CHAPTER 1

INTRODUCTION

1.1 Introduction

The title of this book, Reliability of Safety-Critical Systems, embraces a wide range of issues and may be too broad to truly represent the content of the book. Our intuitive understanding of a safety-critical system is a system whose failure may lead to harm to people, economic loss, and/or environmental damage. Some failures may lead directly to undesired consequences, while other failures may increase the risk of damage.

Whether or not a system is considered to be safety critical depends on the possible consequences of its failure. If the failure can result in consequences that are judged to be unacceptable, we say that the system is safety-critical.

Safety-critical systems are used in many products and application areas. The safety-critical systems that are considered in this book are technical systems and may, or may not, involve human operator actions. The scope is delimited to systems that are designed to perform one or more safety functions. A safety function is usually implemented to protect against a specific undesired event that can cause harm. The system that is protected by the safety-critical system is called equipment under
control (EUC). When the safety-critical system is medical equipment, the EUC may be a person.

Examples of safety-critical systems that may be assessed by the models and methods described in this book include:

- Automobiles (e.g., airbag systems, brakes, steering, electronic stability program (ESP) systems)
- Process industry (e.g., emergency shutdown (ESD) systems, fire and gas systems, gas burner management systems)
- Machinery (e.g., guard interlocking systems, emergency stop systems)
- Railway transport (e.g., signaling systems, automatic train stop (ATS) systems)
- Nuclear power industry (e.g., turbine control systems, fire prevention systems)
- Medical devices (e.g., heart pacemakers, insulin pumps, electronic equipment used in surgery)

EXAMPLE 1.1 Interlock

An interlock is a device that is used to prevent a technical system (e.g., a machine) from harming people or damaging itself by stopping the system. An interlock can be a strictly mechanical item, such as a switch, but can also be rather sophisticated and based on infrared beams and photodetectors.

Consider an industrial robot that is used to stack boxes. The robot is often equipped with an interlocking system comprising a fence to avoid contact between moving parts of the robot and the human operator. If the operator opens the door, for example, to remove a misplaced box, the power is automatically isolated from the robot and the robot stops. Closing the door is normally not enough to re-power the robot. A reset button must also be pressed, to make sure that the operator has left the area inside the fence (e.g., see Department of Labour, 1987).

Another word in the title of the book is reliability. The reliability of an item is defined as "the ability of the item to perform a required function, under given environmental and operational conditions and for a stated period of time" (e.g., see Rausand & Hoyland, 2004). The reliability of an item is always related to its required functions and it may therefore be more relevant to talk about the reliability of a function. In this book we are especially concerned about safety functions and the reliability of these functions. Several quantitative reliability measures for safety functions are defined and used in the following chapters.

A safety function that is performed by a safety-critical system may be categorized as follows:
Safety control function. A safety function that is a normal part of the operation of the EUC and/or integrated into the EUC control system (e.g., a railway signaling system, the braking system of an automobile).

Safety protective function. A dedicated safety function that is separate from the EUC control system and is only activated when the safety function is demanded (e.g., the ESD system in a process plant, the airbag system in an automobile).

Many safety-critical systems are based on electrical, electronic, or programmable electronic (E/E/PE) technology. The development of programmable electronics and computers continues at a fast pace, and the new technology gets more functions and becomes steadily cheaper, and finds its way into more and more advanced safety-critical systems.

In this book, we mainly consider safety-critical systems where E/E/PE technology plays an important role, often together with mechanical or other technology items. The important standard IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems designates these systems by the term E/E/PE safety-related systems. This term is long and difficult to pronounce, and the author therefore prefers to use the term safety-instrumented system (SIS), which is the corresponding term used in the process industry.

The IEC 61508 standard is introduced briefly in Section 1.3.1 and further discussed in Chapter 2. A notable feature of IEC 61508 is that it is risk-based, which means that reliability requirements for the E/E/PE safety-related systems (i.e., SISs) must be allocated based on the results from a risk analysis. We therefore start with a brief introduction to risk and risk analysis.

1.1.1 Risk and Risk Analysis

The term risk is complex and has been given a wide range of definitions (e.g., see Rausand, 2011). In this book, we define risk as the combined answer to the following three questions:

1. What can go wrong?
2. How probable is it?
3. What are the consequences?

To answer the first question, we have to identify the possible undesired events\(^1\). Most undesired events are related to energy of some sort and occur when this energy is released. Examples of undesired events in the process industry are gas leaks, runaway reactions, fires, explosions, falling objects, and so on. To answer the second question, we often need to study the causes of each undesired event and use

\(^1\)An undesired event is called a hazardous event in Rausand (2011), which is a more suitable term. The term undesired event is used in this book because the term hazardous event is used with a slightly different meaning (see Chapter 2)
experience data and expert judgment to estimate the probability or frequency of the undesired event. Most EUCs are protected by one or more safety barriers that are installed to remove or mitigate the consequences of the undesired events. The answers to questions two and three therefore depend on how well the safety barriers are functioning.

The process of answering the three questions is called a risk analysis and is sometimes illustrated by a bow-tie diagram, as shown in Figure 1.1, where the safety barriers are illustrated as gray rectangles. A thorough introduction to risk analysis is provided in Rausand (2011).

1.1.2 Safety Barriers

Safety barrier is a common term in most risk analyses and is partly overlapping with our definition of a safety-critical system. A safety barrier system may be a technical system or some dedicated human and organizational effort. Safety barrier is therefore not the same concept as safety-critical system. An emergency procedure may, for example, be a safety barrier but is not a safety-critical system. The concept of safety barrier is defined and further discussed by Skjet (2006).

EXAMPLE 1.2 Safety barriers in a process plant

A process plant usually has a range of safety barriers. Among these are:

- Fire and gas detection systems
- Emergency shutdown systems
- Fire and explosion walls
- Passive fire protection
- Fire extinguishing systems
- Pressure relief systems
- Fire and evacuation training

EXAMPLE 1.3 Safety barriers related to fires in buildings

Several safety barriers may be used to reduce the risk related to fires in buildings. Among these are:
- Smoke detection and alert system
- Thermal detection and alert system
- Evacuation plans and emergency procedures
- Exits, exit signs, and emergency lighting
- Smoke control and air handling system
- Fire doors and fire walls
- Sprinkler systems

See Robinson & Anderson (2003) for a detailed discussion.

Safety barrier systems are also called defenses, safeguards, countermeasures, or protection layers. A safety barrier system may perform one or more safety barrier functions and may usually be split into several safety barrier subsystems and elements.

Classification of Safety Barriers. Safety barriers may be classified according to whether they are active or passive, technical or human/organizational, how often they are demanded, and so on. We introduce briefly some of these classifications.

Proactive Versus Reactive Safety Barriers. Proactive and reactive safety barriers are illustrated in the bow-tie diagram in Figure 1.1.

Proactive safety barrier. A safety barrier that is installed to prevent one or more undesired events in the EUC from occurring. A proactive safety barrier is also called a frequency-reducing barrier because it should reduce the frequency of the undesired event(s).

Reactive safety barrier. A safety barrier that is installed to remove or mitigate the consequences of one or more undesired events in the EUC (if they should happen). A reactive safety barrier is also called a consequence-reducing barrier.

Passive Versus Active Safety Barriers. Safety barriers may also be categorized as passive or active safety barriers:

Passive safety barrier. A barrier whose safety function is always available as an inherent property of the EUC or workplace. Examples of passive safety barriers are fire walls, means for physical separation (e.g., fences, shields), housing used to protect equipment from gas or water intrusion, and so on.

Active safety barrier. The safety function of an active safety barrier is not always available, but will be performed in response to certain events. An ESD system in a process plant is an active safety barrier and is only activated when a dangerous situation occurs.

Only active safety barriers are covered in this book.
Table 1.1 Demand modes for some selected safety barriers.

<table>
<thead>
<tr>
<th>Safety barrier</th>
<th>Low-demand</th>
<th>High-demand</th>
</tr>
</thead>
<tbody>
<tr>
<td>Emergency shutdown system (ESD) in a process plant</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Fire and gas detection in a process plant</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Signaling system for railway applications</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Airbag system in an automobile</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Antilock braking system in an automobile</td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>

Mode of Operation. Safety barriers may be categorized according to how often the barrier functions are demanded. We distinguish between

Demanded mode. These safety barrier functions do not take active part in the control of the EUC and are only activated when a dangerous situation (i.e., a demand, undesired event) occurs. We often distinguish between

- Low-demand mode. A safety barrier is said to operate in low-demand mode when its function is demanded no more often than once per year. The airbag system in an automobile is an example of a safety barrier operating in low-demand mode.

- High-demand mode. A safety barrier is said to operate in high-demand mode when it is exposed to distinct demands that occur more often than once per year. A presence-sensing safeguarding device for a moving robot is (usually) an example of a safety barrier operating in high-demand mode.

Continuous mode. A safety barrier is said to operate in continuous mode when its function is always crucial. In this case, the safety barrier is integrated with the EUC control system, and an undesired event will occur when the safety barrier fails. Examples of safety barriers operating in continuous mode are (i) fly-by-wire systems for flight control of aircrafts and (ii) dynamic positioning systems (DPS) for ships and offshore platforms.

Some examples of safety barrier systems that operate in low-demand and high-demand mode are listed in Table 1.1.

Technical Versus Human/Organizational Safety Barriers. Safety barriers may also be classified according to their nature.

Technical safety barriers. A technical safety barrier is a safety barrier where the barrier function is performed by a technical system. Technical safety barriers may partly be based on E/E/PE technology.

Human and organizational safety barriers. A human barrier is a safety barrier where the barrier function is carried out by one or more persons, sometimes by using technical safety barrier elements. The term organizational safety barrier is used
to designate safety barriers in the form of laws, regulations, procedures, training, and so on.

1.1.3 Layers of Protection

In the process industry, safety barriers are often called *layers of protection* or *protection layers* and are sometimes visualized as in Figure 1.2, where the layers are drawn in the sequence they are activated. Following this sequence, it is distinguished between:

(a) Process design (by using inherently safe design principles).

(b) Control, using basic control functions, alarms, and operator responses to keep the system in normal (steady) state.
(c) Prevention, using safety-instrumented systems (SISs) and safety critical alarms to act upon deviations from normal state and thereby prevent an undesired event from occurring.

(d) Mitigation, using SISs or functions implemented by other technologies, to mitigate the consequences of the undesired event. Examples include the protection that is provided by pressure relief valves.

(e) Physical protection, using permanent (and more robust) safety barriers to enhance the mitigation. Examples include the protection that is achieved by having dikes and barricades in place.

(f) Fire and gas detection and distinguishing, as a third strategy to mitigate the consequences by avoiding ignition, and thereby an accident, in relation to explosive gases and mixtures.

(g) Emergency response, using various means to limit the severity of the accident, locally as well as in the community. Examples include rescue procedures, mobilization of rescue teams, and use of emergency exits.

1.1.4 Safety Performance Criteria

A simplified demanded SIS or technical safety barrier is illustrated in Figure 1.3. The safety barrier is installed in an EUC to reduce the risk related to a specific type of demands that occurs with frequency \( \lambda_{de} \) (see Chapter 5). The objective of the safety barrier is to stop the demands or to reduce the frequency or consequences of the demands. In most cases, the safety barrier is not 100% effective and some demands may pass the safety barrier and have negative effects on the EUC. The frequency of these negative effects is denoted \( \lambda_{effect} \). If the safety barrier were not installed, all the demands would have negative effects. We may therefore use the relative reduction of the demand frequency as a measure of the risk-reduction performance of the safety barrier as

\[
\text{Risk reduction}_1 = \frac{\lambda_{de} - \lambda_{effect}}{\lambda_{de}} = 1 - \frac{\lambda_{effect}}{\lambda_{de}}
\]

Reactive safety barriers are installed in the EUC to remove or reduce the consequences of demands. The risk-reduction performance of these safety barriers can be assessed based on the relative reduction of the consequences obtained. Let \( C_{\text{without}} \) and \( C_{\text{with}} \) be the assessed consequences of demands without and with the safety barrier, respectively. The risk-reduction obtained is then

\[
\text{Risk reduction}_2 = \frac{C_{\text{without}} - C_{\text{with}}}{C_{\text{without}}} = 1 - \frac{C_{\text{with}}}{C_{\text{without}}}
\]

**Categories of Safety Performance Criteria.** The main performance criteria for an active safety barrier are related to:

Functionality/effectiveness. This criterion concerns how effectively the safety barrier can reduce the risk related to a specific demand, and also the safety barrier's ability to handle different situations and variants of the demand.

Reliability/availability. An active safety barrier can never be completely reliable and available. The reliability and availability (see Chapter 5) are therefore important performance measures.

Response time. To reduce the risk, the safety barrier must often be activated quickly. Sometimes, a maximal response time is specified as part of the functional requirements.

Robustness. The safety barrier must sometimes function in hazardous situations where it is exposed to external stresses. It is therefore important that the safety barrier is robust and not vulnerable to these stresses. This criterion is sometimes referred to as survivability (e.g., see NORSOK S-001, 2008).

1.1.5 Safety-Instrumented Systems

A SIS consists of at least three subsystems:

1. Sensor subsystem – detects a potential danger and produces an appropriate electrical signal that is sent to the logic solver. Examples of sensors are pressure transmitters, level transmitters, temperature gauges, and so on.

2. Logic solver subsystem – detects the electrical signal exceeding a given threshold and sends a signal to the final elements. Logic solvers can be computers, programmable electronic controllers (PLCs), and relay circuits.

3. Final element subsystem – performs the safety function. Examples of final elements are shutdown valves, circuit breakers, motors, fans, and so on.

The three subsystems must act in concert to detect the deviation (i.e., demand) and bring the EUC into a safe state. In brief, a SIS shall detect, react, and avert. A sketch of a simple SIS that is used for pressure protection of a pipeline is shown in Figure 1.4. Three pressure transmitters monitor the pressure in the pipeline and
send this information to the logic solver subsystem. The logic solver compares the received values with predefined set points and, when high pressure occurs, a signal is sent to the two shutdown valves (SDVs) to close the flow in the pipeline.

Each subsystem can have one or more channels. The sensor subsystem in Figure 1.4 has three channels (i.e., pressure transmitters) and the final element subsystem has two channels (i.e., shutdown valves).

**Functional Safety.** Safety is often defined as a state where the risk has been reduced to, and is maintained at, a level that is as low as reasonably practicable (ALARP) and where the remaining risk is generally accepted. Most well-designed EUCs that are exposed to hazards have a control system and one or more safety barriers that protect the EUC and the environment from being harmed by the hazards. The control and safety barrier functions are more and more often being carried out by E/E/PE technology, with increasingly complex software.

The term *functional safety* is used in the title of the important standard IEC 61508, and this term is therefore used to denote the part of the overall system safety that depends on the correct functioning of active control and safety systems. Functional safety relies on active safety barriers, while passive safety barriers are not part of functional safety.

IEC 61508 and associated standards are often called *functional safety standards*.

### 1.2 Objectives and Scope

This section outlines the objectives and the scope of the book. In addition, the author presents some views on the importance of the subject area.

#### 1.2.1 Objectives

The main objective of this book is to provide a comprehensive introduction to reliability assessment of SISs and the various parts of such systems.

More specific objectives are:

(a) To present the terminology used in reliability assessment of a SIS.
(b) To identify and classify the possible failure modes of a SIS.

(c) To define and discuss relevant reliability measures for a SIS.

(d) To present models and methods that can be used to analyze and quantify the reliability of a SIS and to discuss the adequacy of each method.

(e) To discuss problematic issues, such as common-cause failures and imperfect proof-testing, and show how these issues can be incorporated into the reliability analysis.

(f) To discuss negative side effects of a SIS in the form of spurious trips.

(g) To discuss the uncertainty of the reliability measures that are produced by the various analyses.

1.2.2 Scope

The book is directed towards suppliers, system integrators, and users of SISs, along with reliability analysts who carry out the required analyses in the design and development stages of the systems. The terminology and the presentation in the book are adapted to IEC 61508.

Although the focus is on the reliability of a SIS, most of the methods presented in the book are also relevant for safety systems based on other technologies, such as mechanical, hydraulic, and/or pneumatic devices.

1.2.3 Delimitation

The book is limited to reliability analysis of the hardware of SISs. Software, human, and organizational issues are not treated in the book.

The operational phase of a SIS is not addressed in any detail in this book. In this phase, the system operator (called the end-user in this book) has to verify that the required reliability of the SIS is maintained by testing, maintenance, modifications, and updating of reliability analyses. For this purpose, it is important that the end-user is familiar with the reliability analyses that have been used to prove compliance with IEC 61508 and the strengths and weaknesses of these analyses. The book should therefore also be of interest to SIS end-users.

The reasons why software reliability is not treated in the book are twofold: (1) quantitative software reliability analyses are not required to claim compliance with IEC 61508, and (2) software reliability assessments are usually done by software specialists and not by traditional system reliability engineers, who are the intended readers of this book.

1.2.4 The Importance of Functional Safety

Every day, people are injured and killed, large material and financial assets are lost, and the environment is polluted because of failures of safety-critical systems and
lack of functional safety. The accidents may range from single-person accidents up to disasters such as the Macondo accident in the Gulf of Mexico in 2010 and the Fukushima Daiichi nuclear power accident in Japan in 2011. If the safety-critical systems had functioned as intended, many of these accidents might have been avoided.

The next section presents briefly a number of functional safety standards. The objective of these standards is to ensure that SISs are specified, designed, manufactured, installed, and operated such that they will reliably perform their intended safety functions. To achieve a sufficiently high reliability, a number of detailed reliability analyses have to be performed, especially in the design phase. The intention of this book is to help reliability analysts to perform adequate reliability analyses that can contribute to improving the functional safety.

System designers are trained to develop systems that are able to perform the desired functions, but they often forget to consider how the systems can fail. This is the role of reliability engineers and reliability analysts who should be part of the design team. A number of analytical methods are available for identifying potential system failures and the causes of these failures. Some of the methods are qualitative, some are quantitative, and some are both qualitative and quantitative. The most important output from the reliability analyses is the improved understanding of how the system may behave and how it can fail in the different operational situations. This knowledge can help the design team to improve the system reliability and to avoid failures.

The quantitative reliability measures that are produced from the reliability analyses are important but sometimes get too much focus. The quantitative methods described in this book will, in many cases, give approximately the same reliability measures and we may therefore ask whether it is necessary to learn to use more than one method. The answer to this is that by using different methods, you will understand different aspects of the proposed design. In this book, you will, for example, learn the two methods of fault tree analysis and Petri net analysis. By using fault tree analysis you will understand how combination of component failures can produce system failures and by Petri net analysis, you will better understand the dynamic features of the system. The quantitative results obtained by the two methods are, however, rather similar.

Some people claim that reliability analysis is only playing with numbers and has no real value. The author disagrees with these statements. As reliability analysts, we can make a big difference; we can improve the reliability of safety-critical systems, avoid failures, and even prevent accidents. In many cases, we can contribute to saving lives—even the lives of our loved ones.

What we, as reliability engineers or reliability analysts, have to do is to obtain a thorough knowledge of the tools and methods we are using and carry out our job with the seriousness it deserves. The author hopes that this book can help you to do an even better job.
1.3 Functional Safety Standards

This section gives a brief survey of some of the most important functional safety standards.

1.3.1 The Generic IEC 61508 Standard

The international standard *Functional safety of electrical/electronic/programmable electronic safety-related systems* (IEC 61508, 2010) is a generic, performance-based standard for safety-related systems that involve E/E/PE technology. IEC 61508 provides a basis for specification, design, and operation of all types of SISs. The objective of the standard is to give overall requirements and to serve as a basis for development of sector-specific standards.

IEC 61508 has several main characteristics. First is the *life cycle approach* that defines the necessary requirements for a SIS "from cradle to grave." Another main characteristic is that it is *risk-based*, such that requirements for the SIS have to be based on a risk assessment.

The standard has seven parts (see box) and introduces 16 life cycle phases, which may be split into five main stages.

1. *Risk assessment* (covering phases 1-5), the outcome of which is the formulation of the required safety functions and the associated reliability targets.

2. *Design and construction* (covering phases 9-11), the outcome of which is a SIS comprising hardware and software elements.

3. *Planning* for integration, overall validation, and operation and maintenance (covering phases 6-8).

4. *Operation and maintenance*, including management of change (covering phases 14-15). Any change to the SIS should initiate a return to the most appropriate life cycle phase when a modification has been requested.

5. *Disposal*, which ends the life of the SIS.

The life cycle phases are further described in Chapter 2.

1.3.2 Sector-Specific Standards

Sector-specific standards related to IEC 61508 have been developed for several sectors, such as process industry, machinery systems, nuclear power plants, railway applications, and automotive industry. This section gives a brief introduction to some of these standards.

*Process Industry.* The standard *Functional safety – Safety instrumented systems for the process industry sector* (IEC 61511, 2003) is based on IEC 61508 and is the
IEC 61508:  
Functional safety of electrical/electronic/programmable electronic safety-related systems  

Normative parts:  

PART 1: General requirements  
Defines the overall safety life cycle model. The standard employs qualitative or quantitative techniques to identify the process risk to the safety-related system. These techniques focus on project management, quality assurance, and configuration management.  

PART 2: Requirements for electrical/electronic/programmable electronic safety-related systems  
Provides objectives for the safety development of the E/E/PES. Software is further defined in Part 3. However, it should be noted that Part 2 maintains jurisdiction.  

PART 3: Software requirements  
Provides objectives for the safety development of the software residing in the E/E/PES.  

PART 4: Definitions and abbreviations  
Contains definitions, abbreviations, and terminology used in the safety process that must be adhered to in order to establish and maintain consistency.  

Informative parts:  

PART 5: Examples of methods for the determination of safety integrity levels  
Provides the formal approach for determining the safety integrity level (SIL) of the safety system (SIL is described in Chapter 2).  

PART 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3  
Provides specific guidelines for applying IEC 61508 parts 2 and 3.  

PART 7: Overview of techniques and measures  
Provides details of the safety techniques and measures relevant to parts 2 and 3.  

Supplement:  

PART 0: Functional safety and IEC 61508  
This is a technical report (TR) with number IEC/TR 61508-0 and is not formally a part of IEC 61508. Part 0 explains and gives comments to the standard.  

In this book, reference to the parts of the standard is given as IEC 61508-1, and so on.  

Main standard for the application of SISs in the process industry, including the oil and gas industry.  
IEC 61511 is mainly concerned with SISs operating in low-demand mode, that is, where demands for the SIF are discrete events that occur rather infrequently. The SIS is consequently an independent protection layer in addition to the basic process control system (BPCS). The SIS does not play any active role during normal operation and is only activated if a demand should occur.  
IEC 61511 applies when a SIS is based on proven technology or technology whose design has been verified against the requirements in IEC 61508. Development of new technology is beyond the scope of IEC 61511. For this reason, IEC 61511 is
IEC 61511: *Functional safety. Safety instrumented systems for the process industry sector*

**PART 1:** *Framework, definitions, system, hardware and software requirements*

**PART 2:** *Guidelines for the application of IEC 61511-1*

**PART 3:** *Guidance for the determination of the required safety integrity levels*

IEC 61511 is the sector-specific standard for the process industry, including the oil and gas industry. In this, SISs are assumed to operate mainly in low-demand mode.

sometimes called the end-user's and system integrator's standard, whereas IEC 61508 is called the manufacturer's standard.

Guidelines have been published to ease the application of IEC 61508 and IEC 61511. Two notable guidelines are:


- *Application of IEC 61508 and IEC 61511 in the Norwegian Petroleum Industry* published by the Norwegian Oil and Gas Association (NOG-070, 2004).

► **Remark:** The process industry has traditionally separated control functions and safety functions. The aim is to avoid a failure in the control system having an impact on the SIS. Despite this advantage, there are now many industry applications where control and safety functions are integrated, sometimes motivated by cost and efficiency. Merging control and safety may also be due to space limitations that pose restrictions on the design philosophy.

**Machinery Systems.** Machinery safety in Europe is regulated by the EU Machinery Directive (EU-2006/42/EC, 2006). The first edition of this directive was approved in 1989 and it has been amended and updated several times. The EU Machinery Directive gives the essential health and safety requirements (EHSRs) related to design and use of machinery and leaves the details to harmonized standards. It is not mandatory to follow the standards, but if one complies with a harmonized standard, the associated EHSR is fulfilled.

SISs have a high priority in the Machinery Directive and the EHSRs related to such systems are listed in §1.2. The first few lines of these requirements are:

Control systems must be designed and constructed in such a way as to prevent hazardous situations from arising. Above all, they must be designed and constructed in such a way that:

- they can withstand the intended operating stresses and external influences,

- a fault in the hardware or the software of the control system does not lead to hazardous situations,
– errors in the control system logic do not lead to hazardous situations,
– reasonably foreseeable human error during operation does not lead to hazardous situations.

The first standard that was developed for machinery control systems was EN 954-1 (1997). As the requirements of the EU Machinery Directive have been accepted and implemented in the national laws of many countries around the world, the related EN standards have been transferred into international standards. The EN 954-1 was therefore transferred, in a slightly modified form, into ISO 13849-1 (2006). The EN 954-1 was developed before the IEC 61508 was made and consequently does not fully comply with IEC 61508. The same applies for ISO 13849-1.

Another standard, IEC 62061 “Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems” was therefore developed, based on IEC 61508. Today, both ISO 13849-1 and IEC 62061 are accepted as harmonized standards related to E/E/PE based control systems of machinery. The relationship between ISO 13849-1 and IEC 62061 is described in the technical report IEC TR 62061-1.

When discussing control of machinery systems, we will only refer to IEC 62061 in the rest of this book. In this standard, a SIS is called a safety-related electrical control system (SRECS). A special standard has been developed for risk assessment of machinery. This is ISO 12100 “Safety of machinery – General principles for design – Risk assessment and risk reduction.” SISs in machinery systems mainly operate in high-demand or continuous mode and are often integrated with the machinery control system.

**Nuclear Power Industry.** The standard IEC 61513 (2004) was developed as a sector-specific standard for the nuclear power industry, based on IEC 61508. In IEC 61513 a SIS is called an instrumentation and control (I&C) system and is defined as a “system, based on electrical and/or electronic and/or programmable electronic technology, performing I&C functions as well as service and monitoring functions related to the operation of the system itself.” IEC 61513 is not further discussed in this book.

**Automotive Industry.** ISO 26262 (2011) is the sector-specific standard for road vehicles under IEC 61508. It was developed for electric and/or electronic systems installed in series production passenger automobiles with a maximum gross vehicle mass up to 3 500 kilograms. The standard has nine normative parts and a guideline for the use of ISO 26262 as part 10. The standard is not further discussed in this book.

**Railway Transport.** Three European norms: EN 50126, EN 50128, and EN 50129, have been developed with a scope similar to IEC 61508. The three EN-norms have later been transferred into IEC-standards.


– IEC 62279 (EN 50128). Railway applications – Communications, signaling, and processing systems – Software for railway control and protection systems.

The three standards do not have the format of sector-specific standards related to IEC 61508, but meeting the requirements in these standards is considered to be sufficient to ensure that the requirements in IEC 61508 are met.

MODSafe (Modular urban transport safety and security analysis) is an EU research project under the Seventh Framework Program. MODSafe developed knowledge and methods for the analysis of safety-related systems in urban guided transport systems (i.e., light trains, metros, and trams). A number of MODSafe reports discuss issues in the interface between the approach described in the three railway standards and in IEC 61508. The reports are available on the project’s web page http://www.modsafe.eu. Several of these reports give additional insight to many chapters of this book.

1.4 The Main Elements of a SIS

The main elements of a SIS are input elements, logic solver, and final elements. These elements are briefly introduced in this section. A more detailed account of these elements and the technologies used in a SIS is given by Goble & Cheddie (2005); Macdonald (2004a,b); Gruhn & Cheddie (2006); CCPS (2007).

1.4.1 The Fail-Safe Principle

A SIS element can be designed according to two different principles:

Energize-to-trip. The SIS element is de-energized during normal operation and need to be energized (e.g., by electricity, hydraulic pressure, pneumatic pressure) to perform its safety function (i.e., to trip). Loss of energy will, by this principle, prevent the element from performing its safety function.

De-energize-to-trip. The SIS element is energized during normal operation and removal of the energy will cause a trip action. By this principle, loss of energy will cause a spurious (i.e., false) activation of the safety function.

Many SIS elements are today designed according to the de-energize-to-trip principle. This principle is also a basis for the fail-safe principle.

Fail-safe. A design property that causes a SIS element to go to a predetermined safe state in the event of a specific failure or malfunction.

An illustration of the fail-safe principle is given in Example 1.5.

1.4.2 Input Elements

Input elements are used to monitor a certain process or EUC state, for example, temperature, pressure, level, or flow. Input elements may be based on a wide range of
principles and may be designated using terms such as switches, sensors, transmitters, and transducers. A pressure transmitter in a pipeline, comprising a sensing element and a transducer, is illustrated in Figure 1.5.

Many input elements have additional built-in electronics and software and are sometimes referred to as smart sensors. A smart sensor may be able to

- Preprocess the readings (measurements) into meaningful quantities
- Store previous readings and compare with current readings
- Perform self-testing related to some possible failures of the sensor (referred to as diagnostic testing)
- Communicate deviations to the logic solver
- Remember configuration settings

EXAMPLE 1.4 Fire and gas detectors in the process industry

A variety of fire and gas detectors are used in the process industry. Some examples are:

- Infrared (IR) flame detectors
- Camera-based flame detectors
- Ultraviolet (UV) flame detectors
- Combined IR/UV flame detectors
- Ionization point smoke detectors
- Optical point smoke detectors
- Laser point smoke detectors
- Beam smoke detectors

- Aspiration smoke detectors
- Camera-based smoke detectors
- Point heat detectors
- Linear heat detectors
- Infrared absorption combustible gas detectors
- Catalytic gas detectors
1.4.3 Logic Solver

The logic solver determines, based on signals from the input elements, whether an abnormal situation has occurred and initiates the required actions. The logic solver is the “brain” of the SIS and may be based on electrical relays, electronic components (e.g., printed circuit boards), programmable logic controllers (PLC), or computers.

Programmable logic controller. A programmable logic controller (PLC) is a digital computer used for automation and safety of electromechanical processes, such as control of machinery, shutdown systems, and so on. A PLC is typically designed for multiple input and output arrangements and is more robust than a normal computer.

A PLC comprises input cards, one or more central processing units (CPUs), output cards, and associated cables for communication. The logic is mainly implemented by software. The use of software reduces the hardware costs and makes it easier to implement modifications, but, at the same time, it leads to more complex systems with the added features that come with the software. The main elements of a logic solver are illustrated in Figure 1.6.

A logic solver can also be relay-based, sometimes referred to as direct-wired logic, because the input elements interact directly with the final elements via electrical relays. Printed circuit boards are sometimes called solid state logic, and have a fixed (printed) arrangement of electronic components, such as resistors, capacitors, transistors, diodes, and so on.

The decision taken by the logic solver on how to act on the input signals is determined by how the signals are voted. If the input signals are voted \(k\)-out-of-\(n\), the safety function is performed when \(k\)-out-of-\(n\) input elements raise an alarm. The voting may be implemented by software, hardware, or a combination of both depending on the technology being used.

A SIS may use more than one logic solver to perform the safety functions. This approach is sometimes used in railway signaling systems, where two logic solvers (i.e., 2-out-of-2) have to agree on setting a green (go) signal, while it is sufficient that one of the two logic solvers (i.e., 1-out-of-2) sets a red (stop) signal.
1.4.4 Final Elements

Final elements are also called *actuating devices* and may be valves, relays, circuit breakers capable of stopping flow and isolating electrical equipment, and many more. To improve safety and reliability, more than one final element is sometimes used to perform the same function. The physical installation may sometimes determine how the final elements are voted. If two shutdown valves are installed in the same pipeline, it is, for example, sufficient that 1-out-of-2 valves closes to stop the flow.

**EXAMPLE 1.5 Shutdown valve in a subsea oil/gas production tree**

Figure 1.7 is a sketch of a gate valve that is used as a shutdown valve in a subsea oil/gas production tree. The production tree is often called a X-mas tree and the valve is therefore also called a X-mas tree valve. The valve has two main parts: (1) a valve housing where the closing element, called the gate, is a solid steel block with a hole that has the same diameter as the flowtube (normally a diameter of 4.5 to 7 inches), and (2) a hydraulically operated fail-safe actuator where the fail-safe function is accomplished by a strong steel spring. In normal operation, the valve is open (i.e., the hole in the gate is in line with the flowtube) and is kept open by applying hydraulic pressure to the actuator. The hydraulic pressure compresses the steel spring. The valve is therefore said to be normally energized. When the hydraulic pressure is bled off, the valve will close by the spring force and fulfills the *de-energize-to-trip* principle. If there is a leakage in the hydraulic system, the pressure will also be bled off and the valve will go to the safe state "closed." The valve is therefore said to have a *fail-safe* design.

---

2Figure 1.7 is reproduced from Rausand & Hayland (2004) with permission from John Wiley & Sons.
3Read as Christmas tree.
Solenoid valves are normally used to control the hydraulic supply to and from the actuator. A solenoid valve is also called a *pilot valve*.

### 1.5 A Brief History

Many safety initiatives only gain momentum after a major accident. One such accident happened in 1976 at a chemical plant in Seveso, Italy, producing pesticides and herbicides. The accident was triggered by an uncontrolled overheating reaction whose excess pressure destroyed a plant safeguard and released a large cloud of toxic dioxin to the environment. The reactor in question featured no automatic cooling systems and there were neither warning systems nor alarm plans in the installation.

The Seveso accident was the main background for the EU directive on *major accident hazards of certain industrial activities*, also called the Seveso Directive. The Seveso Directive has been amended and updated several times and the most recent version is the Seveso III Directive that was approved in 2012 (EU, 2012).

After the major accidents in Flixborough, UK (1974), Seveso (1976), Bhopal, India (1984), and Piper Alpha in the North Sea (1988), initiatives were taken in many countries to develop regulations and standards that would minimize the risk related to industrial accidents for citizens. In Germany, the important standard DIN V 19250, *Control technology: fundamental safety aspects to be considered for measurement and control equipment*, a forerunner to IEC 61508, was issued in 1989, and the Seveso I directive was adopted in German law with reference to DIN V 19250.

According to DIN V 19250, safety systems should be designed to meet certain safety classes, class 1 through class 8. The class should be chosen based on the level of risk of the process (i.e., the EUC). The standard therefore forces the users to determine the hazards involved in their processes and the integrity of the safety-related systems that would be required. The harmonized standard EN 954-1 to the EU Machinery Directive on control system of machinery was developed in parallel with DIN V 19250. After being adopted in IEC 61508, DIN V 19250 was withdrawn in 2004.

As programmable electronic systems (PESs) made their entrance into safety systems, there was increased concern about how to determine whether the design of the PES was sufficiently reliable for the application and for the DIN V 19250 class. The standard DIN V VDE 0801 *Principles for computers in safety-related systems* was developed in 1990 to address these concerns. The two German standards provided a mechanism for relating risk to PES integrity, but it was always understood that risk reduction had to include the evaluation of the complete SIS.

PESs have been in use for several decades but formal requirements for the reliability of such systems are more recent. One of the first guidelines was the *Guidelines for use of PES for Safety Related Applications* in two parts that was published by the UK HSE in 1987. These guidelines highlighted the need for high levels of safety at every stage of the design, installation, and operation of PES. The safety life cycle concept was formalized whereby safety was not restricted to any particular phase of
a system's design process but spanned the entire design process and continued into commissioning, operation, and maintenance.

In 1996, the US-based International Society of Automation published the standard ISA S84.01 Application of Safety Instrumented System for the Process Industries, and the standard also became an American National Standards Institute (ANSI) standard the same year. The term SIS was first introduced in the United States through this process industry standard. A second edition, ANSI/ISA 84.00.01 (IEC 61511 Mod), was approved in 2004 and is similar to IEC 61511.

The globalization of the process industry during the 1980s and 1990s resulted in a demand for international practices rather than national practices and guidelines for safety systems (CCPS, 2007). The main answer to this demand was IEC 61508. The first edition of the standard was issued in 1997, and the second edition came in 2010, following a thorough review and commenting process by national and international committees.

IEC 61508 and the related sector-specific standards are not harmonized standards according to EU law and are not automatically mandatory unless they are referenced by national authority regulations. Such a reference is, for example, given in the Norwegian Petroleum Safety Authority (PSA) regulations.

1.6 Structure of the Book

This book has 14 chapters, an appendix, and lists of acronyms and symbols used. Chapter 1 gives a brief introduction to the issues that are treated in the book, and presents the objectives and the scope of the book. The book is closely related to a number of international standards and a brief survey of these standards are therefore given with focus on the main “mother” standard, IEC 61508. The main subject of the analyses, a SIS, is briefly described together with its building blocks. A brief historical account of the development of the subject area is also given, mainly as seen from Europe and the United States.

Chapter 2, Concepts and Requirements, presents the main concepts that are related to reliability assessment of a SIS. The quantitative requirements in IEC 61508 and its sector-specific standards are described and put into a safety life cycle framework. The concepts of safety integrity and safety integrity level (SIL) are presented and the reliability measures that are used to document compliance with a specific SIL are introduced.

Chapter 3, Failures and Failure Analysis, defines the main concepts related to failures of a SIS. Among these are random hardware failures versus systematic failures, detected versus undetected failures, and so on. It is very important for the rest of the book to understand these concepts, so spending some time on this chapter is worthwhile. The failure analysis methods FMECA and FMEDA are also introduced briefly in this chapter.

Chapter 4, Testing and Maintenance, is a brief chapter that introduces the ways a SIS is tested and maintained. It is important here to distinguish between proof testing and diagnostic testing.
Chapter 5, *Reliability Quantification*, is a long chapter, which introduces models and methods that can be used to determine the reliability of a system. The presentation is general, but most of the examples are related to SISs. Readers who are familiar with reliability analysis do not need to read the whole chapter, but should check that they are familiar with the terminology used. The following chapters are based on Chapter 5 and give many references to this chapter. To understand the next chapters, it is therefore important to understand the material in Chapter 5.

Chapter 6, *Reliability Data Sources*, is a short chapter that introduces the data required for a reliability assessment of a SIS. Several generic data sources are described and the quality of the available data is briefly discussed. The chapter ends with a discussion of how to obtain parameter estimates for a special application, so-called plant-specific reliability data.

Chapter 7, *Demand Modes and Performance Measures*, is a short chapter that discusses the different demand modes and operational strategies or a SIS, and the implication for choice of reliability measure. A data set is supplied as a basis for the examples that are given in the following chapters.

Chapter 8, *Average Probability of Failure on Demand*, shows how the models and methods introduced in Chapter 5 can be used to determine the PFD_{avg} of a SIS. All the methods suggested in IEC 61508-6, are discussed and formulas are explained and extended to general systems. A number of worked examples are presented and discussed. This chapter is the most important chapter of the book and is long.

Chapter 9, *Frequency of Dangerous Failures per Hour*, is the parallel to Chapter 8, but applied to high-demand and continuous demanded systems. New approximation formulas, extending the formulas in IEC 61508-6, are presented and applied in worked examples. The chapter is shorter than Chapter 8 because some of the approaches that are used to determine the PFD_{avg} can also be used to determine the PFH.

Chapter 10, *Common-Cause Failures*, deals with common-cause failures (CCFs), how they influence the reliability of a SIS, and presents and discusses several approaches to include the effect of CCFs in the reliability assessments. The main focus is on the beta-factor model and the multiple beta-factor model that is an integral part of the PDS method (SINTEF, 2013b). Approaches to determine the beta-factor are outlined.

Chapter 11, *Imperfect Proof Testing*, discusses possible causes of imperfect proof testing and how imperfect proof testing can be incorporated into reliability models.

Chapter 12, *Spurious Activation*, discusses the undesired side effects a SIS has to give spurious activation or spurious trips. New formulas are developed for the spurious trip rate (STR). The formulas are illustrated in several worked examples.

Chapter 13, *Uncertainty Assessment*, discusses the uncertainty of the PFD_{avg} and PFH estimates that are determined by the methods described in this book. The chapter introduces the various categories of uncertainty, such as aleatory and epistemic uncertainty, and classifies uncertainty as completeness, model, and parameter uncertainty.
Chapter 14, Closure, gives some concluding remarks and presents the author's views of the application of the material presented in the book. Several topics that need further research are listed.

The appendix section gives a brief introduction to probability theory and provides lists of acronyms and symbols used in the book.

1.7 Additional Reading

The following titles are recommended for further study related to Chapter 1:


- Safety Instrumented Systems Verification: Practical Probabilistic Calculation (Goble & Cheddie, 2005) has more focus on reliability quantification than the two first books, but can still be considered a supplement to the current book.