a pool fire will result.
If the pool is not ignited, evaporation of the liquid may lead to a harmful exposure hazard downwind, if the material is toxic. Moreover, this can also contaminate groundwater even if is not ignited.
In both the vapor and liquid release cases, a potential exists that released substances will be carried away from the source of the release as an aerosol or as a gas cloud, which will then cool, collect, and rain out of the atmosphere to collect in a pool.
The hazards associated with such condensation pool are essentially the same as the hazards from the direct spill of a liquid, except that they are a quite long distance from the release source.
Due to this, a secondary containment, will most likely, not help mitigating their consequences.

DIGITAL PREVIEW

If you want to request the full hard copy or to read the online full version scan the **QR-code** on the last page of this document.

Chapter 5 Safety Instrumented Systems (SIS)

5.1 Introduction

Safety Instrumented Systems (SIS) are frequently used to reduce process hazards in production plants. For each potentially dangerous process, a design is done to detect the situation and automatically take action to prevent or mitigate the hazardous event.
Each function is called Safety Instrumented Function (SIF).
For each SIF, the required Risk Reduction Factor (RRF) is determined.
A number of SIFs, associated with a particular process, are typically implemented within a single SIS.

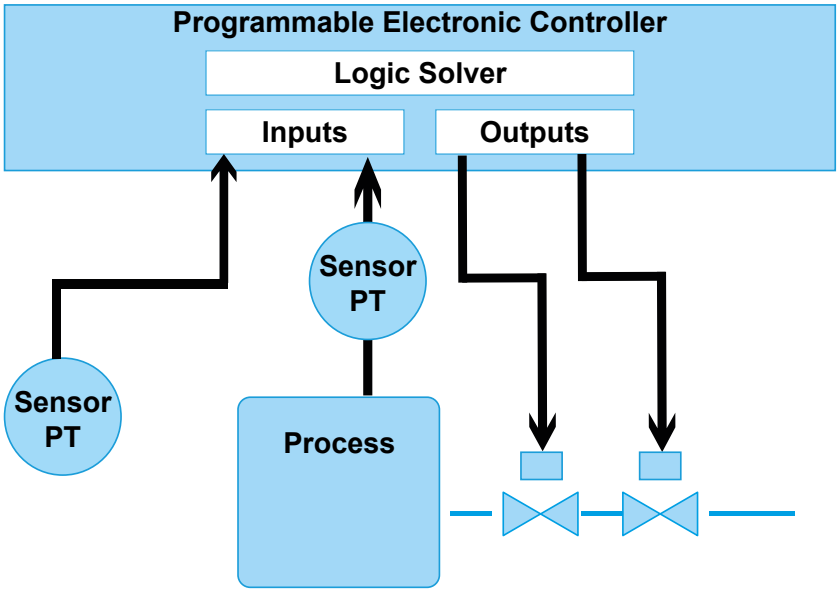

Figure 41, Example of a small SIS

A simple SIS is shown in Figure 41 together with a logic solver in a safety instrumented function.
SIS have many implemented safety functions, one for each potentially dangerous condition, in a single logic solver, which collects and analyzes data information from

sensors to determine if a dangerous condition occurs, and consequently to start a shutdown sequence to bring the process to a safe state. Typically, these control systems are called “safety-related systems”. A potentially dangerous condition is called “demand”.

The majority of SIS are based on the “de-energize to trip” concept, meaning that, in normal working conditions, input and output are energized and the programmed action to prevent or mitigate the dangerous event consists in the opening of a connection by de-energizing an electric circuit. This action is called “trip”.

A SIS is composed of process connections, sensors, logic solver, and final elements.
Sensors may be temperature/pressure measurement devices, flame detectors, toxic gas detectors, emergency switches or many other devices.
Final elements range from simple solenoid valves to large control valves with their associated actuators.

One type of logic solver is a programmable logic controller (PEC) which consists of input circuitry, a logic solver and output circuitry.
The logic solver is implemented using a microprocessor and software. Different types of input output circuitry exist to interface analog or discrete sensors or final elements.
Particular SIS are:

- **ESD:** Emergency Safety Shutdown system
- **BMS:** Burner Management System
- **F&G:** Fire and Gas system

A SIS includes instrumentation and/or controls installed to prevent or mitigate hazardous conditions, or to bring the process to a safe state, in presence of a safety demand. This can happen if specific process conditions are violated, e.g. pressure, level, temperature alarms. SIS are used for any kind of process in which hazard and risk analysis require their use. SIS availability depends on:

- Failure rate and failure mode of components or sub-systems
- Component architectures (1oo1, 1oo2D, 2oo2, 2oo3, etc)
- Voting circuits
- Diagnostic coverage
- Periodic testing frequency

5.2 Safety requirements

SIS functional safety requirements specify:

- logics and actions that a SIS has to comply with;
- process actions a SIS has to perform;
- process conditions to initiate such actions, including manual shutdown, power supply failure, etc.;
- requested SIL level and required performance to achieve it.

IEC 61511 standard specifies requirements that shall be sufficient to design the SIS and shall include the following:

- A description of all necessary SIFs to achieve required functional safety.
- Requirements to identify and take account of common cause failures.
- A definition of the safe state of the process for each identified SIF.
- A definition of any individually safe process state which, when occurring concurrently, creates a separate hazard (e.g. overload of emergency storage, multiple relief to flare system).
- The assumed sources of demand and demand rate of each SIF.
- Requirements for proof-test intervals.
- Response time requirements for the SIF to bring the process to a safe state.
- The SIL and mode of operation (demand/continuous) for each SIF.
- A description of process measurements and their trip point.
- A description of process output actions and the criteria for successful operation (e.g. requirements for tight shut-off valves).
- The functional relationship between process input and output, including logic, mathematical functions, and any required permissions.
- Requirements for manual shutdown.
- Requirements relating to energize or de-energize to trip.
- Requirements for resetting the SIF after a shutdown.
- Maximum allowable spurious trip rate.
- Failure modes and desired response of the SIF.
- Any specific requirements related to the procedures for starting up and restarting the SIF.
- All interfaces between the SIS and any other system, including BPCS and operators.
- A description of the modes of operation of the plant and identification of the SIFs required for operating within each mode.
- Application software safety requirements.
- Requirements for overrides / inhibits / bypasses including how they will be cleared.
- The specification of any action necessary to achieve or maintain a safe state in the event of fault(s) being detected in the SIF.
- The mean time to repair which is feasible for the SIF.
- Identification of the dangerous combinations of output states of the SIS that need to be avoided.
- Identification of the extremes of all environmental conditions which are likely to be encountered by the SIS.
- Identification of normal and abnormal modes for both the plant as a whole (e.g. plant startup) and individual plant operational procedures.
- Definition of requirements for any safety instrumented function necessary to survive a major accident event (e.g. the time required for a valve to remain operational in the event of a fire).

The standard provides requirements for the specification of the application software safety requirements.

It is essential for the application software specifications to be consistent with the safety requirements listed below:

- An application software safety requirements specification shall be developed.
- The input to the specification of the software safety requirements for each SIS subsystem shall include:
  - -specified safety requirements of the SIF;
  - -requirements resulting from the SIS architecture;
  - -any requirements of safety planning.
- The specification of the requirements for application software safety shall be sufficiently detailed to allow the design and implementation to achieve the required safety integrity and to allow an assessment of the functional safety to be carried out.
- The application software developer shall review the information in the specification to ensure that the requirements are unambiguous, consistent and understandable.
- The specified requirements for software safety should be expressed and structured in such a way that they are clear, verifiable, testable, modifiable and traceable.
- The application software safety requirements specification shall provide information allowing proper equipment selection.

DIGITAL PREVIEW

If you want to request the full hard copy or to read the online full version scan the **QR-code** on the last page of this document.

Chapter 6 IEC 61508: Fundamental concepts

6.1 Overall safety lifecycle

The standard is based on two fundamental concepts:

- safety lifecycles;
- safety integrity levels (SIL).

A safety lifecycle is defined as an engineering process that includes all the necessary steps to achieve the required functional safety.
The basic philosophy behind the safety lifecycle is to develop and document a safety plan, execute it and document its execution (showing that the plan has been met) and continue to follow it all the way to decommissioning with appropriate documentation throughout the life of the system.
Changes during the process must similarly follow the pattern of planning, execution, validation, and documentation.

The safety lifecycle referred to in IEC 61508 is shown in Figure 54.

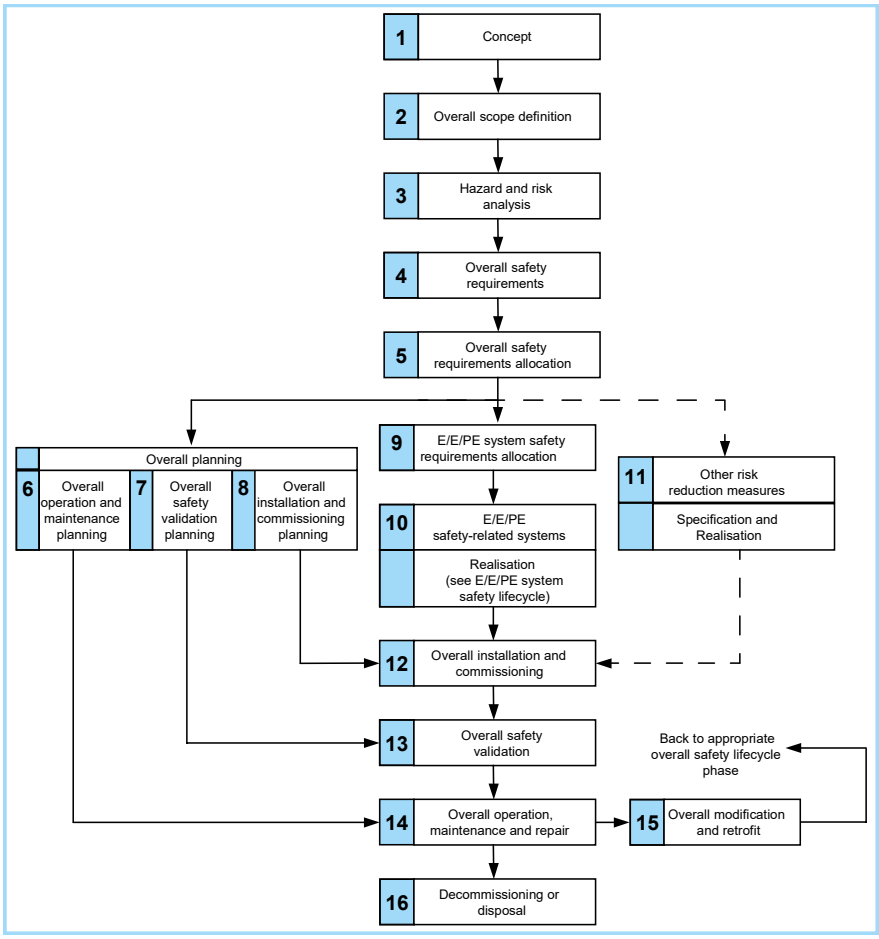

Figure 54, Overall safety lifecycle according to IEC 61508

6.2 Safety Integrity Levels

A Safety Integrity Level (SIL) is defined as a relative level of risk reduction provided by a safety function. IEC 61508 defines four SIL levels.
SIL 1 has the lowest level of risk reduction while SIL 4, the highest.
Table 1 shows SIL levels for each demand mode low and high demand (or continuous) modes of operation.

$$\text{PFDavg} = \frac{\text{Tolerable accident frequency}}{\text{Frequency of accidents without protections}} = \frac{1}{\text{RRF}}$$

SIL Safety Integrity Level	**PFDavg** Average probability of failure on demand per year (low demand mode)	**PFH** Probability of dangerous failure per hour (continuous or high demand mode of operation)	**RRF** Risk Reduction Factor
SIL 4	$\geq 10^{-5}$ to $< 10^{-4}$	$\geq 10^{-9}$ to $< 10^{-8}$	≤ 100000 to > 10000
SIL 3	$\geq 10^{-4}$ to $< 10^{-3}$	$\geq 10^{-8}$ to $< 10^{-7}$	≤ 10000 to > 1000
SIL 2	$\geq 10^{-3}$ to $< 10^{-2}$	$\geq 10^{-7}$ to $< 10^{-6}$	≤ 1000 to > 100
SIL 1	$\geq 10^{-2}$ to $< 10^{-1}$	$\geq 10^{-6}$ to $< 10^{-5}$	≤ 100 to > 10

Table 1, Safety Integrity requirements relation between SIL, PFDavg, PFH and RFF

Operating modes (defined in Part 4 of the standard) are:

- **Low demand mode:**
  where the safety function is only performed on demand, in order to transfer the EUC into a specified safe state, and where the frequency of demands is no greater than one per year;
- **High demand mode:**
  where the safety function is only performed on demand, in order to transfer the EUC into a specified safe state, and where the frequency of demands is greater than one per year;
- **Continuous mode:**
  where the safety function retains the EUC in a safe state as part of normal operation.

While continuous mode appears to be more stringent than demand mode, it should be remembered that the units for the continuous mode are “per hour”.
Demand mode units assume a time interval of roughly one year per definition. Considering the fact that there are about 10000 hours in a year (actually 8760), the two modes are approximately the same in terms of safety matrix.

Basically speaking, functional safety is achieved by properly designing a Safety Instrumented System (SIS) to carry out a Safety Instrumented Function (SIF) at a reliability indicated by the Safety Integrity Level (SIL).
The concepts of risk and safety integrity are further discussed in Part 5 of the standard.

6.3 Part "1": General requirements

6.3.1 Scope

IEC 61508 standard covers safety-related systems when one or more of such systems incorporate electrical/electronic/programmable electronic devices. These include relay-based systems, inherently safe solid-state logic based systems, and, perhaps most importantly, programmable systems based on microcomputer technology.
The standard specifically covers possible hazards created when failures of the safety functions, performed by E/E/PE safety-related systems, occur.
Functional safety is the overall program to ensure that a safety-related E/E/PE system brings about a safe state when it is called upon to do so and is different from safety issues. For example, IEC 61508 does not cover safety issues like electric shock, long-term exposure to toxic substances, etc. that are covered by other standards.
IEC 61508 also does not cover low safety E/E/PE systems where a single E/E/PE system is capable of providing the necessary risk reduction and the required safety integrity of the E/E/PE system is less than safety integrity level 1, (e.g. the E/E/PE system is only reliable 90 % of the time or less).

IEC 61508 is concerned with the E/E/PE safety-related systems whose failures could affect the safety of persons and/or the environment.
However, it is recognized that the methods of IEC 61508 may apply to business loss and asset's protection as well.
Human beings may be considered as part of safety-related system, although specific human factor requirements are not treated in detail in the standard. The standard also specifically avoids the concept of "fail safe" because of the high level of complexity involved with the E/E/PE systems considered.

In regard to this, it is useful to mention an event occurred in Italy in 2002 in an industrial plant highly protected with more than one safety-related systems, (SIL 3 level): in August the plant was almost closed due to holidays, but having received an urgent material request, a young plant manager, decided to set some process control in manual position, in order to complete the production order with the help of just a few workers.
A vessel devoted to the purification of 14 tons of raw organically peroxide exploded, resulting in the top cover blown away up to 50 meters in the air.
Eye witnesses have seen the fireball reach over 100 meters in height.
The vessel cover fell on an energy distribution cabinet nearby without consequences. The hazardous event was not as bad as it could have been.
But, was it possible to stop this inexperienced manager to do such a risky work, forbidden by all user manuals?

Not all accidents caused by human factors are sudden and unpredictable: the disaster in Chernobyl in 1986 for example.

DIGITAL PREVIEW

If you want to request the full hard copy or to read the online full version scan the **QR-code** on the last page of this document.

Chapter 7 IEC 61511 Ed 2.0: Functional safety - Safety Instrumented Systems for process industry sector

This chapter presents a general overview of the “IEC 61511 – Functional safety – safety instrumented system (SIS) for the process industry sector - Normative Part 1: Framework, definitions, system, hardware and software requirements”, edition 2.0. The initial Edition 2.0 of IEC 61511-1 was released in February 2016 and amended in August 2017. The correct consolidated version reference is IEC 61511-1:2016+AMD1:2017 CSV.
The standard has been renamed by international committees to suit their country-specific preferences. For example, the second edition of IEC 61511 was approved in the USA by the ISA84 committee without modification and published as ANSI/ISA-61511-1-2018 in July 2018.

Disclaimer: This text provides a general overview and explanation of the IEC 61511 standard. The information presented reflects the author's own interpretation and opinion and is not intended to replace or supersede the actual content and requirements of the IEC 61511 standard.
Every engineer is responsible for thoroughly analyzing their specific applications and systems and should not rely solely on the general advice provided in this chapter. The IEC 61511 standard remains the authoritative source, and users should refer directly to the standard for the complete and official requirements.

7.1 Introduction

Safety Instrumented Systems (SISs) have long been integral to executing Safety Instrumented Functions (SIFs) in the process industries. To ensure effective and reliable performance, these systems must meet minimum standards and performance levels. The IEC 61511 series provides comprehensive guidance for the application of SISs, addressing their design, engineering, implementation, operation, maintenance, and decommissioning within a structured safety life-cycle framework. Key concepts include the SIS safety life-cycle and Safety Integrity Levels (SILs), ensuring consistency and compliance with functional safety requirements.

The standard emphasizes the importance of Hazard and Risk Assessments (H&RA) to derive SIS specifications and integrates the role of other safety systems only in terms of SIS performance requirements. It applies broadly to electrical/electronic/programmable electronic technologies and extends its principles to other logic solver technologies and final elements. By adopting a systematic and rational approach, the IEC 61511 series harmonizes process industry standards globally, promoting safety and economic efficiency.

Although inherently safe process designs are preferred, the standard recognizes the necessity of protective systems for addressing residual risks, encompassing various technologies such as chemical, mechanical, and electronic. It also accommodates jurisdictional regulations that take precedence, ensuring alignment with local safety mandates. By fostering consistency in terminology, principles, and implementation, IEC 61511 aims to enhance safety and operational integrity across the process industries and is recognized as a Good Engineering Practice guideline.

7.2 History

The first edition of IEC 61511 (Ed. 1.0) was released in 2003, building upon the principles established in the 'umbrella standard' IEC 61508 (Ed. 1.0), which was introduced in 1998. The release of IEC 61508 Ed. 2.0 in April 2010 brought significant updates that have directly influenced the existing IEC 61511 standard and will continue to shape its future revisions.

These two standards have distinct areas of focus. IEC 61508 primarily addresses manufacturers, offering guidance on designing and building safety equipment, instrumentation, and systems. In contrast, IEC 61511 is designed for end users, plant operators, and project teams, focusing on the realization of Safety Instrumented Systems (SIS) within the process industry. This includes sectors such as Oil & Gas, Chemical & Petrochemicals, Food & Beverage, and Pharmaceutical applications.

The global adoption and acceptance of IEC 61511 vary, but in many countries—such as the UK, Norway, and Belgium—it is increasingly recognized as a standard of good practice for SIS implementation in the process industry. While IEC 61511 itself is not a legal requirement, adherence to good engineering practices often is. As such, compliance with IEC 61511 serves as a practical and effective means of meeting these legal obligations.

7.3 General overview of IEC61511 Ed. 2.0

IEC 61511 Edition 2.0 is a performance-based standard that balances flexibility with prescriptive elements to guide the design, implementation, and maintenance of Safety Instrumented Systems (SIS). While the standard includes more prescriptive definitions and extensively uses the term "SHALL" to outline requirements, it does not function as a rigid, recipe-driven guide. Instead, it provides a framework rooted in two key concepts: the safety lifecycle and Safety Integrity Levels (SIL).

The safety lifecycle is a systematic and rational engineering process designed to promote good engineering practices throughout the design, engineering, and maintenance of SIS, ensuring consistent and reliable performance. SIL serves as a metric to express the expected reliability and performance of safety functions.

IEC 61511 Edition 2.0 encompasses both technical and non-technical (management) requirements, highlighting the importance of integrating organizational practices with engineering principles to achieve functional safety. This dual focus supports a comprehensive approach to safety and underscores the standard's role as a cornerstone for best practices in SIS within the process industries. See Figure 80 (ref. IEC61511 Ed. 2.0 part 1).

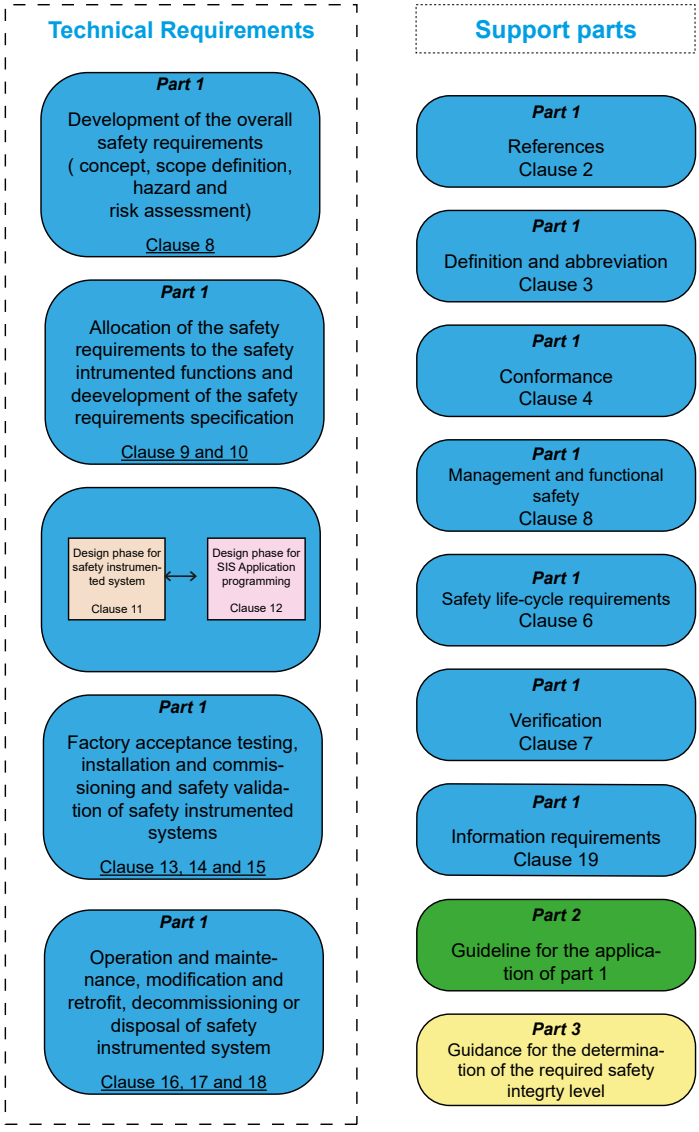

Figure 80, Overall framework of this standard

In Edition 2.0 of IEC 61511, the standard remains divided into three parts, consistent with the structure of IEC 61511 Edition 1.0:

Part 1 (IEC 61511-1:2016+AMD1:2017 CSV, August 2017) is normative and includes: Framework, definitions, and requirements for systems, hardware, and software.
This part defines the compliance requirements outlined in Clauses 5 through 19. It addresses project planning, management, documentation, and competency requirements, as well as the technical requirements necessary to achieve safety throughout the safety lifecycle.

Part 2 (IEC 61511-2, July 2016) is informative and provides: Guidelines for the application of IEC 61511-1. This part offers guidance to help users read, interpret, and apply the requirements described in Part 1.

Part 3 (IEC 61511-3, July 2016) is informative and provides: Guidance for determining the required Safety Integrity Levels (SILs).This part offers general guidance on risk and SIL determination. It includes:
Annex A: Risk and safety integrity – general guidance
Annexes B through I: Both quantitative and qualitative approaches to SIL selection, such as event tree analysis, safety layer matrix methods, risk graphs, LOPA (Layer of Protection Analysis), and risk matrices.
Annex J: (new since ed. 2.0) addressing multiple safety systems and the management of systemic dependencies
Annex K: The ALARP principle (As Low As Reasonably Practicable).

In general, the IEC61511 standard:

- Requires that a process hazard and risk analysis be performed.
- Mandates the allocation of safety functions to protection layers.
- Specifies that when tolerable risk cannot be achieved, additional protection layers must be defined in the Safety Requirements Specification (SRS) for the Safety Instrumented System (SIS).
- Outlines requirements for system architecture, hardware configuration, application programming, and system integration.
- Defines techniques and numerical targets (SIL levels) to measure the performance of the SIS.
- Requires the collection of Quality field data through operational and mechanical integrity program activities to assess actual SIS performance.
- Implements a safety lifecycle, detailing activities and responsibilities essential for functional safety management and compliance.
- Establishes requirements for testing, analysis, and documentation to verify performance, as well as the need for functional safety assessments and audits, taking competency and independence into account.

DIGITAL PREVIEW

If you want to request the full hard copy or to read the online full version scan the **QR-code** on the last page of this document.

Chapter 8 IEC61511 Ed. 2.0 - SIS Safety Requirement Specification (SRS)

Important Note
This chapter presents a general overview of the SIS Safety Requirement Specification (SRS) - Normative Part 1: Framework, definitions, system, hardware and application programming requirements", edition 2.0. This is based on the FDIS version (65A-61511-1-Ed2-IS-FDIS-OE, 2015-06-17, FDIS=Final Draft International Standard). At the time of editing this chapter the forecasted publication date of IEC61511 Ed. 2.0 – part1 is for 2016-02. Please note that there may be additional or different changes to the final published version of the IEC 61511 Ed 2.0.

8.1 Introduction

In 2003 the Health and Safety Executive (HSE) from the UK released the 2nd edition of a study called 'Out of control: Why control systems go wrong and how to prevent failure?'. This was based on 34 international incidents, concluding that 44% of the causes were related to specification issues. It is clear that when it comes to safety specification, there should be no assumptions on how to build, operate or maintain it.

Despite having the IEC61511 Edition 1.0 out since 2004, observations from a Functional Safety Competency Trainer point of view, it is clear that the majority of the participants know what the purpose of a SRS should be, unfortunately the only thing most people have in common is the title of the document "Safety Requirements Specifications or simply SRS". There is plenty of evidence that in general the Process Industry is struggling to meet the SIS safety requirements (10.3 - IEC61511-1). One has to say that, although the content of the SRS is explained in a bullet list, there is very little guidance of how to implement those, therefore many projects are left with a serious gap on 'what should have been described' versus 'what cut/copy paste' many engineer manage to reproduce again.

The 61511 Ed. 2.0 part 1 has again a normative requirement to develop a SIS Safety Requirements Specification (Phase 3, clause 10) with some additional (new) requirements compared to edition 1.0 in clause 10 as one of the more important activities of the safety life cycle. The SRS requirements should address the basic and functional design specifications and should be prepared before starting design, installation and operation. The aim is to have every single Safety Instrumented Function (SIF or safety loop) described in such a way that anyone wherever and whenever need to understand the SIF; or build-, maintain-, operate-, repair- and test- that SIF; will have a precise, clear, verifiable, maintainable and feasible information available.

8.2 Content of the SRS

The SIS SRS may be a single document or a collection of several documents including procedures, drawings and corporate standard practices. The SRS should be the master document. Referenced documents are subordinate to the SRS. Of course 1 single SRS document is easier to maintain and control, multiple and various documents all linked together can lead to more human – failures (systematic) failures, and this is exactly what a good engineering practice standard like the IEC61511 is trying to avoid. However, all is depending on the owner organization practices and standards.

The SIS SRS will be a key document that should be generated in Phase 3 (clause 10, Safety requirements specification for the safety instrumented system) and preferably be finished (although reality it never is) before starting at Phase 4 (clause 11, SIS design and engineering & clause 12, SIS application program development).
There is also a recommendation from the IEC61511 standard to perform a Functional Safety Assessment (FSA) known as 'stage 1' in the lifecycle assessment by an independent senior competent person(s), in order to determine that the SRS document meets the functional safety objectives.
These requirements may be developed by the Hazard and Risk Assessment (HRA) team and/or the project team itself. Final validation of the SIS is carried out using this SRS document. However, the SRS will need to be maintained and be available for those that need it for the duration of a complete lifecycle of any project. It is not just valuable for the design phase only, the SRS will remain a key document for the successful operation and maintenance of the SIS system.

Inputs to the SRS are coming from the preceding life cycle phases:

- Phase 1 (clause 8, Process hazard and risk assessment)
- The hazard description
- The frequency of occurrence
- The consequence
- Phase 2 (clause 9, Allocation of safety functions to existing protection layers)
- This is typically done by Layer Of Protection Analysis (LOPA)

When the tolerable risk cannot be met, then additional protection layers will need to be specified in the SRS for the SIS:

- Specifies requirements for system architecture, hardware configuration, application program and system integration
- Specifies techniques and numerical targets (SIL levels) to measure the performance of the SIS

Typical content of a SRS may contain things like:

- General Functional SIS Requirements that all SIFs have in common within the SIS, e.g. user interface for the operator/maintenance personnel, etc.;
- Specific SIF Safety Functional Requirements, HOW it should work;

- Specific SIF Safety Integrity Requirements, HOW well it should work;
- Specific SIF Safety Integrity Requirements, HOW well it should work and HOW long it should work for;
- Application Program Safety Requirements
- Non-Functional SIS requirements, such as code and standard, application specific standards, environmental conditions, client-plant-project specific guidelines, etc.

8.2.1 General Requirements (61511-1, clause 10.2)

There is no such thing as one 'generic' SRS that can be used for everyone and every application in the process industry. The SRS will need to be customized to the client or plant/project specific guidelines and specifications.

However, there are some general requirements that could be applicable for all, below are some examples given:

- What type of process application (continuous or batch)?
- What type of general hazards and their potential to harm people, environment and capital investment?
- What process or facilities are in the neighborhood?
- Which environmental conditions can influence the SIS equipment?
- Which standards, codes and local legislation are applicable?
- What type of utility supplies, e.g. net power, uninterrupted power supply (ups), diesel generated power, instrument air compressor, etc.?
- What is the required Plant Life Time for the SIF?

8.2.2 SIS Safety Requirements (61511-1, clause 10.3)

Similar as the previous edition of the 61511 part 1, clause 10.3 contains in total 29 requirements as an itemized list. Those requirements **SHALL** be sufficient to design the SIS and **SHALL** include the below description of the intent and approach applied during the development of the SIS safety requirements as applicable. The word **SHALL** make those individual requirements **mandatory** to consider for every project providing you claim compliance to the IEC 61511 standard.
Below are some potential example(s) based upon personal interpretation and experiences of such requirements

8.2.2.1 A description of all the Safety Instrumented Function necessary to achieve the required functional safety

Following the demand on the Safety Instrumented Function (SIF), a detailed description of the actions that are designed to interface with that SIF to prevent the hazardous condition. Sometimes the SIF can be referred to as the IPF (Instrumented Protective Function) list of all Safety Instrumented Function (SIF), Equipment Protective Functions (EPF) and Manual

Protective Functions (MPF).
Example:

- Low level (LAL-103) in a LNG tank 100A causes the suction pump (P-101) to trip;
- LAHH-201 shall protect the LP Gas system from Hi Hi level of LP Gas Scrubber by closing ESDV-203;
- High-high storage tank level (LAHH-901) closes tank inlet valve SDV-904;
- High reactor temperature (TAH-506) closes the two reactor feed valves XV-501A and XV-501B;
- High column temperature (TAH-333) closes the re-boiler steam valve XV-301.

Describe the following:

- Process variables being measured and which devices used (typically a tag name);
- Process conditions under which SIF need to act (trip point or alarm);
- Logic of the SIF that needs to be executed;
- Final element or action that the SIF will result in (actuator(s), safe state, tag name).

8.2.2.2 A list of the plant input and output devices related to each SIF which is clearly identified by the plant means of equipment identification

This is typically done by a field I/O or tag list, but in relation to 'how' the SIF functionality is built or connected to those tag names, a detailed SIF or a safety loop description supported by a loop diagram is recommended.
Every single SIF can contain several devices or subsystems as the IEC61508 defines them.

Example of a simple 1oo1 SIF graphical represented in Figure 88.

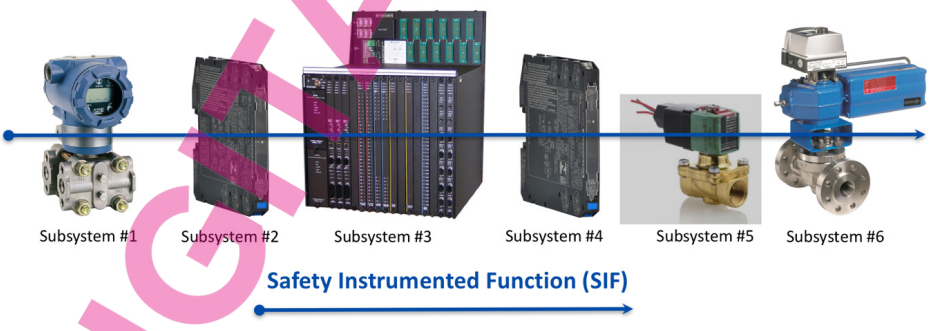

Figure 87, Example of a simple 1oo1 SIF

8.2.2.3 Requirements to identify and take account of common cause failures

The potential common causes that could affect fault tolerant / redundant architectures

DIGITAL PREVIEW

If you want to request the full hard copy or to read the online full version scan the **QR-code** on the last page of this document.

Chapter 9 Functional safety manual

Manufacturers are required to provide a safety manual for each device, sensor, controller or final element that is part of a safety-related system and for which it is necessary to prove compatibility with IEC 61508 and IEC 61511.
The purpose of this short chapter is to provide a “checklist” of requirements for such manual.

The main purpose of this document is to specify user responsibilities for installation and operation, in order to maintain the designed safety level.
Many users consider it to be a pre-sales document, since they want to see if there are serious limitations in the use of a product before purchasing it.

9.1 Requirements

IEC 61508 requires that manufacturers:

- Provide procedures required for a test to detect known “dangerous failures” as identified by the failure rates analysis of the product. The procedures must include a statement that results of such testing are recorded. Any tools required must be identified. The expected skill level of those in charge of accomplishing the task must be specified. Diagnostic coverage factor for the specified test must be stated.
- Provide procedures to repair or replace the product. These must include a statement that all failures must be reported to the manufacturer.
  Any tools required must be identified. The expected skill level of those accomplishing the work must also be specified.
- Provide any necessary installation and site acceptance test procedures required in order to achieve safety.
- If a product firmware upgrade is possible, procedures must be given and all needed tools must be identified. The expected skill level of those carrying out the task must be specified.
- The safety manual must contain estimated failure rates and an estimate of the beta factor for use when redundant devices are designed into the safety instrumented function.
- If there are any unknown product lifetime limits, these must be stated. Otherwise a statement that there are no known wear-out mechanisms.
  Note: Although not required, it may be advisable to make some statements about product lifetime even if there are no known wear-out mechanisms.

All required parameter setting assumed for safety must be stated.
Any application limitations and environmental limits must be stated (or a reference pointing to another document).
Worst case diagnostic test time must be stated for the claimed diagnostic test coverage.

IEC 61508-2, in section 7.4.7.3, specifies the following information which shall be available for each safety-related subsystem:

- A functional specification of those functions and interfaces of the subsystem which can be used by the safety functions.
- The estimated rates of failure (due to random hardware failures), in any modes which could cause a dangerous failure of the E/E/PE safety-related system, which are detected by the diagnostic tests.
- Any limits on the subsystem environment which could be observed in order to maintain the validity of the estimated rates of failure due to random hardware failures.
- Any limit on the lifetime of the subsystem which should not be exceeded in order to maintain the validity of the estimated rates of failure due to random hardware failure.
- Any periodic proof test / or maintenance required.
- Diagnostic coverage.
- Diagnostic test interval.
- Any additional information (for instance repair time) which is necessary to allow the derivation of the mean time to restoration (MTTR) following detection of a fault by the diagnostics.
- All information which is necessary to enable the derivation of the safe failure fraction (SFF) of the subsystem as applied in the E/E/PE safety-related system.
- The hardware fault tolerance of the subsystem.
- Any limits on the application of the subsystem which should be observed in order to avoid systematic failures.
- The highest safety integrity level (SIL) that can be claimed for a safety function which uses the subsystem on the base of:
  - Measure and techniques used to prevent systematic failures being introduced during the design and implementation of the hardware and software of the subsystem,
  - Design features which make the subsystem tolerant against systematic failures.
  Note: this is not required in the case of those subsystems which are considered to have been proven in use.

Any information which is required to identify the hardware and software configuration of the subsystem in order to enable the configuration management hardware and software of the secondary system, to allow the management of the E/E/PE safety-related system in accordance with IEC 61508-1, 6.2.1.
Documentary evidence that the subsystem has been validated.

IEC 61511-1, in section 1.2.4.4.7, defines the following requirements which the safety manual shall address:

- Use of diagnostics to perform safety functions.
- List of certified / verified safety libraries.
- Mandatory test and system shutdown logics.
- Use of watchdogs.
- Requirements for, and limitation of, tools and programming languages.
- Safety integrity level for which the device or system is suitable.

9.2 What's new in IEC 61508 Edition 2

IEC 61508:2010 Ed. 2 has focused on new aspects related to safety, both adding new requirements and expanding requirements already present in the previous edition.
In this chapter we will quickly discuss the following topics:

- Systematic SIL Capability (see 9.3),
- Safety Manual requirements (see 9.4).

9.3 Systematic SIL Capability

When dealing with the safety of modules, subsystems or systems, two major sources of failure must be considered:

- random failures,
- systematic failures.

Random failures are those arising without an evident link to other external conditions and have a nearly constant rate during the useful life of the equipment, when used according to the design limits. They are typically hardware defects, usually defined by a Failure Rate figure expressed in FIT (failures in 1 billion operating hours)
Systematic failures are those arising with an evident link to external conditions, so that, when an operating condition is reproduced, their failure rate heavily increases.
Both can be hardware and/or software defects.

Techniques to avoid both random and systematic failures have been discussed in Edition 1; this new Edition focuses on defining the Systematic Capability of a compliant item to:

- drastically limit systematic failures caused by hardware design, environmental stress and operational failure;
- eliminate systematic failures during software development.

Methods to obtain such results depend on both a Quality Management System, oriented to IEC 61508 requirements, and some specific design techniques used during product development.

Chapter 10 Functional Safety Management in Safety Instrumented Systems (SIS)

10.1 Disclaimer

This text is provided as a general overview and explanation of the IEC 61511 standard. The information presented is the author interpretation and opinion and is not intended to replace or supersede the actual content and requirements of the IEC 61511 standard. Every engineer is responsible for thoroughly analysing their specific application and system and should not rely solely on the general advice provided here. The IEC 61511 standard remains the authoritative source, and users should refer directly to the standard for the complete and official requirements.

10.2 Introduction

Functional Safety is a critical aspect of engineering and operations within industries that rely on Safety Instrumented Systems (SIS) to mitigate risks. The successful implementation of SIS is governed by rigorous standards such as IEC 61511, which provides a structured approach to ensure the design, operation, and maintenance of these systems achieve and maintain safety integrity levels (SIL). This chapter explores the key aspects of functional safety management as outlined in Clause 5 of IEC 61511, focusing on essential management activities, competency, risk evaluation, safety planning, implementation, and monitoring, as well as Functional Safety Assessments. All clause references in this chapter are based on the IEC/ISA 61511 second edition (2016/17-2018).

10.3 Objective of Functional Safety Management (FSM) (Clause 5.1)

10.3.1 FSM Objectives

FSM aims to define, document, monitor, and assess requirements for technical and managerial activities throughout the SIS lifecycle. For instance:

- During hazard analysis, FSM ensures that LOPA and HAZOP studies are reviewed by qualified personnel.
- It oversees that risk reduction targets are clearly communicated and integrated into the Safety Requirements Specification (SRS).
- Similarly, during operations, FSM tracks proof test intervals and field failure data,

ensuring that operational feedback informs maintenance strategies and mitigates systematic failures effectively.

FSM specifies responsibilities across individuals, departments, and organizations, ensuring that functional safety objectives are met effectively.

10.3.2 Systematic Failures

FSM specifically targets systematic failures, often caused by human errors, which cannot be predicted using mathematical models. For example, in the oil and gas industry, systematic failures might involve incorrect calibration of pressure sensors during routine maintenance, leading to inaccurate readings and potential operational hazards. In the chemical processing industry, programming errors in logic solvers could cause unintended activation of safety mechanisms, disrupting production.

These examples underscore the need for tailored training, rigorous review protocols, and structured validation processes to mitigate such risks effectively. Common issues include errors during SIS configuration, insufficient testing of logic solvers, and miscalibration of sensors. Mitigation strategies involve implementing:

- Rigorous change management protocols.
- Regular training programs for personnel.
- Detailed assessment and audits to identify potential vulnerabilities early.

This highlights the importance of quality assurance throughout the SIS lifecycle.

10.3.3 FSM as a Quality Mechanism

FSM is a dynamic and evolving system designed to maintain functional safety throughout the SIS's operational life. It integrates monitoring tools like FSAs and audits to enhance quality by identifying and rectifying errors early. FSM must be planned, the plan or procedure may be in conjunction with organisation’s Quality Management System.

10.3.4 Mandatory FSM Procedures

Organizations making functional safety claims for products or services must have an FSM system. Procedures should be established to demonstrate the adequacy and compliance of these systems.

10.3.5 Lifecycle Integration

FSM encompasses all aspects of the lifecycle, including organization, risk evaluation, safety planning, implementation, monitoring, and revision. A robust FSM framework

includes mechanisms for handling change, traceability, and competency evaluations.

10.3.6 Common Misconceptions

FSM is equally critical for all SIL levels, not just higher ones. It is not a static, checklist-based process but a living system requiring continual updates and attention. Grandfather clauses for existing systems still require ongoing FSM and performance monitoring.

Clause 5.1 emphasizes the importance of identifying management activities necessary to achieve functional safety objectives. The management of functional safety encompasses planning, resource allocation, organizational structure, and the establishment of administrative systems that mitigate human errors—a significant contributor to SIS failures. This section highlights the necessity of ensuring competent personnel are involved in all phases of the SIS lifecycle. Key activities include:

- Planning and resource development.
- Defining organizational roles and responsibilities.
- Conducting Functional Safety Assessments and audits.
- Verification and validation activities, detailed further in Clauses 7 and 15, respectively.

10.4 Requirements for Management Activities (Clause 5.2)

10.4.1 Policy and Strategy (Clause 5.2.1)

Organizations must define a policy and strategy for achieving functional safety, including methods for evaluating success and ensuring effective communication. These policies are typically documented in corporate or site-specific SIS standards. The strategy outlines the execution of functional safety activities and the evaluation methods employed to ensure objectives are met. Effective communication mechanisms, including training programs and competency tracking, are vital to disseminate responsibilities throughout the organization.

The strategy for functional safety should integrate with existing organizational frameworks such as risk management policies or quality management systems. This ensures a cohesive approach where functional safety objectives align with overarching corporate goals. Moreover, this strategy should include the use of modern tools and software for lifecycle management to enhance accuracy and efficiency.

10.4.2 Organization and Resources (Clause 5.2.2)

Clause 5.2.2 highlights the necessity of assigning roles and responsibilities for each phase of the SIS lifecycle. Rather than assigning tasks to specific individuals, activities are allocated to roles, ensuring continuity despite personnel changes.
For example:

- Planning for Layer of Protection Analysis (LOPA) may be assigned to a Process Safety Management Coordinator.
- SIL verification tasks may fall under the remit of an SIS Subject Matter Expert (SME).

This allocation ensures clarity and accountability, often supported by Human Resources systems that define job descriptions and competencies. Additionally, organizations must establish a clear structure to oversee SIS lifecycle activities, potentially creating specialized teams or roles dedicated solely to functional safety management.
A **Responsibilities Matrix**, as outlined in Annex C of ISA-TR84.00.04-2020, is a powerful tool for ensuring accountability. For example, during the commissioning phase of the SIS lifecycle, this matrix might define:

- **Functional Safety Manager:** Responsible for overall lifecycle compliance and coordinating assessments.
- **Process Engineer:** Accountable for validating the safety requirements related to process design.
- **Control Systems Engineer:** Consulted for ensuring correct SIS hardware and software integration.
- **Maintenance Technician:** Responsible for executing pre-startup tests and ensuring readiness of field devices.
- **Operations Supervisor:** Informed of operational procedures and trained to handle the SIS interface.

This practical example highlights how responsibilities are clearly delineated to ensure tasks are executed efficiently and without overlap, fostering accountability and operational continuity. This matrix explicitly defines the roles and responsibilities across various disciplines involved in functional safety management, such as engineering, operations, and maintenance. It provides:

- Role Clarity: Clearly delineates who is responsible, accountable, consulted, and informed (RACI) for each task in the SIS lifecycle.
- Competency Assurance: Links required competencies and training to each role to ensure that personnel can effectively execute their responsibilities.
- Operational Continuity: Facilitates a smooth transition of responsibilities in case of personnel changes, reducing risks associated with knowledge gaps.

Examples of roles typically included in such a matrix are:

- Functional Safety Manager
- Process Engineer
- Control Systems Engineer
- Maintenance Technician
- Operations Supervisor

DIGITAL PREVIEW

If you want to request the full hard copy or to read the online full version scan the **QR-code** on the last page of this document.

Index of Figures

Index of Tables

Reference

- IEC 61508, IEC 61511 Standard
- “Control System Safety Evaluation & Reliability” 2nd edition William M. Goble. ISA (ISBN 978-1-55617-996-9)
- “Use and Development of Qualitative Reliability and Safety Analysis in New Product Design” William M. Goble. EXIDA
- “Safety Instrumented Systems: Design, Analysis, and Justification” Paul Gruhn and Harry L. Cheddie, ISA (ISBN: 978-1-55617-956-3).
- “Safety Integrity Level Selection - Systematic Methods Including Layer of Protection Analysis” Edward M. Marszal, P.E., Dr. Eric W. Scharpf, MIPENZ, ISA (ISBN 978-1-55617-777-4)
- “What Went Wrong?: Case Histories of Process Plant Disasters”, Trevor A. Kletz, Gulf Publishing, 1998
- “Still Going Wrong!: Case Histories of Process Plant Disasters and How They Could Have Been Avoided” Trevor A. Kletz, Elsevier 2003
- “SFPE Handbook of Fire Protection Engineering” NFPA, Philip J. Di Nenno, Society of Fire Protection Engineers
- “What is a PFDavg?” Julia V. Bukowski, Jan Rouvroye and William M. Goble
- “Gestione Integrata della Sicurezza” Angelo Papagno, ASI ESTESA
- “Valve Ranking and Partial Stroke” G. Ramachandran. ISA Technical Conference, Long Beach CA , 2004
- “Determining the Required Safety Integrity Level for your Process” Lawrence Beckman, ISA Transactions 1998
- “Easily Assess Complex Safety Loops” Lawrence Beckman, Chemical Engineering Progress, March 2001
- “Analisi di rischio ed affidabilità dei sistemi di allarme e blocco” Fabrizio Gambetti, Conferenza Snam Progetti.
- "Establishing Preventative Safety and Maintenance Strategies by Risk Based Management – The Tools of the Trade", Tilman Rasche, Ken Wolly Minerals Industry Health and Safety Centre, Australia, 2000
- “Maintainability & Maintenance Management” Joseph D. Patton, Jr., ISA 2005 (ISBN 9781556179440)
- "API/CMA Recommended Practice 752 - Management of Hazards Associated with Location of Process Plant Buildings" SCSRA Risk Resources, April 1995
- “Guidelines for Evaluating Process Plant Buildings for External Explosions and Fires” Center for Chemical Process Safety, ISBN 9780816906468
- “Out of Control, Why control systems go wrong and how to prevent failure.” HSE (HSG238) 2003.

- “Reliability Assessments of Repairable Systems”
  K G L Simpson and M Kelly (Silvertech Safety Consultancy Ltd.)
- “Guidelines for Safe and Reliable Instrumented Protective Systems” (2007)
  CCPS
- “IEC61508 Ed. 2.0 Functional Safety of electrical/electronic/programmable electronic safety-related systems”, parts 1-7 (2010)
  IEC
- “IEC61511 Ed. 2.0 Functional Safety: Safety Instrumented Systems for the Process Industry sector”, parts 1-3 – (CDV version 65A/691/CDV – 2014)
  IEC
- “Changes /What is it with IEC61511?”
  Norwegian University of Science and Technology NTNU 2012, Mary Ann Lundteigen
- “IEC61511-1 Ed. 2, Initial Reflections on an Evolving Standard”
  TÜV Rheinland International Symposium 2012, Dirk Hablawetz – BASF SE
- “IEC61511-1 Ed. 2, When and what”
  TÜV Rheinland International Symposium 2014, Heidi Fuglum and Cato Bratt – ABB Norway

Denial of responsibility

Information presented in this publication is for the general education of the reader. Because the authors do not have control over the use of the information by the readers, the authors disclaim any and all liability of any kind arising out of such use.
The reader is expected to exercise sound professional judgment in using any of the information presented in a particular application.
Additionally, the authors have investigated or considered the effect of any patents on the ability of the reader to use any of the information in a particular application. The reader is responsible for reviewing any possible patents that may affect any particular use of the information presented.
Any references to commercial products in the work are cited as examples only. Any referenced trademarks or tradenames, belong to the respective owner of the mark or name.

Examples are provided as simple illustrations of the topics discussed and, as such, are not intended as a guide to manage plant safety. The readers should use and apply only the guidance provided in the standards pertaining to their applications.

IEC 61508 Ed.2 and IEC 61511 Ed.2 are certainly the leading standards in terms of safety related equipment: The knowledge of their requirements and the ability to fulfil them are essential to both manufacturers and customers.

This manual is updated according to the latest edition of both standards and includes a new chapter about Safety Requirements Specification.

DIGITAL PREVIEW

This is only a Preview; if you want to request the full hard copy or to read the online full version scan this QR-code

www.gminternational.com

gmi technology for safety