Preprint version of article in proceedings of ESREL 2003,
European Safety and Reliability Conference 2003, Maastricht, The Netherlands.

Investigation of barriers and safety functions related to accidents

Lars Harms-Ringdahl
Industrial Economics and Management, Royal Institute of Technology, Stockholm, Sweden, and, Institute for Risk Management and Safety Analysis, Stockholm, Sweden

e-mail: Lars_Harms-Ringdahl@lector.kth.se

ABSTRACT
A new approach to investigating accidents has been developed and tested. In any such investigation, barriers and safety functions related to an accident or near-accident are identified and classified. The method is described, and a case study of an incident at an electricity distribution company is used to illustrate the type of results obtained. One finding was that a large number of safety functions failed in relation to the incident. In particular, the analysis indicated low efficiency of functions related to higher organisational levels. Another experience was that people and work groups quickly obtained an intuitive understanding of the safety function concept, and its practical application.

1 INTRODUCTION
When an accident has taken place, the course of events leading to its occurrence is usually the main target of investigation. A question is also how it could happen. 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 analysis of why the safety system failed.

Concepts and terminology related to safety features vary considerably (e.g. Harms-Ringdahl, 1999; Hollnagel, 1999). One common term is "barrier", which often has a concrete technical meaning related to energies. The term can also be used more generally to encompass organisational aspects (e.g. Johnson, 1980). Other commonly used terms are "barrier function" (Svenson, 1991),"defence" (Reason, 1997), and "protection layer" (CCPS, 1993).

There are a number of accident-investigation approaches that focus on barriers and the like. Management Oversight and Risk Tree (MORT) – the classical method (Johnson, 1980) – can be used for accident investigations, while the Accident Evolution and Barrier Function Method (Svenson, 1991) is specifically designed for analysis of accidents and incidents. Also, Safety Barrier Diagrams (Taylor, 1994) offer a way of presenting and analysing barriers to accidents.

One of the starting points for this paper lay in an interest in exploring whether the generic concept of "safety function" could be used to advantage in accident investigations. The author had had favourable experiences of applying the concept in safety analysis (Harms-Ringdahl, 2000; 2001).

The general purpose of the study presented here was to test the extent to which "safety function" can be a valuable concept in practical accident investigations. A more specific aim was to obtain a summary of safety features in the workplace under study.

2 APPROACH

2.1 The concept of safety function

Safety function (SF) is a rather common term, but there are no clear definitions available in the specialised literature. Even the "Standard on Functional Safety" (IEC, 1998), where the term is used several times, does not contain a definition. Accordingly, the term may be used in divergent senses in different applications.

A general definition of safety function has been proposed by Harms-Ringdahl (2001). This is worded as follows:

> *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.*

Human actions are here regarded as part of the organisational component. Safety function is a broad concept and, in specific applications, requires more concrete characterisation. This can be achieved using a set of "parameters". For example, the same reference proposes the following:

a) Level of abstraction.
b) Systems level.
c) Type of safety function.
d) Type of object.

2.2 Study approach

This case study was performed in four broad steps:

- Selection of accident to investigate.
- Deviation Investigation of the event.
- Identification of safety functions (SFs).
- Analysis of SFs.

Thus, the study involved two specific methods, which are briefly described below.

2.3 Deviation Investigation

The Deviation Investigation method (e.g. Harms-Ringdahl, 2001) contains three major steps:

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

The identification of deviations is supported by means of a checklist of technical, human and organisational functions. The identification results in a list, which is sometimes quite extensive. There is a need to select the most important deviations, for which proposals are then developed to improve the system. This procedure is supported by simple systematics.

2.4 Safety Function Analysis

Based on the concept of safety function, a methodology called Safety Function Analysis (SFA) has been developed (Harms-Ringdahl, 2000; 2001). The goals of a Safety Function Analysis (SFA) are to achieve:

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

In principle, SFA has two general applications. The first is to review a system (e.g. a work-place) and its hazards and safety features. The second is to conduct an accident investigation, designed to draw conclusions about SFs and their weaknesses on the basis of an accident or near-accident event.

The major steps in an SFA are:
- Identification of SFs.
- Classification and structuring of SFs, based on the parameters a) - d) in Section 2.1 above.
- Evaluation of the SFs.
- Generation of proposals for improvements (optional).

3 THE CASE STUDY

3.1 The investigated incident and workplace

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 (according to task schedule) 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. 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 organisational structure was the product of having split up one original company into several smaller ones, and also an outsourcing process.

This particular incident was chosen from among a few others because it appeared, at least at first sight, to provide a simple test of the method. A prior investigation had been made by the company in question. It concluded that a time delay had occurred that had placed stress on technicians. They deviated from normal work procedure, which gave rise to the mistake. The proposed counter-measure was that technical staff should be told always to follow formal rules, even when time is scarce.

3.2 Deviation Investigation of the incident

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

For the case study, an ad-hoc group was created, representing both the companies and the trade-union involved. The group evaluated and discussed the results. First, the list was scrutinised, and somewhat modified. Second, the deviations were evaluated on a four-point scale in order to select the ones that needed better prevention or management. There was complete agreement on all deviation estimates except one.

The final step was to propose ideas for essential improvements. Table 1 summarises the number of deviations and proposed measures. The investigation found 42 deviations prior to the incident, with the majority related to management issues. For example, one of the ideas for improvement was formulated as a "need to analyse the whole organisation". A number of specific deviations had to be considered in this analysis. These are counted as separate proposals in Table 1.

Table 1. Summary of results from the Deviation Investigation.

Type of results	Number
Identified deviations	42
Deviations evaluated as essential	27
Proposals for safety improvements	29

3.3 Identified safety functions

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 studied.

The SFs were classified into two groups: technical and organisational. The latter included three human actions, which in this case meant that a person had been supposed to perform a certain action. The SFs were then structured and grouped as in the list below. The first two were technical, and the rest organisational. The structuring was also based on different systems level, from workplace (3) to societal functions (7),

1. General technical SFs.
2. Local technical SFs.
3. Local organisational SFs.
4. Company management.
5. Co-ordination between companies.
6. Corporate safety management.
7. Societal SFs.

In this case, the SFs were evaluated according to whether or not they had performed their intended function during the incident. The SFs related to a suggested improvement are shown in a separate column. Table 2 provides a summary of the SFs and their evaluation.

Table 2. Summary of safety functions at incident at electric power station.

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%	-

*SI = A safety function noted as Suggested Improvement.

In all, 40 SFs were recorded and structured under 7 main headings. As an illustration Group 6, "Corporate safety management", comprised 5 safety functions, none of which were in satisfactory operation. The SFs were:
- Corporate policy for safety (out of date, inadequate).
- Information and distribution of policy (hard to find).
- General agreement between companies expected to regulate their co-operation on safety (out of date, unsatisfactory).
- In commercial agreements, clarify how competing goals shall be handled (proposal).
- In commercial agreements, clarify how policy shall be applied (proposal).

Another way of illustrating the results is shown in Figure 1. It is intended to provide a clearer hierarchical view, and it provides other examples of functions at a more detailed level.

4 DISCUSSION

4.1 The incident and the company's safety work

The incident was first thought to be "simple", and the event sequence was envisaged as uncomplicated. However, the analysis found many deviations prior to the incident. A natural question is whether all the deviations were relevant or whether the identifying step exaggerated problems and the situation.

This question was answered during the evaluation round, when most of the deviations were regarded as essential (Table 1) by the ad-hoc group. The evaluations were made virtually in consensus. The group also made a substantial number of suggestions for improvements.

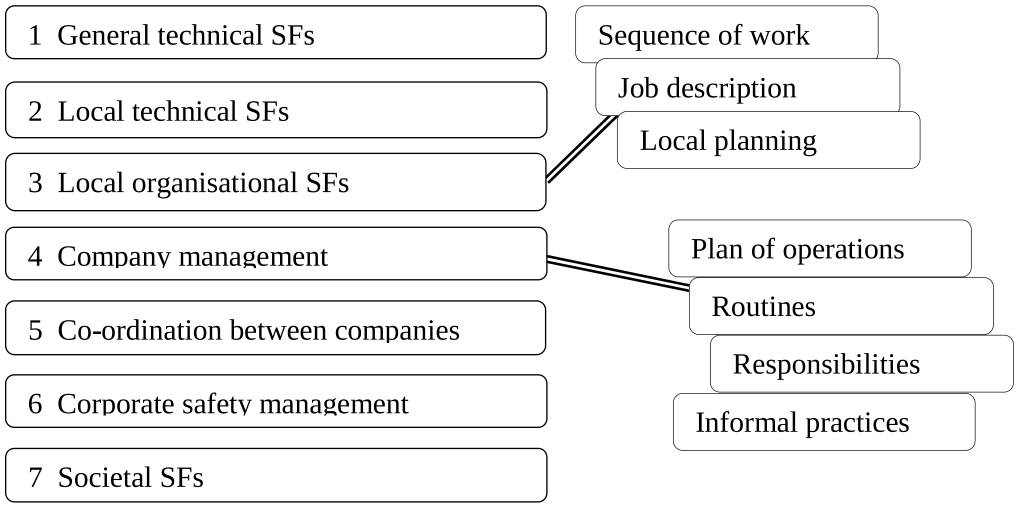

Figure 1. Summary of safety functions related to the incident, with examples of functions at a more detailed level.

This can be interpreted as a large discrepancy between how the people involved would like planning and safety procedures to operate, and what was observed in the investigation. The final list of proposed improvements covered 29 issues.

A further analysis showed that as many as 40 SFs were recorded as directly related to the incident. A larger number of SFs would have been obtained if a complete summary had been the aim, but this was not the case here.

Of the recorded SFs, a majority did not actually operate satisfactory, and only 20% worked as expected (the OK column in Table 2). Thus, the analysis indicated low efficiency of functions. It should be remembered, however, that the aim was to identify problems, not all SFs.

Nevertheless, it is essential also to look at absolute numbers. As many as 32 SFs did not work or needed improvement. Most were at higher organisational levels (4, 5 and 6 in Table 2), where there were 20 unsatisfactory SFs out of 21.

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, some of the companies had quality systems in place, and there were preparations to implement ISO 14000, which here was intended to also cover safety issues. Obviously, these systems were not adequately working 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. There were also some suggestions to strengthen co-operation of this kind, e.g. by considering it carefully in the education of technicians.

4.2 About the methodology

The investigation in this case study had two distinct parts. The first - Deviation Investigation - is concerned with uncovering facts about an incident and proposing improvements to a system. The second part - Safety Function Analysis - structures the results obtained from Deviation Investigation for evaluation and presentation.

The result of a Deviation Investigation is a list, usually a fairly long one, that is not necessarily arranged in cause-consequence sequence. The main reason for this is that there is not always strict coupling between a specific deviation and the final event. It is most common for any one deviation to affect just the *probability* of other events and deviations occurring. An advantage of not having to show all direct connections is that it makes the analysis rather quick. In this case it took slightly more than two days to perform the Deviation Investigation.

Here, the intention was to use SFA in a limited way so as to obtain a structured and evaluated summary of existing SFs. One experience was that the people involved quickly gained an intuitive understanding of the safety function concept and its practical application.

From another perspective, SFA can be regarded as a way of presenting the results of an investigation performed using another method. The results appear in the format of a fairly simple table and illustration (see Table 2 and Figure 1), which are easily communicable. In particular, the role of management and its related problems become more obvious through this type of analysis.

In this study, SFA was used in a limited way by just re-arranging existing material, but more steps could be included in an SFA analysis. One additional part might be to obtain a fuller picture of existing SFs. In addition to those identified, there were several other obvious SFs that had not been clearly entered into the protocol. One further step might be to suggest improvement that would give better coverage or efficiency to a system of SFs.

4.3 General comments

What is special (and new) about SFA compared with other barrier-oriented methods is that it is not based on a predetermined set of SFs, such as in MORT (Johnson, 1980). Instead, the functions are based on what is observed in the system.

Another characteristic of SFA is that there is no demand for the establishment of causal relationships between the different SFs and the chain of events. By contrast, this is the case, for example, in the Accident Evolution and Barrier Function Method (Svenson, 1991) and in Safety Barrier Diagrams (Taylor, 1994). Identification and structuring is simple in SFA.

An additional feature of SFA is that it provides an opportunity to work at various levels of abstraction and different system levels. It is also of value to be able to include problems and potential improvements on the same "dimension".

These characteristics give considerable flexibility, but the analysis is supported by a simple principle, which enables it to be performed in a consistent manner.

The evaluation of the SFs, based on whether or not they were satisfactorily operating during the incident or not, was simple but sufficient in this case.

Looking at the findings of the investigation, it was surprising to see that the role of management showed so many deficiencies. This indicates that the methodology might be relevant to specialised investigations where management systems have high priority.

5 Conclusion

Investigation of a simple incident identified a large number of deficiencies, especially concerning higher management.

The approach involved the adoption of a new method, called Safety Function Analysis (SFA). The safety function concept proved to work, in the sense that it was easily understood by the people involved. The concept also provided a foundation on which to present the results of investigation in a consistent manner.

The experience of this case was generally positive. It appears that safety function might be an interesting concept to work with further in accident investigations. The analysis methodology could be developed to include further steps so as to enable more thorough identification and evaluation of safety functions.

Acknowledgement

The project was supported by the National Centre for Learning from Accidents, which is a part of the Swedish Rescue Services Agency, the Swedish Council for Working Life and Social Research, and Ångpanneföreningen's Foundation for Research and Development. The interest and co-operation of the people in the companies involved in the case study are greatly appreciated.

6 References

CCPS (Centre for Chemical Process Safety), 1993. *Guidelines for Safe Automation of Chemical Industries*. New York: American Institute of Chemical Engineers.

Harms-Ringdahl, L. 1999. On the modelling and characterisation of safety functions. In Schueller, G.I. and Kafka, P. (eds), *Safety and Reliability ESREL'99*. Rotterdam: Balkema.

Harms-Ringdahl, L. 2000. Assessment of safety functions at an industrial workplace - a case study. In Cottam, M.P., Harvey, D.W., Pape, R.P., and Tait, J. (eds): *Foresight and Precaution*, *ESREL2000*. Edinburgh: Balkema.

Harms-Ringdahl, L. 2001. *Safety analysis - Principles and practice in occupational safety* (2nd edition). London: Taylor & Francis.

Hollnagel, E, 1999. Accident Analysis and Barrier Functions. Kjeller (Norway): Institute for Energy Technology.

IEC (International Electrotechnical Commission), 1998. Functional safety: safety related systems (IEC 1508) Geneva: IEC.

Johnson, W.G. 1980. *MORT Safety Assurance Systems*. Chicago: National Safety Council.

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

Svenson, O. 1991. The accident evolution and barrier function (AEB) model applied to incident analysis in the processing industries. *Risk Analysis* 11 (3): 499–507.

Taylor, J.R. 1994. *Risk analysis for process plan, pipelines and transport*. London: E & FN Spon.