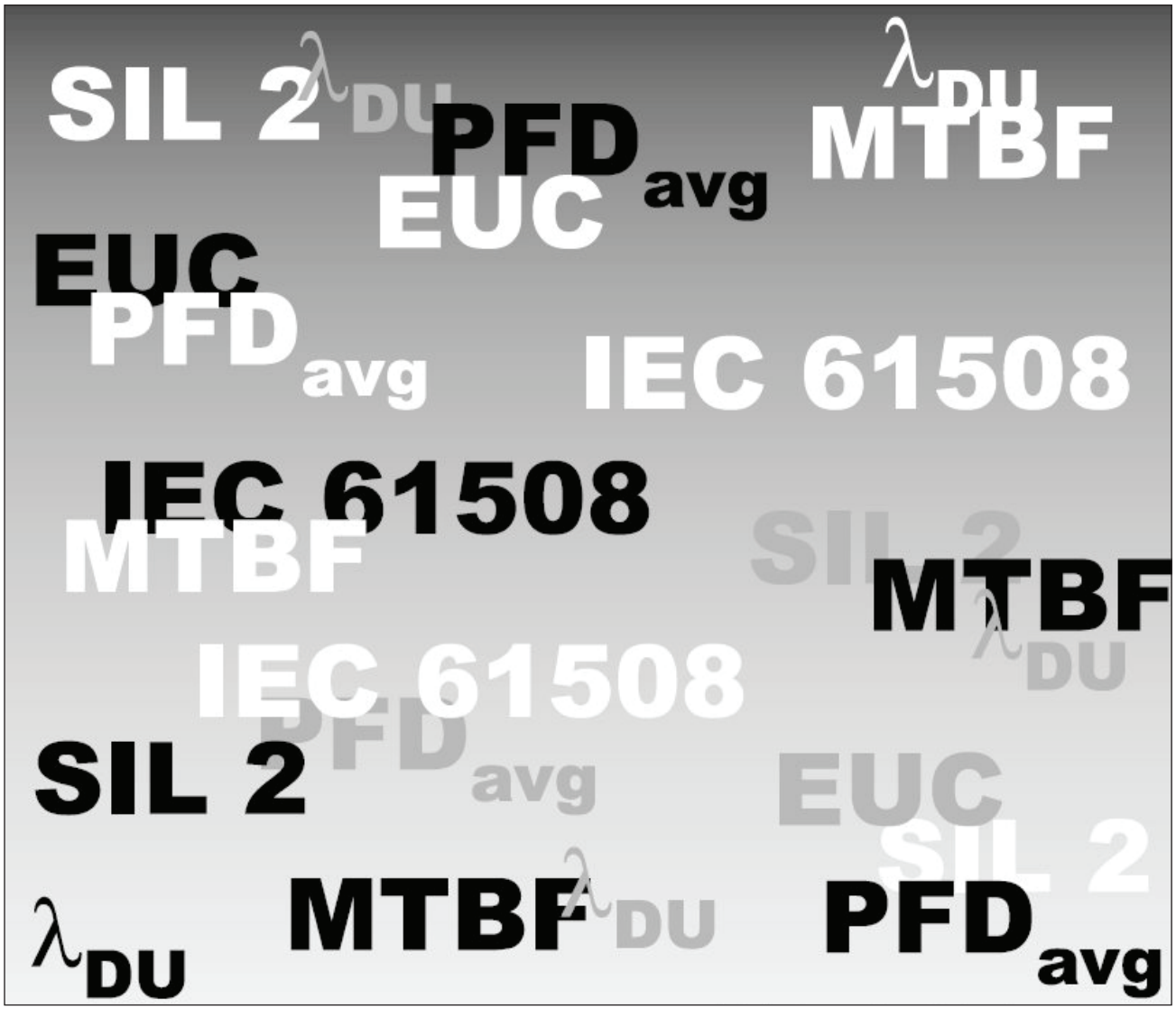
Application note
Functional safety

October 2016
AN9025 Rev 4

CROUSE-HINDS
SERIES

An introduction to Functional Safety and IEC 61508



EATON
Powering Business Worldwide

Contents

Page

1 INTRODUCTION

Instrumented safety systems are not new. It has long been the practice to fit protective systems to industrial process plant where there is a potential threat to life or the environment should something go wrong. These systems are independent of the normal process control, and take some action to render the plant safe in the event of a malfunction.

Until recently, such systems have generally been designed according to established practice within the company concerned, or in accordance with local codes of practice. Some of the necessary equipment, for example shut-down control systems, was available designed and certified for safety applications, but much of the peripheral equipment was not. Designers and installers had to do the best they could with the equipment that was available.

This situation is now changing rapidly. The broad acceptance of the IEC 61508 standard* is giving safety equipment suppliers and users a common framework on which to design products and systems for safety-related applications.

The benefits to users are: a more scientific, numeric approach to specifying and designing safety systems is possible; the nature of the risk can be quantified and a protective system appropriate to the risk can be designed. Because the protective system is assessed against a widely accepted standard, its suitability can be clearly demonstrated to all. Under- or over-specifying of protective systems is less likely and, in many cases, a less expensive solution may be shown to provide adequate protection.

Equipment suppliers, such as MTL, are now providing products certified to IEC 61508 for use in functional safety systems. The data provided with these products allow the user to integrate them into safety systems, to the IEC 61508 standard, and then state with confidence that the system meets the safety requirements.

This application note is intended to provide a brief introduction to the IEC 61508 standard, and to illustrate how it is applied. It does not claim to be a complete interpretation of the standard; that would be impossible in so few pages. However, we hope you will find it helpful, especially if the subject is new to you.

This area is likely to develop rapidly, as more certified products become available and the standard becomes more widely used. We expect to update this application note as more information becomes available and we would very much like to hear your comments. Please forward them to MTL by mail or telephone (see the back cover for details) or e-mail to AN9025comments@mtl-inst.com

2 FUNCTIONAL SAFETY

2.1 Aspects of safety

Storey (1996) identifies three aspects of system safety. The first is 'primary safety', which concerns such risks as electric shock and burns inflicted directly by hardware. The second is 'functional safety', which covers the safety of the equipment (the EUC - see below) that depends on the risk-reduction measures in question, and is therefore related to the correct functioning of these measures. The third is 'indirect safety', which concerns the indirect consequences of a system not performing as required, such as the production of incorrect information by an information system such as a medical database.

IEC 61508 claims to cover the second of these aspects, functional safety, and its definition of this (see the glossary below) coincides with that of Storey. However, as pointed out in Section 3.3 on Scope, its principles are applicable generally and, once it has been decided to use the standard, it would be inconsistent not to apply its principles to aspects of safety other than functional safety.

2.2 Glossary of terms

The definitions given in this glossary of terms are direct quotations from Part 4 of IEC 61508. The terms selected for definition are those considered to be most important to readers of this document. In a few instances, this author has added text for clarification, and this is enclosed in square brackets.

2.2.1 Systems

Equipment under control (EUC): equipment, machinery, apparatus or plant used for manufacturing, process, transportation, medical or other activities.

EUC control system: system which responds to input signals from the process and/or from an operator and generates output signals causing the EUC to operate in the desired manner.

EUC risk: risk arising from the EUC or its interaction with the EUC control system, i.e. the risk associated with functional safety. [The EUC risk is a reference point, so it should be assessed independently of countermeasures to reduce it.]

Safety-related system: designated system that:

- Implements the required safety functions necessary to achieve or maintain a safe state for the EUC; and
- Is intended to achieve, on its own or with other E/E/PE safety-related systems, other technology safety-related systems or external risk reduction facilities, the necessary safety integrity for the required safety functions.

Programmable electronic system (PES): system for control, protection or monitoring based on one or more programmable electronic devices, including all elements of the system such as power supplies, sensors and other input devices, data highways and other communication paths, and actuators and other output devices.

Electrical/electronic/programmable electronic system (E/E/PE): as for PES.

2.2.2 Safety and risk

Harm: physical injury or damage to the health of people either directly, or indirectly as a result of damage to property or to the environment. [This definition excludes damage to property or the environment which does not result in injury to people, and so it is not in conformity with modern definitions].

Hazard: potential source of harm.

Hazardous situation: circumstance in which a person is exposed to hazard(s). [Again, this definition is restricted to humans and is not as broad as other modern definitions].

Hazardous event: hazardous situation which results in harm.

Safety: freedom from unacceptable risk.

Functional safety: part of the overall safety relating to the EUC and the EUC control system which depends on the correct functioning of the E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities.

Safety function: function to be implemented by an E/E/PE safety-related system, other technology safety-related system or external risk reduction facilities, which is intended to achieve or maintain a safe state for the EUC, in respect of a specific hazardous event.

Risk: combination of the probability of occurrence of harm and the severity of that harm.

Tolerable risk: risk which is accepted in a given context based on the current values of society.

Residual risk: risk remaining after protective measures have been taken.

* IEC 61508 “Functional safety of electrical/electronic/programmable electronic safety-related systems”

2.2.3 Safety integrity

Safety integrity: probability of a safety-related system satisfactorily performing the required safety functions under all the stated conditions within a stated period of time.

Software safety integrity: measure that signifies the likelihood of software in a programmable electronic system achieving its safety functions under all stated conditions within a stated period of time.

Hardware safety integrity: part of the safety integrity of the safety-related systems relating to random hardware failures in a dangerous mode.

Safety integrity level (SIL): discrete level (one out of a possible four) for specifying the safety integrity requirements of the safety functions to be allocated to the E/E/PE safety-related systems, where SIL 4 has the highest level of safety integrity and SIL 1 the lowest.

2.2.4 Safety requirements

Safety requirements specification: specification containing all the requirements of the safety functions that have to be performed by the safety-related systems.

Safety functions requirements specification: specification containing the requirements for the safety functions that have to be performed by the safety-related systems. [One part of the safety requirements specification].

Safety integrity requirements specification: Specification containing the safety integrity requirements of the safety functions that have to be performed by the safety-related systems. [This is integrated into the safety requirements specification.]

3 OVERVIEW OF IEC 61508

3.1 Origins of IEC 61508

By the 1980s, software had become the first choice of most designers of control systems. Its apparent speed of production, the cheapness of its reproduction, and the ease with which it facilitates the introduction of new facilities, made it more attractive than purely hardware solutions. Its increased use included more and more safety-related applications, and there were uncertainties about the wisdom of this. It was recognised that it was almost impossible to prove software correct, and even if it were correct with respect to its specification, the difficulty of getting the specification correct was well known.

At that time, software engineering was still more art than engineering, and safety engineering was unknown in the software development community. Further, because safety was not in most cases studied in its own right, there was an implicit assumption that if a product or plant functioned reliably it would be safe. But safety and reliability are not synonymous. Moreover, with systems becoming larger and more complex, questions started to be asked about how safety might be 'proved' and how the use of software in safety-related applications might be justified.

The questions and uncertainties were not limited to software. At the same time, hardware, in the form of microelectronics, was also becoming extremely complex and difficult to prove correct.

The awareness of these issues led to two studies being set up by the International Electrotechnical Commission (IEC), one on 'systems' (hardware) and the other on software, both within the context of the functional safety of modern programmable electronic systems. The purpose behind each was the development of a standard to guide system designers and developers in what they needed to do in order to claim that their systems were acceptably safe for their intended uses.

In the early 1990s the two studies were merged, and in 1995 a draft standard, IEC 1508, was produced. This advocated a new approach to functional safety. Instead of designing and building a system as well as possible and then assuming that it would be safe, the draft standard called for a risk-based approach, in which the safety activities should be based on an understanding of the risks posed by the system. With an understanding of the risks, and a determination of which risks needed to be reduced, safety requirements would be defined to effect the risk reduction. As these 'safety requirements' would be specified separately from the functional requirements, they could be implemented as simply as possible and also validated separately. This would result in direct evidence of safety planning and should lead to confidence that the risk reduction measures were commensurate with the risks.

Feedback on the draft standard led to further development, and between 1998 and 2000 the seven parts of its successor, IEC 61508, were ratified as an international standard. The principles embodied in the new standard were accepted internationally.

IEC 61508 is a 'generic' standard, intended to satisfy the needs of all industry sectors. It is a large document, consisting of seven parts and a total of about 400 pages. Ideally it should be used as the basis for writing more specific (e.g. sector-specific and application-specific) standards, but it is also intended to be used directly where these do not exist. It has become a requirement of many customers, and its principles are perceived as defining much of what is considered to be good safety-management practice.

3.2 The physical form of the standard

The standard consists of seven parts. The first four are 'normative' - i.e. they are mandatory - and the fifth, sixth and seventh are informative - i.e. they provide added information and guidance on the use of the first four.

- Part 1 (General Requirements) defines the activities to be carried out at each stage of the overall safety lifecycle, as well as the requirements for documentation, conformance to the standard, management and safety assessment.
- Part 2 (Requirements for Electrical/ Electronic/ Programmable Electronic (E/E/PE) Safety-Related Systems) and Part 3 (Software Requirements) interpret the general requirements of Part 1 in the context of hardware and software respectively. They are specific to phase 9 of the overall safety lifecycle, illustrated in Figure 4.
- Part 4 (Definitions and Abbreviations) gives definitions of the terms used in the standard.
- Part 5 (Examples of Methods for the Determination of Safety Integrity Levels) gives risk-analysis examples and demonstrates the allocation of safety integrity levels (SILs).
- Part 6 (Guidelines on the Application of Parts 2 and 3) offers guidance as per its title.
- Part 7 (Overview of Techniques and Measures) provides brief descriptions of techniques used in safety and software engineering, as well as references to sources of more detailed information about them.

In any given application, it is unlikely that the entire standard would be relevant. Thus, an important initial aspect of use is to define the appropriate part(s) and clauses.

3.3 Scope of the standard

IEC 61508 is not merely a technical guideline. Indeed, its primary subject is the management of safety, and it is within this context that it addresses the technical issues involved in the design and development of systems. The standard seeks to introduce safety management and safety engineering, not only into software and system engineering, but also into the management of all aspects of systems. The standard embraces the entire life-cycle of a system, from concept to decommissioning.

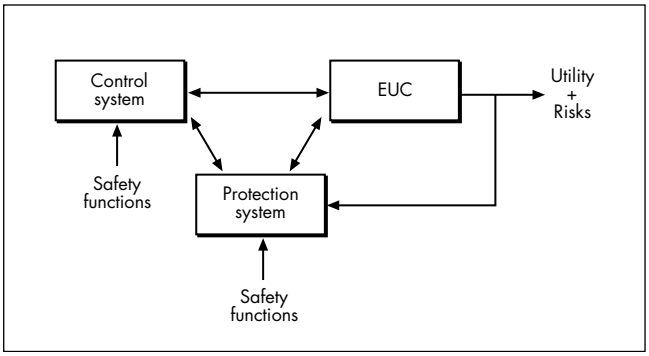


Figure 1 Risk and safety functions to protect against it

Although the standard formally limits itself to those aspects of safety that depend on the hardware and software of electrical/electronic/programmable electronic (E/E/PE) systems, its principles are general and form a framework for addressing all aspects of the safety of all systems.

3.4 The standard's rationale

The wording of the standard is based on the model of Figure1. In this, there is 'equipment under control' (EUC) which, with its control system, provides a utility (for example, electricity generation, railway signalling), but which, in order to do this, poses one or more risks to the outside world.

The standard requires that each risk posed by the EUC and its control system should be identified and analysed and tested against tolerability criteria. All risks found to be intolerable must be reduced, as shown in Figure 2. A risk-reduction measure may be to change the design of the EUC or its control system, but there comes a point when it is not effective to make further such improvements, or when, even if they have been made, the required level of safety cannot be demonstrated. If any of the residual risks is still intolerable (or cannot be shown to be tolerable), then 'safety functions' must be incorporated either within the control system or in one or more added 'protection systems' (see Figure 1). In principle, their separation from the control system is preferred.

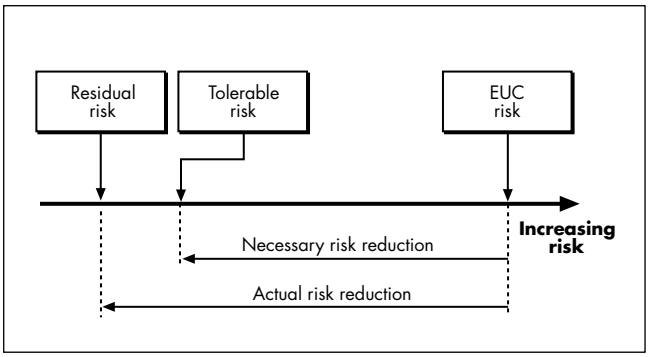


Figure 2 The determination of the necessary risk reduction

The model of Figure 1 is based on the process industry, and it may not be perceived as representing many modern systems - for example, information systems whose handling of data is safety-related, such as medical databases. Even though the wording of the standard does not obviously refer to such systems, the standard's principles do.

Figure 2 shows that the risk reduction that must necessarily be achieved is the difference between the risk posed by the EUC (and its control system) and the level of risk that is deemed, in the given circumstances, to be tolerable. The risk reduction is achieved by 'safety functions', and these must be based on an understanding of the risks. However, risk values are always approximate, and the actual reduction achieved by risk-reduction measures can never be determined exactly, so it is assumed in Figure 2 that the achieved risk reduction will be different from (and greater than) the reduction deemed to be necessary. The figure thus shows that the residual risk is not exactly equal to the tolerable risk - and nor is it zero.

The development of safety functions, which embody the main principles of the standard, requires the following steps:

- Identify and analyse the risks;
- Determine the tolerability of each risk;
- Determine the risk reduction necessary for each intolerable risk;
- Specify the safety requirements for each risk reduction, including their safety integrity levels (SILs);
- Design safety functions to meet the safety requirements;
- Implement the safety functions;
- Validate the safety functions.

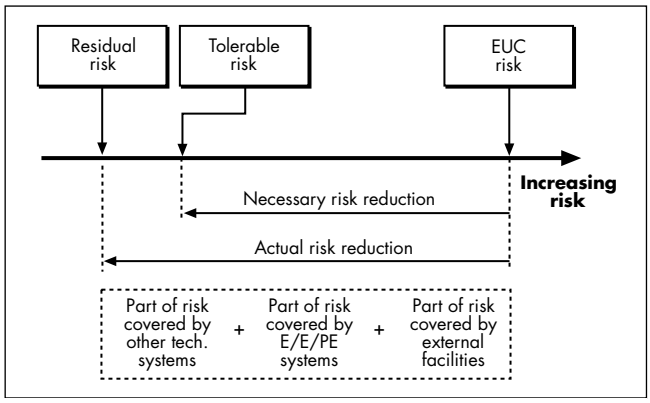


Figure 3 Understanding the risk and the means of reduction

Although the standard formally addresses only safety-related E/E/PE systems, it points out (see Figure 3) that safety functions may also be provided in other technologies (such as hydraulic systems) or external facilities (for example, management procedures). The principles of the standard should be applied in all cases.

3.5 The overall safety lifecycle

The overall safety lifecycle (see Figure 4) is crucial to IEC 61508. Not only does it offer a model of the stages of safety management in the life of a system, but it also forms the structure on which the standard itself is based. Thus, the standard's technical requirements are stated in the order defined by the stages of the overall safety lifecycle.

The purpose of the overall safety lifecycle is to force safety to be addressed independently of functional issues, thus overcoming the assumption that functional reliability will automatically produce safety. Then, specifying separate safety requirements allows them to be validated independent of functionality, thus giving higher confidence of safety under all operating and failure conditions. The paradox, however, is that safety activities should not be carried out, or thought of, as totally disconnected from other project or operational activities. They need to be integrated into a total perspective of the system at all lifecycle phases.

In the overall safety lifecycle, Phases 1 and 2 indicate the need to consider the safety implications of the EUC and its control system, at the system level, when first they are conceived of. In Phase 3, their risks are identified, analysed, and assessed against tolerability criteria. In Phase 4, safety requirements for risk-reduction measures are specified, and in Phase 5 these are translated into the design of safety functions, which are implemented in safety-related systems, depending on the selected manner of implementation, in Phases 9, 10 and 11. However the safety functions are realised, no claim for safety can be made unless its planning considers the overall safety context, and this is reflected in Phases 6, 7 and 8. Then, again, carrying out the functions of installation and commissioning, safety validation, and operation and maintenance, is shown in Phases 12, 13 and 14 to be on the overall systems, regardless of the technologies of the safety-related systems. Phases 15 and 16 cover later modification and retrofit of the system and decommissioning, respectively.

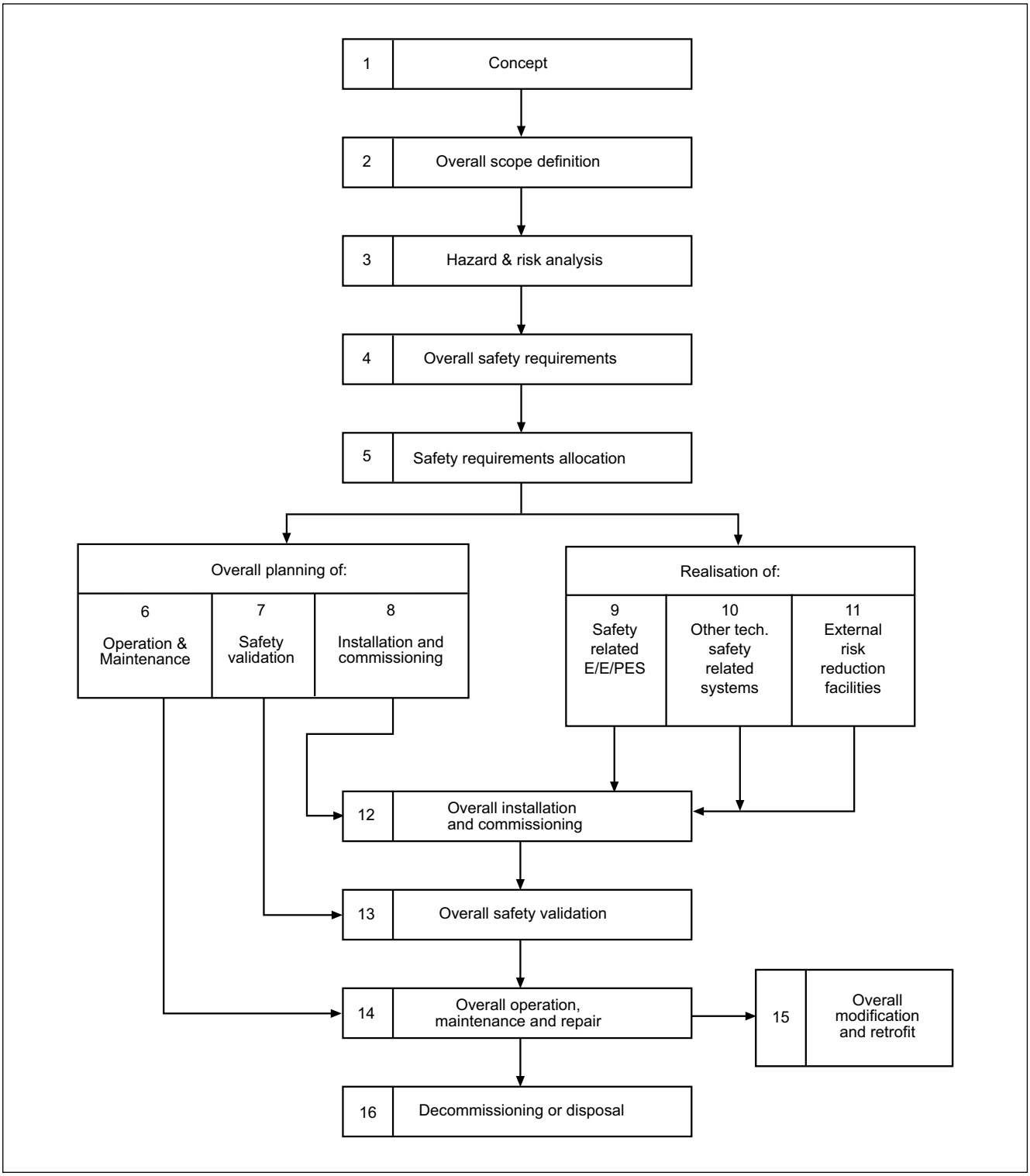


Figure 4 The overall safety lifecycle (from IEC 61508-1- Figure 2)

The overall safety lifecycle covers not merely the development of a system, but its entire life cycle, and this is illustrated by the inclusion of Phases 12 to 16. At the same time, like all models, this one is an approximation. Its phases are shown sequentially, so the iteration between them is not portrayed. For example, if modification and retrofit (Phase 15) is carried out to an operational system, all activities, from risk analysis, through specification, to revalidation, would need to be carried out, but this is not explicit in the model. A lesson from this is that a model cannot be a substitute for good engineering or good management, should never be relied on entirely as a guide to what to do, and should only be used in support of well-understood good practice. Other omissions from the lifecycle are activities, such as management, documentation, verification, quality assurance and safety assessment, that are essential to all phases - but these are set out as requirements in the clauses of the standard.

3.6 Risk and its analysis and reduction

A fundamental principle of the standard is that the measures taken to ensure safety should be commensurate with the risks posed by the EUC and its control system. Thus, a thorough risk analysis must be carried out, as required by Phase 3 of the overall safety lifecycle and by Clause 7.4 of Parts 1, 2 and 3 of the standard.

Risk analysis is normally defined as consisting of three stages - hazard identification, hazard analysis, and risk assessment - and some examples of how it may be carried out are offered in Part 5 of the standard.

Hazard identification consists of an attempt to identify the potential sources of harm. For simple systems that have already been in operation for some time, methods such as brainstorming and the use of a checklist may be adequate. But for systems that are novel or complex, a team effort is required. An EUC and its control system may pose many hazards, and as many as possible must be identified, for the risks associated with unidentified hazards will not be analysed or reduced. The importance of hazard identification cannot be emphasised too strongly, and the standard points out that identifying hazards concerned only with normal operation is not sufficient. Those arising from failures and 'reasonably foreseeable' misuse must also be identified. For this, professionals in the domain, functioning in a carefully chosen and well managed team, are required.

Hazard analysis is the study of the chains of cause and effect between the identified hazards and the hazardous events (accidents) to which they might lead. The analysis is intended to determine causes and consequences, so that the risk attached to each hazard can be derived. It may be quantitative or qualitative. In a quantitative analysis, the probabilities of events are estimated, as are numeric values of their consequences. Then, the risks are calculated by multiplying the two. But qualitative analysis is also admissible, and the standard's definition of risk, as the combination of likelihood and consequence, facilitates this. Various qualitative methods of analysis, using the risk matrix and the risk graph, are illustrated in Part 5 of the standard.

In the case of simple hardware with a history of use in conditions that are the same as those of the safety-related application, the probabilities of certain events, such as equipment failures, may be estimable from data on past frequencies. Similarly, consequences may also be expressed numerically, for example as the number of lives lost, or some financial value of the total resulting losses. However, the standard recognises that, because software failure is systematic and not random, qualitative methods must be used in the case of software.

In the risk-assessment stage of risk analysis, the risk values determined in the previous stage are compared against tolerability criteria to determine if they are tolerable as they are, and, if not, by how much they need to be reduced. There is necessarily a great deal of subjectivity in this process, not least in the decision of what level of risk is tolerable. It should be noted that tolerability may be different for each risk posed by the EUC and its control system, for it depends not only on the level of risk but also on the benefits to be gained by taking the risk and the cost of reducing it. The subject of tolerability is discussed in Section 5.

3.7 Safety requirements and safety functions

The safety requirements are those requirements that are defined for the purpose of risk reduction. Like any other requirements, they may at first be specified at a high level, for example, simply as the need for the reduction of a given risk. Then they must be refined so that their full details are provided to designers. The totality of the safety requirements for all risks forms the safety requirements specification.

At the design stage, the safety requirements are provided by means of safety functions. These are implemented in 'safety-related systems' which, as seen in Figure 3, need not be restricted to any given technology. For example, a braking system may be hydraulic. A safety requirement may be met by a combination of safety functions, and these may be implemented in systems of different technologies - for example, a software-based system along with management procedures, checklists, and validation procedures for using it.

When a safety function is implemented via software, there also needs to be a hardware platform, in which case a computer system is necessary. Then, the same demands are made of the entire system as of the software. Further, the standard allows for more than one software-safety function to be implemented on the same hardware platform, and it imposes rules for this.

3.8 Safety integrity levels

If there is an important job to be done, the means of doing it must be reliable, and the more important the job, the more reliable they should be. In the case of a safety-related system, the job is to achieve safety, and the greater the system's importance to safety, the lower should be the rate of unsafe failures. A measure of the rate of unsafe failures is the safety integrity of the system, which is defined in Part 4 of IEC 61508 as 'the likelihood of a safety-related system satisfactorily performing the required safety functions under all the stated conditions, within a stated period of time'.

If the rate of unsafe failures could always be measured numerically, there would be no need for safety integrity levels (SILs) because SILs are categories of safety integrity - and categories would be unnecessary if exact values were available. In the standard a SIL is defined as 'a discrete level (one of 4) for specifying the safety integrity requirements of safety functions'. Thus, a SIL is a target probability of dangerous failure of a defined safety function, and was originally intended for use when qualitative hazard analysis has been carried out and numerical risk values are not available, as in the case of software.

The standard demands that whenever a safety requirement is defined it should have two components: its functional component and its safety integrity component. Considering Figure 2, the safety requirement arises out of the need for risk reduction. Thus, at the highest level, the functional component is to 'reduce the risk'. The safety integrity component consists of a SIL (between 1 and 4), and this is related to the amount of risk reduction that is required. As said earlier, the more important the job, the more reliable the system must be. Here, the greater the risk reduction needed, the greater the extent to which safety depends on the system that provides the risk reduction, so the higher the SIL.

Table 1 Safety integrity levels for continuous operation

Safety Integrity Level	Continuous/ High-demand Mode of Operation (Prob. of a dangerous failure per hour)
4	$\geq 10^{-9}$ to $<10^{-8}$
3	$\geq 10^{-8}$ to $<10^{-7}$
2	$\geq 10^{-7}$ to $<10^{-6}$
1	$\geq 10^{-6}$ to $<10^{-5}$

Table 2 Safety integrity levels for low demand operation

Safety Integrity Level	Low demand Mode of Operation (Average prob. of failure on demand)
4	$\geq 10^{-5}$ to $<10^{-4}$
3	$\geq 10^{-4}$ to $<10^{-3}$
2	$\geq 10^{-3}$ to $<10^{-2}$
1	$\geq 10^{-2}$ to $<10^{-1}$

The standard equates SILs with numeric probabilities of unsafe failures in two tables (Tables 1 and 2), one for systems whose operation is continuous and one for on-demand (or low-demand) systems. The standard's definition of low-demand is 'no greater than one demand per year', hence the difference of 10^4 in the values in the two tables (where one year is approximated to 10^4 hours). Assuming a failure rate of once per year, the SIL 4 requirement for the low-demand mode of operation is no more than one failure in ten thousand years.

As stated in their definition, SILs are intended to provide targets for developers. In the case of simple electromechanical hardware, it may be possible to claim achievement of the SIL, using historic random-failure rates. But for complex systems, and for software, whose failures

are systematic and not random, such a claim is unsupportable by evidence. Thus, SILs are used to define the rigour to be used in the development processes. In other words, because evidence of the rate of dangerous failures of the product cannot be determined with confidence, attention is turned to the development process. Here, SIL 1 demands basic sound engineering practices and adherence to a quality management standard, such as ISO 9000. Higher SILs, in turn, demand this foundation plus further rigour, and guidance on what is required is found for hardware and software in Parts 2 and 3 of the standard respectively.

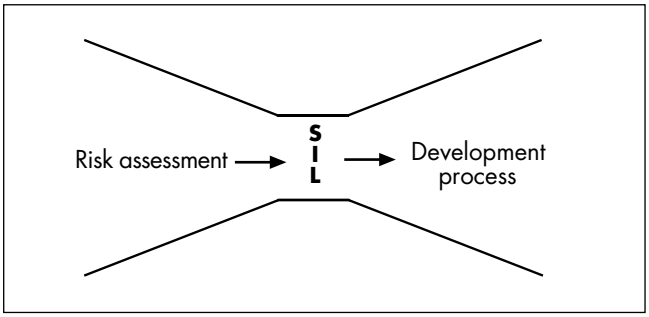


Figure 5 The "Bowtie Diagram" showing the derivation and application of SILs

The derivation and application of SILs may be illustrated by the 'bowtie diagram' of Figure 5 (from Redmill (1998)). The funnelling-in process consists of risk analysis, which leads to the determination of the required risk reduction. This is translated into a SIL, which then informs the funnelling-out, or expanding, development process.

3.9 Safety assessment

Since zero risk is not possible, complete safety cannot be achieved. And since it is never possible to prove safety, it is necessary to try to increase confidence to as high a level as is appropriate to the circumstances. Increasing confidence is done by demonstrating what has been achieved, so safety engineering has two goals: to achieve safety and to demonstrate the achievement. It is the responsibility of those claiming that a system is sufficiently safe to demonstrate that their claim is valid, and they need to do this by building up a safety case (see below).

The validation of the claim needs to be performed by independent safety assessors, and the standard defines three levels of independence: independent person, independent department, and independent organisation. The level required in any given case depends on the SIL of the system being assessed.

3.10 Principles not covered by the standard

3.10.1 Human factors

The phrase 'human factors' is a general term used to embrace all issues involving humans. It covers the ergonomic aspects of a system, the operator of the system, and, sometimes, management.

It is said that most accidents are caused, at least in part, by humans. Thus, in identifying and analysing hazards, it would be sensible for human factors to be considered. Yet, in many risk analyses they are not, for two main reasons: first, it is traditional to base risk analysis on equipment failure and, second, engineers are not familiar with human reliability assessment techniques. If this is to change, new standards need to provide advice on when and how to include human factors in risk analyses.

However, although IEC 61508 mentions human factors in passing, and advises that it should be taken into consideration, it offers no guidance on what to do or how or when to do it.

In the light of modern understanding of human error, it cannot be argued that human causes of accidents are wholly unpredictable, so a review of a risk analysis in the context of an investigation is likely to question the omission of human factors. Information on the subject may be found in Reason (1990) and Redmill and Rajan (1997).

3.10.2 The safety case

The development and maintenance of a safety case has become expected practice in many industries. A safety case is a logically presented argument, supported by a sufficient body of evidence, for why a system is adequately safe to be used in a particular application. To be both convincing and a record of why a system was accepted into service, the case needs to be documented. However, as few systems remain static for long, and changes are made to them both in the development stage and during operation and maintenance, the safety case needs to record all changes and be updated so that its argument remains valid. It should, thus, be a 'live' system of documentation.

The concept of the safety case originated in regulated industries in which a license was required before a system could be brought into operation. The goal-based, rather than prescriptive, nature of modern standards (such as IEC 61508), means that developers and operators cannot simply claim adherence to a set of rules as evidence of safety. They must carry out risk analysis, set goals for risk reduction, and then meet those goals. Further, during the process, they must demonstrate both that their safety targets are well founded and that the safety functions that they put in place to meet them are adequate.

Similarly, safety assessors and regulators cannot simply check that given rules have been followed. They need to ensure that the risk-reduction goals were reasonable and that all processes in the design, construction and testing of the safety functions have been discharged to the required safety integrity level.

To enable such safety management by the system developers and operators as well as the safety assessors and regulators, it is not sufficient simply to document everything. That results merely in a bulk of documentation from which it may be impossible to derive proof of anything. What is needed is structured documentation with, at the top level, the safety argument. Then, the documentation of the various parts of the processes involved becomes accessible and referenced evidence in support of the safety argument. This is the principle of the safety case.

Although the safety case is currently mandatory only in licensed industries, the principle is being adopted in more and more organisations. Yet, IEC 61508 does not provide guidance on it. The standard offers some guidance on carrying out safety assessments, and points out that in all cases there should be a level of independence, the level depending on the safety integrity level of the system in question. But there is no guidance on the safety case, or on how information should be collected, documented, and structured in order to facilitate the development of a safety argument.

4 SOME RELATED STANDARDS

IEC 61508 is a generic standard, intended as the basis for drafting standards that are tailored more specifically to a particular industry sector, or to a particular company. When an industry- or company-specific standard does not exist, IEC 61508 is also intended to be used directly. However, its size and the breadth of its generic scope suggest that when this is done, it is necessary to define very carefully what parts of the standard should be used and how its requirements should be interpreted in the given context.

In the field of instrumentation, there are three sector-specific standards which it is worth mentioning in the context of IEC 61508. The German standard, DIN 19250 was developed before even the early drafts of the international standard, and its content was used in it; the US standard, S84, was developed concurrently with the forerunner of IEC 61508, and it was made to reflect its principles; the international standard, IEC 61511, is being developed after IEC 61508 so as to be a genuine sector specific interpretation of it for the process industry. Some notes on these three standards follow.

4.1 DIN 19250

This is a German 'pre-standard' (draft standard) entitled 'Grundlegende Sicherheitsbetrachtungen für MSR-Schutzeinrichtungen' (Fundamental safety aspects to be considered for measurement and control equipment), last issued in 1994. It was influential in the preparation of the risk-analysis examples in IEC 61508, and its content is to be found in Part 5 of that standard. As this pre-standard covers only a small part of the safety lifecycle, the whole of which is covered by IEC 61508, it cannot be considered to be a sector-specific interpretation of the international standard.

DIN 19250 is application independent and was intended to provide guidance to standardisation committees that wish to define technical rules for carrying out risk analyses. It describes a qualitative risk analysis process, using the risk graph, that leads to the identification of the appropriate 'requirements class'. (Anforderungsklassse - usually abbreviated to AK.)

Risk classes are of the same nature as the safety integrity levels (SILs) of IEC 61508, so DIN 19250 provides guidance on carrying out risk analysis (limited to qualitative analysis and the risk graph method) up to the point of determining the equivalent of the SIL. The purposes of requirements classes are: first to reflect the level of the risk that needs to be mitigated, and, second, to define the reliability of the functions that will carry out the mitigation. Thus, the greater the risk, the higher the risk class. Whereas IEC 61508 defines four safety integrity levels, DIN 19250 defines eight requirements classes. A correspondence between the two categorisations may be derived.

Once the analysis has been carried out and the requirements class determined, the user of the pre-standard needs to turn to other DIN standards (DIN V VDE 0801 and DIN 19251) to determine the precise constraints that they place on the development of the mitigating safety functions. Like in IEC 61508, these constraints are defined in terms of bundles of technical and organisational measures, which are intended to ensure that the risk in question will be reduced at least to the required level.

As the guidance given in these standards, including DIN 19250, has been subsumed into IEC 61508, the standards themselves are declining in use in favour of the international standard.

4.2 S84

This is an American standard whose full title is: 'ISA-S84.01, Application of Safety Instrumented Systems for the Process Industries'. It is specific to the process industries and addresses the application of safety instrumented systems (SIS). It was developed in the early 1990s, in parallel with the development of the 1995 draft of IEC 61508(called IEC 1508), and its developers ensured that it was in conformity with the IEC principles. Indeed, a feature of S84 is a clause which describes the main differences between it and IEC 1508 (it should be pointed out that these differences may now not all apply to IEC 61508, as this was published some years later, after further development).

Because it addresses only safety instrumented systems, and not the equipment under control (see the earlier description of IEC 61508), S84 does not cover the entire safety lifecycle. However, it defines the full life cycle and then points out that its use assumes that the early activities, up to risk analysis and the determination of SILs, has already been carried out. Thus, it places itself clearly in the context of IEC 61508, and this is stated in its introduction. It should be said, however, that in an annex, intended for information only, the standard provides information and examples on the determination of SILs, as per IEC 61508.

S84 shows, within its life-cycle model, that identified hazards may be prevented, or risks reduced, by the use of 'non-SIS protection layers'. However, the standard does not cover these and restricts itself to good practice in the provision of safety instrumentation systems, from their specification to their decommissioning.

4.3 IEC 61511

This international standard, entitled, 'Functional Safety: Safety Instrumented Systems for the Process Industry Sector', is currently under development by the same IEC committee that produced IEC 61508. It is defined as being 'process industry specific within the framework of the International Electrotechnical Committee (IEC) Publication 61508'. It is therefore intended to perform the same function internationally that S84 performs in the USA.

It defines safety instrumented systems as including sensors, logic solvers and final elements, and states that it covers all these components of an SIS as well as all technologies by which they may be constructed.

This standard is broader in scope than S84, for it covers the early hazard and risk analysis and the specification of all risk-reduction measures, which S84 assumes to have been done. It also contains sections on such issues as how to show conformity with the standard, so it is of much greater length than S84.

IEC 61511 follows the IEC 61508 overall safety lifecycle and uses the system of safety integrity levels described in that standard. In short, it is a sector-specific interpretation of the generic standard.

5 THE TOLERABILITY OF RISK

Individuals and organisations make frequent decisions about risks, choosing which to accept and which to reject. Risks are rejected because of such considerations as conservatism, fear, and a responsible attitude to danger to oneself or others. Risks are accepted because of the possibility of reward, which may take the form of profit, pleasure, or simply the gratification of a spirit of adventure. There is a trade-off implied in risk acceptance.

Risks not immediately rejected are not necessarily accepted unconditionally, or as presented. They may be accepted if the reward is increased. Or they may need to be reduced before acceptance. A person wanting to cross a road does not either cross the road or not. They may wait until the risk has been reduced, due to a reduction in the flow of traffic, or because traffic lights change colour. Similarly, the design of production plant is not simply accepted or rejected, but may be accepted subject to a certain risk being reduced by the inclusion of a safety instrumented system.

It should be added that a risk deemed tolerable by one individual may not be so determined by another. For example, different pedestrians will accept different levels of risk in crossing a road, and one businessman may accept the risks of a financial venture whereas another would not. Thus, there is subjectivity in risk acceptance. Likewise, risk acceptance involves ethical and moral values as well as risk estimates. For example, even when the likelihood and consequences of something going wrong are accepted by all parties, some people are willing to accept the risk while others are not, perhaps because of their concern for the environment.

The law in the UK requires risks to be reduced 'so far as is reasonably practicable', and the Health and Safety Executive's (HSE) model for how this should be achieved is the ALARP (as low as reasonably practicable) principle. The word 'practicable' is deliberately chosen over 'practical', as the latter would imply that a risk should be reduced as far as possible, and what is intended is that the cost of reducing the risk should be taken into account. However, the ALARP principle places the onus on the creator of the risk to justify the residual risks by demonstrating that further reduction would not be reasonably practicable.

The ALARP principle first appeared in The Tolerability of Risk from Nuclear Power Stations (HSE 1988), but its application has been extended by the HSE from its original context in the nuclear industry to regulation in all industry sectors.

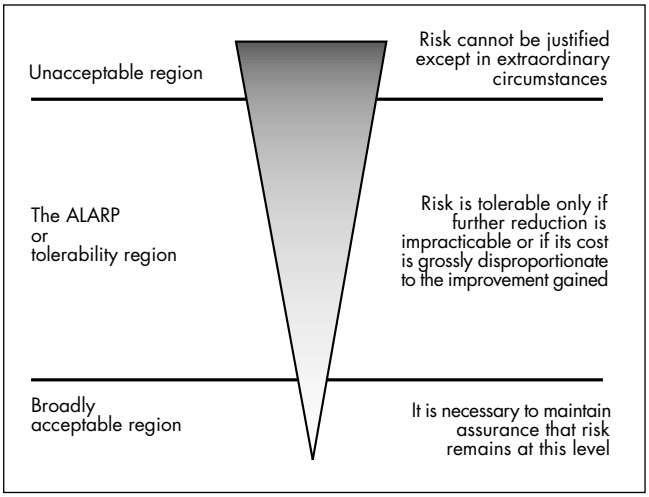


Figure 6 The Health and Safety Executive's ALARP model

Summarised in Figure 6, the ALARP principle defines a risk as being in one of three categories or regions. If any risk lies in the 'unacceptable' region, the process, procedure, plant, or activity which poses the risk cannot be deployed. The risk must first be reduced at least as far as the ALARP region. In the lowest, or 'broadly acceptable', region, the risk is considered to be negligible and would be accepted without reduction - though it would normally be necessary to monitor it in case it increased. In the 'tolerability' region, the risk is neither automatically acceptable nor automatically unacceptable and may be accepted or rejected depending on the cost of reducing it and the benefits to be gained.

The boundary with the broadly acceptable region may be taken to indicate the 'safe' level', but this is not a level of zero risk. Similarly, the boundary with the unacceptable region defines 'unsafe', but it is not a point of certain catastrophe or even of maximum risk.

The HSE distinguishes 'tolerable' from 'acceptable' and defines it as indicating 'a willingness to live with a risk so as to secure certain benefits in the confidence that the risk is one that is worth taking and that it is being properly controlled' (HSE 1999). As such, a tolerable risk is not necessarily one that would, in the absence of the potential benefit, be judged acceptable by those taking it. Nor should it be accepted unthinkingly; it should be tested for appropriateness and value.

In the model, the triangle's breadth is intended to show that the practicable cost of risk reduction increases as the risk increases. Thus, the higher the risk, the higher must be the cost of its reduction for it to be deemed impracticable and for the unreduced risk to be justified. This is not to say that the reduction of a significant risk necessarily requires significant expenditure. In many cases, the cost of even significant risk reduction can be small.

The ALARP principle is a description both of what regulators look for in making assessments and of what the creators of risks need to do in determining the tolerability of the risks that they pose.

6 HOW IEC 61508 IS APPLIED

6.1 Introduction

This section considers the design of a pressure relief system as an illustration of how IEC 61508 may be applied in a practical case. It illustrates the use of apparatus which has a third-party certified SIL rating, in combination with apparatus which does not.

This example focuses on the design of the protective system and is not intended to be a full interpretation of IEC 61508. References to the IEC 61508 standard are shown in italics.

6.2 Installation

The installation being considered (Figure 7) is a pressure vessel, used in a batch process that has a weekly cycle. The vessel is brought, in a controlled manner, to a prescribed pressure using the control loop indicated in the diagram. The perceived hazard is that the control system might fail, subjecting the vessel to overpressure.

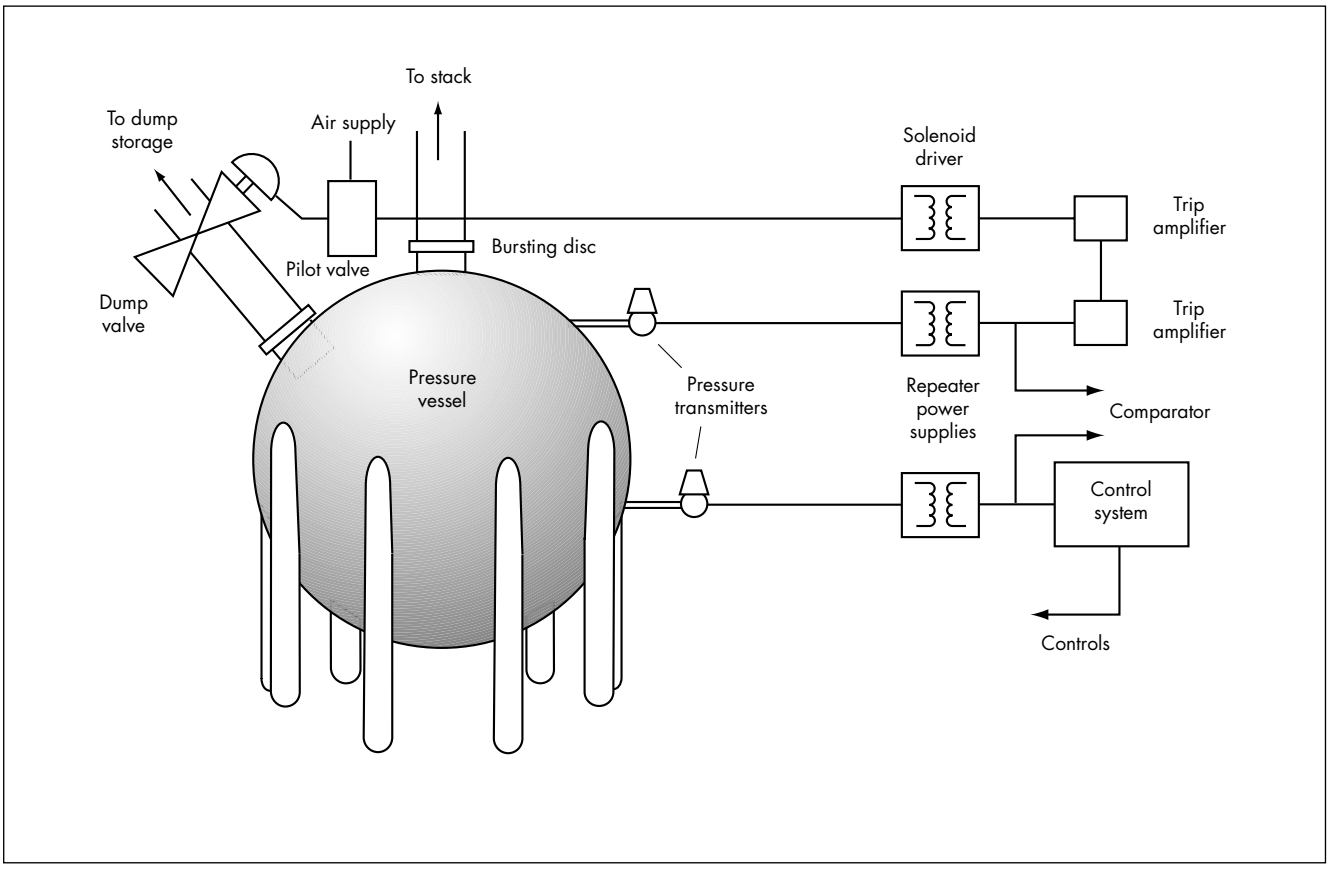


Figure 7 Overview of installation

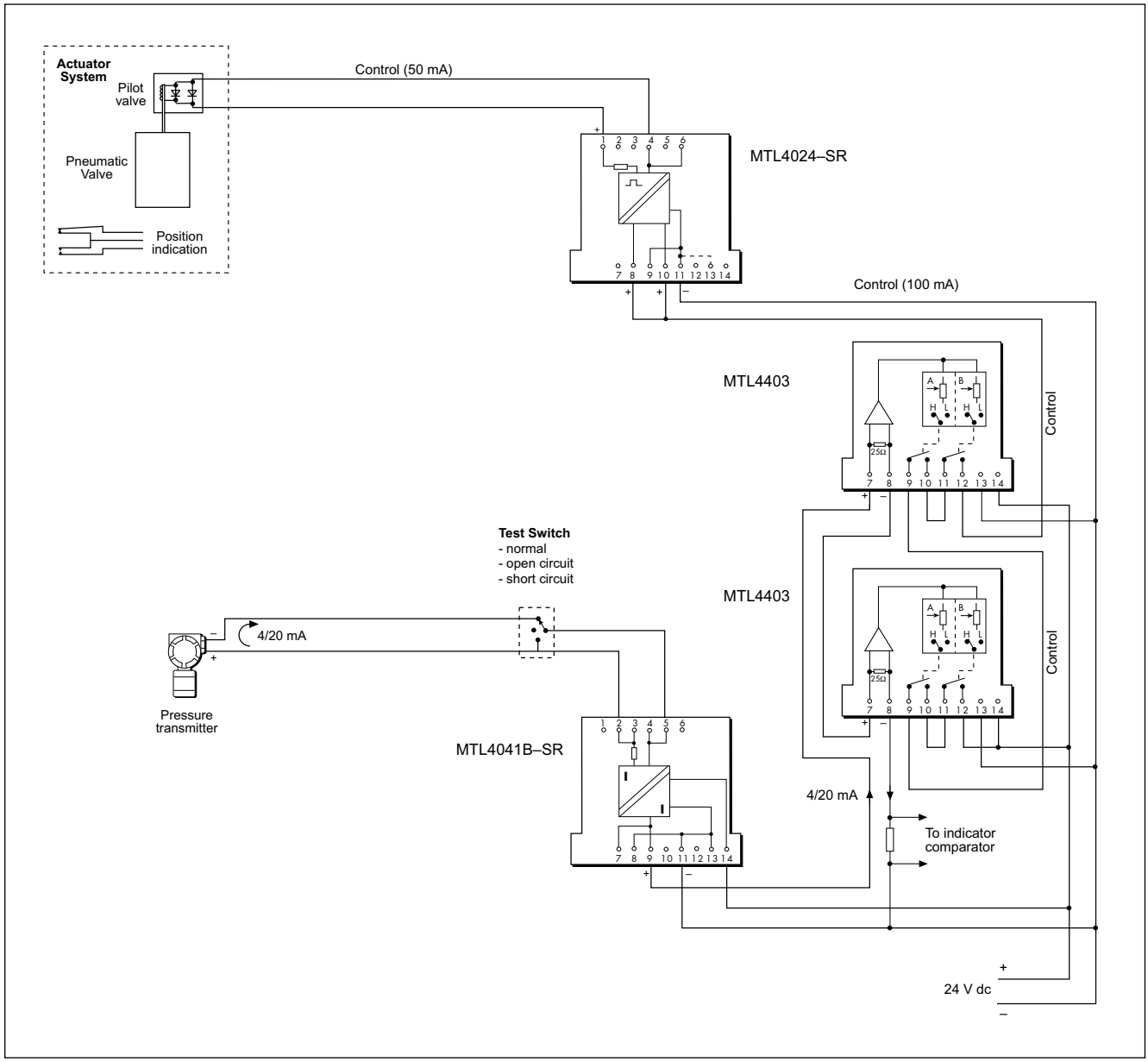


Figure 8 Pressure relief system

The final safeguard is a bursting disc, which discharges to a stack, releasing the contents of the vessel into the atmosphere. The bursting disc is considered to be 100% reliable but its operation is not considered desirable for environmental and public relations reasons. An acceptable level of risk is a 10% probability of a release once in the plant's expected life of ten years. IEC 61508 defines this as the *tolerable risk*, in this case a frequency of no greater than once in 100 years, or once per 10^6 hours (based upon 1 year being approximately 10,000 hours).

An analysis of the control system and other related factors, indicates that it might fail once a year in an expected life cycle of ten years. Hence the Equipment Under Control risk (EUC risk) is once per year, or once per 10^4 hours.

It is apparent that a safety-related protection system (*safety function*) is required to reduce the EUC risk to the tolerable level. IEC 61508 considers safety functions differently depending on whether they are in a high or a low demand mode. In this case, the safety function may be called on to operate once per year, which places it in the low demand mode category. (IEC61508-4 3.5.12)

The required *average probability of failure on demand* (PFD_{avg}) of the safety function is the difference between the EUC risk and the tolerable risk (IEC 61508-5 Annex C).

$$PFD_{avg} \leq 10^{-6}/10^{-4}$$
$$\leq 10^{-2}$$

From IEC 61508-1 Table 2, we see that the required safety integrity level (SIL) of the safety function is SIL 2. In practice, the design of the safety function is usually iterative; a solution is proposed and then analysed to determine whether it meets (or exceeds) the requirements, then it is modified accordingly.

6.3 Safety function

The proposed safety function dumps the contents of the vessel into a storage vessel for disposal. Its operation is controlled by the loop indicated in Figure 7 and shown in more detail in Figure 8. A smart pressure transmitter with a 4/20mA analogue output senses the pressure. The 4/20mA signal is then transferred via an MTL4041B-SR isolator to two MTL4403 trip amplifiers. The trip amplifiers are configured 1oo2*, so that the safety function is activated, i.e. the dump valve is opened, if either is tripped. The valve actuator is then driven through an MTL4024-SR isolator.

* 1oo2 is shorthand for one out of two - either of the two trip amplifiers can activate the safety function.

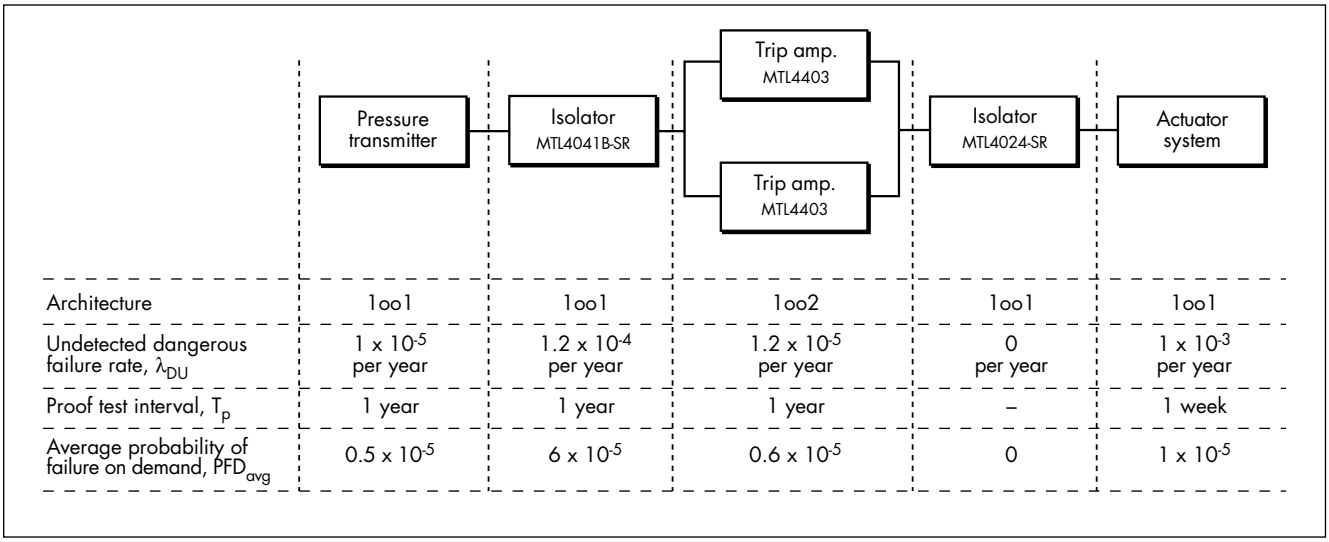


Figure 9 Sub-system structure

Figure 9 shows the subsystem structure in reliability terms (IEC 61508-6 Annex B.2). Since all dangerous detected failures result in the safety function being activated, it is only necessary to consider the dangerous undetected failures in this analysis.

The functional safety of each element is discussed in the following paragraphs.

6.3.1 The pressure transmitter

The pressure transmitter is required to be at least SIL 2. Types certified to IEC 61508 are commercially available, e.g. Siemens Moore 345 XTC, and ABB Safety 600T.

Ideally, the transmitter should be of a different manufacture to that used in the control loop so as to reduce the probability of common mode failure. If this is not possible, then transmitters from different manufacturing batches could be used.

In this type of apparatus, a dangerous failure is typically regarded as having occurred when the signal is in error by more than 2 %. An undetected dangerous failure is a failure which produces a signal within the range of 3.8 mA to 21 mA. This is because, in this range, an erroneous signal cannot be distinguished from a correct signal.

These specially designed transmitters typically have a failure rate of 4×10^{-4} per year and an undetected dangerous failure rate of 1×10^{-5} per year. Note that, although this failure rate far exceeds the requirement for SIL 2, the architecture restricts the use of the transmitter to SIL 2 safety functions, because the failure of a single component can cause a dangerous failure (IEC 61508-2-7.4.3.1). This analysis assumes that the transmitter has a dangerous failure rate of 4×10^{-4} per year and a rate of undetected failure of 1×10^{-5} per year, and is suitable for use in a SIL 2 safety function.

The transmitter must be periodically proof tested, ideally by applying pressure over the range in which the system is set to trip, and checking that its output is correct. (A suitable manifold could be fitted to facilitate the proof test without dismantling the transmitter from the vessel). A proof test interval of 1 year is more than adequate to achieve the necessary PFD_{avg}. If it is impractical to apply the ideal proof test, a lesser test may be adequate provided that the required PFD_{avg} is obtained (IEC 61508-6 Annex B.2.5).

6.3.2 MTL4041B-SR isolator

The MTL4041B-SR repeater power supply has a BASEEFA certificate number BAS 01SP9196X which indicates that the unit can be used in a SIL 2 safety function. It has a detected dangerous failure rate of 1.2×10^{-3} per year and an undetected dangerous failure rate of 1.2×10^{-4} per year. Again, the architecture restricts its use to a SIL 2 safety function. As for the transmitter, assume a full proof test is carried out once per year.

6.3.3 1oo2 MTL4403 trip amplifier combination

The MTL4403 trip amplifier is not currently available with independent certification to IEC 61508. Its suitability for this application is justified from the available failure rate data, and by the 1oo2 configuration, which greatly increases the reliability. The analysis presented is relatively simple and errs on the side of caution and consequently is acceptable for this particular application.

Firstly, consider the constraints on the SIL due to the architecture of the MTL4403 (IEC 61508-2-7.4.3.1). The *hardware fault tolerance* of the MTL4403 is 0, since the failure of one component, for example relay contacts sticking, may cause loss of the safety function. Since a formal failure modes and effects analysis (FMEA) has not been performed, assume that the MTL4403 is a type B subsystem according to IEC 61508-2-7.4.3.1.3. (A subsystem is type B if the failure modes are not completely defined, or there is insufficient field experience to support the claimed failure rates.) IEC 61508-2 table 2 gives the SIL restrictions for type B subsystems. SIL 1 can be claimed for a hardware fault tolerance of 0 if the *safe failure fraction* (SFF) is 60% or more. This means that at least 60% of the failure modes result in a safe state, which in this case means that the relays open. It seems reasonable to assume that a greater proportion of faults will cause the relays to open than to remain closed, so we can say with some confidence that a single MTL4403 meets the requirements for SIL 1.

However, the safety function is required to meet SIL 2. If two MTL4403s are used in a 1oo2 configuration, the SFF is unchanged but the hardware fault tolerance is now 1 - the safety function is maintained in the event of a fault occurring in either MTL4403, and so the architectural requirements for SIL 2 are met. (IEC 61508-2-7.4.3.1.6).

A single MTL4403 has a calculated mean time between failures [MTBF] of 289 years at 20°C and 113 years at 60°C. [These figures were calculated to MIL-HDBK-217F, Notice 1, using Milstress version 3.31 for a ground benign environment.] The relay contacts are open when the relay is de-energised or the power supply is lost. In this application, one alarm is set to open the contacts when the signal falls below 3.8 mA and the other to operate when the signal reaches the value corresponding to the maximum overpressure. An MTBF of 113 years corresponds to an operational failure rate of 8.8×10^{-3} per year. Assuming a SFF of 60%, the dangerous undetected failure rate is then conservatively estimated as 3.5×10^{-3} per year for a single MTL4403, and 1.2×10^{-5} for a 1oo2 combination.

A full proof test, to ensure that the relays of each MTL4403 trip at the correct current, would probably have to be performed offline, so a one year proof test interval is also appropriate here.

The MTL 4403 is designed and manufactured using the same quality control system as all other products in the MTL4000 series. The system is subject to ISO 9001 approval and BASEEFA surveillance and hence satisfies the quality control requirements of IEC 61508.

6.3.4 MTL4024-SR isolator

The MTL 4024-SR has a BASEEFA reliability assessment with a certificate number BAS 01SP9257X. Provided that loss of output is a safe condition, there are no failures which can produce a failure to danger. The certificate states that the unit is suitable for use in a SIL 3 safety function.

6.3.5 Valve actuator system

There is a long history of fail-safe designs in pneumatic valve technology and since these valves are regularly exercised (to prevent sticking) the combination should achieve an undetected rate of failure to danger of 1×10^{-3}. This value is assumed for the purposes of this example and becomes the failure rate for the actuator system.

The reliability of solenoid pilot valves is high, but the majority of suppliers state their reliability as a very high number of operations (10^5 to10^7), which is not relevant to this application. At least one manufacturer [Eugen Seitz AG] supplies an intrinsically safe pilot valve which is third party certified as AK-7/SIL 4. The use of a pilot valve with such a high reliability rating ensures that achieving the required failure rate to danger of 10^{-3} per year is largely decided by the dump valve.

The proof test for the actuator is included in a regular system test, described below.

6.4 System test

The system is relatively easy to test because the pressure vessel is used in a batch process and operates on a weekly cycle. Comparing the outputs of the control and monitoring loops can very effectively monitor the operation of the pressure loop. This has the merit of checking the sampling connection as well as the transmitter and isolator. There are several possible techniques available to achieve this which do not adversely affect the reliability of either system, and using one of these techniques together with utilising the smart capability of the transmitter could also ensure that the annual proof test of the transmitter was adequately covered.

The safety function other than the transmitter can be checked before each batch by a test cycle initiated by the test facility indicated in Figure 8. Initially, the cable from the pressure transmitter is open-circuited, creating a low alarm and opening the dump valve. The cable is then shorted, creating a high alarm and again opening the valve. This switching operation could be done manually, or automatically using an MTL 4216 switch-operated relay. The dump valve would normally have limit switches, which are used to confirm the valve position. They could be used to verify that the valve has operated correctly during the test.

The frequent testing decreases the probability of failure, not least because it exercises the dump valve thus reducing the probability of it being stuck in the closed position.

6.5 Calculating PFD_{avg}

For each component of the safety system, the PFD_{avg} is calculated from the undetected dangerous failure rate, λ_{DU}, and the proof test interval, T_p. Provided the failure rate is small, $PFD_{avg} = {}^1/_2 \lambda_{DU} T_p$. Figure 9 shows the PFD_{avg} calculated for each component.

The PFD_{avg} for the system is simply the sum of the PFD_{avg} of each component, in this case 8.1×10^{-5}. This is a much lower failure rate than the 10^{-2} required for a SIL 2 system, but the architectural constraints discussed above prevent a higher SIL being claimed.

6.6 Operational reliability

The over-pressure protection loop is not acceptable if it produces too many 'fail-safe' operations not initiated by high pressure (false trips). A malfunction of once per year, which is the same as the control system, is considered to be acceptable in this application. Not all failures would result in the product being dumped, but the majority would. Testing the system once a week results in the actuator system being more reliable, and any faults which are not self-revealing being quickly detected. However, it does not change the probability of a random failure causing a malfunction.

An analysis of the operational reliability of the system requires an estimate of:

a) the failure rate of both the air and electricity supplies.
b) the failure rate of the cabling.
c) the operational failure rate of the equipment. The operational failure of either of the trip amplifiers will trip the system

The MTL components have calculated operational failure rates of 0.88×10^{-2} per year for the MTL 4403, 1.2×10^{-2} per year for the MTL 4041B-SR, and 1.3×10^{-2} per year for the MTL 4024-SR at 60°C. The combined failure rate of the units used in the system is 4.26×10^{-2} per year. This figure is conservative because the equipment is used at a lower ambient temperature and not all faults result in the product being dumped. A figure of 1×10^{-2} per year is a more reasonable assumption.

To achieve an overall system reliability of one false operation per year the remaining components, power supplies and cabling would have to achieve a very high standard and failure rates of the order of 1×10^{-2} per year are necessary. In practice, some of these failure rates are difficult to quantify.

The requirement for operational reliability reinforces the need for simplicity in safety interlock systems. However, in this particular system the introduction of a second trip amplifier to improve the safety integrity level does not materially affect the operational reliability of the system.

6.7 Conclusion

The above example, although relatively simple, demonstrates how IEC 61508 may be applied to a real installation. The tolerable risk and the EUC risk are first defined, from which the required PFD_{avg} and hence the SIL of the safety-related protection system are derived.

A design for the safety-related protection system is proposed and analysed, and shown to meet the requirements.

This example discusses only the design of the safety-related system. It must be appreciated that the scope of IEC 61508 is wider than this, and other requirements, as outlined in Section 3, must be met in order to claim compliance.

7 UNDERSTANDING AND USING IEC 61508 APPROVALS

7.1 What IEC 61508 certificates should tell you

Having read this far, it should be clear that the design of a safety system involves more than simply specifying subsystem components that are approved for use at the required safety integrity level (SIL). The designer must demonstrate that the average probability of failure on demand (PFD_{avg}) of the design as a whole meets the required SIL. He must also set appropriate intervals for periodic proof tests; these intervals also have a bearing on the PFD_{avg}. (This applies to safety systems operating in low demand mode. For systems operating in high demand mode, the probability of dangerous failures per hour, PFH, is considered instead of PFD_{avg}.)

The IEC 61508 approval certificate for a component (such as a safety-related isolator) should contain the information that the system designer needs. Some of this is mandatory: IEC 61508-2 7.4.7.3 states "The following information shall be available for each safety-related subsystem…. ".

The following paragraphs have the same numbering as the subclauses of IEC 61508-2 7.4.7.3 and define the meaning of each term and explain how it is used.

a) Functional specification

The specification of those functions and interfaces which can be used by safety functions. A subsystem may have specification limits for use in a safety function that differ from the normal catalogue values given for general use. For instance, accuracy tolerances may be larger.

b) Estimated rates of failure in dangerous mode detected by diagnostic tests (λ_{DD}), and

c) Estimated rates of failure in dangerous mode undetected by diagnostic tests (λ_{DU})

These are failure rates due to random hardware failures. They are determined more often by a failure modes and effects analysis (FMEA) of the design, or for well-established products, by well-documented field reliability data (proven in use). They are expressed as failures per hour, or failures per year. The total of safe and dangerous failure rates is the reciprocal of the MTBF (mean time between failures).

Some potentially dangerous failures may be detected by diagnostic tests, either in the subsystem itself, or by external equipment. For example, the MTL4041B-SR Repeater Power Supply has a number of failure modes that are shown by analysis to drive the output out of range, either < 3.6 mA or > 21 mA. Such failures can be detected by the control system or trip amplifier, which can then take appropriate action (IEC 61508-2 7.4.6).

The safety system designer uses λ_{DD} and λ_{DU} to calculate the PFD_{avg}.

d) Environmental limits

Mandatory or advisory limits on environmental aspects such as temperature, exposure to dust and water, vibration, and electromagnetic interference. As for the functional specification, the limits for use in a safety function may differ from the normal catalogue values.

e) Lifetime limits

There may be a limit to the service lifetime of the subsystem when used in a safety function if any of the parts used are liable to wear out within the normal, expected service life. This is because reliability data (MTBF) is calculated assuming a constant failure rate and does not account for wear-out (IEC 61508-2 7.4.7.4).

f) Periodic proof test and maintenance requirements

The minimum or recommended proof test and maintenance necessary to maintain the safety reliability of the subsystem. The proof test interval is decided by the system designer within any limits specified in this section, and is used in calculating the PFDavg.

g) Diagnostic coverage

Strictly, the fractional decrease in the probability of dangerous hardware failures due to the diagnostic tests, if any (IEC 61508-2 Annex C, and IEC 61508-4 3.8.6). Some MTL certificates use this section to stipulate the diagnostic tests that must be performed by external equipment.

h) Diagnostic test interval

Specifies the diagnostic test interval, when required.

i) Additional information regarding mean time to restoration (MTTR)

When a dangerous fault is detected by a diagnostic test, the safety function may be designed to go immediately to a safe state, or it may be designed to alert the operator. The equipment under control may be permitted to continue running, with reduced safety, until the safety function is repaired. The MTTR is the mean time to repair the safety function in this event.

If the safety function is operated in this way, the diagnostic coverage and the MTTR are used in the calculation of the PFDavg, which can become quite complicated.

j) Safe failure fraction (SFF)

The fraction of hardware failures which results in a safe state. (Dangerous failures detected by diagnostic tests count as safe failures in calculating the SFF.)

k) Hardware fault tolerance

The hardware fault tolerance is N, if N+1 faults can cause loss of the safety function.

Together with the safe failure fraction, this figure is used to determine the highest safety integrity level that can be claimed for the safety function according to the architectural constraints (IEC 61508-2 7.4.3.1).

l) Application limits to avoid systematic failures

Other limitations in use not covered in a), d), or e).

m) Highest safety integrity level (SIL) that can be claimed for a safety function using this subsystem.

Strictly, the limit given here is only concerned with systematic faults. The architectural constraints are derived from the hardware fault tolerance and the safe failure fraction, as discussed above. For clarity, MTL certificates specifically state the maximum permitted SIL.

n) Hardware configuration

Defines the build standard of the subsystem to which the certificate applies, for example by drawing issue number or by date code.

o) Evidence of validation

Where an independent third party has issued a certificate, the certificate itself is the documentary evidence of validation.

7.2 Calculating the average probability of failure on demand

IEC 61508-6 Annex B shows in detail how to calculate the PFD_{avg} or PFH, for low and high demand modes respectively. This section of the application note does not attempt to cover the same ground; it simply introduces the basis of the calculation. To avoid complication, a low demand mode is assumed.

For simplicity, let us also assume that the safety function is designed to trip to a safe state on the detection of a dangerous fault, so that we do not need to be concerned with diagnostic coverage and MTTR. The safety function can only be in one of two states: running or tripped. The example described in section 4 is like this.

Failure rates are assumed to be constant with time, which means that it is assumed that a subsystem component is just as likely to fail during next week, as it is during this week, or during any week. This means that the probability of the component working reduces with time – the longer the component has been working, the more time it has had in which to fail. Mathematically, the probability of performing correctly at time t is given by $R(t) = e^{-\lambda t}$. Figure 10 illustrates this.

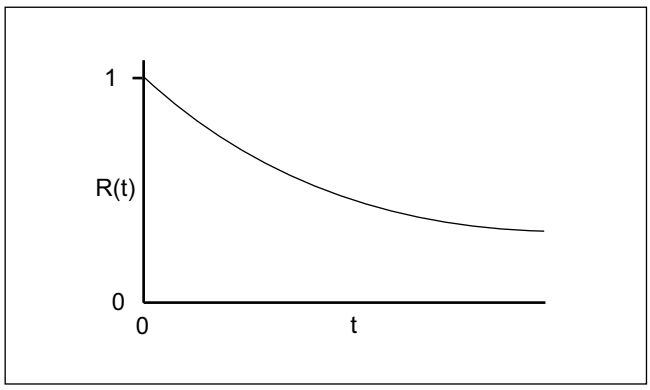


Figure 10 The probability of correct operation

Conversely, the probability of the component having failed at time t is given by $F(t) = 1 - e^{-\lambda t}$ - see Figure 11. The component is completely reliable at t = 0 and thereafter the probability of failure increases with time. For a safety function, we are only concerned with dangerous failures, λ_{DU} is the appropriate failure rate to use, and Figure 11 shows that the probability of failure to carry out the safety function on demand increases with time.

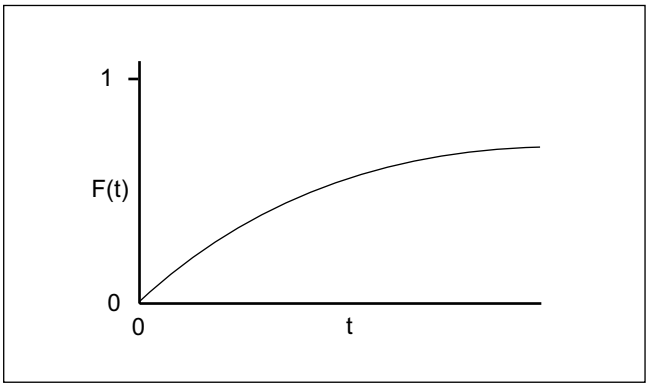


Figure 11 The probability of failure

Every time a proof test is carried out, the safety function is proven to work, and so the probability of failure on demand is reset to zero. Figure 12, where T_p is the proof test interval, illustrates this.

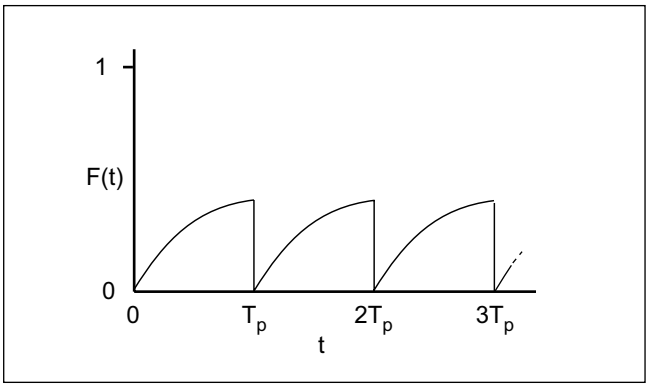


Figure 12 Probability of failure with regular proof testing

The average probability of failure on demand is given by:

$$PFD_{avg} = \frac{1}{Tp} \int_0^{Tp} 1 - e^{\lambda_{DU} t} \; dt$$

For $\lambda_{DU} T_p \ll 1$, this simplifies to:

$$PFD_{avg} = \tfrac{1}{2} \lambda_{DU} T_p,$$

which is the form used in the application example in section 4.5.

8 SOURCES OF INFORMATION

HSE (1988). Health and Safety Executive: The Tolerability of Risk from Nuclear Power Stations. Discussion Document, HMSO, London. Revised edition, 1992.

HSE (1999). Health and Safety Executive: Reducing Risks, Protecting People. Discussion Document, HSE Books.

IEC 61508 (2000). International Electrotechnical Commission. International Standard IEC 61508: Functional Safety of Electrical/Electronic/Programmable Electronic Safety Related Systems. IEC, Geneva. www.iec.ch

Frequently asked questions, on IEC's own website: www.iec.ch/61508/index.htm

Reason J (1990). Human Error. Cambridge University Press.

Redmill (1998). "IEC 61508: Principles and Use in the Management of Safety". Computing & Control Engineering Journal, 9, 5, 1998. IEE, London.

Redmill (2000). "Safety Integrity Levels - theory and problems". In Redmill F and Anderson T (eds): Lessons in System Safety - Proceedings of the Eighth Safety-critical Systems Symposium, Southampton, UK, 2000. Springer-Verlag, London.

Redmill (2001). A paper on what is necessary for using IEC 61508

Redmill F and Rajan J (1997). Human Factors in Safety-critical Systems. Butterworth-Heinemann, Oxford.

Storey (1996). Safety-critical Computer Systems. Addison-Wesley, Harlow.

AUSTRALIA
MTL Instruments Pty Ltd,
10 Kent Road, Mascot, New South Wales, 2020, Australia

Tel: +61 1300 308 374 Fax: +61 1300 308 463
E-mail: mtlsalesanz@eaton.com

BeNeLux
MTL Instruments BV
Ambacht 6, 5301 KW Zaltbommel
The Netherlands

Tel: +31 (0)418 570290 Fax: +31 (0)418 541044
E-mail: mtl.benelux@eaton.com

CHINA
Cooper Electric (Shanghai) Co. Ltd
955 Shengli Road, Heqing Industrial Park
Pudong New Area, Shanghai 201201

Tel: +86 21 2899 3817 Fax: +86 21 2899 3992
E-mail: mtl-cn@eaton.com

FRANCE
MTL Instruments sarl,
7 rue des Rosiéristes, 69410 Champagne au Mont d'Or
France

Tel: +33 (0)4 37 46 16 53 Fax: +33 (0)4 37 46 17 20
E-mail: mtlfrance@eaton.com

GERMANY
MTL Instruments GmbH,
Heinrich-Hertz-Str. 12, 50170 Kerpen, Germany

Tel: +49 (0)22 73 98 12- 0 Fax: +49 (0)22 73 98 12- 2 00
E-mail: csckerpen@eaton.com

INDIA
MTL India,
No.36, Nehru Street, Off Old Mahabalipuram Road
Sholinganallur, Chennai- 600 119, India

Tel: +91 (0) 44 24501660 /24501857 Fax: +91 (0) 44 24501463
E-mail: mtlindiasales@eaton.com

ITALY
MTL Italia srl,
Via San Bovio, 3, 20090 Segrate, Milano, Italy

Tel: +39 02 959501 Fax: +39 02 95950759
E-mail: chmninfo@eaton.com

JAPAN
Cooper Crouse-Hinds Japan KK,
MT Building 3F, 2-7-5 Shiba Daimon, Minato-ku,
Tokyo, Japan 105-0012

Tel: +81 (0)3 6430 3128 Fax: +81 (0)3 6430 3129
E-mail: mtl-jp@eaton.com

NORWAY
Norex AS
Fekjan 7c, Postboks 147,
N-1378 Nesbru, Norway

Tel: +47 66 77 43 80 Fax: +47 66 84 55 33
E-mail: info@norex.no

RUSSIA
Cooper Industries Russia LLC
Elektrozavodskaya Str 33
Building 4
Moscow 107076, Russia

Tel: +7 (495) 981 3770 Fax: +7 (495) 981 3771
E-mail: mtlrussia@eaton.com

SINGAPORE
Cooper Crouse-Hinds Pte Ltd
No 2 Serangoon North Avenue 5, #06-01 Fu Yu Building
Singapore 554911

Tel: +65 6 645 9864 / 5 Fax: +65 6 487 7997
E-mail: sales.mtlsing@eaton.com

SOUTH KOREA
Cooper Crouse-Hinds Korea
7F. Parkland Building 237-11 Nonhyun-dong Gangnam-gu,
Seoul 135-546, South Korea.

Tel: +82 6380 4805 Fax: +82 6380 4839
E-mail: mtl-korea@eaton.com

UNITED ARAB EMIRATES
Cooper Industries/Eaton Corporation
Office 205/206, 2nd Floor SJ Towers, off. Old Airport Road,
Abu Dhabi, United Arab Emirates

Tel: +971 2 44 66 840 Fax: +971 2 44 66 841
E-mail: mtlgulf@eaton.com

UNITED KINGDOM
Eaton Electric Ltd,
Great Marlings, Butterfield, Luton
Beds LU2 8DL

Tel: +44 (0)1582 723633 Fax: +44 (0)1582 422283
E-mail: mtlenquiry@eaton.com

AMERICAS
Cooper Crouse-Hinds MTL Inc.
3413 N. Sam Houston Parkway W.
Suite 200, Houston TX 77086, USA

Tel: +1 281-571-8065 Fax: +1 281-571-8069
E-mail: mtl-us-info@eaton.com

Powering Business Worldwide

Eaton Electric Limited,
Great Marlings, Butterfield, Luton
Beds, LU2 8DL, UK.
Tel: + 44 (0)1582 723633 Fax: + 44 (0)1582 422283
E-mail: mtlenquiry@eaton.com
www.mtl-inst.com

Publication No. AN9025 Rev 4 191016
October 2016

EUROPE (EMEA):
+44 (0)1582 723633
mtlenquiry@eaton.com

THE AMERICAS:
+1 800 835 7075
mtl-us-info@eaton.com

ASIA-PACIFIC:
+65 6 645 9888
sales.mtlsing@eaton.com