Preprint version of Harms-Ringdahl L. *Analysing Safety Functions and Barriers – Experiences from Different Industrial Sectors*. In Spitzer, U., Schmocker, U., and Dang, V.N. (eds.) *Probabilistic Safety Assessment and Management*. Springer (pp 100 – 109) 2004. Proceedings of ESREL 2004.

Analysing Safety Functions and Barriers – Experiences from Different Industrial Sectors

Lars Harms-Ringdahl[1]
Royal Institute of Technology, Stockholm, and
Institute for Risk Management and Safety Analysis,
Stockholm, Sweden

Abstract

The paper gives a summary of approaches to describing and modelling safety characteristics, including safety functions and barriers. In three examples, the safety function concept has been used to describe how actual safety systems worked. The examples are an incident investigation, a safety analysis of a part of a pharmaceutical plant, and safety rules in the railway industry. Advantages and disadvantages of the concept and approach are discussed.

1 Introduction

There are many approaches to the description and analysis of safety characteristics in industry and in the workplace. General examples are barriers related to energy and safety management systems. An overview [1] found varying terminology, sometimes with poorly defined terms, which can be expected to cause confusion in many situations.

As a result of the study, further work has been performed on modelling safety in different types of industrial systems, using the concepts of safety functions and barriers. The aim of this paper is to give examples of theoretical and practical applications of the safety function concept.

2 The Safety Function Concept

2.1 Different aspects

Energy models have been used for a long time in a safety context, and they usually involve technical and also sometimes organisational aspects of barriers. In MORT [2], barriers are defined as physical and procedural measures to direct energy in wanted channels and control unwanted release. The energy concept and energy barriers fit quite naturally into many applications. The term "defence" [3] can represent several types of safety features. In simple terms, defences shall prevent hazards from causing losses. Such defences can be combined into several layers, but may be weakened by various kinds of problems.

Within certain industrial sectors, special concepts are applied; for example, the nuclear industry uses the term *"defence in depth"* whereas the chemical industry employs the term "*protection layer"*. For references and further examples see [1].

One scheme for the classification of barriers has been proposed by Hollnagel [4]. It contains four main categories:

- Material, or physical, barriers.

[1] e-mail LHR@irisk.se

- Functional (active or dynamic) barriers.
- Symbolic barriers.
- Immaterial barriers (monitoring or prescribing).

The terminology used to describe safety features varies considerably. “Safety function” is a rather common term, but no clear definition was found in a literature study [1] from 1999. Even in the “Standard on Functional Safety” [5] where the term is used several times, it is not defined. It might therefore be used in different senses in various applications.

2.2 Definition and characteristics

Due to the varying terminology, a general definition of safety function has been proposed [6]:

> *A safety function is a technical, organisational or combined function that can reduce the probability and/or consequences of accidents and other unwanted events in a system.*

Quite deliberately, safety function (SF) is defined as a broad concept. The actions of individuals are included within the organisational function, although they might be clearly spelled out in an alternative definition.In principle, SF covers all the concepts presented earlier in this chapter. In specific applications, however, it requires more concrete characterisation. For practical and operational applications, any SF can be described by a set of parameters. One suggestion [1] is that it should encompass:

a) Level of abstraction.

b) Systems level.

c) Type of safety function.

d) Type of object.

a) *Level of abstraction* starts at the lowest level with a concrete solution, e.g. a safety relay or an operator checking a temperature meter. At higher levels, it can refer to protection again excess temperature or a theory of temperature control.

b) *Systems level* is related to the systems hierarchy. Examples of levels are component, subsystem, machine, department, and a whole factory. The concept can also be extended to societal level so as to include fire brigades, emergency services in general, laws regulating safety, and so on.

c) *Type of safety function* describes what is included in an SF. It can be divided into more specific and detailed types of technical and organisational functions. Also, functions where safety is not the main objective may have key safety features.

d) *Type of object* characterises the object, i.e. the system that is to be safe. This may be a technical system, software, control room and related equipment, etc.

2.3 Measuring Efficiency and Importance

An SF can be described by a set of characteristics intended to describe its contribution to overall safety, and which also provides a basis for its evaluation. Examples of characterisations are as follows.

- “*Efficiency*” is intended to give a measure of how well an SF can fulfil its aim. A general definition has not yet been formulated, but examples are given in the first two application examples (see below). An SF can be defined in terms of a success rate, or categorised as working or not.
- The "*importance*" of an SF can be measured in various ways. One categorisation is based on the effects of the failure of an SF. For example, failure might lead directly to an accident, give rise to a latent failure, or have some effect on the probability of an accident.
- The "*robustness*" of the SF to deviations, interruptions to procedures, etc. gives a kind of quality measure.

3 Application Examples

3.1 Accident Investigations

Method

When an accident has taken place, the course of events leading to its occurrence is usually the main target of investigation. A further question is how the accident could have happened. Especially in systems with large hazards, there are several safety features in place to prevent accidents from occurring. Accordingly, an essential complementary aim of any investigation is to analyse why the safety system failed.

In this example, a method [7] for event investigation based on SFs has been applied. The investigation was performed in five broad steps:

1) Selection of accident to investigate.
2) Deviation Investigation of the event.
3) Identification of SFs.
4) Classification and structuring of SFs.
5) Analysis of SFs.

The second step, the Deviation Investigation [6], contains three principal steps:

- Identification of deviations prior to the accident.
- Evaluation of the importance and seriousness of the deviations.
- Proposals for potential improvements.

The third main step (Identification of SFs) involves scrutiny of the list of deviations. If any SF is identified among these, it is recorded in a list of SFs. Also, proposed improvements give information about any SFs that are connected to the incident.

The fourth step, that of structuring SFs is based on the parameters a) to d) referred to above. The analysis in the fifth step was quite simple in this case. The classification was based on if whether or not the SF had performed intended function when the accident occurred.

The incident

The case study was based on an incident at an electrical power distribution station in direct connection with a hydropower station. Part of the electricity net had been disconnected when servicing was performed. When the service was finished, one of the technicians reconnected the station to the electric power line.

By mistake, he went to a wrong coupling booth, adjacent to the correct one. When he made the connection, a high voltage line was connected to earth. A number of companies were involved in service operations in the workplace. Each of them had a specific role; one was concerned with the hydropower station, one with the power lines, and two with service tasks. This organisational structure was the product of having split up one original company into several smaller ones, and also an outsourcing process.

Results

Deviations were identified in interviews with three persons, and through the scrutiny of documentation. The investigation found 42 deviations prior to the incident, with the majority related to management issues. More than half of these were evaluated as essential to consider further. The investigation generated around 30 proposals for improvements.

In this example, the identification of safety functions was based entirely on the Deviation Investigation protocol. The text of the protocol was studied, and any issue interpreted as involving a safety function noted down. Both deviations and ideas for improvements were examined.

The SFs were classified into two groups: technical and organisational. The SFs were structured and grouped as in Table 1. The first two rows include technical SFs, and the rest

organisational. The structuring was also based on different systems levels, going from the workplace (3) to societal functions (7).

Safety function	**Σ**	**Performed intended function**				***OK***
		Yes	Partly	No	SI*	
1 General technical SFs	1	0	0	0	1	0%
2 Local technical SFs	6	2	1	1	2	33%
3 Local organisational SF	11	4	1	5	1	37%
4 Company management	6	0	0	5	1	0%
5 Co-ordination between companies	10	1	1	1	7	10%
6 Corporate safety management	5	0	0	2	3	0%
7 Societal SFs	1	1	0	0	0	100%
Total	40	8	3	14	15	20%
Share	100%	20%	7%	35%	38%	-

Table 1. Summary of safety functions at incident at electric power station. (SI means that a safety function was noted as Suggested Improvement.)*

Comments

Of the recorded 40 SFs, a majority did not operate satisfactorily, and only 20% worked as expected (the OK column in Table 1). Thus, the analysis indicated low efficiency of functions. It should be remembered, however, that the aim was to identify problems, not all SFs.

As many as 32 SFs did not work or needed improvement. It is interesting to note that most problems were at higher organisational levels (rows 4, 5 and 6 in Table 1), where there were 20 unsatisfactory SFs out of 21.

One experience was that people and work groups quickly obtained an intuitive understanding of the safety function concept, and its practical application.

3.2 Analysis of an industrial installation

The site

The second example concerned an industrial installation, where SFs were identified and analysed [8]. The case study was performed at a section in a pharmaceutical plant. In principle, there is simple batch production, where different substances are added and mixed. An essential part of the work is manual, guided by formal procedures and batch protocols. In the workplace, 20 people are employed in total, and production is run in shifts. The workplace forms part of a large factory with an over-arching organisational hierarchy. This means that overall production planning also sets guidelines for health and safety work.

Method

A Safety Function Analysis (SFA) [6, 8] was performed on the system. The goals of the analysis were to achieve:

- A structured description of the system's safety functions.
- An evaluation of their adequacy and weaknesses.
- Proposals for improvements, if required.

An SFA normally contains six main steps. Like other methods, it also includes a preparation and a concluding part.

1. Selection of a set of hazards for which safety is to be analysed.
2. Identification of existing safety functions for these hazards.
3. Structuring and classifying these functions.

4. Estimating the efficiency and other characteristics of the safety functions.
5. Assessing whether improvements are necessary.
6. Proposing improvements.

In this case, the identification step (Step 2) consisted in a structured interview with a person who knew the system well. He had also participated in a previous risk analysis when hazards had been studied. For a set of specific hazards or accident scenarios, you pose questions like:

- How is the likelihood of an accident kept low?
- How are consequences kept at a low level?
- How is damage reduced if an accident should occur?

Results

The outcome was a list of around 50 SFs, which were analysed and structured into six major groups. At a second round of analysis, estimates of characteristics of the SFs were made. Three persons independently estimated e.g. the "efficiency" of each SF. Here, it was defined as the probability that the intended SF was achieved. Table 2 shows a summary of results.

SF Group		**Efficiency***		
	Number of SFs	Low	Medium	High
1 Containment, vessel	11	0%	8%	92%
2 Control system	14	14%	32%	54%
3 Reduction of consequences	4	83%	17%	0%
4 Formal routines	8	0%	29%	71%
5 Informal routines	7	28%	50%	22%
6 Company management	10	45%	50%	5%
Total	54	26%	31%	43%

Table 2. Summary of identified safety functions and estimates of their efficiency.

Judgements of efficiency were grouped into three classes: "Low" meant a probability of functioning of less than 50%; "High" was an estimate greater than 99%; and, "Medium" was an estimate between these two probability values.

The estimates of efficiency revealed several weaknesses in the system. In all, 26% of the safety functions were regarded as having low efficiency. These estimates were useful later, when the need for improvements was assessed. Discussions about how efficiency could be increased helped create ideas for improvements.

As a conclusion of the analysis, improvements were suggested by the analysis team. This step generated 47 suggestions, more than half of which were related to management issues.

3.3 Modelling of Safety Rules for Railways

A study [9] has been performed of different ways of describing safety rules for railways. The safety function concept has been tried – both for classification of a general structure, and also at a more detailed level. In both these exercises, a top-down approach was adopted.

A tentative general structure for railway safety based on a set of SFs was sketched out. The chain from abstract to more concrete safety functions is illustrated in Figure 1. It contains a set of elements. Except for the hazards, all elements can be described as SFs, which run from an abstract to a more concrete level.

- In the system, a number of hazards need to be controlled.
- The "General SF" can reduce probability and/or consequences of accidents.
- There are a number of "functional resources" (techniques, organisations, people).
- Some of these resources can be formalised as a set of safety rules.
- Finally, technical solutions and organisational actions transform demands into practical reality.

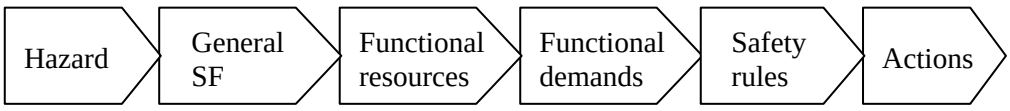

Figure 1. Model for railway safety rules, going from an abstract to a more concrete function.

General structure

Structuring of a railway safety system can be performed in various ways. In this case, three main parameters were selected:

1) *Dependence*; the SF can be internal to one organisation or shared between several organisations.
2) *Solution*; the SF can be realised as either a technical or an administrative solution, or a combination of the two.
3) *The system state* can be classified as "Normal" (working as planned), "Planned deviation", or "Disturbance" (unplanned, occurring quickly).

This was considered to be a fairly simple way of encompassing all types of situations for which safety actions were needed. Combining these parameters generated a matrix with 18 basic cells. The matrix boxes were then filled in with more specific safety features by a group of specialists. Between three to eight subheadings might be relevant to each box, giving around 100 subheadings.

Communication between actors

The activity "Communications between actors" was chosen as an example. It was analysed and divided into 6 basic headings, representing high-order functions:

1) General procedures for communication.
2) Communication across legislative borders.
3) Terminology and methods.
4) General conventions.
5) Special conventions.
6) Responsibilities and decisions.

Based on this structure, SFs at a more detailed level were identified. This was achieved by going from an abstract function to a more concrete one, and from a high systems level to a lower one. A supplementary procedure consisted in focusing on requirements and problems that needed solutions. A coarse risk analysis was made of scenarios related to communication. This resulted in the identification of around 60 SFs related to communication.

4 Discussion and Conclusions

4.1 Concept and method

The definition

The definition of safety function is general and intended to cover various types of barriers and defences. A comparison can be made with the concept of "barrier", which usually has a concrete meaning. By contrast, an SF can be either highly abstract or very specific. Important additions to the SF concept are the parameters (a) abstraction and (b) systems level, which allows more holistic and comprehensive modelling of safety features. For example, this makes it easier to include unofficial safety functions, such as the informal behaviour of work groups.

Basic modelling approaches

Three examples of applications have been described. The accident investigation and the system analysis represent a bottom-up approach. In both cases, specific SFs in the system were identified and listed. These concrete findings were then arranged in a structure, using the parameters (a) to (d) (Section 2.2) as support.

The third example, of rule modelling, represents a top-down approach. The starting point is usually at a fairly high systems level, and, again, the parameters in Section 2.2 are relevant. It is

also possible to start at intermediate level. For example, in Figure 1, you can start with "safety rules" and look both forwards and backwards.

Evaluations

Two ways of practical evaluation were tried out. In the accident investigation, a classification was made with regard to whether or not an SF had performed its intended function. This is a fairly simple and straight-forward approach.

In the system analysis case, a judgement was made of the efficiency of the SFs. This is more difficult and has a higher degree of subjectivity. However, there was fairly good agreement between the three independent assessors [8].

In the third example, the modelling of rules, there was no obvious way of making an evaluation. However, several approaches might be considered. One is to identify potential gaps between different levels and systems, another is to verify the logical consistency in the system.

In general, much more can be done with regard to applying methodologies for the evaluation of SFs, and the exercises here should be seen just as examples.

4.2 Experiences

General experience

Around ten studies with practical applications of SFs have been made. A general experience is that several functions in each system were easily identified. In the bottom-up cases, the number of SFs has been around 50. In top-down approaches the number can very large, which means that some kind of “stop rule” is usually needed. However, in descriptions based on barriers or the like, the numbers are usually much lower. This indicates that the barrier approach usually covers a subset of the items encompassed by a general SF approach

Understanding the concept

The SF concept has been applied in several work groups and in different settings. A general impression is that the concept has been easy to understand without any lengthy explanations. These experiences concerns applications with people in a participating role, it would be more difficult to apply the concept independently.

Management aspects

Management issues had a prominent role in the case studies. In the accident investigation case, 33 management SFs were identified. Six of these had performed their intended function, giving a "success rate" of less than 20%. Considering company management (elements 4, 5 and 6 in Table 1), just one out of 21 worked satisfactorily.

In the case of the systems analysis, there were around 25 SFs associated with management. Also here, the efficiency was considered low, especially for corporate management (Element 6 in Table 2).

In both these cases, several informal SFs were identified and included in the structure and analysis. Most of them were ranked as important for safety, but they *had not been considered* as a part of regular safety work.

The problems with management came as a surprise to the companies concerned, both of which had formal quality and environmental management systems. This indicates a potential to use SFs as a basis for alternative auditing.

About SFs

Based on the author's experience there are a number of advantages and disadvantages with the safety function concept and its methodology. Positive aspects are that it can:

- Identify management issues relevant to safety quite efficiently compared with some other methods [8].
- Handle fairly large numbers of functions.

- Give a holistic perspective on system safety.
- Provide for consistent handling of technical and organisational SFs.
- Handle informal SFs and not be reliant on a hierarchical form of thinking.
- Create understanding of how safety is controlled in reality.
- Offer an alternative tool for safety auditing.

Disadvantages are that:
- The concept is fairly new and not well tested.
- The structuring of a system can be done in several ways.
- Results can be complex when there are many SFs, which can make analysis difficult.

Acknowledgement

The project was supported by the Swedish Council for Working Life and Social Research, and Ångpanneföreningen's Foundation for Research and Development.

References

1. Harms-Ringdahl L. On the modelling and characterisation of safety functions. In Schueller & Kafka (eds): Safety and Reliability. A.A.Balkema, Rotterdam. pp. 1459-1462, 1999.
2. Johnson W.G. MORT Safety assurance systems. Marcel Dekker, New York, 1980
3. Reason J. Managing the risks of organizational accidents. Ashgate Publishing, Aldershot, 1997.
4. Hollnagel E. Accident Analysis and Barrier Functions. Institute for Energy Technology. Kjeller, Norway, 1999.
5 IEC (International Electrotechnical Commission). Functional safety: safety related systems (Standard IEC 1508). IEC, Geneva, 1998.
6. Harms-Ringdahl L. Safety analysis - Principles and practice in occupational safety (2nd edition). London: Taylor & Francis, 2001.
7. Harms-Ringdahl L. Investigation of barriers and safety functions related to accidents. In Bedford & van Gelder (eds.): Safety and Reliability. A.A.Balkema, Rotterdam, pp. 763-769, 2003.
8. Harms-Ringdahl L. Assessing safety functions – results from a case study at an industrial workplace. Safety Science 2003, Vol. 41, Issue 8, pp. 701 – 720, 2003.
9. Harms-Ringdahl L. and Kecklund L. Safety Functions in Railways - a Structural Analysis of Safety Rules. Submitted, ESREL 2004, Berlin.