TU/e technische universiteit eindhoven

NTNU Det skapende universitet

Human and organisational factors in the operational phase of safety instrumented systems: A new approach

Master's Thesis

Martin Schönbeck

13th June 2007

Martin Schönbeck, student number: 493542
Graduate programme in Industrial Engineering and Management Science

This master's thesis is submitted at:
Eindhoven University of Technology (TU/e)
Department of Technology Management
Section of Quality and Reliability Engineering

The research has been carried out at:
Norwegian University of Science and Technology (NTNU)
Faculty of Engineering Science and Technology
Department of Production and Quality Engineering
Section of Reliability, Availability, Maintainability, and Safety

Thesis supervisors:
dr. ir. Jan Rouvroye (TU/e)
professor Marvin Rausand (NTNU)

Abstract

This thesis presents a new approach to address human and organisational factors in the operational phase of safety instrumented systems. This approach gives a prediction of the operational SIL and can be used to improve safety. It shows which human and organisational factors are most in need of improvement and it provides guidance for preventive or corrective action.

Summary

Computer-based safety systems are increasingly used in many different applications, ranging from automatic train stop systems to emergency shutdown systems in chemical plants. Such computer-based safety systems, composed of sensors, logic solvers and actuating items, are often referred to as *safety instrumented systems.* A very important aspect of a safety instrumented system is its reliability, and reliability certification of such systems has received a lot of attention during the past decade with the emergence of the new international standard IEC 61508. This standard requires quantification of the achieved risk reduction, expressed as a *safety integrity level* (SIL).

The required SIL is based on a hazard and risk analysis, combined with risk acceptance criteria. Next, the standards sets out quantitative and qualitative requirements for the design and implementation of safety instrumented systems in order to achieve the required risk reduction. Human and organisational factors affect the performance of safety instrumented systems during operation and may threaten the achieved SIL, but this is usually not explicitly accounted for. Therefore, the main objective of this research is to develop an approach to assess the impact of human and organisational factors on the achieved SIL in the operational phase of safety instrumented systems.

This research objective is translated into a research model, leading to two research questions: (1) *What is the contribution of existing theories and models for human and organisational factors to the operational phase of safety instrumented systems?* and (2) *Which relationship can be established between human and organisational factors and the achieved SIL in the operational phase of safety instrumented systems?* To answer these questions, a theoretical approach based on scientific literature is followed, combining existing theories and models and adapting them to a specific domain.

Human errors contribute significantly to accidents and system failure, and there are many theories that seek to explain human error. Nowadays, it

is widely recognised that human errors often are caused by aspects of the working environment and the organisation, thus shifting focus from human errors to the underlying human and organisational factors. Several models are available that link safety with human and organisational factors, ranging from qualitative accident investigation models to quantitative methods to include human and organisational factors into probabilistic safety assessment. The *Swiss cheese model* of organisational accidents (Reason, 1997) is highly relevant for the operational phase of safety instrumented systems, because it visualises the influence of human and organisational factors on the performance of safety barriers (in this case, safety instrumented systems). Furthermore, it can be used to predict the general likelihood that an accident may happen. Among the quantitative models, the ARAMIS approach (Duijm & Goossens, 2006) is particularly interesting, because it directly links organisational factors to the reliability of safety barriers.

To develop an approach to assess the impact of human and organisational factors on the achieved SIL, eight safety influencing factors are formulated, based on the Swiss cheese model. These factors are then linked to the achieved SIL using a quantification procedure similar to the ARAMIS approach. The resulting approach consists of five steps and gives a prediction of the achieved SIL during operation (the *operational SIL*), which may be lower than the achieved SIL upon system start-up (the *design SIL*), due to the impact of human and organisational factors. The calculation of the operational SIL is based on the proportion of the design SIL that can be explained by human and organisational factors, the relative weights of the safety influencing factors, and the state of each safety influencing factor, which is measured during an audit using checklists. The approach can also be used to improve safety; it shows which safety influencing factors are most in need of improvement and it provides guidance for preventive or corrective action. The approach has not (yet) been applied in practice, and there are some issues that need further consideration. To validate the approach, field data from the real operation of safety instrumented systems could be used.

An illustrative case study shows the preventive character of the approach: improve relevant human and organisational factors before they threaten the achieved SIL. Furthermore, the proposed approach can be used as part of a SIL monitoring strategy in order to maintain the achieved SIL at the required level during the operational phase. Further research is needed to explore other issues that should be followed up in the operational phase of safety instrumented systems, and to assess their impact on the operational SIL.

Preface

The topic of this master's thesis is a truly multidisciplinary one: it combines the rather technical area of safety and reliability with insights from sociology and psychology. Given my educational background from the graduate programme in Industrial Engineering and Management Science at TU/e, complemented with a number of courses in social sciences at NTNU, it gave me the opportunity to integrate totally different parts of my studies. The project has of course had its ups and downs, and from time to time I have experienced a quite heavy workload, but I dare to say that I am pleased with the results. Special thanks go to my thesis supervisors, Jan Rouvroye at TU/e and Marvin Rausand at NTNU, for their enthusiastic support and constructive criticism, as well as for their availability and fast feedback. Furthermore, I would like to thank Aarnout Brombacher at TU/e and Jan Ola Strandhagen at NTNU for their assistance in the initial stage of this international research project.

Trondheim, June 2007

Martin Schönbeck

Contents

Chapter 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, making them more flexible, but also more complex. The question is: can we rely on these complex, computer-based safety systems? Reliability certification of such systems has received a lot of attention during the past decade with the emergence of the new international standard IEC 61508 (IEC, 2000). This standard is performance-based and requires quantification of the achieved risk reduction.

This chapter gives a brief introduction to computer-based safety systems and to the IEC 61508 standard. Within this context, it outlines the research objective of this thesis. For a general introduction to the reliability of safety systems, the reader is referred to the literature review that has been performed as a preparation for this master's thesis (Schönbeck, 2006).

1.1 Safety instrumented systems

Computer-based systems are increasingly used in safety-critical applications. The benefits of these programmable systems are increased flexibility to change

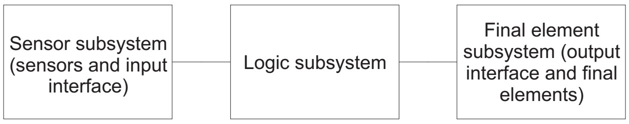
Sensor subsystem (sensors and input interface)
Logic subsystem
Final element subsystem (output interface and final elements)

Figure 1.1: Subsystem structure of a safety instrumented system (IEC, 2000)

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. 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*. The general subsystem structure of a safety instrumented system is shown in Figure 1.1.

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, which the IEC 61508 standard (IEC, 2000) defines as "equipment, machinery, apparatus or plant used for manufacturing, process, transportation, medical or other activities."

A very important aspect of a safety instrumented 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." 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*. On the other hand, a safety instrumented system shall not be activated without the presence of a predefined process demand in the equipment under control. Such a false alarm is called a *spurious trip*.

When assessing the reliability of a safety system in terms of fail to function, two main options exist, depending on the operation mode. If a 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, whereas the probability of a dangerous failure per hour is used for safety systems operating in high demand or continuous mode (Brown, 2000). 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, which use different methodologies that may lead to different results (Rouvroye & Brombacher, 1999).

1.2 IEC 61508 standard

The IEC 61508 standard (IEC, 2000, approved by CENELEC as European standard EN 61508 in 2001) provides a general framework for the design and implementation of safety instrumented systems, which are called "electrical/electronic/programmable electronic safety-related systems" in this standard. This is a generic standard common to several industries, independent of the technology used. A main objective of this standard is to facilitate the development of application specific standards, such as IEC 61511 for the process industry (IEC, 2004, approved by CENELEC as European standard EN 61511 in 2004). The IEC 61508 standard consists of seven parts, some of which are normative, whereas other parts are informative and provide examples and guidelines. An overview of the standard and its different parts is given by IEC (2005). 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 instrumented system, from the initial concept until eventual decommissioning. The safety lifecycle is shown in Figure 1.2.

The IEC 61508 standard requires quantification of the achieved risk reduction, expressed as a *safety integrity level* (SIL). The standard defines four safety integrity levels, where SIL 4 is the highest level and SIL 1 the lowest. Each level corresponds to an interval of the average probability of failure on

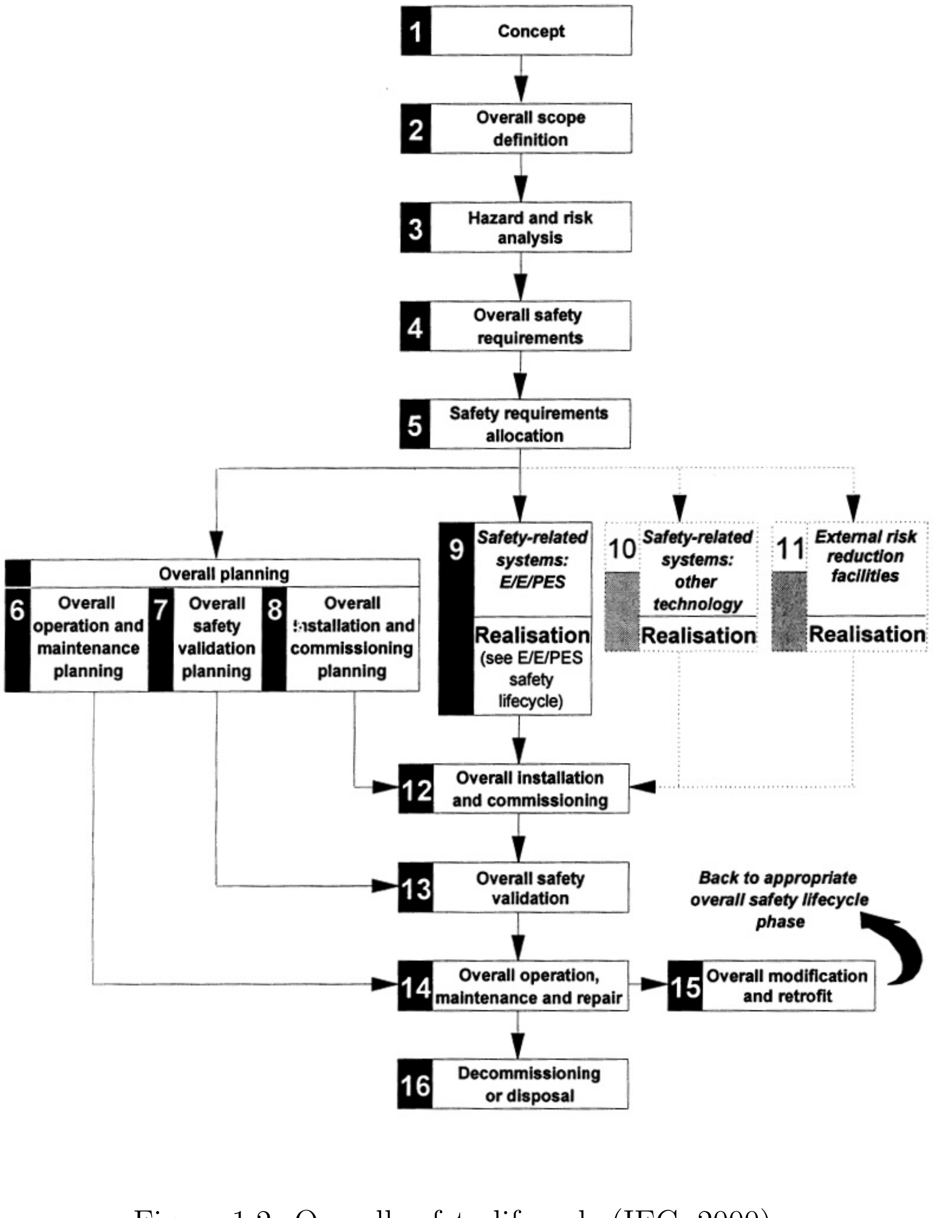
1 Concept
2 Overall scope definition
3 Hazard and risk analysis
4 Overall safety requirements
5 Safety requirements allocation
Overall planning
6 Overall operation and maintenance planning
7 Overall safety validation planning
8 Overall installation and commissioning planning
9 Safety-related systems: 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
14 Overall operation, maintenance and repair
15 Overall modification and retrofit
Back to appropriate overall safety lifecycle phase
16 Decommissioning or disposal

Figure 1.2: Overall safety lifecycle (IEC, 2000)

demand (for low demand mode of operation) and the probability of a dangerous failure per hour (for high demand or continuous mode of operation), as shown in Table 1.1.

Table 1.1: Intervals of the average probability of failure on demand (PFD) and the probability of a dangerous failure per hour (PFH) corresponding to the safety integrity levels (IEC, 2000)

SIL	PFD	PFH
4	$\geq 10^{-5}$ to $< 10^{-4}$	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-4}$ to $< 10^{-3}$	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-3}$ to $< 10^{-2}$	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-2}$ to $< 10^{-1}$	$\geq 10^{-6}$ to $< 10^{-5}$

The *required SIL* is determined based on a hazard and risk analysis, combined with risk acceptance criteria. Next, one or more safety instrumented systems are designed that achieve the required risk reduction (possibly together with safety systems based on other technology). Apart from the quantitative target failure measures shown in Table 1.1, the standard sets out different qualitative requirements for the system design and several other lifecycle phases, depending on the required SIL. Together, these quantitative and qualitative requirements determine for which SIL a safety instrumented system could be qualified upon system start-up, that is, the *achieved SIL*. Generally speaking, the higher the required 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.

Human factors are addressed both explicitly and implicitly in several phases of the safety lifecycle, but there is no specific requirement to analyse these factors quantitatively. Nevertheless, the standard states that the design “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).

1.3 Research objective

Although the IEC 61508 standard takes a lifecycle approach that also includes operation and maintenance, there is little focus on how to ensure that the achieved SIL is maintained at the required level during the operational phase. Most literature is concerned with determining the required SIL and demonstrating the achieved SIL upon system start-up. However, the performance of a safety instrumented system in the operational phase is influenced by many factors; not only by the system design and the related testing and maintenance strategies, but also by the operating conditions in the wider socio-technical system it is part of. This includes both human and organisational factors. These factors may threaten the achieved SIL in the operational phase, but this is usually not explicitly accounted for.

The main objective of this research is to develop an approach to assess the impact of human and organisational factors on the achieved SIL in the operational phase of safety instrumented systems. This involves exploring a range of theories and models for human and organisational factors, as well as reviewing the possible contribution of these theories and models to the operational phase of safety instrumented systems.

1.4 Structure of the thesis

The structure of this master's thesis is a special one, because the main body is written in the form of a research paper. This paper will be submitted for publication to a scientific journal, possibly slightly revised. The paper is self-contained and has its own abstract, introduction, and reference list. It is included as a chapter in this thesis; the other chapters serve to place the paper in a wider context and to provide more details of the research.

The research methodology is covered in detail in Chapter 2. The research paper is included as Chapter 3. It outlines the theoretical background of the research and presents a new approach to address human and organisational factors in the operational phase of safety instrumented systems. The approach is also applied to an illustrative case. Finally, the paper gives concluding remarks and discusses further research. Chapter 4 of the thesis presents some suggestions for further improvement of the new approach and discusses how it can be applied and validated. More details of the new approach and the case study are given in, respectively, Appendix A and B.

Chapter 2

Methodology

This chapter outlines the methodology of the research. It covers the design of the research model, the formulation of research questions, and the research strategy followed.

2.1 Research model

The main objective of this research is to develop an approach to assess the impact of human and organisational factors on the achieved SIL in the operational phase of safety instrumented systems. This objective is translated into a research model, according to the principles for research design described by Verschuren & Doorewaard (2000). The research model is shown in Figure 2.1.

The research object is *achieved SIL in the operational phase of safety instrumented systems*. This object is studied from the perspective of *human and organisational factors*, because the goal is to assess the impact of human and organisational factors on the achieved SIL. The research perspective is based on relevant theories and models for human and organisational factors, which form the theoretical background. Hence, a range of theories and models for human and organisational factors is explored and their possible contribution to the operational phase of safety instrumented systems is reviewed. Next, a combination of relevant theories and models is adapted to the operational phase of safety instrumented systems and linked to the achieved SIL, which

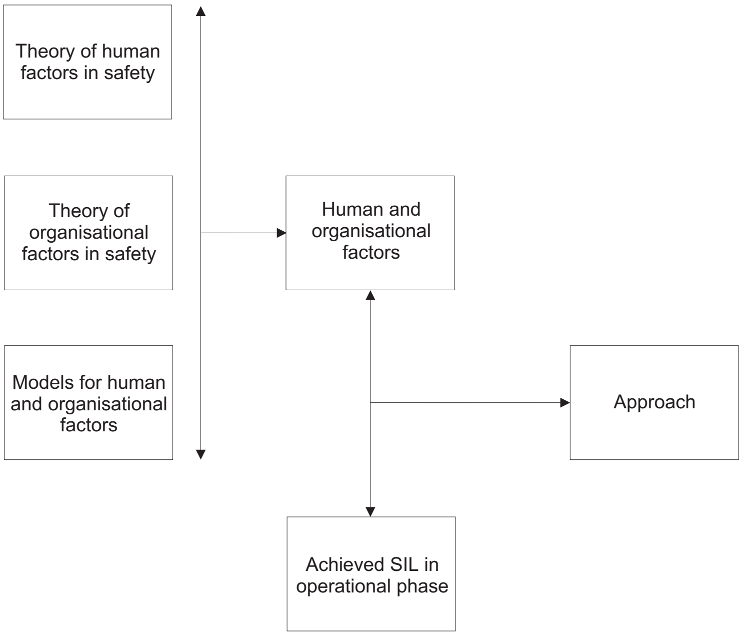
Theory of human factors in safety
Theory of organisational factors in safety
Models for human and organisational factors
Human and organisational factors
Approach
Achieved SIL in operational phase

Figure 2.1: Research model

leads to an approach to assess the impact of human and organisational factors on the achieved SIL in the operational phase of safety instrumented systems.

2.2 Research questions

The research model can serve as a basis for formulation of research questions. These questions are obtained by splitting the model into different parts, in line with the principles from Verschuren & Doorewaard (2000). The first part of the model, shown in Figure 2.2, leads to the first research question:

What is the contribution of existing theories and models for human and organisational factors to the operational phase of safety instrumented systems?

The second part of the model, shown in Figure 2.3, leads to the second research question:

Which relationship can be established between human and organisational factors and the achieved SIL in the operational phase of safety instrumented systems?

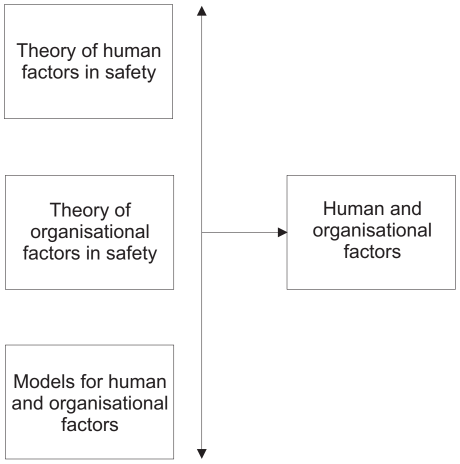
Theory of human factors in safety
Theory of organisational factors in safety
Models for human and organisational factors
Human and organisational factors

Figure 2.2: Part of the research model leading to research question 1

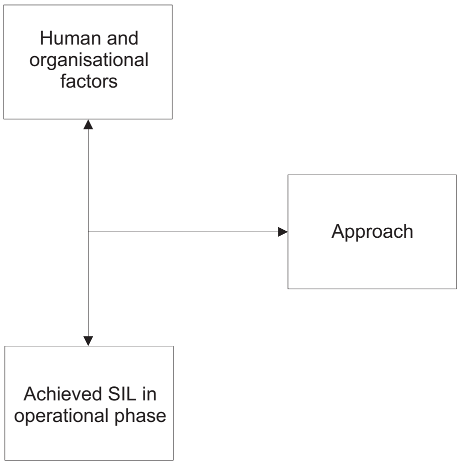
Human and organisational factors
Approach
Achieved SIL in operational phase

Figure 2.3: Part of the research model leading to research question 2

Subsequently, these research questions are split into subquestions. This makes the research questions more specific and indicates what type of knowledge is needed to answer them. This leads to the following questions and subquestions:

1. What is the contribution of existing theories and models for human and organisational factors to the operational phase of safety instrumented systems?
    - What do relevant theories say about the impact of human and organisational factors on safety?
    - Which relevant models for human and organisational factors exist?
    - What is the possible contribution of these theories and models to the operational phase of safety instrumented systems?
2. Which relationship can be established between human and organisational factors and the achieved SIL in the operational phase of safety instrumented systems?
    - What kind of indicators can be used for human and organisational factors in the operational phase of safety instrumented systems?
    - Which relationship can be established between these indicators and the achieved SIL?

2.3 Research strategy

To find answers to the research questions, a certain research strategy has to be followed. This involves decisions about the type of research and the way the research is conducted. Given the nature of the research objective and the research questions, a theoretical approach based on scientific literature is most appropriate. This means that existing theories and models are compared and adapted to create something new. The relevant literature is studied specifically from the perspective of the research questions and applied to a new domain. The goal of this research strategy is to develop a new approach for a specific domain (the operational phase of safety instrumented systems), based on existing theories and models. Hence, this theoretical research approach is more than a literature review.

The scientific literature used for this research consists mainly of papers from established scientific journals (e.g., Reliability Engineering and System Safety), as well as conference proceedings and a number of books. Together, this material covers all relevant parts of the research area, although it is not a complete overview. In addition to the scientific literature, reading a number of practice-oriented books (e.g., Kjellén, 2000; Kletz, 2001; Redmill & Rajan, 1997) provided valuable insight into the role of human and organisational factors in safety and into practical applications of safety instrumented systems. The research strategy followed has certain implications for the validity and applicability of the results. These are discussed in Chapter 4.

Chapter 3

Research paper

The main body of this thesis is written in the form of a research paper, which is included as chapter 3. This paper will be submitted for publication to a scientific journal, possibly slightly revised. The paper is self-contained and has its own abstract, introduction, and reference list.

Human and organisational factors in the operational phase of safety instrumented systems: A new approach

Martin Schönbeck

Abstract

The international standards IEC 61508 and IEC 61511, which provide a general framework for the design and implementation of safety instrumented systems, require quantification of the achieved risk reduction, expressed as a safety integrity level (SIL). Human and organisational factors affect the performance of safety instrumented systems during operation and may threaten the achieved SIL, but this is usually not explicitly accounted for. This paper presents a new approach to address human and organisational factors in the operational phase of safety instrumented systems. This approach gives a prediction of the operational SIL and can also be used to improve safety. It shows which human and organisational factors are most in need of improvement and it provides guidance for preventive or corrective action. Finally, the approach can be used as part of a SIL monitoring strategy in order to maintain the achieved SIL at the required level during the operational phase.

Key words: Human factors, Organisational factors, Operational phase, Safety instrumented system, Safety integrity level

1 Introduction

Safety instrumented systems are increasingly used across a wide range of industries to perform safety functions. These computer-based safety systems are generally composed of sensors, logic solvers and actuating items. Reliability certification of such systems has received a lot of attention during the past decade with the emergence of the new international standard IEC 61508 (IEC, 2000), which provides a general framework for the design and implementation of safety instrumented systems (called "electrical/electronic/programmable electronic safety-related systems" in this standard). A main objective of this standard is to facilitate the development of application specific standards, such as IEC 61511 for the process industry (IEC, 2004). These standards, which have been approved by CENELEC as European standards, require quantification of the achieved risk reduction, expressed as a *safety integrity level* (SIL).

The IEC 61508 standard (IEC, 2000) defines four safety integrity levels, where SIL 4 is the highest level and SIL 1 the lowest. Each level corresponds to an interval of the average probability of failure on demand (low demand mode) and the probability of a dangerous failure per hour (high demand or continuous mode). The *required SIL* is determined based on a hazard and risk analysis, combined with risk acceptance criteria. Next, one or more safety instrumented systems are designed that achieve the required risk reduction (possibly together with safety systems based on other technology). Apart from the quantitative target failure measure, the standard sets out different qualitative requirements for the system design and several other lifecycle phases, depending on the required SIL. Together, these quantitative and qualitative requirements determine for which SIL a safety instrumented system could be qualified upon system start-up, that is, the *achieved SIL*. Although the standard takes a lifecycle approach that also includes operation and maintenance, there is little focus on how to ensure that the achieved SIL is maintained at the required level during the operational phase. Most literature is concerned with determining the required SIL and demonstrating the achieved SIL upon system start-up.

The performance of a safety instrumented system in the operational phase is influenced by many factors; not only by the system design and the related testing and maintenance strategies, but also by the operating conditions in the wider socio-technical system it is part of. Accident rates for similar equipment vary considerably between different organisations (Hurst et al., 1996), and industrial accidents indicate that the performance of a highly complex socio-technical system is dependent upon the interaction of technical, human, social, organisational, managerial, and environmental elements (Gordon, 1998; Pidgeon & O'Leary, 2000). Moreover, a significant part of all industrial accidents is caused by unanticipated actions of people during operation and maintenance (Bea, 1998; HSE, 2003), and the organisational perspective on safety shows that these human errors often are caused by aspects of the organisation and the working environment (Kletz, 2001; Reason, 1997). According to Bley et al. (1992, p. 18), "any model that fails to examine the organisational factors is guaranteed to underestimate the overall risk by an undetermined amount."

Applying this line of thought to the operational phase of safety instrumented systems, it becomes clear that human and organisational factors affect the performance of safety instrumented systems and may threaten the achieved SIL, but this is usually not explicitly accounted for. The IEC 61508 standard (IEC, 2000) proposes a number of preventive measures related to human and organisational factors, but there is no specific requirement to undertake a quantitative analysis of these factors and their impact on the achieved SIL. Carey (2000, p. 31) points out 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."

Few authors have addressed human and organisational factors in the context of safety instrumented systems. Carey & Purewal (2001) have developed a framework for integrating human factors requirements into IEC 61508 and show that the level of effort required on human factors increases with the SIL. Brombacher (1999) introduces the maturity index on reliability as a method to analyse business processes in an IEC 61508 certification. However, this method deals only indirectly with the safety and reliability of the products realised and operated by these business processes. The reliability prediction method for safety instrumented systems developed by SINTEF (Hauge et al., 2006) proposes a way to quantify the effect of measures to avoid or control systematic failures. Some of these measures are related to human and organisational factors. In the general context of quantitative risk assessment and probabilistic safety assessment, several models have been developed to incorporate human and organisational factors into these assessments (Davoudian et al., 1994a,b; Duijm & Goossens, 2006; Embrey, 1992; Modarres et al., 1992; Mosleh et al., 1997; Øien, 2001a; Papazoglou et al., 2003; Paté-Cornell & Murphy, 1996). However, there are currently no models available that directly link human and organisational factors to the achieved SIL.

The main objective of this paper is to develop an approach to assess the impact of human and organisational factors on the achieved SIL in the operational phase of safety instrumented systems. It is also shown how this approach can be used to improve safety. The remainder of this paper is organised as follows: Section 2 explores the contribution of a range of human and organisational factor theories to the operational phase of a safety instrumented system, while models that link safety with human and organisational factors are discussed in Section 3. Together, these two sections provide the necessary background for the development of a tailored approach for the operational phase of safety instrumented systems, which is described in Section 4. The new approach is applied to an illustrative case in Section 5. Finally, Section 6 gives concluding remarks and discusses further research.

2 Human and organisational factors

Although estimates of the contribution of human errors to system failure and accident causation vary significantly, there seems to be a common understanding that human errors have a significant impact on safety. The terms *human factors* and *human error* are often used interchangeably, but, as pointed out by Gordon (1998), it is important to distinguish between the underlying causes of accidents (human factors) and their immediate causes (human errors). Traditionally, human factors are defined as the interaction between man and machine, although many variations exist (see Wogalter et al., 2001). Human error can be defined as "the failure of planned actions to achieve their desired ends – without the intervention of some unforeseeable event" (Reason, 1997, p. 71). According to Wagenaar et al. (1994), accidents are preceded by human behaviour that constitutes a necessary condition. This behaviour is called an *unsafe act*. Hence, a human error can be considered as an unsafe act by a system operator, which may cause an accident. Such an unsafe act may either involve doing something wrong (e.g., applying a wrong test procedure), or failing to do something (e.g., skipping a test).

Human errors can be categorised in many ways. Based on Rasmussen's three-level theory of human performance (Rasmussen, 1982, 1983) and Norman's distinction between slips and mistakes (Norman, 1981), Reason (1990) categorises errors into *skill-based slips and lapses*, *rule-based mistakes*, and *knowledge-based mistakes*. Furthermore, he distinguishes a separate type of unsafe acts called *violations*, which refer to (deliberate or erroneous) deviations from safe operating procedures, standards or rules (Reason, 1990). In the area of human reliability analysis, many attempts have been made to indentify human errors and to assess their likelihood, sometimes quantitatively (see Blackman et al., 1998; Hollnagel, 2000). Hollnagel (1998) argues that most recognised methods for human reliability analysis are in an uneasy position between probabilistic safety analysis and information processing psychology. Therefore, he proposes an alternative called *cognitive reliability analysis*, recognising that performance always takes place in a context, and that cognition is intrinsic to all actions, hence to all errors. This approach establishes a relationship between error modes and underlying causes, thus implicitly linking human errors to human factors.

According to Jacobs & Haber (1994), human errors may be of various origins and part of larger, organisational processes that encourage unsafe acts, which ultimately produce system failures. The importance of the underlying causes of unsafe acts is also stressed in the generalised accident scenario, which is part of the Tripod method (Van der Want, 1996; Wagenaar et al., 1994, 1990). According to this scenario, unsafe acts are preceded by reasons, motives, expectations, plans, and ways of reasoning, which together are labelled *psychological precursors*. Subsequently, the environmental conditions that cause these psychological precursors are called *latent failures*. Such latent failures are in principle under the control of management (Wagenaar et al., 1994). This view on the underlying causes of human errors is supported by Reason (1997, p. 126): "Human error is a consequence, not a cause. Errors. . . are shaped and provoked by upstream workplace and organisational factors." Furthermore, he writes that "we cannot change the human condition, but we can change the conditions under which people work" (Reason, 1997, p. 25). Or, as Kletz (2001) formulates the theme of his book: "Try to change situations, not people." According to this line of thought, focus shifts from human errors to the underlying *human* and *organisational factors*. Several relationships between human and organisational factors have been proposed, and terminology is sometimes overlapping. Some authors (e.g., Gordon, 1998) use *human factors* as a general term encompassing both organisational factors (such as procedures) and individual factors (such as motivation), whereas others (e.g., Øien, 2001a) define organisational factors as including both individual factors and aspects of the working environment.

The organisational perspective on safety has received a lot of attention during the past decades and is highly relevant for the operation of safety instrumented systems (Westrum, 1997). Perrow (1984, 1999) argues that the complexity of tightly-coupled technical systems leads to nearly inevitable catastrophic accidents, so-called *normal accidents*. According to this theory, introduction of safety devices and organisational redundancy increases complexity and coupling, resulting in systems that are more prone to error than they were previously. Hence, some accidents are inevitable. Vaughan (1999) addresses the *dark side of organisations* and states that mistake, misconduct, and disaster are the result of the interconnection between organisational environment, organisational characteristics, cognition, and choice. A research group at Berkeley has developed the concept of the *high reliability organisation*, based on qualitative investigation of normal operations in high-risk industries (see, e.g., La Porte & Consolini, 1991; Roberts, 1990; Rochlin, 1993; Rochlin et al., 1987). As pointed out by Moray (2000), their approach can be considered the inverse of that by Perrow (1984, 1999), because it emphasises the possibility of reliability rather than the danger of accidents. This line of research tries to find characteristics of organisations that operate extremely safely, although their activities are potentially very dangerous. Examples include air traffic control, submarines and power distribution.

According to Rochlin (1999), high reliability organisations show a positive engagement with the construction of operational safety that extends beyond controlling or mitigating unexpected events and seek instead to anticipate and plan for them. This is closely related to safety culture. Although there is no common understanding of the term *safety culture* (Guldenmund, 2000; Wiegmann et al., 2004), its importance is widely recognised. The term implies that it is part of a larger *organisational culture*, which is shared by the members of an organisation, and which manifests itself at three levels: observable artifacts, espoused values, and basic underlying assumptions (Schein, 1990). A popular definition of organisational culture, often used in management literature, is “the way we do things around here” (Deal & Kennedy, 1982, p. 4). As pointed out by Sorensen (2002), the term *safety culture* is sometimes used in a broader perspective to capture not only part of the organisational culture, but all organisational factors related to safety. On the other hand, some authors adopt a narrower definition and distinguish between safety culture and *safety climate* (see, e.g., Glendon & Stanton, 2000; Guldenmund, 2000; Wiegmann et al., 2004), the latter referring to attitudes towards safety.

Several studies across a wide range of industries have shown a positive correlation between organisational factors and safety performance (e.g., Donald & Canter, 1994; Hurst et al., 1996; Itoh et al., 2004; Lee, 1998; Mearns et al., 2003). However, the mechanism by which aspects of the organisation influence safety performance is not clear, and there is no common understanding of which organisational factors are relevant. An abundant amount of organisational factor frameworks and other lists of organisational factors can be found in literature (overviews are given by Flin et al., 2000; Sorensen, 2002; Vaquero et al., 2000; Wilpert, 2000). In line with the classification by Vaquero et al. (2000), these frameworks can be divided into two main categories: *deductive* and *inductive*. Deductive frameworks (e.g., Jacobs & Haber, 1994) are based on a theoretical model of an organisation, whereas inductive frameworks are derived from empirical observations (e.g., Lee, 1998) or accident investigation (e.g., Dien et al., 2004), sometimes combined with expert elicitation. A great deal of these frameworks focus on safety culture or safety climate, but some take a broader perspective and include also structural aspects of the organisation, such as procedures, responsibilities and coordination. Le Coze (2005) argues that organisations, due to their complexity, cannot be studied in the same way as technical systems and that one should take a multidimensional approach, including dimensions such as power relations, organisational culture, and the organisational environment. This is in line with the view of safety management presented by Hale (2003).

3 Models linking safety with human and organisational factors

Several models are available that try to link safety with human and organisational factors, ranging from qualitative accident investigation models to quantitative methods to include human and organisational factors into probabilistic safety assessment. A general – and by now famous – approach is Reason's model of organisational accidents, better known as the *Swiss cheese model* (Reason, 1990, 1997). This model is based on the generalised accident scenario described in Section 2. Recently, the Swiss cheese model has been subject to criticism (for a review, see Reason et al., 2006), and several new approaches have been proposed (e.g., Leveson, 2004), but still it is widely used in practice. An organisational accident can be defined as "the concurrent failure of several defences, facilitated, and in some way prepared, by suboptimal features of the organisation design" (Reason et al., 2006, p. 9). This can be visualised as an accident trajectory passing through holes in successive "slices", which gave rise to the Swiss cheese label.

A later variant of the Swiss cheese model shows how the performance of de-

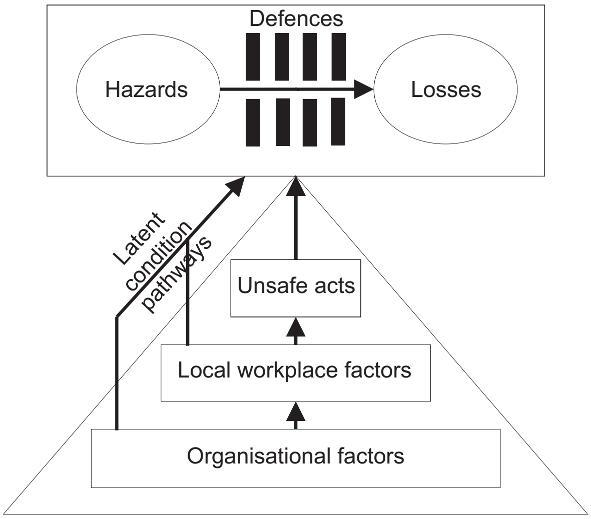

Fig. 1. Model of organisational accidents, adapted from Reason (1997)

fences is influenced by upstream human and organisational factors, as illustrated in Figure 1. The upper part represents the main elements of accident causation: hazards, defences (safety barriers), and losses. This is similar to a general accident model known as the *energy model* (Gibson, 1961/1964; Haddon, 1980). The lower part of Figure 1 shows the development of an organisational accident: organisational factors (strategic decisions and generic organisational processes, shaped by the organisational culture) influence local workplace conditions (time pressure, insufficient training, ambiguous procedures, etc.), which combine with natural human tendencies to produce unsafe acts (Reason, 1997). These unsafe acts may create holes in the defences. According to Reason (1997), workplace and organisational factors may also lead directly to failed defences, as indicated by the *latent condition pathways*. The Swiss cheese model is highly relevant for the operational phase of safety instrumented systems, because it visualises the influence of human and organisational factors on the performance of safety barriers (in this case, safety instrumented systems). Although the Swiss cheese model was originally developed for accident investigation, it can also be used as a predictive model. It proposes a number of *general failure types*, which give an indication of the current state of "safety health" (Reason et al., 2006). This gives a prediction of the general likelihood that an accident may happen.

Another category of models tries to incorporate human and organisational factors into quantitative risk assessment and probabilistic safety assessment. These models vary in scope and are not totally comparable, but they try to achieve more or less the same ends (for a review, see Øien, 2001b). One of the first attempts in this area is MACHINE (Model of Accident Causation using Hierarchical Influence NEtwork), developed by Embrey (1992). This model focuses on human errors (classified into active, latent and recovery failures), and their relationship with error inducing factors (e.g., procedures) and higher level organisational factors (called policy deficiencies). Modarres et al. (1992) describe a framework that has been developed for the assessment of performance indicators, but which also can be used to assess the impact of organisational factors on safety. It covers both organisational hierarchy and behavioural aspects. The Work Process Analysis Model (WPAM), developed by Davoudian et al. (1994a,b), explores the work processes in an organisation and tries to identify the organisational factors that interfere with particular tasks. It is based on the 20 organisational factors identified by Jacobs & Haber (1994), which, according to Weil & Apostolakis (2001), can be reduced to six.

Another approach is the SAM (System-Action-Management) framework (Murphy & Paté-Cornell, 1996; Paté-Cornell, 1990, 1993; Paté-Cornell & Bea, 1992; Paté-Cornell & Murphy, 1996), which uses human decisions and actions as an intermediate variable between the performance of the system and the organisation. Unlike most of the other models described here, SAM has been applied in practice in several industries. Mosleh et al. (1997) developed the ω-factor approach to model the influence of organisational factors on reliability of components and on operator performance. This approach is similar to the β-factor model for common cause failures. Based on a review of existing organisational factor frameworks, Øien (2001a) developed an organisational model to analyse leak events on offshore installations. Furthermore, he proposes organisational risk indicators and a methodology to quantify the impact of the organisation on risk. A European project called I-Risk (Integrated Risk) led to an approach to integrate the technical model of a chemical process plant with a safety management model, including risk quantification (Papazoglou et al., 2003). I-Risk served as the basis for ARAMIS (Accidental Risk Assessment Methodology for IndustrieS), which is another European project, aimed to support harmonised implementation of the SEVESO II directive (Salvi & Debray, 2006). As part of ARAMIS, a methodology has been developed to quantify the influence of safety management on the reliability of safety barriers, using a safety management audit and a safety culture questionnaire (Duijm & Goossens, 2006). This approach is particularly interesting for the operational phase of safety instrumented systems, because it directly addresses the reliability of safety barriers.

Øien (2001b) evaluated all models described above according to a predefined structure (Øien & Sklet, 2000), except for the newer ARAMIS methodology. A similar but narrower review can be found in Sorensen (2002). Many of these models (e.g., MACHINE, SAM, ω-factor) use influence diagrams as a modelling technique, combining an intuitive representation with the possibility to quantify the model using Bayesian probability theory. However, regardless of the modelling technique, explicit quantification of the effect of organisational factors in a practical situation is difficult and time-consuming. Therefore, conditional probabilities or weight factors are often derived from expert judgement (see, e.g., Paté-Cornell & Murphy, 1996). Some of the models focus solely on organisational factors (e.g., ARAMIS), whereas others take human factors into account as well, often as a layer between the organisation and the technical system (e.g., SAM). Which human and/or organisational factors are included, varies considerably between the models. Sometimes an existing organisational factor framework is used (e.g., for WPAM), in other cases the set of organisational factors is developed as part of the model (e.g., ARAMIS) or adapted to each specific situation (e.g., SAM). Apart from that, there is no consensus about the mechanism by which the organisational factors affect safety. Most models include such a mechanism, for example human decisions and actions (SAM), error inducing factors and human errors (MACHINE), or work processes (WPAM). A different approach is adopted in ARAMIS: the organisational factors are here linked directly to the reliability of safety barriers. This is a simplification of reality, but it makes the approach practical.

In the operational phase of safety instrumented systems, human and organisational factors may have a *common cause* effect on failure probabilities, because they function as a source of dependency between components or human actions (Davoudian et al., 1994a; Mosleh et al., 1997). According to Mosleh et al. (1997), the most likely form of dependency is through increase or decrease in failure probabilities of components or human actions, rather than simultaneous failure. Therefore, the ω-factor model assumes dependency in cause, but not in time. Zitrou et al. (2007) take a different approach and propose a way to include organisational factors in common cause failure models. They use an influence diagram to model the effect of organisational factors (called defences) on root causes and coupling factors. However, this model is still in its developmental stage and considers only common cause failures.

4 A new approach

As pointed out in the introduction, it is important to consider the impact of human and organisational factors on the achieved SIL. However, none of the models described above can be applied directly to the operational phase of a safety instrumented system. This section presents an approach for this specific domain, building on previous work and experiences. Its aim is to capture the impact of human and organisational factors in a practically feasible way, with a sound theoretical foundation from human and organisational factor research. First, a framework for human and organisational factors is selected. Next, a quantification procedure is proposed to establish a relationship between human and organisational factors and the achieved SIL. Finally, it is shown how the approach can be used to improve safety.

When selecting a framework for human and organisational factors, one should keep in mind that it may not be possible to capture the entire complexity of an organisation and its informal social aspects in a model (see discussion by Le Coze, 2005; Rochlin, 1999), but still one can try to identify a few dominant factors that significantly influence safety. The *general failure types* corresponding to the Swiss cheese model (Reason, 1997), later called *basic risk factors* (Tripod Solutions, 2007), are based on many years of research and analysis of hundreds of accident scenarios and they can, as such, be considered as a good example of a list of dominant factors influencing safety. They were originally published by Wagenaar et al. (1990) and have later been slightly revised (Reason, 1997; Wagenaar et al., 1994). These general failure types provide the basis for the approach presented here. The main reasons for selecting this framework are that it is theoretically founded in human and organisational factor research and that it captures both structural and behavioural aspects, as opposed to many other frameworks. It should be noted that the general failure types do not refer to system failures, but to the latent failures discussed in Section 2. Using the relationships between basic lifecycle processes and the eleven general failure types (Reason, 1997), these are reduced to eight and slightly reformulated in order to reflect human and organisational factors in the operational phase of safety instrumented systems. Defence planning, hardware, and design are eliminated. The remaining eight will here be called *safety influencing factors* and are listed in Table 1.

Table 1
Safety influencing factors in the operational phase of safety instrumented systems

Safety influencing factor	Description
1. Maintenance management	Management, rather than execution, of maintenance activities
2. Procedures	Quality, accuracy, relevance, availability and workability of operating and maintenance procedures
3. Error-enforcing conditions	Conditions that force people to operate in a manner not foreseen during system design
4. Housekeeping	Orderliness in the workplace
5. Goal compatibility	Compatibility of goals at and between individual, group, and organisational level
6. Communication	Possible lack of communication due to system failures, message failures, and misinterpretation
7. Organisation	Possible deficiencies in organisational structure and responsibilities
8. Training	Specific expertise relevant to the operators' jobs

As can be observed from Table 1, safety culture is not listed separately. However, safety culture is closely related to all safety influencing factors and it could be argued that it is indirectly represented in the safety influencing factors. Adopting a broader definition of safety culture (in line with Sorensen, 2002), the safety influencing factors can be considered as aspects of the safety culture. Many different methods to measure safety culture (or safety climate) have been developed (for an overview, see Flin et al., 2000), and a comparison of these methods with the safety influencing factors from Table 1 could provide additional insight into the relationship between them. When comparing the safety influencing factors used here with other frameworks for human and organisational factors, a certain degree of similarity can be observed. Factors like procedures, goals, communication, and training can be found in most frameworks. Finally, it should be noted that the approach presented in the remainder of this section in principle also can be combined with other frameworks for human and organisational factors.

The next step is to establish a relationship between the safety influencing factors and the achieved SIL. This is done using a quantification procedure similar to the ARAMIS approach (Duijm & Goossens, 2006), but there are some important differences. First of all, the approach presented here assesses the impact of both human and organisational factors, using the safety influencing factors from Table 1. Secondly, the approach is developed specifically for the operational phase of safety instrumented systems, which eliminates the need to distinguish between different types of safety barriers. A shared feature with the ARAMIS approach is the direct link between the safety influencing factors and the achieved SIL using weight factors, as opposed to other models that explicitly include the mechanism by which the human and organisational factors influence safety. Of course, such an influence mechanism exists, but the unsafe acts and latent condition pathways (see Figure 1) are not modelled explicitly. This is in line with the use of the Swiss cheese model as a *weakly predictive model*, which gives a prediction of the general likelihood that an accident may happen, but not of where and when (Reason et al., 2006). For practical applications, this has a considerable advantage, because it significantly reduces the effort needed to collect data and to apply the approach. If higher precision is desired in a specific case, it is possible to model part of the influence mechanism explicitly.

The quantitative and qualitative requirements set out by the IEC 61508 standard (IEC, 2000) determine for which SIL a safety instrumented system could be qualified upon system start-up. The achieved SIL upon system start-up will here be referred to as the *design SIL*. The approach presented here gives a prediction of the achieved SIL during operation, called *operational SIL*, which may be lower than the design SIL, due to the impact of human and organisational factors in the operational phase. According to Duijm & Goossens (2006), good safety management cannot improve the reliability of a technical system, but bad safety management can very well deterioriate it. This philosophy assumes that the design SIL is based on an ideal situation in which humans and organisations function optimally (i.e., good enough to maintain the design SIL during the operational phase). For simplicity, the same philosophy is adopted

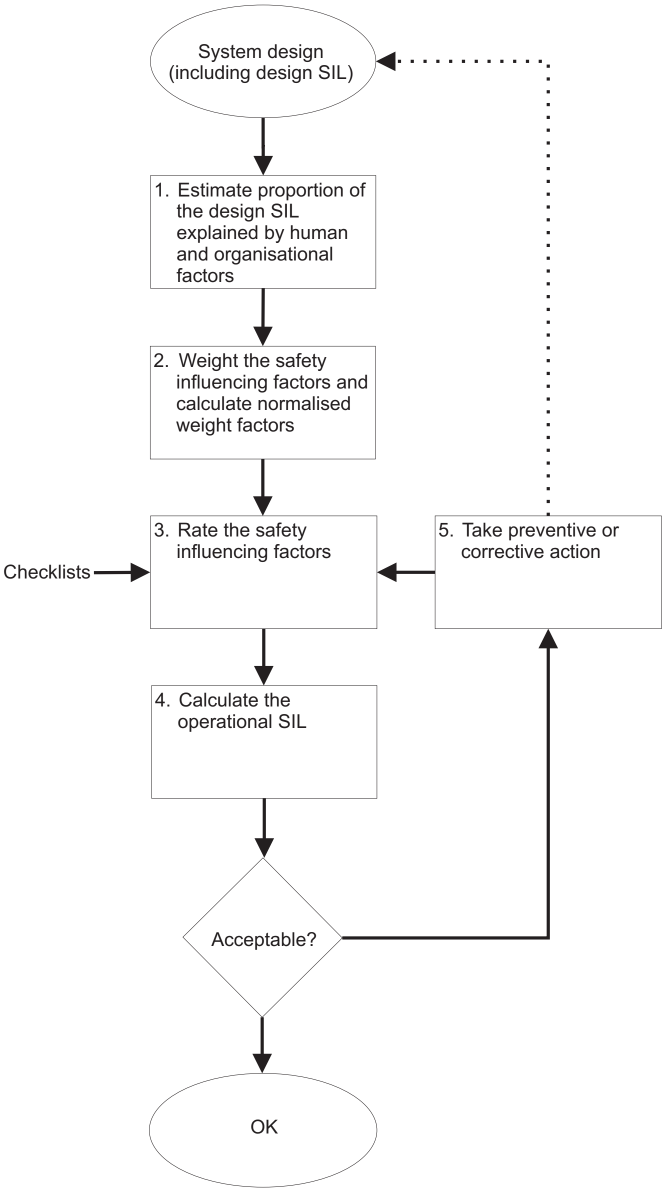
System design (including design SIL)
1. Estimate proportion of the design SIL explained by human and organisational factors
2. Weight the safety influencing factors and calculate normalised weight factors
3. Rate the safety influencing factors
Checklists
5. Take preventive or corrective action
4. Calculate the operational SIL
Acceptable?
OK

Fig. 2. Steps of the approach

here; failure probabilities may increase due to human and organisational factors, but not decrease. Hence, the operational SIL cannot be higher than the design SIL.

Figure 2 shows the steps of the approach, which starts with a given system design, qualified for a certain design SIL. The first step is to estimate the proportion of the design SIL that can be explained by human and organisational factors. Depending on the system design and the operating conditions, some safety instrumented systems are more sensitive to human and organisational factors than others. This proportion, denoted θ, can be estimated for a specific system using expert judgement, or it can be based on previous experience with similar systems under similar operating conditions.

In the second step, each safety influencing factor i from Table 1 is assigned a relative weight $\widetilde{W}_i$ ($\widetilde{W}_i \geq 0$ for all $i = 1, 2, ..., 8$). These weights can be established as part of a safety audit, making them specific for the system or site under consideration, or they can be determined for an entire application domain (e.g., offshore) using expert elicitation. As shown by Duijm & Goossens (2006), it is also possible to derive the weights from accident causation statistics. However, given the low accident rate in some application domains, it may be difficult to collect enough data. In that case, a possible solution might be to use data from dangerous detected failures, assuming that their causes are investigated as well. When each safety influencing factor has been assigned a relative weight, these weights have to be normalised. The weight factor W_i for safety influencing factor i is calculated in such a way that $\sum_{i=1}^{8} W_i = 1$:

$$W_i = \frac{\widetilde{W}_i}{\sum_{i=1}^{8} \widetilde{W}_i} \tag{1}$$

The next step is to rate the safety influencing factors. The state of each safety influencing factor in Table 1 is measured during an audit using checklists and questionnaires. A commercial software tool to facilitate the audit is also available (Tripod Solutions, 2007). Each safety influencing factor is rated on a scale from 0 to 1, with 0 being the best rating (improvement not needed) and 1 the worst (immediate attention required). These ratings are based on a set of specific, measurable indicators for each safety influencing factor, preferably in the form of a question that can be answered with "yes" or "no". For example, "Is there sometimes more than one version of the same procedure in circulation?" may be one of the indicators for procedures. In this case, if the question is answered with "yes", the indicator scores in the direction that causes concern. Subsequently, the number of indicators that cause concern is divided by the total number of indicators used for that safety influencing factor, which yields the rating R_i for safety influencing factor i. It should be noted that there are also other techniques for safety audits (see, e.g., Guldenmund et al., 2006; Hurst et al., 1996), which could provide valuable input for the rating process.

In step four, the operational SIL is calculated as follows:

$$\mathrm{SIL}_{\mathrm{operational}} = \left(1 - \theta \sum_{i=1}^{8} R_i W_i\right) \mathrm{SIL}_{\mathrm{design}} \tag{2}$$

where θ is the proportion of the design SIL that can be explained by human and organisational factors ($0 \leq \theta \leq 1$), R_i is the rating for safety influencing factor i ($0 \leq R_i \leq 1$ for all i), and W_i is the weight factor for safety influencing factor i ($0 \leq W_i \leq 1$ for all i). The outcome of (2) is rounded to the nearest integer, because the SIL only can be expressed by whole numbers. If the rounded operational SIL deviates from the design SIL, corrective action should be taken. Nevertheless, the unrounded outcome provides useful information and should be saved as well. Especially if the rounded operational SIL is equal to the design SIL, while the unrounded operational SIL value is significantly lower than the design SIL (e.g., 1.6 when the design SIL is 2), it is wise to take preventive action.

Step five provides guidance for preventive or corrective action. The safety influencing factors with the highest weighted ratings (R_iW_i) contribute most to the difference between the design SIL and the operational SIL, and are therefore most in need of improvement. The information from the audit can be used as a starting point for an in-depth analysis of these safety influencing factors, aimed at finding the causes of the unfavourable ratings. Then these causes can be eliminated in order to improve the corresponding safety influencing factors. To avoid suboptimising the indicators that are used to measure the safety influencing factors, it is advisable to use slightly different indicators during the next audit. This is in accordance with the Tripod method, where only some items recur from one checklist to the next (Wagenaar et al., 1994). When the safety influencing factors have been improved, one should go back to step three to obtain new ratings and to calculate the new operational SIL.

Another possibility for preventive or corrective action is to modify the system design and/or the related testing and maintenance strategies. In some cases this may be easier or cheaper than improving human and organisational factors. First of all, one can increase the design SIL, for example by using equipment with a lower failure rate, reducing the test interval, or improving the coverage of diagnostic tests. One can also try to make the system less sensitive for human and organisational factors in general, which leads to a lower value for θ. Finally, one can modify the design in such a way that the system becomes less sensitive for a specific safety influencing factor that systematically receives an unfavourable rating. This leads to a lower relative weight for this safety influencing factor. If the system design has been modified, one should start again with step one.

5 Case study

In this section the proposed approach is applied to an illustrative case. The data presented here do not necessarily reflect an existing system or industry average. Given a safety instrumented system that is qualified for SIL 3 upon system start-up, the steps shown in Figure 2 are addressed successively.

First, the proportion of the design SIL that can be explained by human and organisational factors is estimated. In this case, θ is taken to be 0.5. This corresponds roughly with weight factors derived from investigation of incidents in

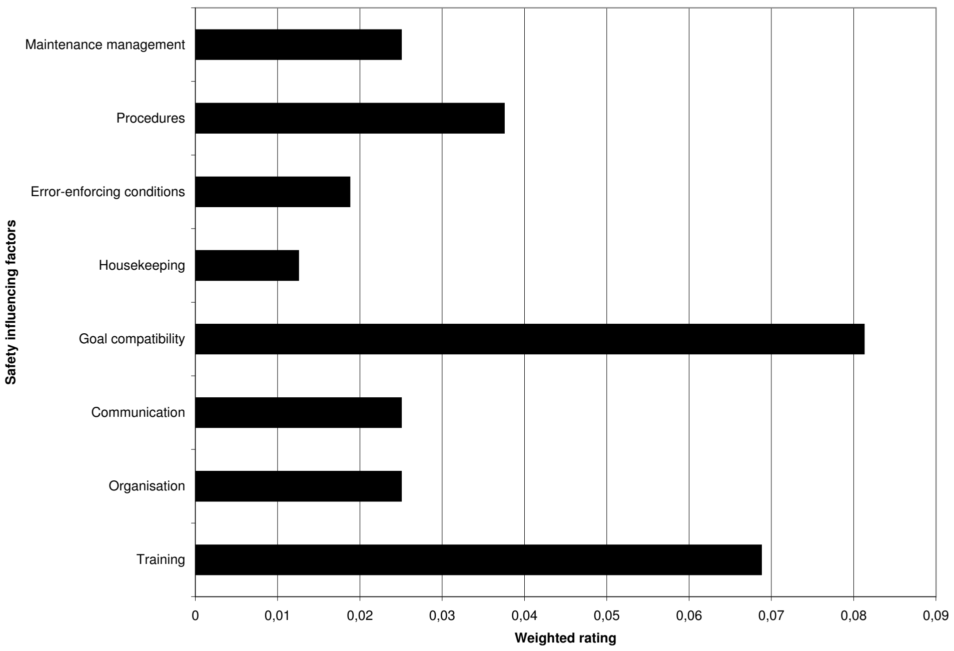

Fig. 3. Weighted ratings for the safety influencing factors

the process industry (Hurst et al., 1996; Papazoglou & Aneziris, 1999). As long as there is no other evidence, it is assumed that all safety influencing factors are equally important. Therefore, each safety influencing factor is assigned an equal weight, say $\widetilde{W}_i = 1$. These weights are then normalised using (1), which yields $W_i = 0.125$ for each safety influencing factor i. The ratings R_i for the safety influencing factors are obtained from an audit, containing a set of specific, measurable indicators for each safety influencing factor. Finally, filling in (2) yields an operational SIL of 2.6, which is rounded to 3. The weighted ratings for the safety influencing factors, obtained by multiplying each rating R_i with the corresponding weight factor W_i, are shown in Figure 3.

Although the rounded operational SIL is equal to the design SIL in this case, the results indicate that it is wise to take preventive action, before the operational SIL falls down to SIL 2. As can be observed from Figure 3, goal compatibility and training have the highest weighted ratings and are most in need of improvement. The information from the audit is then used as a starting point for an in-depth analysis of these safety influencing factors, aimed at finding the causes of the unfavourable ratings. In this way, one can take preventive action to improve the corresponding safety influencing factors. For example, if the high rating for goal compatibility turns out to be caused by informal norms of a work group that are incompatible with the safety goals of the organisation (one of the levels of goal conflict, see Reason, 1997), management can try to intervene in this work group. Should training be rated high because all operators hired more than ten years ago were never formally educated to use the new emergency alarm system, a special training session for them can be arranged. When goal compatibility and training have been improved, one should go back to step three to obtain new ratings and to calculate the new operational SIL.

6 Conclusions and discussion

As becomes clear from the case study, the approach does not only give a prediction of the operational SIL, but can also be used to improve safety. It shows which safety influencing factors are most in need of improvement and it provides guidance for preventive or corrective action. In many situations the rounded operational SIL will be equal to the design SIL, while the unrounded operational SIL value is significantly lower than the design SIL, like in the case study. This shows the preventive character of the approach: improve relevant human and organisational factors in the operational phase of safety instrumented systems before these factors threaten the achieved SIL. In this way, the approach can be used as a tool for continuous improvement in the operational phase. It can be considered as a periodic "test" of the organisation, which should be repeated from time to time. This also provides the opportunity to monitor ratings over time and to discover trends in the safety influencing factors.

Although the approach presented here already can be applied in practice, there are some issues that should be considered further. A consequence of expressing the impact of the safety influencing factors as a linear variation in the achieved SIL, like in (2), is that a change in a rating corresponds to an exponential variation in the failure probability. As indicated by Duijm & Goossens (2006), one can question whether this is the most appropriate way of modelling. Another issue is that the reliability data used to determine the design SIL already may contain some influence of human and organisational factors and therefore not necessarily represent the design SIL. This is currently not accounted for in the calculation of the operational SIL. On the other hand, field data are not always available, and in some application domains failures are so rare, that it is not possible to use historical failure data at all. Ensuring consistency over time in the ratings of the safety influencing factors is also an issue for further consideration. This requires careful selection of valid indicators. Finally, estimating θ and weighting the safety influencing factors may be difficult in practice, especially if little previous experience with similar equipment under similar operating conditions is available. For now, expert judgement seems to be the best information source, balancing accuracy and effort. The approach can also be extended with an influence diagram. This may lead to more accurate weight factors, but it requires considerable resources.

The approach for human and organisational factors presented here can be used as part of a larger SIL monitoring strategy in order to maintain the achieved SIL at the required level during the operational phase of safety instrumented systems. Further research is needed to explore other issues that should be followed up in the operational phase, including the effects of system modifications and aging of equipment, and to assess their impact on the operational SIL. It may be appropriate to incorporate other safety influencing factors, next to those that reflect human and organisational factors. Furthermore, it would be interesting to explore the relationship between the approach presented here and the common cause failure defence approach developed by Lundteigen & Rausand (2007), because potential common cause failures are often introduced by human and organisational factors during operation and maintenance. When field data from the real operation of a safety instrumented system become available, these data can be used to update failure rates, test intervals, and the β-factor for common cause failures. The effect of changes in these parameters on the operational SIL has to be investigated further.

References

Bea, R. G. (1998). Human and organization factors: Engineering operating safety into offshore structures. *Reliability Engineering and System Safety*, *61*, 109–126.

Blackman, H. S., Siu, N., & Mosleh, A. (Eds.). (1998). *Human reliability models: Theoretical and practical challenges.* Center for Reliability Engineering, University of Maryland.

Bley, D., Kaplan, S., & Johnson, D. (1992). The strengths and limitations of PSA: Where we stand. *Reliability Engineering and System Safety*, *38*, 3–26.

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

Carey, M. (2000). Human factors in the design of safety-related systems. *Computing & Control Engineering Journal*, *11*(1), 28–32.

Carey, M., & Purewal, S. (2001). Developing a framework for addressing human factors in IEC 61508. In *People in control – Second international conference on human interfaces in control rooms, cockpits and command centres* (pp. 42–47). (IEE Conf. Publ. No. 481)

Davoudian, K., Wu, J.-S., & Apostolakis, G. (1994a). Incorporating organizational factors into risk assessment through the analysis of work processes. *Reliability Engineering and System Safety*, *45*, 85–105.

Davoudian, K., Wu, J.-S., & Apostolakis, G. (1994b). The work process analysis model (WPAM). *Reliability Engineering and System Safety*, *45*, 107–125.

Deal, T. E., & Kennedy, A. A. (1982). *Corporate cultures: The rites and rituals of corporate life.* Reading, MA: Addison-Wesley.

Dien, Y., Llory, M., & Montmayeul, R. (2004). Organisational accidents investigation methodology and lessons learned. *Journal of Hazardous Materials*, *111*(1-3), 147–153.

Donald, I., & Canter, D. (1994). Employee attitudes and safety in the chemical industry. *Journal of Loss Prevention in the Process Industries*, *7*(3), 203–208.

Duijm, N. J., & Goossens, L. (2006). Quantifying the influence of safety management on the reliability of safety barriers. *Journal of Hazardous Materials*, *130*, 284–292.

Embrey, D. E. (1992). Incorporating management and organisational factors into probabilistic safety assessment. *Reliability Engineering and System Safety*, *38*, 199–208.

Flin, R., Mearns, K., O'Connor, P., & Bryden, R. (2000). Measuring safety climate: Identifying the common features. *Safety Science*, *34*, 177–192.

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

Glendon, A. I., & Stanton, N. A. (2000). Perspectives on safety culture. *Safety Science*, *34*, 193–214.

Gordon, R. P. E. (1998). The contribution of human factors to accidents in the offshore oil industry. *Reliability Engineering and System Safety*, *61*, 95–108.

Guldenmund, F. (2000). The nature of safety culture: A review of theory and research. *Safety Science*, *34*, 215–257.

Guldenmund, F., Hale, A., Goossens, L., Betten, J., & Duijm, N. J. (2006). The development of an audit technique to assess the quality of safety barrier management. *Journal of Hazardous Materials*, *130*, 234–241.

Haddon, W. J. (1980). The basic strategies for reducing damage from hazards of all kinds. *Hazard Prevention*, *16*, 8–12.

Hale, A. R. (2003). Safety management in production. *Human Factors and Ergonomics in Manufacturing*, *13*(3), 185–201.

Hauge, S., Hokstad, P., Langseth, H., & Øien, K. (2006). *Reliability prediction method for safety instrumented systems – PDS method handbook.* Trondheim: SINTEF.

Hollnagel, E. (1998). *Cognitive reliability and error analysis method: CREAM.* Oxford: Elsevier.

Hollnagel, E. (2000). Looking for errors of omission and commission or *The Hunting of the Snark* revisited. *Reliability Engineering and System Safety*, *68*, 135–145.

HSE. (2003). *Out of control – Why control systems go wrong and how to prevent failure.* Sudbury, UK: HSE Books.

Hurst, N. W., Young, S., Donald, I., Gibson, H., & Muyselaar, A. (1996). Measures of safety management performance and attitudes to safety at major hazard sites. *Journal of Loss Prevention in the Process Industries*, *9*(2), 161–172.

IEC.(2000). *IEC 61508 – Functional safety of electrical/electronic/programmable electronic safety-related systems. Part 1 to 7.* Geneva: International Electrotechnical Commission.

IEC.(2004). *IEC 61511 – Functional safety – Safety instrumented systems for the process industry sector. Part 1 to 3.* Geneva: International Electrotechnical Commission.

Itoh, K., Andersen, H., & Seki, M.(2004). Track maintenance train operators' attitudes to job, organisation and management, and their correlation with accident/incident rate. *Cognition, Technology & Work*, *6*(2), 63–78.

Jacobs, R., & Haber, S. (1994). Organizational processes and nuclear power plant safety. *Reliability Engineering and System Safety*, *45*, 75–83.

Kletz, T. (2001). *An engineer's view of human error* (3rd ed.). New York: Taylor & Francis.

La Porte, T. R., & Consolini, P. M. (1991). Working in practice but not in theory: Theoretical challenges of "high-reliability organizations". *Journal of Public Administration Research and Theory*, *1*, 19–47.

Le Coze, J.-C. (2005). Are organisations too complex to be integrated in technical risk assessment and current safety auditing? *Safety Science*, *43*, 613–638.

Lee, T. (1998). Assessment of safety culture at a nuclear reprocessing plant. *Work Stress*, *12*(3), 217–237.

Leveson, N.(2004). A new accident model for engineering safer systems. *Safety Science*, *42*, 237–270.

Lundteigen, M. A., & Rausand, M. (2007). Common cause failures in safety instrumented systems on oil and gas installations: Implementing defense measures through function testing. *Journal of Loss Prevention in the Process Industries*, *Article in press*, doi:10.1016/j.jlp.2007.03.007.

Mearns, K., Whitaker, S. M., & Flin, R. (2003). Safety climate, safety management practice and safety performance in offshore environments. *Safety Science*, *41*(8), 641–680.

Modarres, M., Mosleh, A., & Wreathall, J.(1992). A framework for assessing influence of organization on plant safety. *Reliability Engineering and System Safety*, *38*, 157–171.

Moray, N.(2000). Culture, politics and ergonomics. *Ergonomics*, *43*(7), 858–868.

Mosleh, A., Goldfeiz, E., & Shen, S.(1997). The ω-factor approach for modeling the influence of organizational factors in probabilistic safety assessment. In *Global perspectives of human factors in power generation – Proceedings of the 1997 IEEE sixth conference on human factors and power plants* (pp. 9/18–9/23).

Murphy, D. M., & Paté-Cornell, M. E.(1996). The SAM framework: Modeling the effects of management factors on human behavior in risk analysis. *Risk Analysis*, *16*(4), 501–515.

Norman, D. A. (1981). Categorization of action slips. *Psychological Review*, *88*(1), 1–15.

Øien, K. (2001a). A framework for the establishment of organizational risk indicators. *Reliability Engineering and System Safety*, *74*, 147–167.

Øien, K. (2001b). *Risk control of offshore installations – A framework for the establishment of risk indicators.* PhD thesis, NTNU, Trondheim.

Øien, K., & Sklet, S. (2000). A structure for the evaluation and development of organizational factor frameworks. In S. Kondo & K. Furuta (Eds.), *Proceedings of the international conference on probabilistic safety assessment and management (PSAM 5), Osaka, Japan* (pp. 1711–1717). Tokyo: Universal Academy Press.

Papazoglou, I. A., & Aneziris, O. (1999). On the quantification of the effects of organizational and management factors in chemical installations. *Reliability Engineering and System Safety*, *63*, 33–45.

Papazoglou, I. A., Bellamy, L. J., Hale, A. R., Aneziris, O. N., Ale, B. J. M., Post, J. G., et al. (2003). I-Risk: Development of an integrated technical and management risk methodology for chemical installations. *Journal of Loss Prevention in the Process Industries*, *16*, 575–591.

Paté-Cornell, M. E. (1990). Organizational aspects of engineering system safety: The case of offshore platforms. *Science*, *250*(4985), 1210–1217.

Paté-Cornell, M. E. (1993). Learning from the Piper Alpha accident: A post-mortem analysis of technical and organizational factors. *Risk Analysis*, *13*(2), 215–232.

Paté-Cornell, M. E., & Bea, R. G. (1992). Management errors and system reliability: A probabilistic approach and application to offshore platforms. *Risk Analysis*, *12*(1), 1–18.

Paté-Cornell, M. E., & Murphy, D. M. (1996). Human and management factors in probabilistic risk analysis: The SAM approach and observations from recent applications. *Reliability Engineering and System Safety*, *53*, 115–126.

Perrow, C. (1984). *Normal accidents – Living with high-risk technologies.* New York: Basic Books.

Perrow, C. (1999). *Normal accidents – Living with high-risk technologies* (2nd ed.). Princeton, NJ: Princeton University Press.

Pidgeon, N., & O'Leary, M. (2000). Man-made disasters: Why technology and organizations (sometimes) fail. *Safety Science*, *34*, 15–30.

Rasmussen, J. (1982). Human errors: A taxonomy for describing human malfunction in industrial installations. *Journal of Occupational Accidents*, *4*, 311–333.

Rasmussen, J. (1983). Skills, rules, knowledge: Signals, signs and symbols and other distinctions in human performance models. *IEEE Transactions on Systems, Man and Cybernetics*, *13*, 257–267.

Reason, J. (1990). *Human error.* Cambridge: Cambridge University Press.

Reason, J. (1997). *Managing the risks of organizational accidents.* Aldershot, UK: Ashgate.

Reason, J., Hollnagel, E., & Paries, J. (2006). *Revisiting the "Swiss cheese"* *model of accidents.* Brussels: Eurocontrol Experimental Centre.

Roberts, K. H. (1990). Some characteristics of one type of high reliability organization. *Organization Science*, *1*(2), 160–176.

Rochlin, G. I. (1993). Defining "high reliability" organizations in practice: A taxonomic prologue. In K. H. Roberts (Ed.), *New challenges to understanding organizations* (pp. 11–32). New York: Macmillan.

Rochlin, G. I. (1999). Safe operation as a social construct. *Ergonomics*, *42*(11), 1549–1560.

Rochlin, G. I., La Porte, T. R., & Roberts, K. H. (1987). The self-designing high-reliability organization: Aircraft carrier flight operations at sea. *Naval War College Review*, *40*(4), 76–90.

Salvi, O., & Debray, B. (2006). A global view on ARAMIS, a risk assessment methodology for industries in the framework of the SEVESO II directive. *Journal of Hazardous Materials*, *130*, 187–199.

Schein, E. H. (1990). Organizational culture. *American Psychologist*, *45*(2), 109–119.

Sorensen, J. N. (2002). Safety culture: A survey of the state-of-the-art. *Reliability Engineering and System Safety*, *76*, 189–204.

Tripod Solutions. (2007). *Tripod Delta proactive.* Retrieved 25th May from http://www.tripodsolutions.net.

Van der Want, P. G. D. (1996). Tripod incident analysis methodology. In J. van Steen (Ed.), *Safety performance measurement* (pp. 99–106). Rugby, UK: Institution of Chemical Engineers.

Vaquero, C., Garcés, M. I., & Rodríguez-Pomeda, J. (2000). Impact of organization and management on complex technological systems safety: The nuclear lessons. *International Journal of Technology Management*, *20*(1/2), 214–241.

Vaughan, D. (1999). The dark side of organizations: Mistake, misconduct, and disaster. *Annual Review of Sociology*, *25*, 271–305.

Wagenaar, W. A., Groeneweg, J., Hudson, P. T. W., & Reason, J. T. (1994). Promoting safety in the oil industry. *Ergonomics*, *37*(12), 1999–2013.

Wagenaar, W. A., Hudson, P. T. W., & Reason, J. T. (1990). Cognitive failures and accidents. *Applied Cognitive Psychology*, *4*, 273–294.

Weil, R., & Apostolakis, G. (2001). Identification of important organizational factors using operating experience. In B. Wilpert & N. Itoigawa (Eds.), *Safety culture in nuclear power operations* (pp. 139–168). London: Taylor & Francis.

Westrum, R. (1997). Social factors in safety-critical systems. In F. Redmill & J. Rajan (Eds.), *Human factors in safety-critical systems* (pp. 233–256). Oxford: Butterworth-Heinemann.

Wiegmann, D. A., Zhang, H., Von Thaden, T. L., Sharma, G., & Gibbons, A. M. (2004). Safety culture: An integrative review. *The International Journal of Aviation Psychology*, *14*(2), 117–134.

Wilpert, B. (2000). Organizational factors in nuclear safety. In S. Kondo & K. Furuta (Eds.), *Proceedings of the international conference on probabilistic* *safety assessment and management (PSAM 5), Osaka, Japan* (pp. 1251–1265). Tokyo: Universal Academy Press.

Wogalter, M. S., Dempsey, P. G., & Hancock, P. A. (2001). Defining ergonomics/human factors. In W. Karwowski (Ed.), *International encyclopedia of ergonomics and human factors* (pp. 35–37). London: Taylor & Francis.

Zitrou, A., Bedford, T., & Walls, L. (2007). An influence diagram extension of the unified partial method for common cause failures. *Quality Technology & Quantitative Management*, *4*(1), 111–128.

Chapter 4

Discussion

In addition to the issues for further consideration that are discussed in the research paper, the first part of this chapter presents some suggestions for further improvement of the proposed approach. The second part of this chapter discusses how the approach can be applied and validated.

4.1 Further improvement of the new approach

As discussed in the paper, the operational SIL cannot be higher than the design SIL, which is in line with the ARAMIS approach. This philosophy assumes that the design SIL is based on an ideal situation in which humans and organisations function optimally (i.e., good enough to maintain the design SIL during the operational phase). In practice, a certain influence of human and organisational factors may already be included in the design SIL, either because the calculation of the design SIL is based on field data that contain some influence of human and organisational factors, or because the system designers have increased the technical reliability of the system to compensate for the influence of human and organisational factors. This is currently not accounted for in the calculation of the operational SIL. A possible solution would be to redefine the rating process in order to allow for a positive contribution of the safety influencing factors to the achieved SIL, in case the state of safety influencing factors is better than what is required to maintain the design SIL during the operational phase. On the other hand, it makes some sense to say that one cannot claim higher reliability of a technical system just because the humans and organisations surrounding it function so well. This issue is also related to the anchoring of the optimal state of the safety influencing factors (good enough, average, or best) and should be considered further.

A consequence of expressing the impact of the safety influencing factors as a linear variation in the achieved SIL is that a change in a rating corresponds to an exponential variation in the failure probability, because of the exponential relationship between SIL and failure probabilities. As pointed out in the paper, one can question whether this is the most appropriate way of modelling. However, there is one more aspect of the relationship between the achieved SIL and the failure probability that needs further consideration. The safety integrity levels are defined as intervals of the failure probability (see Table 1.1), with fixed upper and lower bounds. For example, if a safety instrumented system operating in low demand mode has an average probability of failure on demand that is greater than 10^{-3}, this system cannot achieve SIL 3. Therefore, one can argue that it is incorrect to round the operational SIL to the nearest integer. A possible solution would be to base the calculation of the operational SIL on the average probability of failure on demand (PFD) according to the design, instead of on the design SIL. This would lead to the following equation:

$$\mathrm{SIL}_{\mathrm{operational}} = \left(\theta \sum_{i=1}^{8} R_i W_i - 1\right) \log \mathrm{PFD}_{\mathrm{design}} \tag{4.1}$$

The outcome of (4.1) is then cut off, instead of rounded to the nearest integer (e.g., if the outcome is 2.6, this yields an operational SIL of 2). This equation may give a more realistic prediction of the operational SIL. Moreover, it provides the opportunity to use equipment with a lower average probability of failure on demand in order to compensate for the influence of human and organisational factors, without having to comply with the other requirements of a higher SIL. However, this equation also has some disadvantages. The equation presented in the paper covers both low demand mode and high demand or continuous mode, whereas (4.1) only covers low demand mode. This issue could be solved with a modified version of (4.1) that is based on the probability of a dangerous failure per hour according to the design.

The main drawback is that the achieved SIL is not only determined by the failure probability, but also by a number of qualitative requirements for the system design and several other lifecycle phases. The achieved SIL may be lower than what is theoretically possible based on the failure probability, if the system does not comply with other requirements. Moreover, human and organisational factors are likely to have an impact on the fulfilment of the qualitative requirements as well. Hence, using (4.1) may yield a prediction of the operational SIL that is too optimistic. This issue could possibly be solved by limiting the design failure probability used as input for (4.1) to the lower bound of the interval corresponding to the design SIL. For now, the calculation of the operational SIL is based on the design SIL, as proposed in the paper, but the possibility to use (4.1) should be investigated further.

4.2 Validation and application

As indicated in Chapter 2, the research strategy followed has certain implications for the validity and applicability of the results. The proposed approach to address human and organisational factors in the operational phase of safety instrumented systems is developed based on existing theories and models, not on first-hand field experience. Moreover, the approach has not (yet) been tested in practice, and the implementation is limited to an illustrative case study. On the other hand, the building blocks of the approach are based on field experience and have been tested in practice. However, combining valid theories and models and adapting them to a specific domain does not guarantee that the resulting approach is valid as well. Therefore, a new validity test is needed, which should compare the results of the proposed approach with field data.

Such a validity test can be based on failure rates and accident statistics from the real operation of safety instrumented systems, as far as these are available. However, in some application domains failures are so rare that other safety performance indicators may have to be used instead, for example near-misses. Testing the validity of the proposed approach consists of two parts: validation of the calculation of the operational SIL (i.e., the aggregated impact of human and organisational factors on the achieved SIL), and validation of the individual safety influencing factors (i.e., the impact of each safety influencing factor on the achieved SIL).

When validating the calculation of the operational SIL, the fundamental question is whether human and organisational factors actually have the predicted negative impact on the operational SIL. As the achieved SIL cannot be measured directly, failure rates have to be used instead. One way to validate the calculation of the operational SIL is to correlate the difference between the design SIL and the operational SIL with the difference between the expected failure rate (from generic data used during design) and the real failure rate (obtained from field data collected during operation). However, this does not say anything about the causal relationship, because other factors may influence the failure rate as well. A more specific validation can be obtained using data from accident investigation. One could for example correlate the difference between the design SIL and the operational SIL with the proportion of failures that can be traced back to human and organisational factors.

To test the validity of the individual safety influencing factors, one could change the state of a safety influencing factor (e.g., launch a new training programme to improve the safety influencing factor *training*) and compare the failure rates before and after the change. The weighted rating for this safety influencing factor is then correlated with the failure rate. Again, data from accident investigation can be used as well. In this case, the correlation between the weighted rating for a specific safety influencing factor and the proportion of failures that can be traced back to this factor could be explored. It should be noted that these accident statistics also can be used to weight the safety influencing factors, as described in Section 4 of the research paper.

Roughly speaking, there are two ways to collect comparison data for the validity test. One can compare failure data for similar equipment between different organisations (with different ratings of the safety influencing factors), or within the same organisation over time (to see the effect of changes in ratings of the safety influencing factors). However, collecting enough field data for statistical validation will require considerable effort. Especially the second part of the validity test is a challenge, because changing the state of one safety influencing factor may have an impact on the state of other safety influencing factors, and because a failure will often be related to several safety influencing factors. Therefore, a practical recommendation is to perform only the first part of the validity test to check whether human and organisational factors actually have the predicted negative impact on the operational SIL. If this is the case, one may assume that the individual safety influencing factors are valid as well, because previous research (Wagenaar et al., 1994) has shown their validity as predictors of accidents, although not specifically in the context of safety instrumented systems.

Regarding the practical application of the proposed approach, it is worth mentioning that the approach has not been developed for a specific domain. This is in line with the IEC 61508 standard, which is a generic standard common to several industries, independent of the technology used. The approach can be tailored to a specific situation with parameters for the relative importance of the safety influencing factors and for the overall importance of human and organisational factors for the performance of the system under consideration. Moreover, these parameters can be adjusted using field experience. This makes that the approach, in principle, can be applied to any safety instrumented system.

References

Beck, U. (1997). *De wereld als risicomaatschappij.* Amsterdam: De Balie.

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

Duijm, N. J., & Goossens, L. (2006). Quantifying the influence of safety management on the reliability of safety barriers. *Journal of Hazardous Materials*, *130*, 284–292.

IEC. (2000). *IEC 61508 – Functional safety of electrical/electronic/programmable electronic safety-related systems. Part 1 to 7.* Geneva: International Electrotechnical Commission.

IEC. (2004). *IEC 61511 – Functional safety – Safety instrumented systems for the process industry sector. Part 1 to 3.* Geneva: International Electrotechnical Commission.

IEC. (2005). *IEC 61508-0 – Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 0: Functional safety and IEC 61508.* Geneva: International Electrotechnical Commission.

ISO. (1986). *ISO 8402 – Quality vocabulary.* Geneva: International Standards Organisation.

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

Kletz, T. (2001). *An engineer's view of human error* (3rd ed.). New York: Taylor & Francis.

Rausand, M., & Høyland, A. (2004). *System reliability theory – Models, statistical methods and applications.* Hoboken, NJ: John Wiley & Sons.

Reason, J. (1997). *Managing the risks of organizational accidents.* Aldershot, UK: Ashgate.

Redmill, F., & Rajan, J. (Eds.). (1997). *Human factors in safety-critical systems.* Oxford: Butterworth-Heinemann.

Rouvroye, J. L., & Brombacher, A. C. (1999). New quantitative standards: Different techniques, different results? *Reliability Engineering and System Safety*, *66*, 121–125.

Schönbeck, M. (2006). *Reliability of safety systems.* Literature review, TU/e, Eindhoven.

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

Verschuren, P., & Doorewaard, H. (2000). *Het ontwerpen van een onderzoek* (3rd ed.). Utrecht: Lemma.

Wagenaar, W. A., Groeneweg, J., Hudson, P. T. W., & Reason, J. T. (1994). Promoting safety in the oil industry. *Ergonomics*, *37*(12), 1999–2013.

Wagenaar, W. A., Hudson, P. T. W., & Reason, J. T. (1990). Cognitive failures and accidents. *Applied Cognitive Psychology*, *4*, 273–294.

Appendix A

Development of the new approach

This appendix gives some more details of the proposed approach to address human and organisational factors in the operational phase of safety instrumented systems, which is presented in section 4 of the research paper. It outlines the main steps in the development of the approach and covers some of the choices made, in addition to the explanations given in the paper.

For the development of the approach, a number of design criteria have been formulated that the approach has to fulfil. The approach should:

1. Be suitable for the operational phase of safety instrumented systems
2. Use indicators that reflect relevant human and organisational factors
3. Be linked to the achieved SIL during operation
4. Allow for quantification
5. Be practically feasible (i.e., can be implemented in practice within reasonable resource limitations)
6. Be intuitive and allow for visualisation
7. Be suitable to improve safety

During the selection of the safety influencing factors, which are based on the general failure types corresponding to the Swiss cheese model, these factors have been tailored to the operational phase of safety instrumented systems.

It should be noted that there are several versions of the list of general failure types, which are slightly different. The safety influencing factors are mainly based on the version presented by Reason (1997), but older versions (Wagenaar et al., 1994, 1990) have been studied as well. Reason (1997) describes relationships between basic lifecycle processes and the general failure types. He allocates them to four lifecycle processes (design, build, operate, and maintain) and three general processes (statement of goals, organisation, and management), which are important in all lifecycle phases. The general failure types defence planning (sometimes called poor defences), hardware (sometimes called hardware failures), and design (sometimes called design failures) are exclusively related to the design and build phases. Therefore, these three general failure types are eliminated. The remaining eight general failure types are slightly reformulated to be in line with the term *safety influencing factors*. All general failure types, with the corresponding processes and safety influencing factors, are shown in Table A.1.

Table A.1: General failure types with corresponding processes and safety influencing factors

General failure type	Process	Safety influencing factor
Maintenance management	Maintain	Maintenance man.
Procedures	Operate, Maintain	Procedures
Error-enforcing conditions	Operate, Maintain	Error-enforcing cond.
Housekeeping	Operate	Housekeeping
Incompatible goals	State goals	Goal compatibility
Communications	Manage	Communication
Organisation	Organise	Organisation
Training	Operate, Maintain	Training
Hardware	Build	-
Design	Design	-
Defence planning	Design, Build	-

Error-enforcing conditions is a special general failure type, because it is a source of unsafe acts in itself (conditions that force people to operate in a manner not foreseen during system design), while it may also function as an intermediate layer between other general failure types (e.g., maintenance management) and unsafe acts. The definition of the safety influencing factor focuses on the independent part, and this should be reflected in the checklist used during audits. It can be concluded that the selection of safety influencing factors fulfils design criteria 1 and 2, because the safety influencing factors are tailored for the operational phase of safety instrumented systems,

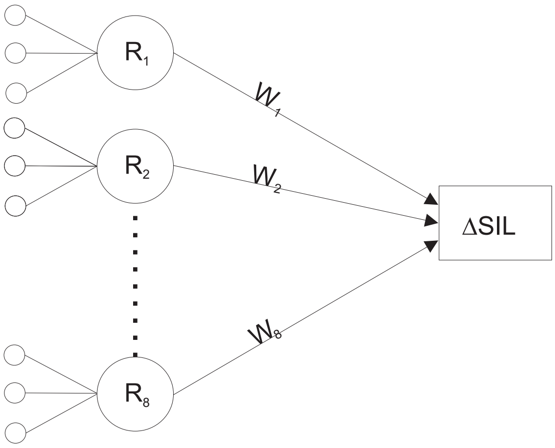

Figure A.1: Link between the safety influencing factors and the achieved SIL

and because their state is measured during an audit based on specific, measurable indicators for each safety influencing factor.

For the quantification procedure, especially design criteria 1, 3, 4, and 5 are important. Criteria 3 and 4 may seem obvious, but most quantitative models for human and/or organisational factors are developed for quantitative risk assessment and cannot be linked directly to the achieved SIL during operation. This makes the ARAMIS approach particularly interesting, because it explicitly addresses the reliability of safety barriers. The ARAMIS approach scores also positively on criterion 5, because it establishes a direct link between organisational factors and the reliability of safety barriers, thus making the approach practical. Criterion 1 is fulfilled by adapting the ARAMIS approach to the operational phase of safety instrumented systems. The ARAMIS approach considers all types of safety barriers (e.g., also firewalls), using different sets of weight factors. This distinction is eliminated.

The direct link between the safety influencing factors and the achieved SIL using weight factors can be visualised as in Figure A.1. The safety influencing factors with the highest weighted ratings (R_iW_i) contribute most to the difference between the design SIL and the operational SIL (ΔSIL). The ratings are based on a set of indicators for each safety influencing factor. The number of indicators is not fixed. It should be noted that Figure A.1 only illustates the influence of the weighted ratings on ΔSIL.

Having developed a quantification procedure to link the safety influencing factors to the achieved SIL, design criteria 6 and 7 still have to be fulfilled. These are met by the five-step approach presented in the paper, which includes a step that provides guidance for preventive or corrective action to improve safety, based on the results of the previous steps. The underlying principles of the approach are visualised by the Swiss cheese model, which shows how the performance of safety barriers (in this case, safety instrumented systems) is influenced by upstream human and organisational factors. Moreover, the order of the five steps is intuitive. If θ is zero (or almost zero), step 2 and 3 can be skipped. If it turns out in step 2 that some safety influencing factors have no or negligible influence (W_i is zero or almost zero), these safety influencing factors do not have to be rated during the audit in step 3. The order of steps 4 and 5 speaks for itself.

Appendix B

Case study

This appendix gives some more details of the case study that is presented in section 5 of the research paper. Each of the steps is treated successively.

In *step 1*, the proportion of the design SIL that can be explained by human and organisational factors, denoted θ, is taken to be 0.5.

The data belonging to *step 2* are shown in Table B.1.

The data from the illustrative rating process in *step 3* are shown in Table B.2.

In *step 4*, the weighted ratings are calculated, as shown in Table B.3. Next, the operational SIL is calculated as follows:

$$\mathrm{SIL}_{\mathrm{operational}} = \left(1 - \theta \sum_{i=1}^{8} R_i W_i\right) \mathrm{SIL}_{\mathrm{design}} = (1 - 0.5 \cdot 0.29375) \cdot 3 \approx 2.6$$

Finally, suggestions for preventive action are given in *step 5*.

Table B.1: Safety influencing factors with relative weights and normalised weight factors

Safety influencing factor i	Weight $\widetilde{W_i}$	Weight factor W_i
1. Maintenance management	1	0.125
2. Procedures	1	0.125
3. Error-enforcing conditions	1	0.125
4. Housekeeping	1	0.125
5. Goal compatibility	1	0.125
6. Communication	1	0.125
7. Organisation	1	0.125
8. Training	1	0.125

Table B.2: Ratings for the safety influencing factors

i	# indicators causing concern	total # indicators	Rating R_i
1	4	20	0.2
2	6	20	0.3
3	3	20	0.15
4	2	20	0.1
5	13	20	0.65
6	4	20	0.2
7	4	20	0.2
8	11	20	0.55

Table B.3: Weighted ratings for the safety influencing factors

i	R_i	W_i	Weighted rating R_iW_i
1	0.2	0.125	0.025
2	0.3	0.125	0.0375
3	0.15	0.125	0.01875
4	0.1	0.125	0.0125
5	0.65	0.125	0.08125
6	0.2	0.125	0.025
7	0.2	0.125	0.025
8	0.55	0.125	0.06875
$\sum_{i=1}^{8} R_iW_i$			0.29375