Martin Schönbeck

Introduction to reliability of safety systems

Summary:

This report gives an introduction to the reliability of safety systems, with special focus on the main international standard for safety systems (IEC 61508), and on the operational phase of a safety system. It gives a general introduction to safety, risk, safety systems and reliability, it describes various ways to classify failures as part of a reliability analysis, it gives an overview of the main principles and requirements of the IEC 61508 standard, it describes the most common analytical tools and methods for safety analysis, and it touches upon some aspects of operation and maintenance.

Preface

This report is based on a literature review performed as a preparation for my master thesis project at the Norwegian University of Science and Technology (NTNU), in cooperation with Eindhoven University of Technology (TU/e) in The Netherlands. The main work was done between September and December 2006. The report gives a general introduction to the reliability of safety systems, and may be of interest to anyone who is new to this field, both students, researchers and professionals. I would like to thank Marvin Rausand, my supervisor at NTNU, and Jan Rouvroye, my supervisor at TU/e, for their input and enthusiastic support.

Trondheim, April 2007

Martin Schönbeck

Table of contents

1. Introduction

Today's industrial society exposes itself to risks created by its technological advancements, and major accidents, for example in the process industry and the transportation sector, regularly draw our attention. According to the German sociologist Ulrich Beck, we are living in a *risk society*, which is shaped by the all-encompassing modern society with its mass consumption (Beck 1997). To protect people and the environment against technological risks, safety systems are used in many different applications. Nowadays, such systems are often based on computer technology. But can we rely on these computer-based safety systems? This increases the need for scientific research in the area of the reliability of safety systems.

This report gives an introduction to the reliability of safety systems, with special focus on the main international standard for safety systems (IEC 61508), and on the operational phase of a safety system. First a general introduction to safety, risk, safety systems and reliability is given. Subsequently, chapter 3 deals with various ways to classify failures as part of a reliability analysis, focusing on safety systems. Chapter 4 introduces the IEC 61508 standard and gives an overview of its main principles and requirements. Chapter 5 describes the most common analytical tools and methods for safety analysis. Finally, some aspects of operation and maintenance are touched upon in chapter 6.

2. Safety systems

Safety is an important aspect of any product or business activity, and in daily life everybody will have some idea of what safety means. However, as soon as we try to define and measure safety, things get a little bit more complicated. What does it mean that a product or process is safe? Can anything be 100% safe? And if not, are there any criteria to determine how safe a product or process should be? Then we have to assess the risks involved, but what is actually “risk” and how can we measure it? Once we have decided which safety level we want, what kind of safety system do we need? And finally, how can we verify that the desired safety level is actually achieved in practice? Before such questions can be answered, we need to define more precisely what is meant by safety.

Safety barriers and risk reduction

Safety is commonly defined as protection of human life, the environment and business assets. According to Karydas and Brombacher (1999), safety is part of the business strategy of progressive companies, and, if well managed, it may provide a significant business advantage. Hence, safety can be considered as a strategic contributor to business performance. Moreover, many industries, such as transportation, offshore and chemical industries, are subject to safety regulations, which often require quantification of the achieved risk reduction. In industrial applications safety systems are used to protect the surroundings against equipment or processes that are not inherently safe (Corneliussen 2002). This has to do with the concept of *safety barriers*, which is often related to an accident model known as the *energy model* (see figure 1).

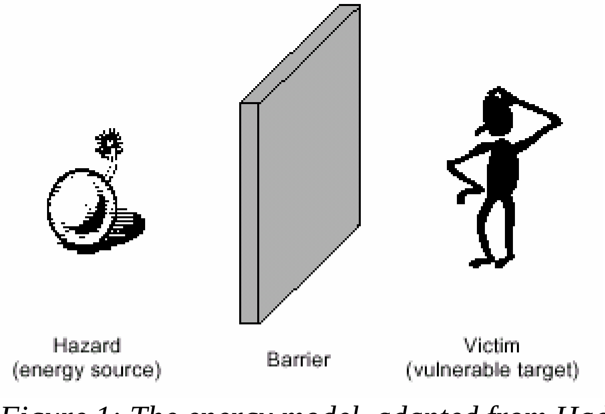

Figure 1: The energy model, adapted from Haddon (1980).

The basic principle of the energy model, which was originally introduced by Gibson (1961), is to separate hazards (energy sources) from victims (vulnerable targets) by safety barriers (Haddon 1980). This model classifies sources of injury according to the forms of physical energy involved and can be related to accident prevention strategies. The process model is another perspective that may serve as a basis for the concept of safety barriers. Process models divide accident sequences in different phases and show how a system gradually deteriorates from a normal state into a state where an accident occurs (Kjellén 2000). According to Sklet (2006), factors that prevent transitions between phases in the accident sequence may be regarded as safety barriers. This is illustrated in figure 2.

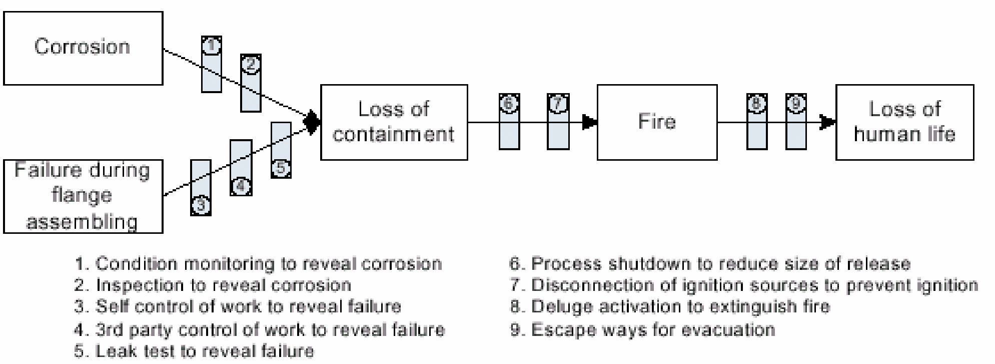
Corrosion
Failure during flange assembling
Loss of containment
Fire
Loss of human life
1
2
3
4
5
6
7
8
9
1. Condition monitoring to reveal corrosion
2. Inspection to reveal corrosion
3. Self control of work to reveal failure
4. 3rd party control of work to reveal failure
5. Leak test to reveal failure
6. Process shutdown to reduce size of release
7. Disconnection of ignition sources to prevent ignition
8. Deluge activation to extinguish fire
9. Escape ways for evacuation

Figure 2: Illustration of barriers influencing a process accident (Sklet 2006).

For the concept of safety barriers no common terminology applicable across sectors has been developed. Sklet (2006) proposes to define safety barriers as “physical and/or non-physical means planned to prevent, control, or mitigate undesired events or accidents”. These means may range from a single technical unit or human action, to a complex socio-technical system. Furthermore, it is recommended to distinguish between safety barriers, their functions, and the barrier systems that realise these functions. A *barrier function* is defined as “a function planned to prevent, control or mitigate undesired events or accidents”; a *barrier system* as “a system that has been designed and implemented to perform one or more barrier functions” (Sklet 2006). A barrier system may have several functions, and in some cases there may be several systems that carry out a barrier function (Sklet 2006).

Generally speaking, safety barriers are used to reduce *risk*. However, no common understanding of the term risk exists, although several authors have tried to come up with quantitative and qualitative definitions of risk (e.g. Aven 2003; Fischhoff et al. 1984; Kaplan & Garrick 1981; Klinke & Renn 2001; Rowe 1977). According to Rowe (1977), risk always involves some aspect of uncertainty. Risk is often associated with something negative, but it can include both gains and losses, considering for instance the use of the term risk in economic theory. The Society for Risk Analysis defines risk as "the potential for realisation of unwanted, adverse consequences to human life, health, property, or the environment", where "estimation of risk is usually based on the expected value of the conditional probability of the event occurring times the consequence of the event given that it has occurred" (SRA 2006). According to IEC 61508, risk is a "combination of the probability of occurrence of harm and the severity of that harm" (IEC 2000), which is somehow in line with the Society for Risk Analysis. Klinke & Renn (2001) take a broader perspective and argue that risk "refers to the possibility that human actions or events lead to consequences that affect aspects of what humans value". In an approach to integrate the natural and technical sciences as well as the social sciences, they develop six further criteria for risk evaluation, in addition to probability of occurrence and extent of damage. Based on these eight criteria, they propose a classification of risks into six classes, which are given names from ancient Greek mythology related to their characteristics. Casually, they make a down-to-earth statement: "it is a characteristic of technological risk that the extent of damage is negatively correlated to the level of probability" (Klinke & Renn 2001).

Since there are so many different types of risks, a wide variety of safety barriers exists to reduce those risks. Most safety barriers are aimed at reducing the *probability* that harm occurs or at reducing the *severity* of harm. Probability reduction can for instance be achieved by using a safer process or by installing technical systems to increase process safety. Examples of severity reduction are dikes around storage tanks and automatic fire-extinguisher systems (Rouvroye 2001). This distinction between probability reduction and severity reduction confronts us with a difficult question: which of them should be prioritised? According to the regulations of the Norwegian Petroleum Directorate, probability reducing measures should be given priority over consequence reducing measures whenever possible (NPD 2001), but setting such priorities is a rather subjective task which requires individual judgement. The same holds for the required risk reduction, although risk acceptance criteria have been laid down in law in many countries. Within the tolerable risk area, the so-called ALARP (as low as reasonably practicable) or ALARA (as low as reasonably achievable) principle is often applied. Aven (2003) argues that such a type of cost-benefit analysis "gives a strong form of mechanical thinking when dealing with difficult decision situations involving various aspects of cost and benefit", which might encourage achieving risk acceptance instead of a "drive for improvement".

The existence a wide variety of safety barriers calls for the need to classify them. Barrier systems may be classified along several dimensions, for example as passive or active barrier systems, and as physical, technical, or human and operational barrier systems (Sklet 2006). A possible classification is shown in figure 3.

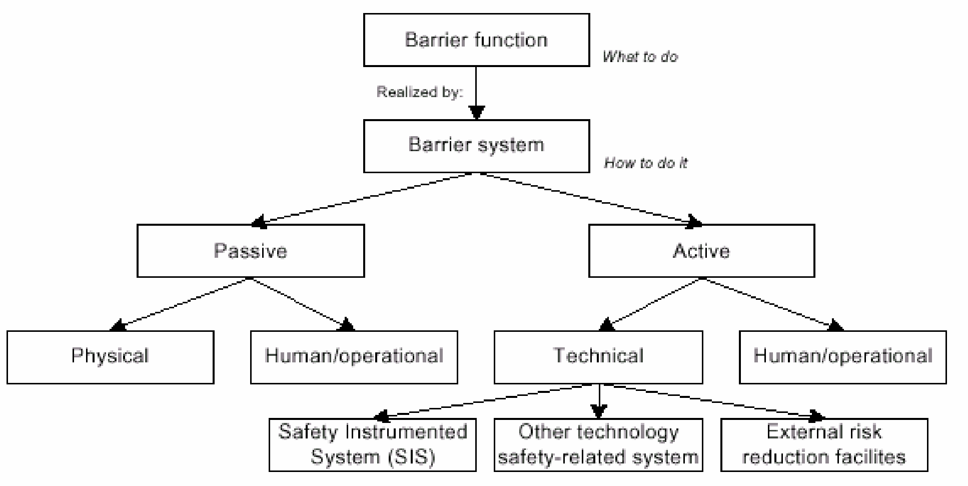

Figure 3: Classification of safety barriers (Sklet 2006).

Some barrier systems are functioning continuously, while others need to be activated. Physical, passive barriers, such as firewalls, are usually functioning continuously. Human and operational barriers can be passive (e.g. safety distances) as well as active (e.g. self control of work). Active human and operational barriers are often an integrated part of a work process. The classification of active, technical barriers as in figure 3 is in accordance with the IEC 61511 standard (Sklet 2006). These barriers will be discussed in more detail in the remainder of this chapter.

Safety instrumented systems

Computer-based systems are increasingly used in safety-critical applications. The benefits of these programmable systems are increased flexibility to change systems and to introduce new functionality, compared to conventional safety systems that are based on mechanical technologies. On the other hand, this flexibility increases the complexity of safety systems and poses demands on system developers, users, as well as regulatory authorities (Corneliussen 2002). A computer-based safety system composed of sensors, logic solvers and actuating items (or final elements) is usually referred to as a *safety instrumented system* (SIS). The general subsystem structure of a safety instrumented system is shown in figure 4.

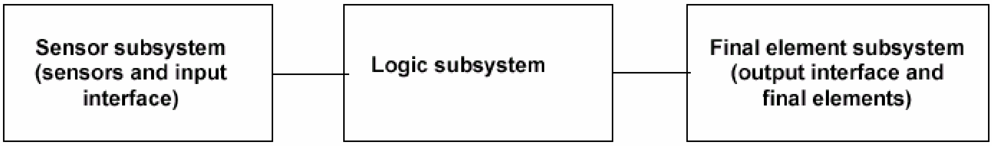
Sensor subsystem (sensors and input interface)
Logic subsystem
Final element subsystem (output interface and final elements)

Figure 4: SIS subsystem structure, adapted from IEC 61508 (IEC 2000).

According to Rausand & Høyland (2004), safety instrumented systems are used in many sectors of society, for example, as emergency shutdown systems in hazardous chemical plants, fire and gas detection and alarm systems, pressure protection systems, dynamic positioning systems for ships and offshore platforms, automatic train stop systems, fly-by-wire operation of aircraft flight control surfaces, antilock brakes and airbag systems in automobiles, and systems for interlocking and controlling the exposure dose of medical radiotherapy machines. In each of these applications, the purpose of the safety instrumented system is to mitigate the risk associated with the so-called *equipment under control* (EUC), which the IEC 61508 standard (IEC 2000) defines as "equipment, machinery, apparatus or plant used for manufacturing, process, transportation, medical or other activities".

As with safety barriers and barrier functions, it is useful to distinguish between safety instrumented systems and their functions. A *safety instrumented function* (SIF) is a function that is implemented by a safety instrumented system and that is intended to achieve or maintain a safe state for the equipment under control with respect to a specific process demand (Rausand & Høyland 2004). A safety instrumented function may be considered as a barrier function, while a safety instrumented system may be considered as a barrier system (Lundteigen & Rausand 2006). In the IEC 61508 standard (IEC 2000) a safety instrumented system is referred to as an "electrical/electronic/programmable electronic (E/E/PE) safety-related system". Correspondingly, this standard defines an electrical/electronic/programmable electronic system (E/E/PES) as a "system for control, protection or monitoring based on one or more electrical/electronic/programmable electronic (E/E/PE) 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". All elements of the system should therefore be taken into consideration when developing or analysing a safety instrumented system.

Reliability of safety systems

A very important aspect of any safety system is its *reliability*. Several definitions of reliability exist, such as the general one given in the standard ISO 8402 (ISO 1986): “Reliability is the ability of an item to perform a required function, under given environmental and operational conditions and for a stated period of time”. Hence, the reliability of a safety system can be expressed as the ability of a safety system to perform its intended safety function(s), under given environmental and operational conditions and for a stated period of time. For a safety instrumented system this means that when a predefined process demand occurs in the equipment under control, the deviation shall be detected by the sensors, and the required actuating items shall be activated and fulfil their intended functions (Rausand & Høyland 2004). A failure to perform this function is called a *fail to function* (FTF). On the other hand, a safety system shall not be activated spuriously, i.e. without the presence of a predefined process demand in the equipment under control (Rausand & Høyland 2004). Such a false alarm is called a *spurious trip* (ST). This would have negative consequences for process availability, due to the fact that safety systems are autonomous and that they are able to shut down the safeguarded process (Rouvroye 2001). Spurious trips might also affect safety, because restarting the safeguarded process can lead to a temporary instable situation during start-up. Moreover, spurious trips will usually imply significant costs and reduce the confidence in the system (Rausand & Høyland 2004). People do not like it if they have to leave their house because of a false fire alarm, and might not react to it anymore in future.

When assessing the reliability of a safety system in terms of fail to function, two main options exist, depending on the operation mode of the safety system. If a safety system experiences a low frequency of demands, typically less than once per year, it is said to operate in *low demand mode*. An example of such a safety system is the airbag in a car (Rausand & Høyland 2004). The brakes in a car are an example of a safety system with a *high demand mode* of operation: they are used (almost) continuously (Rausand & Høyland 2004). For low demand mode safety systems it is common to calculate the average *probability of failure on demand* (PFD), whereas the *probability of a dangerous failure per hour* (PFH) is used for safety systems operating in high demand or continuous mode (Brown 2000; Lundteigen & Rausand 2006). This differentiation is closely related to the classification of failures, which is discussed in the next chapter. The reliability of a safety system in terms of spurious trips can also be quantified, and it is often important to consider this as well. To assess the reliability of a safety system, several analysis techniques exist, some of which are discussed in chapter 5. As shown by

Rouvroye & Brombacher (1999), different analysis techniques use different methodologies and may lead to different results.

One more important aspect of the reliability of a safety system has to be mentioned here. The logic subsystem of a safety instrumented system (see figure 4) performs one or more logic functions based on the input it gets from the sensor subsystem. This logic subsystem operates often with a *k*-out-of-*n* (*k*oo*n*) voting logic, which means that *k* of the *n* sensors must detect a dangerous situation before the safety function is activated. For instance, in a fire detection system with a 1oo2 voting logic, it is sufficient that one detector is functioning for the system to function. The *voting logic* used affects the reliability of the safety system, both in terms of the probability that the safety system will fail to function in case of a dangerous situation, and in terms of spurious trips. A high degree of *redundancy* reduces the probability of failure on demand (or the probability of a dangerous failure per hour in case of a high demand system), but at the same time the spurious trip rate may increase. A 2oo3 voting logic is often chosen as the best configuration for detector systems, because it has a probability of failure on demand in the same order of magnitude as a parallel (1oo2) system, and because it can be made much more reliable than a parallel system when it comes to spurious trips (Rausand & Høyland 2004).

Relevant standards

Reliability certification of safety systems has received a lot of attention during the past decade with the emergence of new international standards, such as IEC 61508 of the International Electrotechnical Commission (IEC 2000) and ISA-SP84 of the Instrument Society of America (ISA 1996). These new standards reflect two trends as observed by Karydas & Brombacher (1999): the use of quantitative safety analysis techniques and the focus on the entire lifecycle of the product. Older standards, like the German standard DIN 19250 (DIN 1994), focus mainly on the development phase and are product oriented. These older standards give detailed, technology dependent design requirements, and certification is granted based on design guidelines, hardware tests, checklists and expert experience (Rouvroye 2001). However, such qualitative analysis techniques give only limited insight into the probability that a safety system will fail, and the likelihood of failure is not only determined by the system itself, but also by the business processes that develop, implement and operate it (Karydas & Brombacher 1999). Therefore, newer standards are performance based and require quantification of the achieved risk reduction. The IEC 61508 standard is currently the main standard for safety instrumented systems and will be the primary focus of this report. This is a generic standard common to several industries, independent of the technology used. It provides a general framework for the design and implementation of safety-related systems that are based on electrical, electronic and/or programmable electronic technology. A major objective of this standard is to facilitate the development of application specific standards, such as IEC 61511 for the process industry (IEC 2003). The IEC 61508 standard is discussed in more detail in chapter 4 of this report.

3. Failure classification

Failure is a fundamental concept of any reliability analysis. It was already touched upon in the previous chapter, when introducing the reliability of safety systems. However, failures can be classified in many different ways and several definitions of failure categories exist, some of which are not mutually exclusive. Below, some basic concepts related to failure analysis will be presented, as well as an overview of the most common failure classifications for safety systems.

Basic concepts

According to Rausand & Øien (1996), the quality of a reliability analysis strongly depends on the analyst's ability to identify all the required functions of the system that is studied. This is not always an easy task, since a complex system might have a high number of required functions. Several techniques exist to perform such a functional analysis: function trees, the function analysis system technique (FAST), and the structured analysis and design technique (SADT), among others (Lambert, Riera & Martel 1999; Rausand & Høyland 2004). It is common to express the various functions in the same way with a verb and a noun, for example "pump water". In the case of safety systems, these functions are usually called safety functions, as discussed in chapter 2. If a safety system fails to perform a required safety function, this is considered a *failure*. However, the term failure is often confused with the terms *fault* and *error*, and various definitions exist (Rausand & Øien 1996). According to the IEC 60050-191 standard (IEC 1990a), an error is a "discrepancy between a computed, observed or measured value or condition and the true, specified or theoretically correct value or condition". According to the same standard, a failure is the event when a required function is terminated (exceeding the acceptable limits), while a fault is defined as "the state of an item characterised by inability to perform a required function, excluding the inability during preventive maintenance or other planned actions, or due to lack of external resources" (IEC 1990a). Hence, a fault is a state resulting from a failure. The relationship between the terms failure, fault and error is illustrated in figure 5.

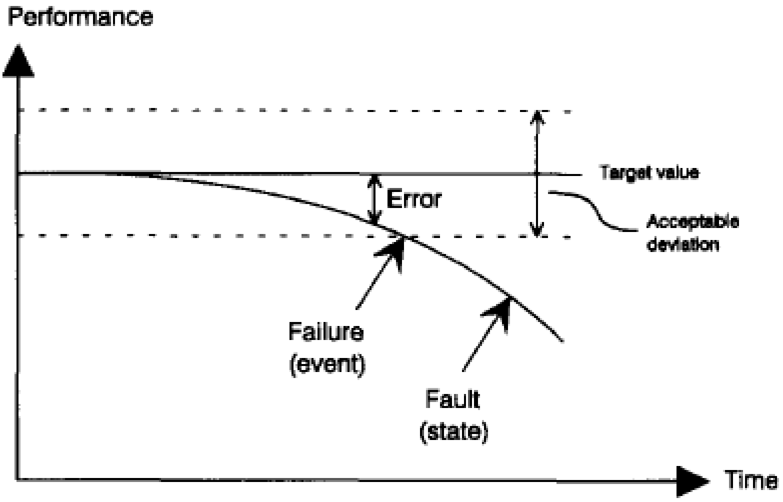

Figure 5: Illustration of the difference between failure, fault and error (Rausand & Øien 1996).

Failures are often classified into *failure modes*. The British Standard BS 5760, part 5 (BS 1991), defines a failure mode as “the effect by which a failure is observed on a failed item”. However, as shown by Rausand & Øien (1996), the failure mode concept does not have a well-defined interpretation. A failure mode is actually a description of a fault (e.g. “valve is not closing completely”), and therefore the term *fault mode* is sometimes used instead of failure mode. Identifying all possible failure modes of a system can be even more difficult than finding all its functions, because each function may have several failure modes. Moreover, no formal procedure seems to exist that can be used to identify and classify the possible failure modes (Rausand & Øien 1996). One way of classifying failures is to distinguish between primary failures, secondary failures, and command faults (see e.g. Henley & Kumamoto 1981). A primary failure is caused by natural aging of the item and occurs under conditions within the design envelope of the item, whereas a secondary failure is caused by excessive stresses outside the design envelope. Such stresses may be caused by neighbouring components, the environment, or by system operators. A command fault is caused by inadvertent control signals or noise. Blache & Shrivastava (1994) have suggested an other classification scheme for failure modes, which is shown in figure 6. Intermittent failures result in a lack of some function for a very short period of time, whereas extended failures will continue until replacement or repair of the system. Complete failures cause complete lack of the required function; partial failures do not. Sudden failures are failures that could not be forecast by prior testing or examination; gradual failures could be forecast. The extended failures are split into four categories, two of which are given specific names: catastrophic failures (sudden + complete) and degraded failures (partial + gradual).

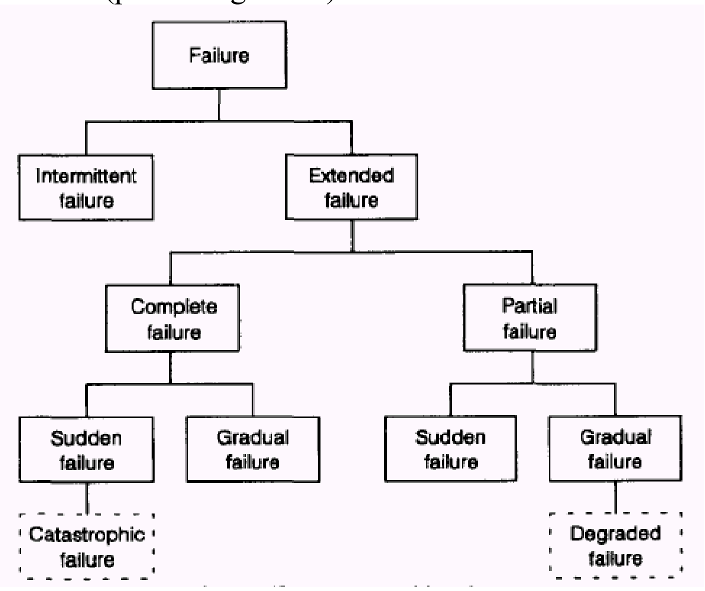

Figure 6: Failure mode classification according to Blache & Shrivastava (1994).

When analysing failure modes, we are usually interested in their causes, in order to avoid failures or to prevent reoccurrence of the same failures. The IEC 60050-191 standard (IEC 1990a) defines failure causes as "the circumstances during design, manufacture or use that have led to a failure", which is a straightforward definition. When considering a system hierarchy where functions are split into sub-functions, failure modes at one level in the hierarchy are often caused by failure modes on the level below them (Rausand & Øien 1996). In this way, failure modes can be traced back to their root causes. These basic concepts of failure analysis are applied to safety systems in the next paragraph, where possible failures of safety systems are classified according to their causes.

Classification by cause

The IEC 61508 standard, which is dealt with in more detail in the next chapter, differentiates between two main categories of failures, according to their causes: *random hardware failures* and *systematic failures*. Random hardware failures result from natural degradation mechanisms in the hardware. Systematic failures are often defined as failures that are "related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors" (IEC 2000). However, these definitions give room for several interpretations. The PDS method[1] (Hauge et al. 2006) narrows the definition of random hardware failures to failures occurring under operating conditions within the design envelope of the system, called *aging failures*. In the PDS method, systematic failures are split into *stress failures*, *design failures* and *interaction failures*, as shown in figure 7. Stress failures occur under excessive stresses, i.e. stresses beyond the design envelope. Design failures are, broadly speaking, introduced during phases prior to operation, for example during system specification, manufacturing or installation. Interaction failures are caused by human errors during operation, maintenance or testing.

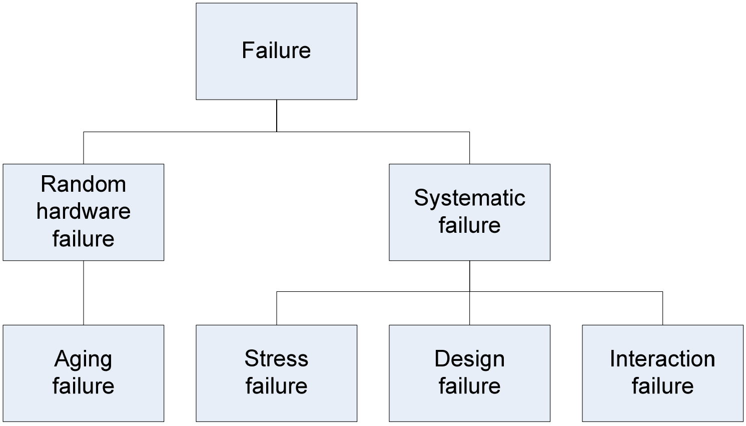

Figure 7: Failure classification by cause of failure according to the PDS method, adapted from Hauge et al. (2006).

It can be argued that stress failures should be classified as a type of random hardware failures, as they were in the previous version of the PDS method, because excessive stresses may result in a physical failure of the system. This has been changed in the new version of the PDS method, because stress failures have the typical characteristics of systematic failures: they can only be eliminated by removing the excessive stresses or by modifying the design (Hauge et al. 2006).

Testing and failure detection

Another way of classifying failures is whether they are detected in tests or not. Safety instrumented systems often carry out automatic (diagnostic) self-tests during operation. However, not all possible failure modes can be detected automatically. The fraction of failures that is revealed by automatic

[1] PDS stands for "pålitelighet av datamaskinbaserte sikringssystemer" and is the Norwegian acronym for reliability of computer-based safety systems. SINTEF has developed a reliability prediction method for safety instrumented systems, called the PDS method, which is continuously updated.

self-tests is often called the *diagnostic coverage factor* (Goble et al. 1998). In the PDS method, this fraction is referred to as the *fault coverage* (Hauge et al. 2006). It should be noted that diagnostic coverage is assessed on the basis of failure rates, not on the basis of the number of failures or failure modes. Apart from failures detected by automatic self-tests, an operator or maintenance crew may detect failures incidentally. The PDS method treats such random failure detection by personnel in conjunction with automatic self-tests, and defines the total coverage factor as reflecting detection both by automatic self-tests and by operators (Hauge et al. 2006).

Since not all possible failure modes are detected during automatic self-tests, *functional testing* is usually performed manually at regular time intervals. It is often assumed that all possible failure modes are detected during such a functional test, and that the item is "as good as new" after the test. Several practices for such tests exist, depending on the nature of the process, the equipment used, the associated risk and the tolerable upsets to the process (HSE 2002). Ideally, functional tests are performed offline, when the safeguarded process is not in operation (Mostia 2002). Since this is not always feasible in practice, safety systems are sometimes tested online during operation. However, online testing seldom has 100% test coverage (Mostia 2002). When such an imperfect functional test is used, the assumption that the item is "as good as new" after a functional test, does not hold. Functional testing might also be imperfect due to systematic failures, such as a testing procedure which is too complicated and therefore misunderstood (Mostia 2002). Hence, even functional testing might leave some parts of the safety function untested, and there is no guarantee that all possible failure modes are detected during a functional test. The PDS-method defines a separate category of failures that are not revealed until an actual demand occurs, called *test independent failures* (Hauge et al. 2006).

In some situations a special type of testing, called *partial stroke testing*, is used. Such a test is performed by e.g. partly closing a valve, which proves that the valve is not stuck in position. However, this does not test whether the valve will fully close and seal completely in case of an actual demand (Gruhn et al. 1998). Hence, not all possible failure modes can be detected during a partial stroke test. Partial stroke testing is often used at regular time intervals in between functional tests, such that the functional test interval can be increased, while maintaining the same reliability level (Mostia 2002). Some partial stroke test arrangements provide automatic operation and can be considered as a form of automatic diagnostics (Mostia 2003). Therefore, it is not always clear whether a partial stroke test should be seen as an (imperfect) functional test or as an automatic self-test. According to Zachary & Summers

(2002), partial stroke testing can significantly improve the reliability of a safety system if it is used to supplement regular full stroke testing. However, partial stroke testing has some limitations as well, and it appears to increase the spurious trip rate, because the actuating item is given a command to move (Mostia 2003).

Classification by failure mode

Failures may also be classified according to their effects, i.e. by failure mode. The IEC 61508 standard differentiates between *dangerous failures* and *safe failures*. It defines a dangerous failure as a “failure which has the potential to put the safety-related system in a hazardous or fail-to-function state”, and a safe failure as a failure which does not have this potential (IEC 2000). This classification may be combined with the previous one, which leads to four categories: dangerous undetected failures, dangerous detected failures, safe undetected failures, and safe detected failures. In this context, a detected failure is interpreted as a failure that is detected immediately when it occurs, for example by an automatic self-test. Undetected failures are revealed only by functional testing or when a demand occurs. This classification does not differentiate between those two types of undetected failures. Moreover, it is not clear whether partial stroke testing should be considered as part of automatic self-tests or as a supplement to functional testing, and, hence, whether the failures detected during partial stroke testing should be treated as “detected” or as “undetected”.

The PDS method considers three failure modes: *dangerous failures*, *spurious trips*, and *non-critical failures*. Spurious trips are defined as failures where the safety system is activated without a real demand from the equipment under control, whereas non-critical failures do not affect the main functions of the system (Hauge et al. 2006). Dangerous failures and spurious trips are split further into detected and undetected, like in the IEC 61508 standard. For convenience, all non-critical failures are classified as undetected. Furthermore, the safe failure category in the IEC 61508 standard is assumed to include both spurious trips and non-critical failures. According to this interpretation, safe detected failures in the IEC notation correspond to detected spurious trips in PDS; safe undetected failures are the sum of non-critical failures and undetected spurious trips (Hauge et al. 2006). Additionally, the PDS method accounts for test independent failures that are not revealed until an actual demand occurs, as explained in the previous paragraph. The relationship between the IEC and PDS notations is illustrated in figure 8.

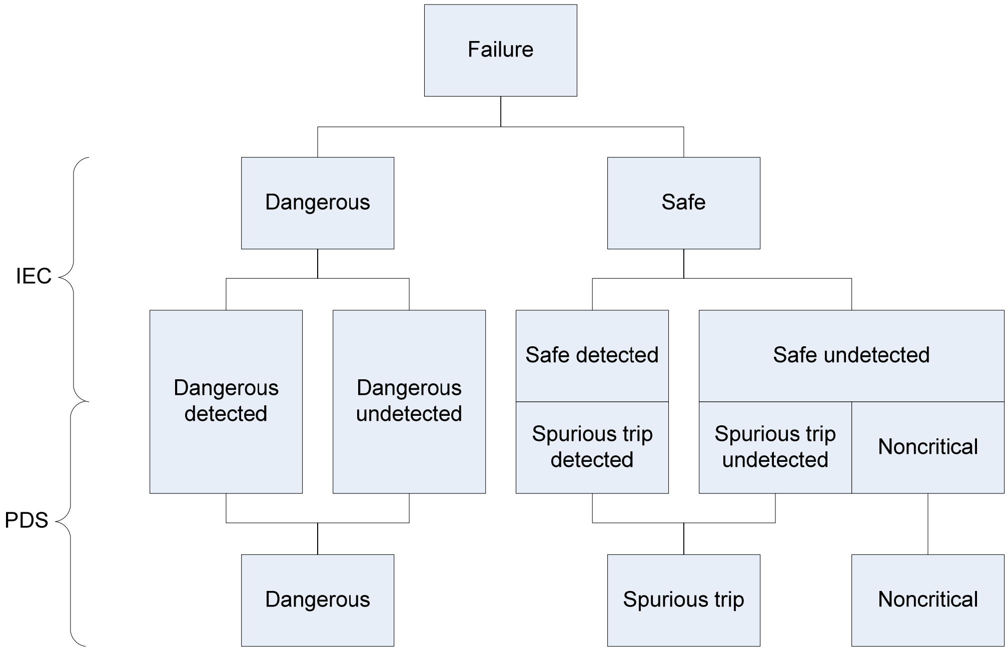

Figure 8: Failure mode classification – IEC versus PDS, adapted from Hauge et al. (2006).

Common cause failures

A special class of failures is constituted by failures that are dependent and have a common cause. As explained in chapter 2, safety systems often have a high degree of redundancy in order to improve their reliability. However, redundant configurations are prone to *common cause failures*, which reduce the positive effect of redundancy. A common cause failure occurs when a single fault results in the corresponding failure of multiple components, for example due to wrong calibration of sensors, incorrect maintenance or environmental stress (Summers & Raney 1999). The IEC 61508 standard defines a common cause failure as a "failure, which is the result of one or more events, causing coincident failures of two or more separate channels in a multiple channel system, leading to system failure" (IEC 2000). However, it is not always clear whether a failure should be considered as a common cause failure or not. Even if two redundant components do not fail simultaneously, but within a certain time interval, they might still have failed due to a common cause, such as exposure to increased temperature (Rausand & Høyland 2004). Quantifying the effect of common cause failures on the reliability of a safety system is not easy, but some approaches exist. These will be described briefly in chapter 5. Summers & Raney (1999) propose to use checklists to identify potential common cause failures of a safety instrumented system during its lifecycle.

4. IEC 61508

The IEC 61508 standard, which was already introduced briefly in chapter 2, is currently the main standard for safety instrumented systems[2]. It is a generic, performance based standard common to several industries, which serves as a basis for the development of application specific standards. The standard itself consists of seven parts, some of which are normative, whereas other parts are informative and provide examples and guidelines. This chapter gives an overview of the main principles and requirements of the standard.

Safety lifecycle

The standard uses a central framework, called the *safety lifecycle*, to structure its requirements and to deal in a systematic way with all activities related to a safety system, from the initial concept until eventual decommissioning. The overall safety lifecycle is shown in figure 9. The term “overall” reflects that contributions from safety systems based on other technologies (e.g. mechanical) and from external risk reduction facilities (e.g. fire walls) also are taken into account when developing the safety requirements for a safety instrumented system (Brown 2000). The safety lifecycle aims to provide a structured approach to manage the implementation of the standard, but, as shown by Van Heel et al. (1999), implementation may still present difficulties, particularly because the lifecycle model lacks an overview of the necessary information in the different phases.

The safety lifecycle starts off with an initial concept, after which the overall scope of the safety analysis has to be defined in terms of the type of hazards and risks to be considered and the boundary of the equipment under control. In phase 3 the hazards and risks associated with the equipment under control are analysed. To identify potential hazards several techniques may be used, such as safety reviews, checklists, failure mode and effects analysis (FMEA), or a hazard and operability study (HAZOP) (Stavrianidis & Bhimavarapu 2000; Summers 1998). For each hazard, the event sequence leading to a potential hazardous event is determined, so that the risk associated with each hazardous event can be evaluated in terms of consequences and likelihood (Brown 1999). The risks associated with each hazard are then compared with the tolerable risks, in order to determine the required risk reduction. Here the

[2] The IEC 61508 standard refers to a safety instrumented system as an “electrical/electronic/programmable electronic (E/E/PE) safety-related system” and also uses the term “electrical/electronic/programmable electronic system” (E/E/PES). For convenience, the term safety instrumented system is used throughout this report.

ALARP principle is often applied, as discussed in chapter 2. The next step is to specify the overall safety requirements in the form of safety functions that are necessary to achieve the required risk reduction. Each safety function is specified in terms of its functionality and its safety integrity, a concept which is clarified in the next paragraph. To convert the results from the hazard and risk analysis into safety requirements, a quantitative risk assessment can be used, as well as several qualitative techniques, such as a risk graph (Summers 1998). Subsequently, the safety functions are allocated to one or more safety instrumented systems, safety systems based on other technologies, or external risk reduction facilities in phase 5 of the safety lifecycle. Figure 10 illustrates the role that safety systems play in achieving the required risk reduction.

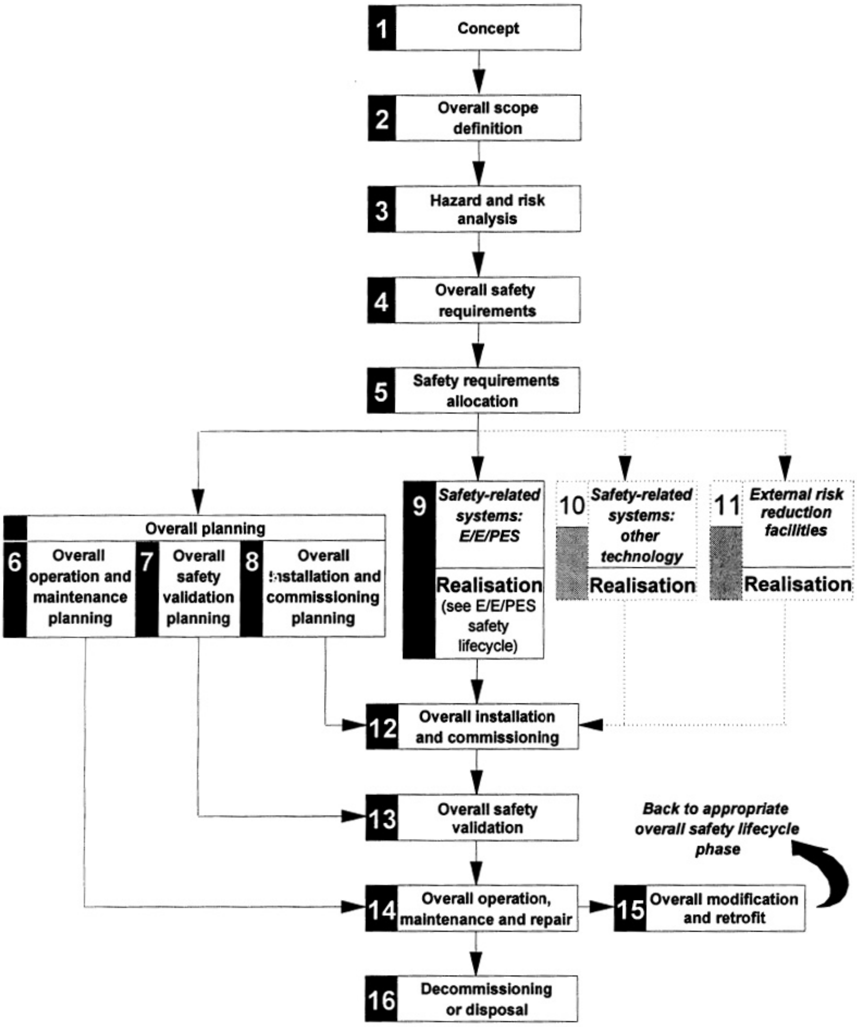
1 Concept
2 Overall scope definition
3 Hazard and risk analysis
4 Overall safety requirements
5 Safety requirements allocation
Overall planning
6 Overall operation and maintenance planning
7 Overall safety validation planning
8 Overall installation and commissioning planning
9 Safety-related systems: E/E/PES
Realisation (see E/E/PES safety lifecycle)
10 Safety-related systems: other technology
Realisation
11 External risk reduction facilities
Realisation
12 Overall installation and commissioning
13 Overall safety validation
Back to appropriate overall safety lifecycle phase
14 Overall operation, maintenance and repair
15 Overall modification and retrofit
16 Decommissioning or disposal

Figure 9: Overall safety lifecycle (IEC 2000).

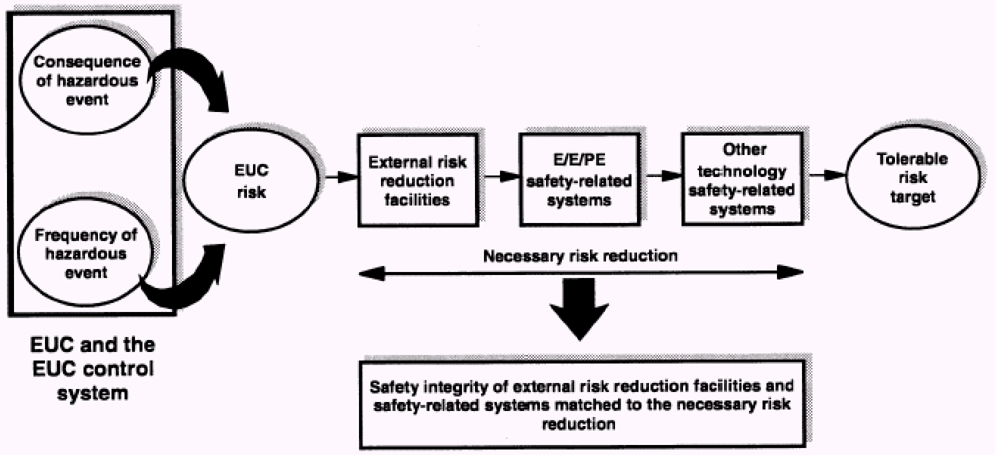
Consequence of hazardous event
Frequency of hazardous event
EUC and the EUC control system
EUC risk
External risk reduction facilities
E/E/PE safety-related systems
Other technology safety-related systems
Tolerable risk target
Necessary risk reduction
Safety integrity of external risk reduction facilities and safety-related systems matched to the necessary risk reduction

Figure 10: Risk and safety integrity concepts (IEC 2000).

When the safety requirements have been allocated to one or more safety systems, these systems have to be realised. The realisation of safety instrumented systems, corresponding to phase 9 in the safety lifecycle, is dealt with later on in this chapter. The realisation of safety systems based on other technologies and the realisation of external risk reduction facilities are outside the scope of the IEC 61508 standard, as indicated by the dotted lines in figure 9. In parallel with the realisation of the safety systems, several planning activities have to be carried out, corresponding to phases 7, 8 and 9 of the safety lifecycle. This includes documentation of the operation and maintenance procedures. Documentation is important – not only during planning, but for all lifecycle activities – to be able to verify that the standard has been followed (Smith & Simpson 2004). When the safety systems have been realised, they should be installed in a controlled manner according to the installation plan. Thereafter, a validation check has to be performed to ensure that the installed safety systems meet the overall safety requirements in terms of safety functions and safety integrity. Last but not least, lifecycle phase 14 and 15 deal with operation, maintenance, repair and modification, which is discussed in chapter 6 of this report.

Safety integrity level (SIL)

Safety integrity is an important concept in the IEC 61508 standard. It can be defined as the "probability of a safety-related system satisfactorily performing the required safety functions under all the stated conditions within a stated period of time" (IEC 2000). The standard defines four *safety integrity levels*, where SIL 4 has the highest level of safety integrity and SIL 1 the lowest. The safety integrity levels are expressed in terms of the average probability of failure on demand (PFD), for safety functions operating in low demand mode of operation, or in terms of the probability of a dangerous failure per hour (PFH), for safety functions operating in high demand or continuous mode of operation. If a quantitative risk assessment is used to develop the safety integrity requirements, the corresponding safety integrity level can be found from table 1 (PFD) or table 2 (PFH). The IEC 61508 standard opens also up for a qualitative determination of safety integrity levels, using for instance a risk graph, which may be more appropriate in some situations (Summers 1998). In that case the quantitative target failure measure, which is needed for failure probability modelling, is taken to be the highest probability of failure associated with the SIL, according to table 1 or 2 (Brown 2000).

Table 1: Safety integrity levels for safety functions operating in low demand mode of operation (adapted from IEC 2000).

Safety integrity level	**Average probability of failure to perform its design function 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 $< 10^{-1}$

Table 2: Safety integrity levels for safety functions operating in high demand or continuous mode of operation (adapted from IEC 2000).

Safety integrity level	**Probability 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 $< 10^{-5}$

But what does SIL actually mean in practice? As pointed out by Summers (1998), the safety integrity level is a statistical representation of the integrity of a safety function when a process demand occurs. In this context it should be noted that the SIL concept only can be applied to an entire safety instrumented system performing one or more safety functions. It is not correct to refer to any individual item (such as a sensor) as having a safety integrity level, because the safety integrity requirements relate to the safety function (Brown 2000). Apart from the quantitative target failure measure shown in table 1 and 2, the SIL also determines several other qualitative and quantitative constraints. Depending on the SIL, the IEC 61508 standard puts different requirements on the design of a safety instrumented system and on several lifecycle activities. Generally speaking, the higher the SIL, the more stringent the requirements to comply with the standard. According to Smith & Simpson (2004), especially SIL 3 and SIL 4 involve significant cost increases and require highly skilled personnel.

Requirements for safety instrumented systems

Within the overall safety lifecycle, the realisation of safety instrumented systems is dealt with specifically in the so-called *E/E/PES safety lifecycle*, which is shown in figure 11. Such a lifecycle should be followed for each safety instrumented system.

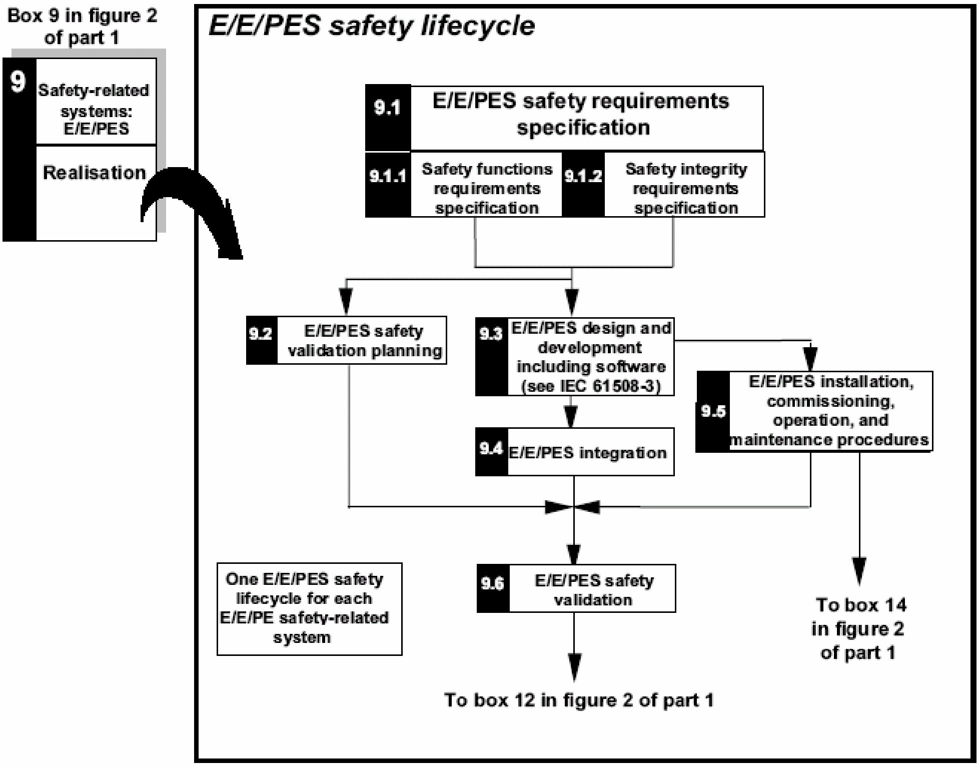
Box 9 in figure 2 of part 1
9 Safety-related systems: E/E/PES
Realisation
E/E/PES safety lifecycle
9.1 E/E/PES safety requirements specification
9.1.1 Safety functions requirements specification
9.1.2 Safety integrity requirements specification
9.2 E/E/PES safety validation planning
9.3 E/E/PES design and development including software (see IEC 61508-3)
9.4 E/E/PES integration
9.5 E/E/PES installation, commissioning, operation, and maintenance procedures
9.6 E/E/PES safety validation
One E/E/PES safety lifecycle for each E/E/PE safety-related system
To box 12 in figure 2 of part 1
To box 14 in figure 2 of part 1

Figure 11: E/E/PES safety lifecycle in realisation phase (IEC 2000).

The standard sets out requirements for both hardware and software of a safety instrumented system. These requirements can be divided into three areas, each of which must be met in order to comply with the standard: quantified failure probability, hardware fault tolerance, and avoidance and control of systematic faults (Brown 2000). First of all, the *failure probability* of each safety function should be analysed quantitatively, taking into account random hardware failures, common cause failures and failures of data communication processes. The failure probability of each safety function has to be lower than the target failure measure corresponding to the SIL. Hardware is also subject to *architectural constraints*, which may impose the use of redundant configurations, to improve the hardware fault tolerance. These constraints depend on the SIL, on the level of confidence in the components used, and on the so-called *safe failure fraction*. In this context, the safe failure fraction is usually interpreted to comprise both safe failures and dangerous detected failures (Lundteigen & Rausand 2006). For both hardware and software, the standard requires that certain measures are taken to avoid *systematic faults*. Examples include modularisation and the use of structured programming methods. Which measures are required, depends on the SIL level. However, the standard does not require quantification of systematic faults, like it is recommended in the PDS-method (Hauge et al. 2006).

There is no specific requirement to undertake a quantitative analysis of *human factors*. Nevertheless, the standard states that the design of safety instrumented systems "shall take into account human capabilities and limitations and be suitable for the actions assigned to operators and maintenance staff. The design of all interfaces shall follow good human-factor practice and shall accommodate the likely level of training or awareness of operators" (IEC 2000). Hence, if a safety function requires human action, such as response to an alarm condition, the likelihood of the correct action being taken should be considered (Brown 2000). Human factors are addressed both explicitly and implicitly in several phases of the safety lifecycle. However, Carey (2000) has a point when he argues that "in comparison to the other aspects of software and hardware engineering involved in the development of a safety-related system, the standard provides minimal specification regarding the design of the user interface and other human related aspects of a system".

5. Analytical tools and methods

As pointed out in chapter 2, new safety standards are performance based and require quantification of the achieved risk reduction. In several phases of the IEC 61508 safety lifecycle a quantitative safety analysis may be performed, for example to check concepts for safety requirements allocation, to compare design alternatives, and later on to validate the achieved safety of the system. However, the standard does not prescribe how such an analysis should be performed and only suggests a number of techniques that may be used. Sometimes qualitative analysis techniques may be used instead of quantitative techniques. As shown by Rouvroye & Brombacher (1999), different analysis techniques may lead to different results. Hence, there is not one single way to assess the reliability of safety systems, and the results from different analyses are not always comparable. This chapter does not intend to provide a manual for reliability analysis of safety systems, but gives a short overview of the most common analytical tools and methods, and discusses some factors that should be taken into consideration when deciding which analysis technique to use in a specific situation.

Qualitative analysis techniques

A number of techniques exist that can be used to analyse a safety system qualitatively. Although these techniques might provide numbers, they are qualitative in the sense that the results only can be used for a rank order – they do not provide exact failure probabilities. A qualitative technique called *expert analysis* is based on previous experience with similar systems. Expert experience can be expressed in different forms, such as codes of practice, standards, design guidelines and checklists. The German DIN standards for safety systems, e.g. DIN 19250 (DIN 1994), rely heavily on expert analysis and give detailed recommendations for avoidance of specific failure modes. This approach results in a ranking of different design alternatives according to predefined requirement classes. Checklists to identify potential common cause failures, like the one proposed by Summers & Raney (1999) and the one included in part 6 of the IEC 61508 standard (IEC 2000), are another example of expert analysis. According to Rouvroye (2001), the advantage of expert analysis is that previous experience is used, but the completeness of the analysis can be questioned, and experience may be invalid for completely new systems.

Another qualitative analysis technique is called *failure mode and effects analysis* (FMEA). This technique involves a bottom-up analysis of a system, by examining all possible component failures and determining the effect of these failures on the entire system (Rouvroye & Van den Bliek 2002). A qualitative indication of failure probabilities and failure consequences is included as well. A detailed description of FMEA can be found in IEC 812 (IEC 1985). Several extensions to FMEA have been developed, such as the *failure mode, effects and criticality analysis* (FMECA), which leads to a ranking for the criticality of different failure modes, and the *failure mode, effects and diagnostics analysis* (FMEDA), which can be used to check which failures modes are detected by online diagnostics (Goble & Brombacher 1999). It is also possible to extend FMEA to take common cause failures into consideration, as shown by Childs & Mosleh (1999). FMEA has a number of disadvantages and the results may be inconsistent, but this technique can be applied at an early stage and it can provide a good starting point for quantitative analysis techniques (Childs & Mosleh 1999; Rouvroye 2001). To identify potential hazards associated with the equipment under control, some other qualitative techniques can be used as well, for example a *hazard and operability study* (HAZOP). This technique provides a prioritised basis for the implementation of risk mitigation strategies, such as safety instrumented systems (Summers 1998).

Quantitative analysis techniques

Next to the qualitative techniques described above, there are several quantitative techniques that can be used for a safety analysis. Some of them are relatively easy and have limited modelling power (e.g. parts count analysis), whereas others are more sophisticated (e.g. Markov analysis). However, as the modelling power increases, the complexity of the analysis increases as well (Rouvroye & Van den Bliek 2002). *Parts count analysis* is the simplest quantitative analysis method. Here, the failure rate of a system is obtained by summing all failure rates of the individual components. This technique is described by e.g. Lewis (1996). Parts count analysis is very simple and does not require a lot of system knowledge, but it does not take into account aspects such as redundancy and testing (Rouvroye 2001). Hence, this technique provides limited insight into the reliability of a safety system. *Reliability block diagrams* give a more realistic picture, because they take redundancy into account. A reliability block diagram consists of functional blocks that graphically show the condition for successful operation (IEC 1991). An example of a reliability block diagram is shown in figure 12. Quantitative evaluation of a reliability block diagram results in the system failure probability at a certain time. This method is often used during early lifecycle phases because of its simplicity, but it has some limitations: blocks can only have one failure mode, testing and repair are not taken into account, common cause failures can only be modelled by introducing extra blocks, and different models are needed to evaluate spurious trips and dangerous failures (Rouvroye 2001).

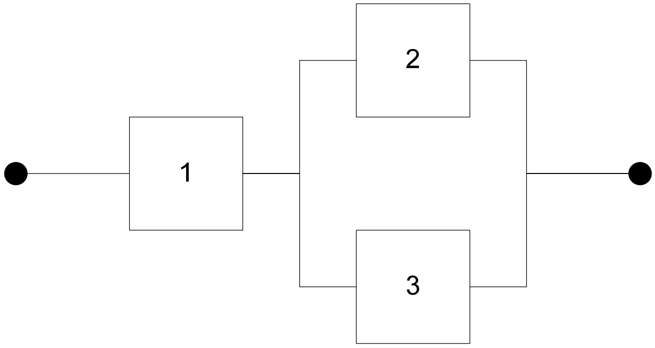

Figure 12: Example of a reliability block diagram

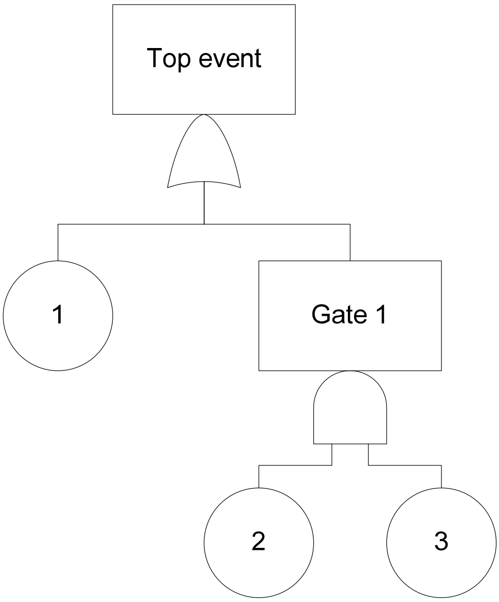

Figure 13: Example of a fault tree

Another graphical technique is called *fault tree analysis*. It involves a top-down analysis aimed at finding causes (basic events) or combinations of causes that can lead to a defined undesirable event, which is referred to as the top event. A fault tree can be used as a qualitative tool, but it is also possible to evaluate a fault tree quantitatively using Boolean algebra. Fault tree analysis is widely used in practice and thoroughly described in literature, for example in an IEC standard (IEC 1990b) and in the fault tree handbook (NASA 2002). An example is shown in figure 13. According to Summers (2000), fault tree analysis is a proven technique that can model even the most complex logic relationships. Systematic failures and common cause failures can be included as well. However, different models are needed for different top events like spurious trips and dangerous failures, and repair models cannot be adequately represented (Rouvroye 2001). A major benefit of fault trees is the availability of software tools to facilitate quantitative evaluation (Summers 2000).

Safety systems can also be analysed quantitatively using *Markov models*, which describe a system using a set of mutually exclusive states and transitions between these states (Rouvroye 2001). Markov models are represented mathematically by a set of differential equations to determine the probability for the system to be in each state. These equations can be solved analytically, but complex Markov models are usually evaluated numerically. An example of a Markov model is shown in figure 14. According to Rouvroye & Van den Bliek (2002), Markov analysis has high modelling power and covers most aspects of system behaviour, but the analysis is complex and requires significant effort. Some authors argue that Markov models are incorrect and should be prohibited (see e.g. Gulland 2003). However, Bukowski (2005) has shown that Markov models give exactly the same results as classical probability techniques, if they are constructed and interpreted properly. Correct application of Markov models is discussed by e.g. Zhang, Long & Sato (2003). It should be noted that Markov models in principle only can be applied within a test interval, because the Markov property has to be fulfilled (i.e. the process has to be memoryless). This can be compensated for by using a repair matrix, which depends on the repair strategy and on the quality of the repair actions (Rausand & Høyland 2004). However, the effects of staggered testing (i.e. testing parallel items at different times) cannot be included in this way. Another limitation of Markov analysis, and of most other safety analysis techniques, is that the effects of data uncertainty cannot be taken into account (Rouvroye & Brombacher 1999). *Enhanced Markov analysis*, which is a combination of Markov analysis, uncertainty analysis (via Monte Carlo technique) and sensitivity analysis, provides a solution for this problem (Rouvroye 2001).

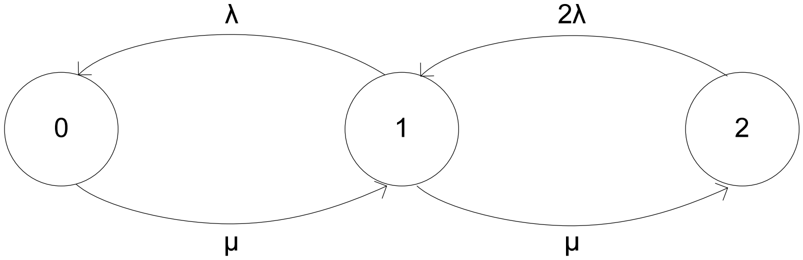

Figure 14: Example of a Markov model

Apart from the quantitative analysis techniques described above, there are some techniques that combine reliability block diagrams with results from other analysis techniques on component level. Such combinations are sometimes referred to as *hybrid techniques* (Rouvroye & Brombacher 1999). This category includes the so-called *simplified equations*, which can be derived from Markov models, assuming the rare event approximation (Summers 2000). These equations can be used to calculate the failure probability for each subsystem of a safety system (sensors, logic solver, final elements and support systems), taking different redundant configurations into account. Subsequently, the failure probabilities of the individual subsystems can be combined according to the principles of reliability block diagrams. As shown by Summers (2000), it is possible to include terms that reflect common cause failures, systematic failures, and second undetected failures during the repair of detected failures. Equations for the spurious trip rate can be derived as well (Rausand & Høyland 2004; Summers 2000). The form in which the simplified equations often are presented, assumes that redundant components have the same failure rate. Nevertheless, it is possible to modify the equations in such a way as to cover redundant components that are dissimilar and, thus, have different failure rates (Beckman 2001). A significant limitation of the simplified equations, however, is that the testing frequency must be the same for all components used in a redundant configuration (Beckman 2001; Summers 2000). Moreover, certain aspects of complex safety systems that can be incorporated into Markov models, are not covered by the simplified equations (Bukowski 2005; Summers 2000). Hence, the simplified equations have less modelling power than Markov models.

PDS method

The PDS method, which was already mentioned briefly in chapter 3, is a comprehensive method for reliability prediction of safety instrumented systems. This method is widely used in the Norwegian offshore industry, but is also applicable to other business sectors (Hauge et al. 2006). According to the classification of analysis techniques by Rouvroye & Brombacher (1999), the PDS method falls into the category of hybrid techniques, because it is based on the simplified equations discussed in the previous paragraph. The PDS method is in line with the IEC 61508 standard, but for some areas like failure classification, modelling of common cause failures and how to treat systematic failures, the PDS method offers a somewhat different approach. For instance, systematic failures are quantified in the PDS method, whereas the IEC 61508 standard only requires qualitative measures to be taken to prevent systematic failures. The PDS method can be considered realistic, because it accounts for all major factors affecting reliability during system operation, such as: all failure causes, common cause failures, automatic self-tests, functional testing, systematic failures, complete safety functions, redundancies, and voting logic (Hauge et al. 2006).

Software

Several software tools exist that can be helpful when quantifying safety. Some of them can provide assistance with a specific analysis technique, for example fault trees, whereas others can be used for a complete functional safety analysis, in order to comply with a relevant standard, such as IEC 61508. Software packages in the latter category include SILence (developed by the German company HIMA) and SILver (developed by the US-based company Exida). Both can be used for safety integrity level calculations. SILence has been verified by the German TÜV and uses safety data from the HIMA database (HIMA 2006). SILver includes a database of failure data as well and is available for use on-line (Exida 2006). Another software tool has been developed in connection with the PDS project, but this tool has not been updated to the newest version of the PDS method and is not used anymore. According to Timms (2003), software tools can help to achieve significant benefits by aiding design, and setting optimal testing and maintenance strategies to meet SIL requirements.

6. Operation and maintenance

Although the IEC 61508 standard takes a lifecycle approach that also includes operation and maintenance, there is little focus on how we can ensure that the required safety integrity level is maintained during the operational phase of a safety system. Most literature is concerned with determining the required safety integrity level and demonstrating that the safety system could be qualified for the required safety integrity level upon system start-up. This chapter will touch upon some aspects of operation and maintenance: the requirements from standards (mainly IEC 61508) for the operational phase, the use of field data, and the impact of human and organisational factors.

Requirements from standards

The IEC 61508 standard does not give many details about the operational phase of a safety system, but some requirements are given. Phase 14 of the overall safety lifecycle deals with operation, maintenance and repair, whereas phase 15 focuses on a related issue: modification and retrofit. The requirements for the operational phase are based on the procedures for operation and maintenance that have been developed in parallel with the realisation of the safety system, as described in chapter 4 of this report. The standard proposes an operations and maintenance management model (see figure 15) and a model for operations and maintenance activities (see figure 16).

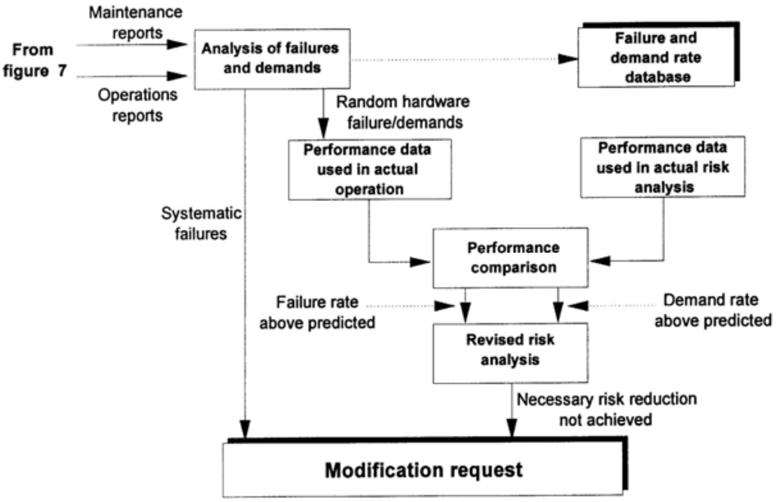
Maintenance reports
From figure 7
Operations reports
Analysis of failures and demands
Failure and demand rate database
Random hardware failure/demands
Performance data used in actual operation
Performance data used in actual risk analysis
Systematic failures
Performance comparison
Failure rate above predicted
Demand rate above predicted
Revised risk analysis
Necessary risk reduction not achieved
Modification request

Figure 15: Operations and maintenance management model (IEC 2000)[3].

[3] The text “from figure 7” in this diagram refers to figure 16 in this report, which corresponds to figure 7 in part 1 of the standard.

The required activities include implementing procedures, following maintenance schedules, and carrying out periodical tests. The test results have to be documented, as well as any modifications that have been made to the system. The standard also requires documentation of the time and cause of demands on the safety system during operation, together with the performance of the system in these cases.

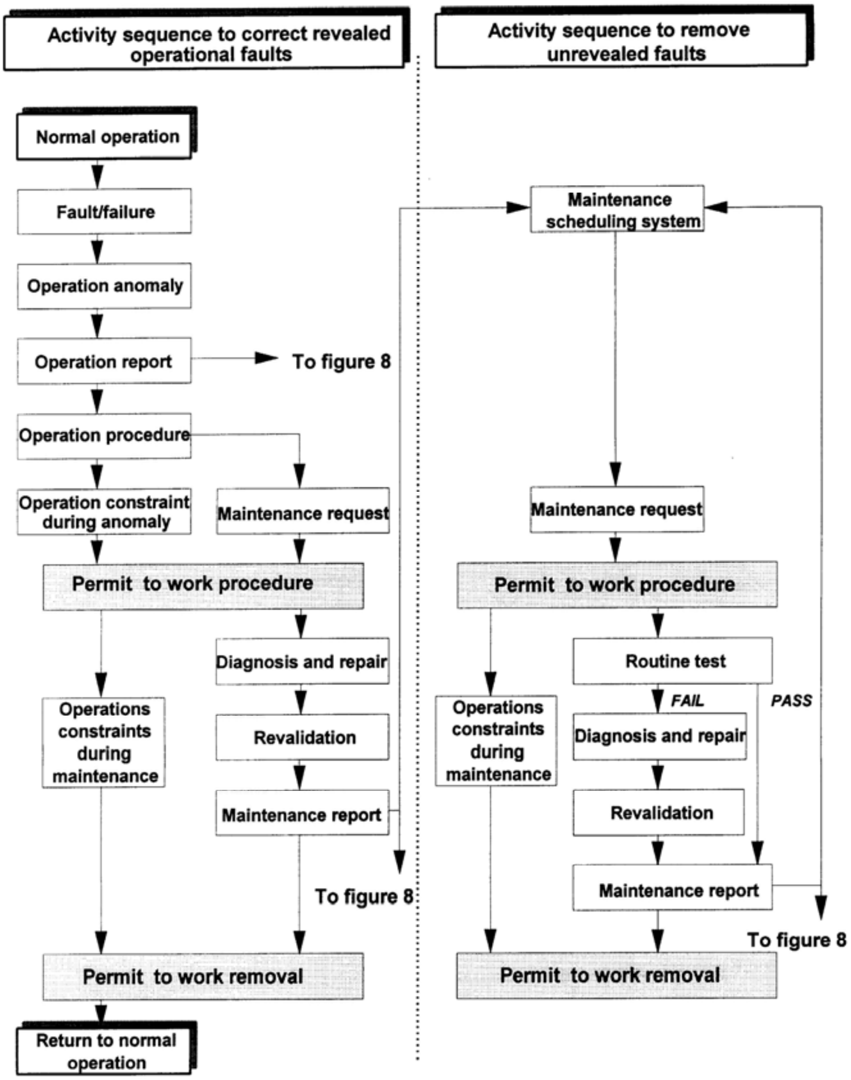

Figure 16: Operations and maintenance activities model (IEC 2000)[4].

[4] The text "to figure 8" in this diagram refers to figure 15 in this report, which corresponds to figure 8 in part 1 of the standard.

As it becomes clear from figure 15, the analysis of failures and demands during actual operation may lead to modification requests. Modifications may also be necessary due to other reasons, such as new legislation or changes to the equipment under control. The standard requires that an impact analysis be carried out before any modifications are made. This analysis has to assess the impact of the proposed modification on functional safety and has to include a hazard and risk analysis. If authorisation for the proposed modification is granted, one has to return to the appropriate phase of the overall safety lifecycle. It should be noted that the standard does not specify which phase is considered appropriate under which circumstances. Next, all subsequent phases have to be passed according to the requirements given by the standard. This may lead to a different safety integrity level, and test procedures may have to be updated as well. The modification procedure is shown in figure 17.

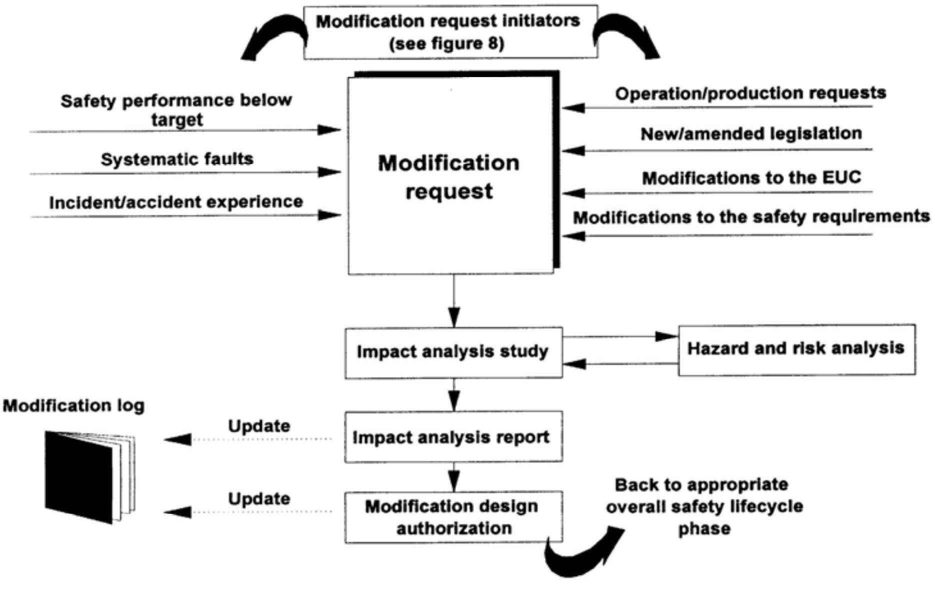
Modification request initiators (see figure 8)
Safety performance below target
Systematic faults
Incident/accident experience
Modification request
Operation/production requests
New/amended legislation
Modifications to the EUC
Modifications to the safety requirements
Impact analysis study
Hazard and risk analysis
Modification log
Update
Impact analysis report
Update
Modification design authorization
Back to appropriate overall safety lifecycle phase

Figure 17: Modification procedure model (IEC 2000)[5].

Field data

The documentation that is collected during operation and maintenance contains useful information about the actual performance of the safety system. These *field data* can be used to update the quantitative reliability prediction models that usually are based on generic data. According to OLF Guideline 070 (OLF 2004), which sets out guidelines for the application of

[5] The text “see figure 8” in this diagram refers to figure 15 in this report, which corresponds to figure 8 in part 1 of the standard.

IEC 61508 and IEC 61511 in the Norwegian petroleum industry, analysis of field data is essential to ensure that the safety system is performing and being maintained as intended, and to ensure that the installation is being operated at an acceptable risk level. Field data may provide a more realistic picture of the reliability of a safety system than the *generic data* that are used initially, because field data reflect the performance of the realised safety system in actual use. Generic data are obtained from large databases, such as the Offshore Reliability Data Handbook (OREDA 2002), and these data are not always based on exactly the same equipment and operating conditions. This introduces an element of uncertainty (Wang, West & Mannan 2004). Moreover, not all generic data sources distinguish between different failure modes, and data about common cause failures are usually not available at all. On the other hand, collecting relevant field data takes a lot of effort and requires information from various, sometimes not compatible sources (Rouvroye 2001). If experience data are collected during the operational phase, as required by the IEC 61508 standard, these data can be used to update the parameters (e.g. failure rate estimates) that are used in the quantitative safety analysis. It is also possible to recalculate the test interval based on field experience, which may allow for a lower frequency of functional testing. However, a change of the test interval should be handled as a modification (OLF 2004). Appendix F of OLF Guideline 070 (OLF 2004) describes an approach for updating test intervals and failure rate estimates as field data become available, but other methods exist as well.

Human and organisational factors

Human factors have a considerable influence on the reliability of safety-critical systems and, as human errors often are caused by certain preconditions in the work context, the same holds for underlying organisational factors (Redmill & Rajan 1997). Furthermore, safety and reliability of products are not only determined by the technical aspects of a product, but also by the business processes in an organisation realising and operating these products (Brombacher 1999). In the context of the IEC 61508 safety lifecycle, human and organisational factors may lead to unforeseen systematic failures initiated during operation and maintenance, corresponding to interaction (or operational) failures in the PDS failure classification (see chapter 3). The IEC 61508 standard proposes a number of measures to be taken to prevent systematic failures initiated by human error during operation and maintenance, but does not require quantification of systematic failures. Nevertheless, systematic failures may significantly influence the actual performance of a safety system in the operational phase (Hauge et al. 2006), and therefore it is important to investigate the impact of human and organisational factors on safety integrity during the operational phase.

Research in this area is limited and there are no models available that directly link human and organisational factors to the achieved safety integrity level. Nevertheless, some relevant approaches exist. Carey & Purewal (2001) have developed a framework for addressing human factors in IEC 61508 and show that the level of effort required on human factors, for operation and maintenance, increases with the safety integrity level. Øien (2001) focuses on organisational factors and proposes a framework for the establishment of organisational risk indicators, which can be used for risk control during operation. However, this framework concentrates on risk and cannot be applied directly to safety analysis. Brombacher (1999) introduces the maturity index on reliability (MIR) as a method that can be used to quantify organisational aspects in the context of IEC 61508. This technique analyses the maturity of business processes in terms of the quality of reliability related information flows and the deployment of this information into the business processes. It should be noted that this technique deals in the first place with the maturity of business processes, and only indirectly with safety and reliability of the products realised and operated by these business processes.

References

Aven, Terje (2003): *Foundations of risk analysis. A knowledge and decision-oriented perspective*. Chichester: John Wiley & Sons.

Beck, Ulrich (1997): *De wereld als risicomaatschappij*. Translated by Inge van der Aart. Amsterdam: De Balie.

Beckman, Lawrence (2001): "Easily access complex safety loops". In: *Chemical Engineering Progress*, vol. 97, no. 3, pp. 57-59.

Blache, K. M. & A. B. Shrivastava (1994): "Defining failure of manufacturing machinery and equipment". In: *Proceedings from the Annual Reliability and Maintainability Symposium*, pp. 69-75.

Brombacher, A.C. (1999): "Maturity index on reliability: covering non-technical aspects of IEC 61508 reliability certification". In: *Reliability Engineering and System Safety*, vol. 66, pp. 109-120.

Brown, S. J. (1999): "Human factors & safety integrity – IEC 61508". *IEE Conference Publication*, no. 463, pp. 156-161.

Brown, Simon (2000): "Overview of IEC 61508 – Design of electrical/electronic/ programmable electronic safety-related systems". In: *Computing and Control Engineering Journal*, vol. 11, pp. 6-12.

BS (1991): *BS 5760-5 – Reliability of systems, equipments and components*. Part 5: *Guide to failure modes, effects and criticality analysis.* London: British Standards Institution.

Bukowski, Julia V. (2005): "A comparison of techniques for computing PFD average". In: *Proceedings from the Annual Reliability and Maintainability Symposium*, pp. 590-595.

Carey, Michael S. (2000): "Human factors in the design of safety-related systems". In: *Computing and Control Engineering Journal*, vol. 11, pp. 28-32.

Carey, M. & S. Purewal (2001): "Developing a framework for addressing human factors in IEC 61508". *IEE Conference Publication*, no. 481, pp. 42-47.

Childs, Joseph A. & Ali Mosleh (1999): "Modified FMEA tool for use in identifying and addressing common cause failure risks in industry". In: *Proceedings from the Annual Reliability and Maintainability Symposium*, pp. 19-24.

Corneliussen, Kjell (2002): *Programmable control and safety systems – an introduction to risk and reliability*. Trondheim: NTNU.

DIN (1994): *DIN V 19250, Grundlegende Sicherheitsbetrachtungen für MSR-Schutzeinrichtungen*. Berlin: Deutsches Institut für Normung.

Exida (2006): SILver Tool. Accessed November 20th at
http://www.exida.com/applications/silver.asp

Fischhoff, Baruch, Stephen R. Watson & Chris Hope (1984): "Defining risk". In: *Policy Sciences*, vol. 17, no. 2, pp. 123-139.

Gibson, J. J. (1961): "The contribution of experimental psychology to the formulation of the problem of safety – a brief for basic research". In: *Behavioral Approaches to Accident Research,* New York: Association for the Aid of Crippled Children, pp. 77-89. Reprinted in W. Haddon, E.A. Suchman and D. Klein (1964): *Accident Research: Methods and Approaches*. New York: Harper & Row.

Goble, W. M. & A. C. Brombacher (1999): "Using a failure modes, effects and diagnostic analysis (FMEDA) to measure diagnostic coverage in programmable electronic systems". In: *Reliability Engineering & System Safety*, vol. 66, no.2, pp. 145-148.

Goble, William M.; Julia V. Bukowski & A. C. Brombacher (1998): "How diagnostic coverage improves safety in programmable electronic systems". In: *ISA Transactions*, vol. 36, no. 4, pp. 345-350.

Gulland, W. G. (2003): "Repairable Redundant Systems and the Markov Fallacy". Downloaded November 16th, 2006, from
http://www.4-sightconsulting.co.uk/Current_Papers/Markov_Fallacy/markov_fallacy.html

Haddon, W. J. (1980): "The basic strategies for reducing damage from hazards of all kinds". In: *Hazard Prevention*, Sept-Oct, pp. 8-12.

Hauge, Stein, Per Hokstad, Helge Langseth & Knut Øien (2006): *Reliability prediction method for safety instrumented systems – PDS method handbook, 2006 edition*. Trondheim: SINTEF.

Henley, E. J. & H. Kumamoto (1981): *Reliability Engineering and Risk Assessment*. Englewood Cliffs, NJ: Prentice-Hall.

HIMA (2006): SILence. Accessed November 20th at http://www.hima.com/Kundenwelt/Process_Applications/Product_overview/_Software/SILence.asp

HSE (2002): *Principles for proof testing of safety instrumented systems in the chemical industry*. Norwich: Health and Safety Executive.

IEC (1985): *IEC 812 – Analysis techniques for system reliability – procedure for failure mode and effects analysis (FMEA)*. Geneva: : International Electrotechnical Commission.

IEC (1990a): *IEC 60050-191 – International Electrotechnical Vocabulary*. Chapter 191: *Dependability and quality of service*. Geneva: International Electrotechnical Commission.

IEC (1990b): *IEC 61025 – Fault tree analysis (FTA)*. Geneva: International Electrotechnical Commission.

IEC (1991): *IEC 61078 – Analysis techniques for dependability – reliability block diagram method*. Geneva: International Electrotechnical Commission.

IEC (2000): *IEC 61508 – Functional safety of electrical/electronic/programmable electronic safety-related systems*. Geneva: International Electrotechnical Commission.

IEC (2003): *IEC 61511-1 – Functional safety – Safety instrumented systems for the process industry sector – part 1: Framework, definitions, system, hardware and software requirements*. Geneva: International Electrotechnical Commission.

ISA (1996): *ANSI/ISA S84.01-1996, Application of safety instrumented systems for the process industry*. N. Carolina: Instrument Society of America.

ISO (1986): *ISO 8402 - Quality Vocabulary*. Geneva: International Standards Organisation.

Kaplan, Stanley & B. John Garrick (1981): “On the quantitative definition of risk”. In: *Risk Analysis*, vol. 1, no.1, pp. 11-27.

Karydas, D. M. & A. C. Brombacher (1999): “Reliability certification of programmable electronic systems”. In: *Reliability Engineering and System Safety*, vol. 66, pp. 103-107.

Kjellén, Urban (2000): *Prevention of accidents through experience feedback*. London: Taylor & Francis.

Klinke, Andreas & Ortwin Renn (2001): “Precautionary principle and discursive strategies: classifying and managing risks”. In: *Journal of Risk Research*, vol. 4, no.2, pp. 159-173.

Lambert, M., B. Riera & G. Martel (1999): “Application of functional analysis techniques to supervisory systems”. In: *Reliability Engineering and System Safety*, vol. 64, no. 2, pp. 209-224.

Lewis, E. E. (1996): *Introduction to reliability engineering*. New York: John Wiley & Sons.

Lundteigen, Mary Ann & Marvin Rausand (2006): “Assessment of hardware safety integrity requirements”. *Proceedings of the 30th ESReDA seminar*, Trondheim, Norway, June 7th-8th.

Mostia, William L. (2002): *Testing of SIS valves*. Downloaded October 23rd, 2006, from http://www.sipi61508.com/ciks/mostia2.pdf.

Mostia, Bill (2003): “Partial stroke testing – simple or not?”. In: *Control Magazine*, vol. 16, no. 11, pp. 63-67.

NASA (2002): *Fault Tree Handbook with Aerospace Applications*. Washington DC: NASA.

NPD (2001): *Forskrift om styring i petroleumsvirksomheten*. Stavanger: Norwegian Petroleum Directorate (Oljedirektoratet).

OLF (2004): *Recommended guidelines for the application of IEC61508 and IEC61511 in the petroleum activities on the Norwegian continental shelf*. Stavanger: Norwegian Oil Industry Association (Oljeindustriens

Landsforening). Downloaded November 2nd, 2006, from http://www.olf.no/hms/retningslinjer/?10173

OREDA 2002: *Offshore Reliability Data Handbook*, 4th edition. Høvik: Det Norske Veritas.

Rausand, Marvin & Arnljot Høyland (2004): *System reliability theory – models, statistical methods, and applications*. Hoboken, NJ: John Wiley & Sons.

Rausand, Marvin & Knut Øien (1996): "The basic concepts of failure analysis". In: *Reliability Engineering and System Safety*, vol. 53, pp. 73-83.

Redmill, Felix & Jane Rajan (ed.) (1997): *Human factors in safety-critical systems*. Oxford: Butterworth-Heinemann.

Rouvroye, J. L. & A. C. Brombacher (1999): "New quantitative safety standards: different techniques, different results?" In: *Reliability Engineering and System Safety*, vol. 66, pp. 121-125

Rouvroye, J. L. (2001): *Enhanced Markov analysis as a method to assess safety in the process industry*. Doctoral thesis, Eindhoven University of Technology.

Rouvroye, J. L. & E. G. van den Bliek (2002): "Comparing safety analysis techniques". In: *Reliability Engineering and System Safety*, vol. 75, pp. 289-294.

Rowe, William D. (1977): *An anatomy of risk*. New York: John Wiley & Sons.

Sklet, Snorre (2006): "Safety barriers – definition, classification and performance". In: *Journal of Loss Prevention in the Process Industries*, vol. 19, pp. 494-506.

Smith, David J. & Kenneth G. L. Simpson (2004): *Functional Safety. A straightforward guide to applying IEC 61508 and related standards*. Oxford: Elsevier Butterworth-Heinemann.

SRA (2006): *Glossary of Risk Analysis Terms*. Society for Risk Analysis. Accessed September 20th at http://www.sra.org/resources_glossary.php.

Stavrianidis, Paris & Kumar Bhimavarapu (2000): "Performance-based standards: safety instrumented functions and safety integrity levels". In: *Journal of Hazardous Materials*, vol. 71, pp. 449-465.

Summers, Angela E. (1998): "Techniques for assigning a target safety integrity level". In: *ISA Transactions*, vol. 37, pp. 95-104.

Summers, Angela E. (2000): "Viewpoint on ISA TR84.0.02 – simplified methods and fault tree analysis". In: *ISA Transactions*, vol. 39, pp. 125-131.

Summers, Angela E. & Glenn Raney (1999): "Common cause and common sense, designing failure out of your safety instrumented systems". In: *ISA Transactions*, vol. 38, pp. 291-299.

Timms, Clive Roger (2003): "IEC 61508/61511 – Pain or gain?". In: *Process Safety Progress*, vol. 22, no. 2, pp. 105-108.

Van Heel, K.A.L., B. Knegtering & A.C. Brombacher (1999): "Safety lifecycle management – A flowchart presentation of the IEC61508 overall safety lifecycle model". In: *Quality and Reliability Engineering International*, vol. 15, pp. 493-500.

Wang, Y., H.H. West & M.S. Mannan (2004): "The impact of data uncertainty in determining safety integrity level". In: *Transactions of the Institution of Chemical Engineers, Part B: Process Safety and Environmental Protection*, vol. 82, pp. 393-397.

Zachary, Bryan A. & Angela E. Summers (2002): "Partial stroke testing and SIF performance". *ISA Technical Papers*.

Zhang, Tieling, Wei Long & Yoshinobu Sato (2003): "Availability of systems with self-diagnostic components – applying Markov model to IEC 61508-6". In: *Reliability Engineering and System Safety*, vol. 80, pp. 133-141.

Øien, Knut (2001): "A framework for the establishment of organizational risk indicators". In: *Reliability Engineering and System Safety*, vol. 74, pp. 147-167.