Preprint version *Safety Science* 47 (2009) 353–363

Analysis of safety functions and barriers in accidents

Lars Harms-Ringdahl [a, b]

a) Institute for Risk Management and Safety Analysis, Bergsprängargränd 2A, SE-116 35 Stockholm, Sweden
b) Karlstad University, Department of Public Health Sciences, SE-651 88 Karlstad, Sweden
e-mail: LHR@irisk.se

Abstract

A new method for accident investigations is presented. It is based on the concept of safety function, which is defined as a technical or organisational function, a human action or a combination of these, that can reduce the probability and/or consequences of accidents and other unwanted events in a system. An analysis starts with the identification of safety functions related to the event. These are structured; an assessment is then made of whether they worked or not, and finally safety improvements are proposed.

The method has been applied to five different incidents, coming from different types of work sites, such as electrical power distribution, a railway, and hospitals. For each case, around 40 safety functions were identified, of which less than half had worked. It was found that technical, organisational and human safety features existed side-by-side. The method supports a consistent analysis of a variety of safety features, and can integrate them into a common format.

Each system contained formal and informal elements in parallel, often overlapping. This can be seen as safety redundancy, which makes the safety system less vulnerable to change that supports the preservation of safety. It might be more adequate to describe this as a safety web rather than a distinct set of barriers, and there is also an analogy with the concept of safety resilience.

Keywords
Accident analysis, Barrier, Incident analysis, Organisational factor, Resilience, Safety function

1 Introduction

The main target of an accident investigation is usually to explain the course of events. An essential question is how the event could have happened. In most systems, especially in the case of large hazards, there are several safety features in place to prevent accidents from occurring. Accordingly, an essential complementary aim of any investigation should be to analyse how the safety system failed.

For a long time, there has been considerable interest in the modelling and analysis of safety features and accident prevention. However, concepts and terminology related to safety features vary considerably (e.g. Sklet, 2006), causing confusion and difficulties in comparing different approaches. There are a number of accident investigation methodologies, which more or less explicitly include barriers and other safety features, and their roles in the course of an accident.

Interest has been especially great in the off-shore, chemical, and nuclear industries, and accordingly research has been heavily oriented towards major hazard installations (e.g. Hale, 2006; Sklet, 2006). There are many research challenges in areas with complex technical and organisational settings, which require sophisticated methods and models to further improve preventive measures.

However, this type of industry and these safety aspects represent only a small fraction of the field of accident prevention. Common workplaces, and to an even larger extent out-of-work situations, produce many more injuries and fatalities than major hazard industries. Despite this, the analysis of barriers and other safety features has received less attention in these types of situations. The transfer of methods from high-risk areas is not uncomplicated, since they represent different kinds of conditions (Harms-Ringdahl, 2004).

There are several contributing elements to the safety level at the workplace, with technical and organisational safety features functioning together. Social factors and informal behaviour can also contribute in essential way.

These considerations have formed an interest to combine technical and formal as well as informal organisational safety features in a consistent framework, which needs to be multidisciplinary. This has also been a major motive for further developing barrier concepts and methodologies for fairly simple settings.

This paper is concerned with how safety characteristics can be modelled and evaluated on the basis of information from accidents and incidents. Its principal aims are to present a method that applies the concept of safety function and to demonstrate how it works in practical accident investigations. A further objective is to present the results that can be obtained from such investigations.

The method is intended to give information about the incident and circumstances at the actual workplace. The results can be used for improvements and learning locally. First after the application on several incidents, more general conclusions can be drawn.

The paper is based on experiences from earlier studies of barriers and safety functions, and is founded in a gradual development. The author has had earlier favourable experiences of applying the generic concept of safety function in safety analysis (Harms-Ringdahl, 2001, 2003a, 2003b). The main attention is on common workplaces rather than major hazard installations. The term accident is used for simplicity, but near-accidents and other unfavourable events are also addressed.

2 Concepts and methods

2.1 Concepts of barriers and safety functions

2.1.1 Safety barriers

There are many approaches to the description of safety characteristics in systems, and terms like barriers and defences are often used to describe them. Energy models have been used for a long time (e.g. Johnson, 1980), and they usually involve technical as well as organisational barriers. Examples are the containment of a chemical substance, and the maintenance procedure of the container.

A common term is *defence*, which is defined by Reason (1997) as “various means by which the goals of ensuring the safety of people and assets can be achieved”. A division has been made between “hard” defences, such as physical barriers and alarms, and “soft” defences e.g. regulation, procedures, and training. Defence is a wider concept than that of barriers. The same reference also refers to defence-in-depth as “successive layers of protection”.

One approach is to focus on the accident sequence and how it can be interrupted. One example is *barrier function*, which represents a function that can arrest the accident evolution so that the next event in the chain will not be realized (Svenson, 1991). A barrier function is identified in relation to the system(s) it protects, has protected, or could have protected.

A comprehensive review by Sklet (2006) found that there is no universal and commonly accepted definition of terms like safety barrier, defence, defence in-depth, layer of protection, safety function, either in the literature, or in regulations and standards. Sklet's review suggests that distinctions should be made between the terms "barrier" and "barrier function", which easily can be confused. Based on his review, Sklet (2006) suggests three definitions related to safety barriers.

- *Safety barriers* are physical and/or non-physical means planned to prevent, control, or mitigate undesired events or accidents;
- A *barrier function* is a function planned to prevent, control, or mitigate undesired events or accidents;
- A *barrier system* is a system that has been designed and implemented to perform one or more barrier functions.

According to Sklet, the barrier function describes the purpose of safety barriers, and it should have a direct and significant effect. A barrier function should preferably be defined by a verb and a noun, e.g. ''Close flow''. According to this set of definitions, a function that has an indirect effect is not classified as a barrier function, but as a risk influencing factor/function. The definitions relate to well-defined system, which are carefully planned and designed, and – as Sklet points out – they refer to major hazard installations.

2.1.2 Safety functions

Safety function is a rather common term, which is used in different situations. However, it is hard to find general definitions in the literature. One highly specialized characterization is given in the standard about electrical/electronic /programmable electronic (E/E/PE) systems (IEC, 2001). It is technically oriented, and assumes a clear intention and a specific hazard. It defines safety function as:

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

In this study, a general definition of safety function has been used (Harms-Ringdahl, 2001):

> *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.*

Safety function (SF) is here defined as a broad concept, and actions by individuals are included as an organisational function. The model behind the SF concept is simple: in a system there is a set of (safety) functions that prevent or reduce the consequences of injuries and losses, which can be caused by external or internal sources of risk. Examples on technical SFs are machine guards, safety relays and interlock circuits, and organisational SFs are safety rules and planning of job tasks. In the case studies more examples are given.

In principle, this definition of SF covers all the concepts presented above. For example, SF can include intentional functions with a direct effect (barrier functions), and also functions with undefined intentions and unclear effects, which are classified as risk influencing factors/function by Sklet (2006). In specific applications, more concrete characterization of the SF under study is required. In practical and operational applications, any SF can be described by a set of parameters (Harms-Ringdahl, 2003a), which may include:

- Level of abstraction;
- Systems level;
- Type of SF;
- Intention of SF.

Level of abstraction starts at the lowest level with a concrete solution, e.g. a safety relay or a temperature guard. At higher levels, it can refer to protection again excess temperature or a theory of temperature control. *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 levels so as to include fire brigades, emergency services in general, laws regulating safety, and so on. *Type of safety function* describes whether the function is technical, organisational, or represents a human intervention. *Intention of SF* can be more difficult to describe. The main intention might be to provide safety, or safety may be a spin-off where the main aim is something different.

2.2 Barrier methods

As well as the method described in this article, there are several accident investigation methods (e.g. Sklet, 2004) that are directly related to barriers and more or less explicitly to similar concepts. *Barrier analysis* is a commonly used term, and there are many variants of methods with that name. One well-established description has been published by the Department of Energy (DOE, 1999). The method is based on the energy model, and a barrier is described as any means used to control, prevent, or impede a hazard from reaching the target. *MORT* (Management Oversight and Risk Tree) is another well-known method, which can be used for accident investigations, and also for risk analyses (Johnson, 1980; Frei et al, 2002).

The *Accident evolution and barrier analysis* (AEB) method (Svenson, 1991, 2001) is used to analyse barriers that can stop the course of events. The objective of an AEB is to understand why a number of barrier functions have failed, and how they could be reinforced or supported by other barrier functions. In *fault trees* and *event trees*, the barriers are clearly modelled. In *Deviation analysis* (Kjellén and Larsson, 1981; Harms-Ringdahl, 2001) deviations related to accident prevention can be identified, which is also essential in SMORT (Kjellén, 2000). Another example in this category is the *Systematic Cause Analysis Technique*, which is related to a model of a safety management system (Bird and Germain, 1985).

2.3 Safety function analysis

2.3.1 General

The *Safety function analysis* method is based on the concept of safety functions described above (Section 2.1.2). The method can be used to draw conclusions about SFs and their properties on the basis of an accident or near-accident (Harms-Ringdahl, 2003b). The general objective of an analysis is to identify and analyse the SFs that were involved in the specific incident under study. The method is generic, and can be applied to most types of systems and events. Specific aims can be defined in a concrete investigation, and examples of results can be:

(a) Identification of SFs related to the accident;
(b) Evaluation of how well the SFs worked;
(c) Suggestions for improvements.

To use an accident as a starting-point means that only a subset of all possible SFs in the system will be identified. The method has another application area, which directly focuses on the system, and aims at a complete identification and analysis of the SFs in the system (Harms-Ringdahl, 2001, 2003a). Such an application is usually more time time-consuming, and also more difficult.

2.3.2 Analysis procedure

The analysis is based on a defined procedure with a set of stages. Like other methods, it includes a preparation phase, where aim, range, assumptions etc. are defined. There is also a concluding phase for the reporting and use of results. Besides from this, an analysis contains five specific main stages.

(1) Data collection;
(2) Identification of safety functions;

(3) Structuring and classification of these functions;
(4) Assessment of the SFs;
(5) Generation of proposals for improvements (optional).

The data collection can vary. An earlier investigation of the accident can provide written material, which is used as a basis for further analysis. Interviews and group discussions can give valuable information, especially about more informal SFs that are not obvious in official documentation.

2.3.3 Identification of safety functions

Approaches for the identification of SFs can be categorized into four partly overlapping groups:
(A) Text analysis;
(B) Interviews;
(C) Sequence oriented analysis;
(D) Comparison with a given set of SFs.

A ***text analysis*** is usually based on documents describing the accident and related circumstances. The analyst follows the text and tries to identify the words or phrases that directly or indirectly indicate a safety function. A practical way of doing this is to use a marking pen to indicate such words or phrases.

A similar kind of identification is obtained from ***interviews and discussions***, which give additional information, and also greater freedom in the search. One procedure is to pose open questions about what happened, what could have prevented the accident, etc. By listening carefully, the analyst can pick up what can be understood as SFs. This is similar to text analysis.

A ***sequence oriented analysis*** follows the course of events, preferably starting with the accident and going backwards. If rescuing and amelioration are of interest, a second round going forwards can be performed. The search can be guided by a set of questions such as:
- What technical mean (could have) prevented the event/state X?
- What human action (could have) prevented the event/state X?
- What organisational routine (could have) prevented the event/state X?

In all the approaches above, the identified SFs are listed in a table. Here, there is a need to find concise formulations in order to clearly describe the functions. The identification will give items at a fairly concrete level, resulting in a list. In practice, it is good to be liberal, including doubtful functions, and then later classify them as important or insignificant.

Comparison with a given set of SFs is a special category of identification. Here, the incident is compared with a predetermined list, and an assessment is made of whether each SF in the list existed and how it functioned. This application can be attractive when several investigations are made of the same or similar systems, and the time for analysis is limited. Otherwise, a study of the functioning of a particular set of SFs can be made.

2.3.4 Structuring of safety functions

The identification stage generates a list of SFs, usually in a rather arbitrary order. The list needs to be arranged in a logical way to facilitate the assessments that follow. The structuring stage is intended to make a model of the safety features involved in the system where the incident took place.

A practical way to proceed is to first establish a structure based on a division into technical, organisational and human functions. At the next step, a classification is made on the basis of the actors and the organisations to which they belong. Usually, the SFs in the list are concrete and at a fairly low systems level. The third step combines items, in order to group SFs at a higher systems level. Examples of SFs and their structuring are given in Section 3.2.2.

During the structuring, it might be found that SFs formulated differently, e.g. coming from different information sources, are actually the same functions. In this way, duplicates can be removed. There is no unique solution to defining SFs, and the final structured list will reflect an iterative process aimed at achieving simple and logical presentation.

2.3.5 Assessment of safety functions

After identification, each safety function in the structured list is assessed. Depending on the situation, different approaches can be adopted. However, it is essential that the assessment is systematic and consistent, and follows a predefined scheme in the concrete situation. Examples of parameters that can be used in assessment are discussed below. The first should be regarded as compulsory, since it is a basic requirement of incident investigations, while the rest can be seen as optional.

Table 1. Classification of safety function performance.

Code	Description
a	Yes, the SF was in place and performed satisfactorily.
b	Partly, the SF worked to some extent but not completely.
c	No, the SF did not perform as expected.
d	Suggested; the SF did not exist and emanates from a suggested improvement.
e	Counter-effect; the SF increased risk in some way.
f	Unclear; performance was uncertain.
g	The SF was not related to the incident.

A basic parameter called *performance* concerns whether or not each SF worked adequately during the studied incident. A classification can be made into seven groups, as shown in Table 1. The first three (a – c) are essential, but sometimes it is advantageous also to include suggested improvements (d). Occasionally, SFs have a negative effect (e), e.g. by lulling someone into false confidence. If an assessment is uncertain, it is better to classify the SF as unclear (f) rather than to make a guess.

Other parameters can be used in the assessment of SFs (Harms-Ringdahl, 2003a). One aspect is whether the system is acceptable or if an improvement is needed. Basically, this stage concerns whether safety functions are good enough, and whether their coverage is sufficient to control the hazards involved. A scale can range from “improvement strongly recommended” to “no change needed”. There is a variation in how important the different SFs are, and it can be useful to assess the importance of each SF. A scale for division might range from “no influence on safety” to “highly important”.

2.3.6 Propose improvements

According to judgements made at the assessment stage, some SFs need to be improved. Suggestions can aim to increase efficiency or to eliminate weak points. Developments can also relate to extending the coverage of a function with too narrow an application area.

3 Results from case studies

3.1 The case studies

Three case studies were chosen to illustrate the principle of the methodology, and to give examples of results. The initial aim of performing the case studies was to collect information on SFs that can be identified from investigating a specific incident, and of their characteristics and performance. The studies have been limited to facts related to the investigated incident in the actual workplace and related organisational issues.

Another aim has been to obtain experience of how the investigation procedure works in practice. One issue was whether the SF concept could be easily understood by the people involved, or if it had a too abstract meaning.

The case studies represent different types of work sites and situations. The first two come from technically oriented workplaces with well-established work procedures. The first was an incident at an electrical power distribution station, and the investigation was made in cooperation with the company involved. The second study was based on an already published investigation of a railway accident. The data have also been used for a classroom exercise, showing the experiences of several users.

The third study was made at a hospital, which represents a different tradition of organising work. Three incidents with medication errors were investigated. The study was made in cooperation with work groups from the affected wards, and it also included the development of improvements. In this third study, the aim also included getting experience of using the method as an aid in local patient-safety work.

3.2 Incident at an electrical power distribution station

3.2.1 Background and incident

The case study was based on an incident at an electrical power distribution station in direct connection with a hydropower station (Harms-Ringdahl, 2003b). This particular incident was chosen, from among others, because at first sight it appeared fairly uncomplicated, and accordingly could provide a simple test of the method.

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, according to the task schedule. 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. Nobody was injured, but the error caused a disruption to electricity supply across a large region.

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 division among several actors was the product of having split up one original company into several smaller ones, and also an outsourcing process.

3.2.2 The investigation methodology

The analysis was performed in two major steps. The first step employed a method called *Deviation analysis* (Kjellén and Larsson, 1981; Harms-Ringdahl, 2001). A deviation is here defined as an event or a state that diverges from the correct, planned or usual function. The function can be a process, a technical function, or a human or organisational activity. The aim of this method is to identify deviations that precede an incident, and then to develop safety proposals.

Deviations were identified in interviews with three persons, and through the study of relevant documentation. The result was a list of around 40 deviations. Examples include:

- Labelling on the transformers and drawings differed.
- There were departures from the planned working process.
- Other jobs were delayed, causing time stress.

A work group at the company was engaged in the further analysis. This included the evaluation of each deviation in order to select the ones indicating a need for better prevention. The final step was to develop safety improvements; 29 proposals were made.

After that, the recorded results were analysed further, with the aim of identifying safety functions. The identification of safety functions was based solely on text analysis of the protocol from the deviation analysis, which also included the suggested improvements. Any issue that was interpreted as involving a safety function was noted down. At the identification stage, 40 SFs were recorded.

At the structuring stage, each SF was classified as technical or organisational. The SFs were also grouped at different system levels – in the workplace and higher up. This grouping was tentative, but was gradually improved until a satisfactory solution was obtained. In order to illustrate the structuring principles, there follow some examples of SFs:

- The transformer was labelled, showing its identity. This is a technical function, which was assigned to *Local technical* level (2).
- Operating the correct switch is a human action (which failed), and is related to *Sequence of work.*
- The *Job description* shows how to identify the correct switch.
- The *Job planning* stipulates who shall do the job, when it shall be done, etc.
- These three items can be grouped under *Local organisational SF* (3).
- *Written routines*, defining how work shall be planned in local workplaces, belong to C*ompany management* (4).
- *Informal practices*, concerning how planning is done, can exist at several levels, but the findings in the case study were best placed at company level.

Figure 1 shows the structure of SFs obtained, where the two groups at the top are technical, and the rest organisational. Each block consists of subgroups, and the figure illustrates how blocks 3 and 4 are divided into smaller parts.

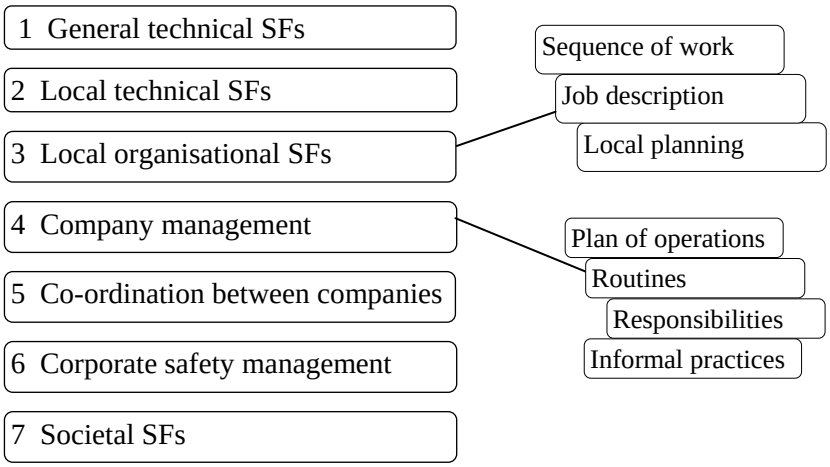

Figure 1. Structure of safety functions in Case Study 1.

3.2.4 Assessment of safety functions

Each SF was assessed with regard to whether or not it had performed its function during the incident. Table 2 provides a summary of the SFs and their evaluation. The Sum column shows how many SFs belonged to each group, where the largest proportion belonged to local organisational SFs. Assessment of performance is classified according to the scale in Table 1.

Of the 40 recorded SFs, 20% performed sufficiently well at the incident (a), and a further 7% worked to some extent (b). It can be seen that the majority (78%) did not operate satisfactorily or needed improvement. Problems with poor performance were most apparent at higher organisational levels (4, 5 and 6 in Table 2), where there were 20 unsatisfactory SFs out of 21.

Table 2. Safety functions in Case Study 1 and a summary of their performance.

Safety function structure	**Sum**	Number of SFs according to performance*			
		a) Yes	b) Partly	c) No	d) Suggested
1 General technical SFs	1	0	0	0	1
2 Local technical SFs	6	2	1	1	2
3 Local organisational SFs	11	4	1	5	1
4 Company management	6	0	0	5	1
5 Co-ordination between companies	10	1	1	1	7
6 Corporate safety management	5	0	0	2	3
7 Societal SFs	1	1	0	0	0
Total number of SFs	40	8	3	14	15
Distribution	100%	20%	7%	35%	38%

* Categories a) – d) are in accordance with the scale in Table 1.

3.2.5 Comments

In the study, no attempt was made to explain exactly why and how the human error did occur. Actually, several hypothetical explanations were possible, and the focus of the discussions was instead on how improvements could be implemented.

According to the findings, deficiencies were greatest at company and corporate management levels, which is somewhat surprising in light of the long tradition of safety work in the electricity distribution field. At the time of the incident, the companies had quality systems in place, and there were preparations to implement ISO 14000. Obviously, these systems were not working adequately in the safety arena.

One of the explanations for the deficiencies lay in the series of organisational changes that had taken place. Electric power distribution has well-established routines, which continued to work rather well during the period of organisational change. Safety work appeared to be preserved by co-operation between people who used to belong to one and the same company. Such informal co-operation (a kind of SF) emerged as essential during discussions with the work group. One impression was that the people involved quickly gained an intuitive understanding of the safety function concept and its practical application.

3.3 Safety functions in a railway accident

3.3.1 Background and accident

This case study is based on an investigation published by the Swedish Accident Investigation Board (2002). At the accident, a set of empty goods wagons ran into a tank lorry. The lorry driver was badly injured, but survived. The lorry was parked at the harbour, pumping oil to a

ship. Around a kilometre away at a shunt yard, goods wagons were being shunted. A set of wagons rolled uncontrollably all the way down to the harbour. The dangerous situation was observed, but the wagons could not be stopped. The situation was complicated, in the sense that both the shunting yard and the harbour were places with lots of activities taking place simultaneously. There were also several organisations in charge of different types of operations.

This accident has been used on a training course in accident investigation (Strömgren et al, 2008). The original investigation was thorough, but without any specific method being employed. For the course, the investigation report of 20 pages was compressed to 3 pages, and this shortened description provided the basis for the analysis.

3.3.2 The safety function analysis

The identification of SFs was a pure text analysis, where the analyst tried to identify words or phrases indicating a safety function. The analysis included the following steps:

- The relevant sentences in the text were marked, and then directly copied to a column in the analysis protocol.
- Where necessary, rephrasing was performed in order to get clear descriptions of the SFs. A new column was then added, which contained a consistent set of SFs.
- This list was in a rather arbitrary order, following the original narrative, and a suitable structure needed to be developed. A division was made between technical and organisational functions, which were then further divided.
- The final step was then to assess whether or not each SF had worked.

Table 3. Safety functions in a railway accident, divided into categories.

	Category SF	Subcategory	N*	OK*
1	Railway system (technical)	a Local tracks and shunt yard b Local signalling c Other d Centrally controlled	12	6
2	Vehicles (technical)	a Railway carriages b Engine c Tank lorry	2	0
3	Local organisations	a Train operator b Shunt yard c Harbour d Central train control	9	3
4	Safety management in local organisations	a – d Instructions and routines in these organisations	5	1
5	Co-ordination between organisations	a Agreement about co-ordination b Routines for co-ordination	4	0
6	Authority regulations	a Occupational safety regulations b Railway regulations	4	0
	Sum		36	10

N* = Total number of identified safety functions.
OK* = Number of SFs that performed as expected or to some extent (a and b in Table 1).

The structure is based on six main categories (1 – 6), which were divided into subcategories. In the text provided, a total of 36 SFs were identified and their performance was assessed. A summary of the analysis is given in Table 3, and the final column (OK) shows how many SFs had performed satisfactorily (a and b in Section 2.3.5). When a function was not relevant to the flow of events, or if it was unclear how well it worked, the function was counted as not working.

3.3.3 The students' exercise

This accident has been used for training at accident investigation courses for four consecutive years (Strömgren et al, 2008). After a short introduction to the method, the students were divided into small groups, and identified SFs directly in the text. The exercise was allocated around one hour, which meant that the focus was on identification.

This exercise has been performed by 16 groups. All groups identified 20 SFs or more. Especially when there were railway employees in a group, they identified additional functions in the text. If results from the different identification sessions were combined, the number of SFs would rise to over 50. Despite the brevity of the text, the variation between groups was fairly high. This means that the identification stage of the analysis is likely to miss a number SFs if it is not carefully performed. On the other hand, the SFs related to a specific incident are only a subset of all SFs, and complete coverage should not be expected. To some extent, this reduces the disadvantages of variability.

One conclusion from the exercise is that the concept of SF appears to be easily intelligible in a short time, and can directly be put into practice for identification. This was also confirmed in discussions and in later evaluations during the courses (Strömgren et al, 2008). Another conclusion is that problems of variability between investigators may be essential. However, this may well also apply to other investigation methods, although this has not been studied.

3.4 Incidents in hospital care

3.4.1 Background and incidents

Patient-safety in medical services is attracting an increasing interest. Among other things, this means that many efforts are directed at how to learn from accidents and incidents (e.g. WHO, 2005), both at local level and generally. One essential question is how incidents should be analysed in order to learn as much as possible.

This case study (Harms-Ringdahl et al, 2006) was made in cooperation with a hospital in order to explore the possibilities of improved learning. The overall aim of the study was to identify the type and amount of information that can be obtained through the use of system-oriented methods for the analysis of accidents and incidents. Another aim was to propose improvements based on the findings of the investigations.

The scope was limited to pharmaceutical incidents in hospital care, since they represent an important problem area. For the test, three incidents were selected. One criterion was that no injury to the patient should have occurred. The reason for this was to avoid a situation associated with blame or penalties, which often is regarded as a large problem in this sector. Other conditions were that the incident should be as simple as possible, and also that the ward involved should participate voluntarily.

Case 1: A doctor at an emergency ward wrote by mistake a "2" instead of "1" when he prescribed medication to a patient. However, fortunately, this was discovered after some time and the patient never got a double dose.

Case 2: An unconscious patient should get nutrition through a feeding pump. At the end of the day, it was found that the patient's blood glucose value was too low, and that the pump did not work, although the measuring equipment had indicated a flow and the alarm system had been silent. Counter-measures were taken immediately, and the patient was not harmed.

Case 3: At registration for planned surgery, the ordinary medication for a patient was not included on the list of prescriptions. The mistake was revealed when the patient a few days later asked the nurse about this.

3.4.2 The investigations

Data were collected from available medical documentation and through interviews, around 5 in each case. The interviews were limited to about an hour, and they consisted basically of a few open questions

- *Are you well acquainted with the event?*
- *Describe the event and circumstances when it happened?*
- *How do you think a recurrence can be prevented?*
- *Do you think something could have prevented the event?*

Three different methods for event analysis were chosen. At the first stage, the course of events was mapped in a manner similar to the *Sequential Timed Events Plotting (STEP)* method (Hendrick and Benner, 1987). Information from the interviews was examined by applying *Deviation analysis* (Harms-Ringdahl, 2001) and *Safety Function Analysis*. The results of this were two lists, of deviations and safety functions, respectively.

Two further steps in the analysis were carried out at meetings with representatives from the wards concerned. At a first meeting, the identified deviations and safety functions were evaluated, and whether or not improvements were needed was determined. At a second meeting, proposals for improvements were discussed and suggested. Approximately five persons from each ward attended, from nursing staff to heads of department.

3.4.3 The safety function analysis

As a preparation, a wide definition of SF was agreed upon. Then, SFs were identified in each interview by careful listening. When something was said indicating a SF, it was directly noted. After the interview, these notes were formulated as functions and summed up on a list. Usually, there were two listeners, and their notes were put together to give a more complete record.

Table 4. Safety functions in hospital incident Case 1 with error in prescription.

	Category SF	Examples	N*	OK*	Sug*
1	The patient	Patient's own knowledge of his disease Conveyed drugs and documents Support from relatives	4	2	0
2	Nursing personnel	Nurse experience (reacts to unusual drug) Check by stand-by doctor	9	7	2
3	Ward (clinical level)	Local praxis at ward Instructions adapted to ward situation Cooperation between units	9	4	1
4	Department (several wards)	Routines for reporting deviations Form for reporting deviations Praxis of learning from mistakes	6	2	1
5	Hospital	Control of approved signatures Local instruction for record of medication	3	1	1
6	County Council	Procedure for prescription of medication Defined responsibilities for prescription Rules for documentation Layout of form for documentation	18	3	10
7	Authority regulations	National rules for documentation of prescriptions Register of available drugs	3	1	2
	Sum		52	20	17

N* = Total number of identified safety functions, including suggestions
OK* = Number of SFs that performed as expected or to some extent (a and b in Table 1).
Sug* = Suggested in interviews

For each case, the findings from the analysis of the documentation and the lists from the interviews were combined into a common table. The different SFs were sorted in order to obtain a logical and consistent structure. In the sorting process, identical or similar SFs were combined into one SF in order to avoid duplicates. This sorting process made the structures of the three cases slightly different.

Results from the first case are shown in Table 4. The table also includes SFs that were suggested during the interviews (shown in the right column), giving a total number of 52. The SFs were arranged in seven groups, starting with the patient and then going upwards in hierarchy. The table shows examples of SFs in the different categories. The first two groups are concerned with what persons do, and are quite informal by nature. Normally, the patient's knowledge about his medication can be of help, but in this case he could not communicate. Another example is the attentive doctor on standby duty, who normally is not supposed to check the prescriptions, but detects that something is wrong. The rest of the SFs are related to general and local regulations, to routines, to filling in forms, etc.

3.4.4 Assessment of safety functions

The performance of the SFs at the incident was assessed (see the scale in Table 1). The summary from Case 1 in Table 4 shows the number of SFs in each category and how they were assessed. Out of a total of 52 SFs, 20 worked, at least to some extent. The highest success rate was for Category 2 (nursing personnel) representing relatively informal activities. On the other hand, SFs related to the County Council had only three working out of 18.

Table 5 shows the number of SFs and how they had performed. Together, there were 125 SFs identified, of which 66 (53%) had worked at least to some extent. Suggestions from interviews (Category d) are shown separately; when these were included, the mean SF value per case came to 55.

It can be noted that three SFs had counter-effects, actually increasing the risk to the patient. For example, in Case 2 there was a valve supposed to prevent spillage of liquid, but it could sometimes also block the flow. Another example is that some doctors expected the nurse to check certain documentation. However, nurses do that only occasionally.

Table 5. Safety functions in three case studies of hospital incidents.

Assessment* **Case**	**1**	**2**	**3**	**Sum**
a) Yes, SF performed satisfactorily	12	14	8	34
b) Partly, SF worked to some extent	8	12	12	32
c) No, SF did not perform satisfactorily	15	17	24	56
e) Counter-effect (negative result)	0	1	2	3
Sum of identified SFs	35	44	46	125
d) Suggested in interviews	17	11	11	39
Total	52	55	57	164

* Categories a) – e) are in accordance with the scale in Table 1

3.4.5 Propose improvements

In the hospital case studies, one aim was to suggest improvements. For each case, this was arranged at a meeting with persons from the affected ward. Initial data for the discussions were lists of assessed deviations and SFs in need of improvement. The points in the list were gone through in stages, starting with the most problematic ones. Suggestions could aim to increase efficiency of a SF, or to extending the coverage of a function with too narrow an application area.

The meetings were planned to take about two hours, and the suggestions were a mix of different ideas. After the discussions, the material was arranged according to responsibility for the accomplishment of the suggestions. In all, 196 suggestions were made, giving a mean value of 65 per case. The County Council was addressed in 80 of these suggestions, although there is an overlap in proposals from the three cases.

3.4.6 Comments

From all three incidents taken together, 143 deviations were identified and evaluated. It was found that 126 deviations (88%) required some kind of improvement. One conclusion is that the identified deviations were meaningful and important for the participants in the ward (which was not obvious at the beginning).

Another result was the identification of 164 SFs, of which around half had functioned. An essential part of the methodology consists in discussion in work groups. At the first meeting, the concept of safety functions was quickly explained, and it appeared that all participants easily understood and could use it. An evaluation by participants in the wards was made anonymously, and showed high satisfaction with the approach and results.

One conclusion is that the investigations indicated a large demand for improvements in the hospital system. Analyses of the three incidents resulted in nearly 200 suggestions for improvements, at different organisational levels. Each analysis resulted in more than 60 suggestions for improvements. Some of these were directly related to the ward; however, a majority of the suggestions concerned higher positions in the organisation. The suggested improvements came from discussions including both deviations and SFs, and it is hard to distinguish between the two related methods.

It might be interesting to deepen the analysis in several respects, for example, the distribution of SFs between different organisational levels, and their success rates. However, a deeper analysis is not within the scope of this article, which focuses on investigation methodology regarding the organisational aspects of hospitals.

4 Discussion and analysis

4.1 Safety functions in the case studies

The results from the case studies consisted in summaries of SFs, which were structured to give a model of the safety features involved. These structures varied between the studies, since they were based on specific findings and not on a predefined model. A further part of the results consisted in assessments of how well the SFs had worked at the incidents, and also proposals for improvements.

Five events were used as test cases for the methodology. Table 6 provides a summary, showing that the mean value identified SFs related to the incidents was 38. However, the investigations only surveyed a subset of all the SFs in the investigated systems. A limiting factor is also the search procedure; data came from analysis of texts, and by listening to what was said in interviews. A larger number could be expected if SFs are more actively searched for. The number of SFs will also be larger if suggestions are also included.

The performance of each identified SF has been evaluated. The principle was to judge whether the SF had worked as could be expected or to some extent (Section 2.3.5). On average, 45% of the SFs had worked at least to some extent (see Table 6). The railway accident showed the lowest rate, which might be explained by the fact that the rest of the cases were near-accidents where the sequence was interrupted before injury occurred.

Table 6. Number of identified safety functions in five incident investigations.

Case	Identified SFs	Performed OK*	Suggested**
a Electrical power distribution	25	44%	15
b Railway accident	36	28%	-
c Hospital Case 1	38	53%	17
d Hospital Case 2	45	58%	11
e Hospital Case 3	46	43%	11
Mean values	38	45%	-

* Proportion of the SFs that worked as expected or to some extent (a and b in Table 1).

** Number of suggested added or improved SFs.

One of the characteristics of the method is that it presents a summary of all identified barriers and SFs, both those that are working and those which are not. It would have been interesting to compare Table 6 with other investigations and studies. However, comparable summaries have not been found. It appears likely that similar numbers of SFs could be found in other accident investigations as well, bearing in mind that the case study from the railway accident actually is based on data from a previous investigation by the Swedish Accident Investigation Board (2002).

One experience is that the identification and structuring of SFs is dependent on the analyst's skill and background knowledge. An estimate of this was given in Section 3.3.3. It means that there is variability between different investigators, and that absolute numbers must be treated carefully. It appears that the assessment of whether a function worked or not worked is less sensitive to the investigator.

Efficiency can be defined as the probability that a concrete SF, e.g. a safety device, exists and performs its intended function when needed (Harms-Ringdahl, 2003a). All case studies indicated low efficiency among identified SFs. One explanation for low efficiency may be that the cases had a bias towards poor performance, since they were selected because incidents had occurred. The defects could also be due to a temporary state of the system.

However, such explanations do not seem very plausible to the author, because, there was a fairly large number of safety features related to the incidents, and only a small proportion worked. An issue to explore more deeply is whether low efficiency is common in these types of systems, or is restricted to these particular cases.

4.2 Principal considerations

4.2.1 Different perspectives

There is a large spread in applications of and approaches to accident investigations. On the one hand, there are advanced companies, sometimes with a potential for major accidents. On the other, there are small companies where safety is managed more informally. The latter group is much larger, concerning both number of companies and number of accidents. One consideration in the studies has been to see whether the SF concept can handle the whole range of company situations, covering both sophisticated and informal safety systems.

The search strategy in the SF investigations presented here represents a bottom-up perspective. The analysis starts with the accident, and is based on detailed information from the persons involved and relevant documents. The findings are then traced higher up in the organisations concerned. The structuring and assessment of the information collected will show what is relevant at the scene of the event.

An investigation from a top-down perspective might basically look at the events and the actors, and then relate them to the formal safety system, with prescribed rules, management systems, and also to technical aspects and barriers. This approach may be most useful in well-defined and detail-regulated types of production.

The case studies were made at organisations that, according to their own ambitions, should have fairly advanced safety systems, some of them also with approved quality systems. However, the findings showed that both formal and informal safety features appear side-by-side in these organisations. This is an argument for the usefulness of a broad definition of SF, which includes the informal dimension.

In the SF definition (Section 2.1.2), actions by individuals were included in organisational function. In the case studies, it was found that human actions play an important role in safety. It would be advantageous if such actions were more prominent in the terminology, but without changing the meaning of SF. Consequently, a more explicit definition is suggested:

> *A safety function is a technical or organisational function, a human action or a combination of these, which can reduce the probability and/or consequences of accidents and other unwanted events in a system.*

4.2.2 Modelling and describing safety

One central result of the investigations is a model of safety features related to a specific event. The model can take the form of a block diagram or table, which is based on collected data combined in a suitable way. In the identification, many SFs are identified, and duplicates should be removed at an early stage of the structuring.

The method does not have any strict rules for the design of models. It is the analyst's task to arrange the material in a suitable manner. However, this flexibility will give rise to differences between individual analysts. Evidently, the analysis of one incident only gives a subset of all safety features in the organisation. However, by combining information from several incidents, the model will become more complete.

An important issue is how useful such a model might be. One aspect is that a model should be refined enough not to be trivial, but simple enough to highlight only the essential characteristics of the real system (Wahlström, 1994). In the case studies, the model was used at group meetings and in the final reports. Experiences can be summarised as follows:

- The resulting list was used as a basis for evaluation and discussion of improvements;
- Information about safety features was arranged to relate different items that normally belong to different areas, such as technical and organisational functions;
- The identified SFs could be treated in a consistent manner;
- The model was easily understandable by the people involved.

One finding from the case studies is that informal aspects of safety are common and often relevant. It can also be seen that there is often overlap between different SFs, and that systems contain formal and informal elements side-by-side. Such overlap can be seen as safety redundancy, which makes the safety system less vulnerable to change. Informal safety work might be of special importance after major reorganisations have taken place, when safety management systems tend to be out-of-date. In some case studies (a, c, d and e), the importance of informal factors became apparent during the interviews.

Sometimes, it might be more adequate to talk about a *safety web* than a distinct set of barriers. Such a web structure may contribute to keeping up safety or, in other terms, improve the safety resilience of the system (see, e.g. Hollnagel et al, 2006). The SF concept could be an aid in exploring how organisations can maintain or develop their safety work despite problems and deficiencies.

The collection of SFs, followed by an assessment of characteristics, also provides a qualitative estimate. The most common characteristic was performance (Section 2.3.5); in the case studies less than half of the SFs worked at least to some extent.

Such a measure is valuable, but it would be advantageous also to distinguish SFs that were important to safety. An estimate of importance would have been useful, but it was not possible to include one in the study. The main reason for this was lack of time at meetings with the work groups. Experiences from a related study (Harms-Ringdahl, 2003a) showed that a majority of the SFs were regarded as important.

4.3 Methodological aspects

4.3.1 Practical experiences

Accident investigations with safety functions were performed in five documented case studies (Section 3), and in a number of exercises where the author was involved as a teacher. From these experiences, an estimate can be made of the time needed for an analysis, which, of course, varies with circumstances.

A simple investigation based on a text analysis can take between one and two days. This applies to the cases described in sections 3.2 and 3.3. The investigations related to hospital care (Section 3.4) were more complicated since they included three different methods. A check on the activities indicated that the extra time for including SFs is at least two days, but can go up to four days. With a higher level of aspiration, an analysis may take even longer. An assumption in the estimates is that the analyst has a basic knowledge of the method. In a study comparing different methods of accident investigation (Strömgren et al, 2008), SF analysis was assessed as a relatively quick method.

The identification of SFs appears to be fairly easy, which is supported by experiences from classroom exercises (Section 3.3.3). The most difficult part is probably to structure the material in order to obtain a suitable model. The method is fairly free, and does not impose strict restrictions on the results. One rule-of-thumb is to make a division into technical and organisational items. Another is to arrange the material according to the systems hierarchy. Such freedom might make structuring more difficult for some analysts, but easier for others.

4.3.2 Advantages and problems

This paper presents a fairly new generic method for accident investigations, which has some characteristic features, with both advantages and disadvantages. From a number of applications and experiences from teaching the method in the classroom (Strömgren et al, 2008), a tentative summary can be presented.

There are some **general characteristics** that have both positive and negative aspects, depending on the user's perspective:

- A general definition that covers most safety features;
- Usually, several SFs are identified (see Table 6);
- No predetermined structure and hierarchy in arranging results (Section 4.2.2);
- Several suggestions for improvements can be generated in an analysis (Section 3.4.5).

Advantages of the approach and methodology include:

- The method focuses on safety characteristics and supports preventive measures by identifying problematic, inefficient and missing SFs;
- The method gives a fairly simple overview of SFs;
- Already existing SFs are scrutinized, which means that new safety features are not added without seeing the whole picture;
- Technical, formal and informal organisational aspects of safety are identified and analysed in a consistent manner;

- The method supports the handling of several SFs relatively easy and in a consistent way; this is obtained through the straight-forward recording of SFs on a list, followed by a structuring process;
- It is not necessary to examine the sequence of events, intentions, or effects (Section 4.2) for the collection and structuring of data. The identification of "root-causes" and different cause-effect relationships (often complex and sometimes disputable) are not needed;
- The concept and results seemed to be easy to understand for participants in the case studies. This understanding facilitated discussions about problems and potential improvements;
- The application of the method has been assessed as fairly easy by students on investigation courses.

Disadvantages of the method are:

- The open definition can be experienced as too wide and leads to a grey zone, where too many items can be seen as safety-related;
- In identification there is variability between investigators, which might be essential. However, this might also apply to other investigation methods, although this has not been studied;
- The arranging of material in a structure can be difficult, and the result will depend on the experience of the analyst;
- The method will give only a subset of all SFs in the system, a drawback common to all accident investigations.

4.3.3 General

The results of an analysis depend not only on the method, but also on the analyst and on cooperation with the organisation where the accident occurred. In the account given here, the author was in charge of the case studies, demonstrating the potential of the method rather than giving an average result.

A fundamental question is whether a new accident investigation is method needed. The main characteristics of this method are its wide definition of what can affect safety characteristics, and the ability to identify and to assess many safety functions in a consistent way. There are few other methods that focus on the analysis of safety features in systems and their weak points. This suggests that the new method has a role to play.

This paper presents the concept of a general method, which is a tool that can be adapted to the needs of the situation. Experiences point to some aspects to develop further. The first concerns the assessment of performance, i.e. how SFs work during an incident. A more developed approach may give a deeper understanding of how safety systems fail, and how their efficiency and robustness might be improved.

The case studies were taken from three different sectors, which have several divergences between them. One aspect in common is that organisational issues are important, and their structures are in principle formal. However, it does not appear necessary to restrict the methodology to such settings.

To the contrary, it is likely to be possible also to apply SF analysis in the home and leisure sector. This is an important and challenging area, as can be seen from accident statistics. In a summary, Zimmermann and Bauer (2006) found that among fatalities in the European Union, workplace accidents account for 4%, traffic accidents for 30%, and home and leisure accidents for 66%.

5 Conclusions

The concept of safety function has been discussed and compared with similar expressions for barriers, based on both practical cases and studies of the literature. There are no commonly accepted terms, which might be explained by the fact that the terms are used in different types of systems and for different purposes. In this study, a wide definition of SF was adopted. This was applied in a method for the investigation of accidents and incidents, which was then tested in five case studies. An investigation started with the identification of SFs related to the studied incident. The obtained material was arranged in a structure that was tailored to the situation and, at a later stage of analysis, assessments were made of the identified SFs.

Five separate incidents were investigated, and a mean of around 40 SFs was identified, of which less than half had worked. In three hospital case studies (Section 3.4), the information from the investigations was also used to suggest improvements, and in each case around 60 proposals were developed, partly on the basis of SF information.

In all the case studies, it was observed that technical, organisational, and human safety features existed side-by-side. A new definition of SF is therefore proposed in which human actions are explicitly included (Section 4.1). It was found that formal organisational functions were common, but also that informal and less clear organisational structures played an important role. The methodology supports consistent analysis of the material available, and can integrate it into a common format. This is an essential argument for a broad concept of SF, which can be useful for the analysis of systems that also comprise informal safety functions.

There often appeared to be an overlap between different SFs, and the systems contained formal and informal elements side-by-side. The overlap can be seen as safety redundancy, which makes a safety system less vulnerable to change. It might be more adequate to describe this as a safety web rather than a distinct set of barriers. Such a web structure might contribute to the preservation of safety or, in other terms, improve the safety resilience of the system (see, e.g. Hollnagel et al, 2006). The SF concept may be an aid to exploring how organisations can maintain or develop their safety work, despite problems and deficiencies

Experiences indicate that the method can be of value in accident investigations. One reason for this is that all the investigations showed a high number of identified SFs, of which less then half were functioning. Such types of results in an investigation might support better understanding of how accidents in complex systems can occur, despite a large number of safety features. One advantage is that the methodology aids proposals for safety improvements, by identifying problematic, inefficient and missing SFs. The concept and the investigation approach appeared easy to understand for participants in all the investigation groups, and also in the classroom exercises.

Acknowledgements
Method development and practical studies of safety function analysis have been supported by the Swedish Council for Working Life and Social Research. Good cooperation with the County Council of Värmland, Sweden, was greatly appreciated.

6 References

Bird, F.E. Jr., Germain, G.L., 1985. Practical Loss Control Leadership. International Loss Control Institute, Georgia, USA.

DOE, 1999. DOE Workbook: Conducting Accident Investigations. U.S. Department of Energy, Washington D.C., USA. (http://hss.energy.gov/CSA/CSP/aip/workbook).

Frei, R., Kingston ,J., Koornneef, F., Schallier P. (Eds.), 2002. NRI MORT User's Manual. The Noordwijk Risk Initiative Foundation, Delft, the Netherlands. (http://www.nri.eu.com/).

Hale, A., 2006. Method in your madness: System in your safety. Delft Technical University, the Netherlands.

Harms-Ringdahl L., 2001. Safety analysis – Principles and practice in occupational safety (Second edition). Taylor & Francis, London.

Harms-Ringdahl, L., 2003a. Assessing safety functions – results from a case study at an industrial workplace. Safety Science 41, 701–720.

Harms-Ringdahl, L., 2003b. Investigation of barriers and safety functions related to accidents. In Bedford, T. and van Gelder, P. (Eds.) European Safety and Reliability Conference 2003, Balkema, Lisse, pp. 763–767.

Harms-Ringdahl L., 2004. Relationships between accident investigations, risk analysis, and safety management. Journal of Hazardous Materials 111, 13-19.

Harms-Ringdahl, L., Kihlström Berg, M., Landbü Roos, A., 2006. Fördjupade utredningar av tillbud i hälso- och sjukvården. Karlstad University, Sweden.

Hendrick K., Benner L. Jr., 1987. Investigating accidents with STEP. Marcel Dekker Inc, New York.

Hollnagel, E., Woods, D. D., Leveson, N. (Eds.), (2006). Resilience engineering: Concepts and precepts. Ashgate Pub Co.

IEC (International Electrotechnical Commission), 2001. Functional safety of electrical/electronic/ programmable electronic safety-related systems (Standard IEC 61508). IEC, Geneva.

Johnson, W.G., 1980. MORT Safety assurance systems. Marcel Dekker, New York.

Kjellén, U., Larsson, T.J., 1981. Investigating accidents and reducing risks – a dynamic approach. Journal of Occupational Accidents 3, 129–140.

Kjellén, U., 2000. Prevention of Accidents Thorough Experience Feedback. Taylor & Francis, London, UK.

Reason, J., 1997. Managing the risks of organizational accidents. Ashgate Publishing, Aldershot.

Swedish Accident Investigation Board, 2002. Collision between goods wagons and tank lorry in the harbour of Västerås (In Swedish, Report RJ 2002:01) Swedish Accident Investigation Board, Stockholm, Sweden.

Sklet, S., 2004. Comparison of some selected methods for accident investigation. Journal of Hazardous Materials 11, 29–37.

Sklet, S., 2006. Safety barriers: Definition, classification, and performance
Journal of Loss Prevention in the Process Industries 19, 494–506.

Strömgren, M, Harms-Ringdahl L. and Bergqvist, A, 2008. Choice and evaluation of accident investigation methods. To be published.

Svenson, O., 1991. The accident evolution and barrier function (AEB) model applied to

incident analysis in the processing industries. Risk Analysis 11, 499–507.

Svenson, O., 2001. Accident and Incident Analysis Based on the Accident Evolution and Barrier Function (AEB). Model. Cognition, Technology & Work 3, 42–52.

Wahlström, B., 1994. Models, modelling and modellers: an application to risk analysis. European Journal of Operational Research 75, 447–487.

WHO (World Health Organization), 2005. Draft Guidelines for Adverse Event Reporting and Learning Systems. WHO, Geneva. [http://www.who.int/patientsafety/events/05/Reporting_Guidelines.pdf].

Zimmermann, N., Bauer, R. (Eds.), 2006. Injuries in the European Union. Statistics summary 2002 – 2004. (Eurosafe) Austrian Road Safety Board, Vienna.