Published in Safety Science 2003, Vol. 41, Issue 8, pp. 701 – 720.

Assessing safety functions – results from a case study at an industrial workplace

Lars Harms-Ringdahl
Institute for Risk Management and Safety Analysis, S-100 44 Stockholm, Sweden, and
Department of Chemical Engineering, Royal Institute of Technology, Stockholm, Sweden

Communication: Lars_Harms-Ringdahl@lector.kth.se

Submitted August 2001, accepted April 2002.

Keywords
Accident prevention, Barriers, Evaluation, Model, Safety analysis, Safety function

Abstract
This study is concerned with how safety characteristics at industrial installations can be modelled and evaluated. The starting point was the concept of safety function, which is defined as a technical, organisational or combined function that can reduce the probability and/or consequences of accidents and other unwanted events in a system. A tentative theoretical framework has been developed, which has been applied in a new method called Safety Function Analysis. A workplace in process industry was analysed in the form of a case study. One result of the application was a model of safety functions in the workplace, including 54 functions. These have been evaluated, and system improvements have been proposed.

A detailed comparison was made with the results of two other methods for safety analysis—Deviation and Energy analysis—applied to the same workplace. Safety function analysis gave essential supplementary information, and especially supported improvement of management issues, both formal and informal. It is concluded that the safety function concept worked well in the practical analysis of safety in the studied system. There is a need for further improvement of the theoretical framework, and of the method.

1 Introduction
Safety at workplaces can be supplemented by various analytical and practical approaches. Safety analysis is a tool that is applied to an increasing extent. In this paper it is broadly defined as a systematic procedure for analysing systems to identify and evaluate hazards and safety characteristics (Harms-Ringdahl, 2001).

Interest has been especially high in the chemicals processing and nuclear industries, with a large literature describing this application area (e.g. Lees, 1996; Taylor, 1994). The application of safety analysis to more common workplaces has received less attention. Nevertheless, the accident literature provides several examples (e.g. Harms-Ringdahl, 2001; Kjellén and Sklet, 1995; Suokas and Rouhiainen, 1993).

Safety analysis has a variety of applications. One type of analysis concerns decisions on whether the risk level is acceptable or not. Another application of safety analysis is to find weaknesses in a system, and then to suggest possible measures that might improve performance.

The last one has similarities with traditional safety work, which also introduces various system changes. This can result in a number of safety measures, more or less co-ordinated. Swuste (1996) points out that in the scientific literature on safety, the solutions to occupational hazards attract only minor attention (by contrast to that paid to analysis of hazards). Swuste explained by the ad-hoc manner in which much of improvements in health and safety are made. These remarks are in line with the author's practical and theoretical experiences.

Methods aimed at the identification and correction of problems are useful tools, but they can be supplemented by other approaches. This kind of consideration suggests a need to address safety features in a more direct way, both in analysis and in system design.

Scope and aim
This paper is concerned with how safety characteristics can be modelled and evaluated. The aim is to report from a case study where a new method called Safety Function Analysis (SFA) was applied. Types of results are given and also comparisons with the results of two other methods, all applied to the same object.

The case study was a practical test, using a general safety function (SF) concept. The idea was to use this framework to address safety features in a direct way in a systemic analysis. The results of the case study contributes to understanding of a number of issues, such as:
- How useful is the SF concept in practical applications?
- How do SFs appear in an actual system? How many are there, how are they structured, etc.?
- Is an analysis method based on the SF concept useful?

2 On the modelling of safety characteristics

2.1 Different approaches

There are many approaches to the description of safety characteristics in systems (e.g. Harms-Ringdahl, 1999). Some examples are briefly presented here. Energy models have been used for a long time (e.g. Johnson, 1980), and they usually involve technical as well as organisational "barriers". A general concept is "defence", which can represent several types of safety features. It has been discussed in detail by Reason (1990 and 1997). In simple terms, defences shall prevent hazards from causing losses. Such defences can be combined into several layers, but may be weakened by different kinds of problems.

Within the nuclear power area, a summary of basic safety concepts is provided by INSAG (1988). Twelve fundamental safety principles are given, and one of the more essential is the "defence in depth" concept (further described in INSAG, 1996).

A comprehensive overview of safety principles in the chemical industrial sector is provided by CCPS (1993). It describes general aspects, and also safety in connection with automated safety and process control systems. The general model is based on a set of "protection layers", which are arranged in order of how they are activated in the case of an escalating accident.

A standard covers the aspects that need to be addressed when electronic systems are used to carry out safety functions (IEC, 1998). The scope is to set out a generic approach, one that is independent of application. Examples are given from process and manufacturing industries, transportation, and the medical arena. The standard is mainly concerned with safety to persons.

Organisational aspects are highly relevant to the modelling of safety characteristics. One example is a framework for modelling safety management systems (Hale et al., 1997). Safety management is seen in terms of a set of problem solving activities at different levels of abstraction, and risks are modelled as deviations from normal or desired process. There are also a number of other interesting alternative approaches for analysing and describing safety characteristics (e.g. Kecklund et al, 1995; Hollnagel, 1999).

2.2 Concept of safety function

The terminology used to describe safety features varies considerably. "Safety function" is a rather common term, but no clear definitions have been found in the literature (Harms-Ringdahl, 1999). Even in the "Standard on Functional Safety" (IEC, 1998), where the term is used several times, it is not defined. It might therefore be used in different senses in various applications.

A general definition of safety function has recently been proposed (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.

Quite deliberately, safety function (SF) is defined as a broad concept. Actions by individuals are included in organisational function, but this might be clearly spelled out in an alternative definition. In principle, SF covers all the concepts presented earlier in this chapter. In specific applications, it requires more concrete characterisation. For practical and operational applications, any SF can be described by a set of parameters. A suggestion by Harms-Ringdahl (1999) encompasses:
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 a temperature guard. 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 a safety function. 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 essential 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.

3 Approach and methods

3.1 General

Approach to the case study

The case study involved three major steps:

- Identification of hazards.
- Safety Function Analysis.
- Examination and comparison of results.

The studied system

The case study was made at a section in a pharmaceutical plant. In principle, there is simple batch production, where different substances are added and mixed following strict procedures. This type of production is common in pharmaceutical, food and other similar process industries.

The technical part of the production system consists of five similar production tanks, each with a volume of about 3 m^3. Between each batch, the production vessel is cleaned following detailed specifications. The cleaning procedure consists in a combination of manual actions and a computer controlled automatic sequence. Through a series of steps, the vessel is cleansed by lye (pH 13.5), and hot (80 ^oC) and cold water. The equipment was new, and production had been going on for about a year at the time of analysis.

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.

3.2 Methods of hazard identification

On the selection of methods

There are a large number of methods of safety analysis (see, e.g., Harms-Ringdahl, 2001; Lees, 1996; Suokas and Rouhiainen, 1993), each with a different field of application. Extensive discussions of relative merits can be found in the literature (e.g. Kjellen and Sklet, 1995).

The selection of methods for hazard identification was based on an interest from the company to try one or two generic methods that could be used by non-specialists. In this case, a choice was made to use Energy Analysis and Deviation Analysis. This section provides a short summary of the two methods used for hazard identification. It also offers an account of how hazards were to be evaluated.

Energy Analysis

Energy Analysis is a straightforward method, based on the energy concept, which has been used for a long time (Haddon, 1980; Johnson, 1980). The method is simple, and is suitable for obtaining a quick overview of existing hazards. An Energy Analysis is performed in a number of defined steps (Harms-Ringdahl, 2001):

1. Dividing the system into a number of parts.
2. Identifying energies with the aid of a checklist.
3. Evaluation of hazards associated with identified energies (can be done in different ways, independent of the method).
4. Making proposals for improvements, supported by a another checklist covering a hierarchy of different strategies.

Deviation Analysis

The concept of deviation is employed in a number of safety analysis methods. The specific method is used to identify deviations in a production system and the hazards to which these may give rise (Harms-Ringdahl, 2001). Further, the method incorporates aids to find safety measures. A Deviation Analysis follows a number of prescribed steps, taken in sequence:

1. Divide the object into a number of sections, based on activities or functions.
2. Identify deviations, with support of a checklist addressing technical, human and organisational aspects.
3. Evaluate hazards associated with the identified deviations (can be done in different ways, independent of the method).
4. Propose improvements on the basis of a simple checklist.

The method can be employed to obtain an overview of hazards, or it can be applied in more detailed and specialised investigations. The method focuses on activities in systems and on functions, i.e. on what people and machines are doing.

Evaluation of hazards

Another methodological choice concerns how identified risks should be evaluated. A common approach is to estimate probabilities and consequences for each identified hazard, and then determine whether or not risks are acceptable. Such an approach, however, was regarded as inappropriate in this case. One reason is that probability values are often hard to obtain, and uncertainties are accordingly large. However, the main reason is that many other factors need to be considered in making decisions on acceptability, e.g. directives of the authorities.

Instead, a judgement can be made on whether the system (or present situation) is acceptable as it is, or whether it needs to be improved. Table 1 shows the scale applied for evaluation. In this study, the judgements were made by a working group. A short set of instructions was given to aid evaluations. The focus was on accident hazards, but consequences related to production disturbances, ergonomic problems, and environmental damage were also considered as relevant. This meant, for example, that identification of an essential production problem would entail a system change.

Table 1. Scale for judgement of acceptability

Code	Description
0	Acceptable, negligible risk
1	Acceptable, no changes required
2	Not acceptable, system change (safety measure) is recommended
3	Not acceptable, system change (safety measure) is necessary

3.3 Safety Function Analysis

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

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

A SFA contains six main stages. 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.

Different ways to proceed can be chosen for each of the main stages, depending on the type of system, hazards, etc. Some comments on the approach adopted in this case study are given further below.

Identification of safety functions

One way of identifying safety functions is to start from specific hazards and pose questions of the following kind:

- 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?

Answers can be obtained from an interview or in a group discussion. The procedure will give items at a fairly concrete level, resulting in a list of safety functions. This was the approach used in the current case study.

Structuring safety functions

The list needs to be arranged in a logical way to facilitate the assessments that follow. There is no unique solution. Rather, the list will reflect an iterative process aimed at achieving a simple and logical presentation. In structuring, it might be of help to consider the parameters of safety functions (see Section 2.2).

Estimation of characteristics

A safety function can be described by a number of characteristics. In this case study three were applied:

- Intention.
- Importance.
- Efficiency.

Intention was divided into four categories:

0) No intended safety function, and no influence on safety.
1) No intended safety function, but some influence on safety.
2) Intended safety function, but main purpose is something else.
3) Intended to provide safety – or reduction of consequences.

Importance from a safety point of view was split into:

0) No influence on safety.
1) Small.
2) Rather large.
3) Large, closely connected to accidents or size of consequence.

The "efficiency" of each SF was estimated. It was defined as the probability that a concrete item, e.g. a safety device, exists and performs its intended function when needed. Sometimes, "probability of success" is a better term. A rather straightforward scale of probability was used in this test. It was divided into eight sections, starting with A = Less than 1% likelihood of success, up to H at 99.99%.

Assessment of safety functions

For each safety function a judgement is made whether the function is acceptable or improvement is recommended. The scale presented in Table 1 was used for the case study. The output of this stage can be approval of the safety system, or parts of it. The stage can also result in a recommendation to improve a certain SF and/or supplement it with one or others.

Basically, this stage concerns whether safety functions are good enough, and whether their coverage is sufficient to control the hazards concerned. It is more difficult to evaluate overall safety system, in particular to see if there are gaps in the system with regard to safety functions.

Propose improvements

Some safety functions might need to be improved, according to judgements made at the assessment stage. Based on previous results, ideas for improvements are generated aiming to increase "efficiency" and/or to eliminate weak points. Improvements can also relate to the coverage of a function with too narrow an application area.

3.4 Accomplishment of the study

The practical accomplishment of the case study is summarised and commented in this section. The background to the case study was that a practically oriented training course in safety analysis should be performed. The particular workplace was selected because it was regarded as technically simple, and with a few obvious hazards.

In order to prepare for the course, two analyses were performed. The methods chosen were Energy Analysis and Deviation Analysis, which were included in the training. In principle, these methods are used for hazard identification. The aim of the analyses was that the results should be used as examples.

Later, it was decided also to apply Safety Function Analysis (SFA) to the system, as part of a research project. Such an analysis was performed about half a year later. For practical reasons, only a restricted part of the system was examined. It was decided to limit analysis to hazards such as lye, hot water and overpressure – all related to the cleaning functions of the system.

Performance of the safety analyses

The Energy Analysis was performed by the author in collaboration with a safety engineer at the company who had a good knowledge of the technical functions of the system. An evaluation of hazards was performed, and ideas for improvements were proposed.

The Deviation Analysis was performed in a workgroup with a supervisor and an operator at the installation, and also included the safety engineer and the author. At a first meeting (of about 3 hours) a list of deviations was produced. During a second meeting the deviations were evaluated, and measures were proposed – mainly based on the views of the supervisor and the operator.

The Safety Function Analysis was based on knowledge of hazards from the previous analyses. Information about safety functions was collected in dialogue with a design engineer, who knew the system and its design history well. He had also participated in the safety analysis course. The data collection started with a discussion of different accident scenarios. A further step was to make a check against the parameters of the general model. This lead to a list of safety functions, which were then arranged and structured.

At a second round of the analysis, estimations of characteristics of the safety functions were made. Three persons were independently asked to estimate (a) intention, (b) importance and (c) efficiency (see Section 3.3). One person was the design engineer, while the two others were the supervisor and the operator participating in the Deviation Analysis. This meant that all those interviewed had good insight into the hazards and problems of the system.

In the interviews, a check was made on whether the description of the safety functions of the system was correct and sufficiently complete. All generally agreed, but a few extra points came up and were added to the description. The three interviews, and also the first modelling discussion, each took less than two hours.

Finally, two safety engineers evaluated whether the system was safe enough, or whether improvements were needed, using the scale presented in Table 1 above. Information from the estimates was available at this evaluation. The engineers also proposed changes when improvements were required.

3.5 Analysis of the case study

The results of the case study were examined. A general comparison was made of results from the other methods used in the same workplace. Some of the methods identify hazards, which are related to energies or deviations. These are not directly comparable with safety functions,

and the term "item" is used to cover results from all approaches. All three methods have two essential features in common; they have a similar principle for evaluation, and they generate ideas for improvements. Aspects compared were:

a) Items identified by the methods.
b) Estimations of identified items.
c) Proposals generated by the methods.
d) Time used on the analysis.

A more detailed comparison was made of the proposed improvements generated by the various methods. Each proposed measure from any one method was categorised and compared with results from the others. If two proposals were judged as having an identical purpose, a special note was made of this. The classifications were then utilised both to compile a package of proposals for the company, and for inter-method comparison.

Considering quality aspects when applying safety analysis is essential. A suggestion is that the aim of safety analysis is to identify the most essential factors affecting the safety of an activity (Rouhiainen, 1992). The quality of a safety analysis can then be expressed in terms of its fitness for use. This represents the degree to which the safety analysis is appropriate for its specified purpose. Rouhiainen (1992) points to four major questions in relation to quality of a safety analysis:

1. How well has the analysis identified hazards?
2. How accurately are the risks of an activity estimated?
3. How effectively has the analysis introduced remedial measures?
4. How effectively are resources used in comparison with results achieved?

The four aspects (a-d) correspond fairly well with the four quality questions. These cannot be answered exactly, but it is interesting to bear them in mind. Relative comparisons can be made between methods, and in particular in comparison with normal design procedure (i.e. without safety analysis).

4 Results of safety analysis

4.1 Identified safety functions

The Safety Function Analysis resulted in a list of 54 identified safety functions (SFs), which were arranged in groups and structured as shown in Figure 1. The number of SFs within each group is shown in Table 2. Structuring into six groups was based on the parameter "Type of safety function" (Section 2.2). The major groups were as follows:

1. *Containment* refers to mechanical devices that separate the hazards (hot water, lye, and mechanical movements) from operators during normal operation.
2. *Automatic control* starts and stops movements, and includes interlocks.
3. *Reduction of consequences* refers both to technical devices (e.g. emergency showers) and related organisational activities.
4. *Formal routines* are regulated in a system of documents, formally approved, and strictly followed.
5. *Informal routines* indicate features of the organisational system and what people do in practice in the workplace. The area is wide, ranging from what operators do in their daily work to written and verbal instructions (but not in the sense of formal routines).

6. *Company control* designates how safety instructions and rules emanate from the top of the company. For example, it includes the system for safety management (operated by the company in question).

The final group (6) shows functions at company level, whereas the others operate at workplace level. The left part of Figure 1 shows "general functions", which are of a fairly abstract nature. The middle section is at a lower level of abstraction, and is called "principal function". The right part shows examples named "functional solutions", which are at a lower system level and more concrete.

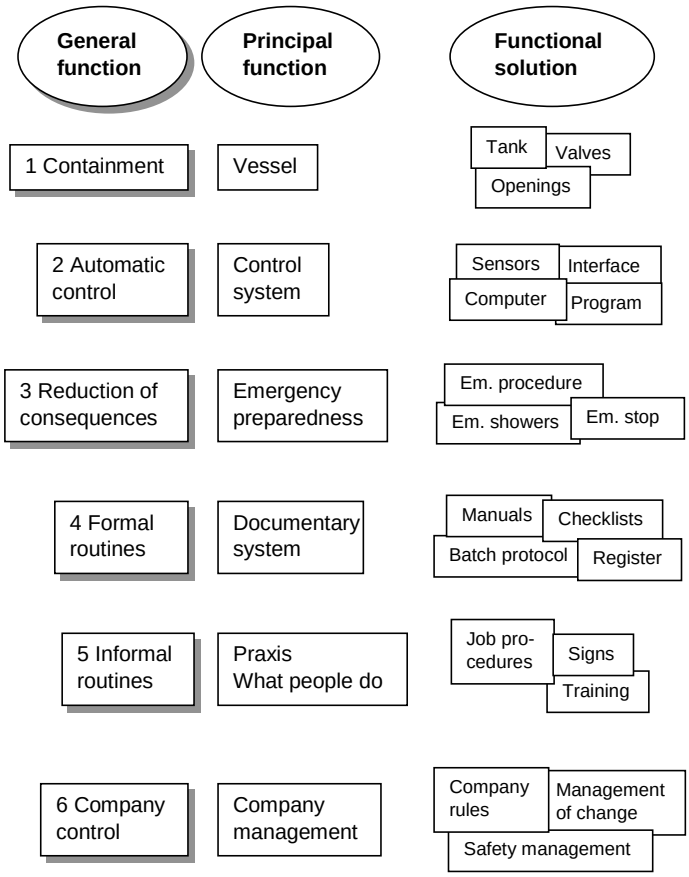

Figure 1. Model of identified safety functions in the case study

As an example, Group 3 (Reduction of consequences) contains four safety functions. They refer to both technical devices and related organisational activities:

3.1 Emergency stop.
3.2 Emergency shower (to reduce consequences if a person was splashed by lye or hot water).
3.3 Emergency eye-wash.
3.4 Pressure relief function (if overpressure occurs the tank should not explode).

.

Another example can be taken from Group 5 (Informal routines), which has seven listed functions:

5.1 Instructions in the workplace, which are mainly in writing, but without any formal check on contents. This group includes several items, such as machine instructions, some job procedures (not all), and safety rules.
5.2 Verbal instructions and rules, e.g. that operators should call for help when there is a computer disturbance.
5.3 Posters and warning signs.
5.4 Training course in handling of computer system.
5.5 Training in emergency actions and first aid.
5.6 The way people in practice learn to do their job.
5.7 Individual actions, e.g. initiatives taken by operators to correct problems.

4.2 Assessment of safety function

Three persons independently judged the 54 safety functions (SFs), giving estimates of three different characteristics (see Section 3.3). Thus, it was intended that each person should make 162 estimates. If a person felt he had insufficient knowledge, he or she could choose not to give an answer.

The first characteristic concerned “intention”. For 37% of the SFs, there were different opinions concerning whether they were intended or not. That safety was intended (Score 2 or 3) was agreed for 33% of the SFs. That it was not intended (Score 0 or 1) was agreed for 29%.

The second characteristic to be estimated was the importance of the SFs. In sum, 41 functions were regarded as important (Score 2 or 3, Section 3.3) by at least one person, corresponding to 76% of the total. For four of the SFs, importance was considered as large (Score 3) by all assessors. It was estimated that 13 functions had no or little importance (Score 0 or 1) by all three persons.

The third characteristic to be judged was “Efficiency”, which was defined as the probability that the intended safety function was achieved. Table 2 shows a summary of results. Judgements of efficiency were grouped into three classes: Low, Medium, and High. These are defined in the table.

For each class, the value given is the fraction of the number of responses belonging to that class and all given estimates for the group of SFs. For example, in the first row, 25 estimates were given, and efficiency was regarded as “high” for 92% of these. “High” means that the probability that the function would be achieved is greater than 0.99.

The groups *Containment* and *Formal routines* had the largest fraction SFs regarded as efficient. The groups *Reduction of consequences* and *Company management* received the lowest scores. In all, 26% of the safety functions were regarded as having low efficiency.

Table 2. Number of safety functions and estimations of efficiency given by three assessors.

Group of SF		Efficiency*			Estimates**	
	Number of SFs	Low	Medium	High	n	Rate
1 Containment, vessel	11	0%	8%	92%	25	76%
2 Control system	14	14%	32%	54%	22	52%
3 Reduction of consequences	4	83%	17%	0%	12	100%
4 Formal routines	8	0%	29%	71%	7	29%
5 Informal routines	7	28%	50%	22%	18	86%
6 Company management	10	45%	50%	5%	20	67%
Total	54	26%	31%	43%	104	64%

* Low = $p < 0.5$; Medium $0.5 < p < 0.99$; High $p > 0.99$. The value given is the fraction of the number of responses and all given estimates in the same row.

** n = number of estimates given.

Rate is the ratio between number of estimates given and all possible estimates

Differences in assessments

In many cases, the assessor refrained from making an estimation. This might have been due to it being hard to define "success" for that function, or due to lack of information. In total, 104 estimates of efficiency were given, which corresponds to 64% of all possible estimates. The two final columns of Table 2 show the proportion of given estimates. *Formal routines* and *Control system* were regarded as especially difficult to assess.

An analysis was made of the variance between assessors' classifications of probabilities. Identical classifications were obtained for 37 SFs, corresponding to 69%. Of the remaining SFs, 16 fell into two classes; and for only one SF, there was complete disagreement.

Agreement was better when efficiency was low or very high. It can also be noted that the best agreement was obtained for *Formal routines* and *Containment*. Poorest uniformity was for *Company management* and *Informal routines*, both of which showed about 40% identity.

4.3 Comparison between methods

Safety analyses with three different methods were applied on the same workplace. A comparison has been made of the results and experiences. A general summary is given in Table 3.

The first row of the table concerns the efforts required by the safety analyses themselves. There was a need for up to three meetings, each taking between two and three hours. The Safety Function Analysis was done as part of a research project, meaning that extra time was spent on that. In a normal application, Safety Function Analysis can be expected to require somewhat more time than Deviation Analysis.

One measure of results consists in the number of identified "items", which varies to some extent according to method. The second row of Table 3 shows that a total of 144 items were identified.

Table 3. Summary of data from three safety analyses.

	Safety Function	Energy	Deviation	All analyses
1 Number of meetings	3	2	2	-
2 Number of identified items	54	34	56	144
3 Items, not acceptable	37	21	34	92
4 Items, not acceptable due to production aspects	3	8	24	35
5 Proposals for actions, total	47	23	48	118
6 Actions, including further investigation	15	13	21	49

Row 3 shows that 92 (64%) of the "items" were evaluated as not acceptable (Score 2 or 3, in Table 1), which called for some kind of system change. Also, production aspects, e.g. potential disturbances, were considered in the evaluation using the same scale. In Row 4, there are 35 items that needed some kind of improvement related to production, some in combination with safety. This applies especially to the Deviation Analysis, where 70% of not-accepted deviations were related to production problems.

The final two rows of Table 3 summarise proposed actions. A total of 118 actions were proposed, most of which were specific proposals for improvement of the production system. But, as many as 41% of the proposals referred to a need for some kind of further investigation. A common reason for such investigation was that insufficient knowledge was available on the system, e.g. with regard to computer control. Uncertainty created a requirement for more data to be gathered before final evaluation could be made (which was then to be left for a later occasion).

4.4 Proposals generated by the various methods

The three methods gave quite different types of result. A practical approach is to compare the proposed improvements generated by the various methods (Section 3.5). The comparison of methods concerns the types of measures they addressed, and also overlap between them.

Types of measures

The analyses generated over a hundred proposals for improvement to the system. These have been grouped into four main categories, labelled:

1. Mechanical
2. Control system (automation)
3. Management
4. General or other

Table 4. Number of proposals generated by each safety analysis – by category and subcategory of improvements.

Category of improvements	Safety Function	Energy Analysis	Deviation Analysis	Total
1 Mechanical	**5**	**14**	**13**	**32**
a Workplace design, ergonomics	0	10	7	17
b Other	5	4	6	15
2 Control system	**10**	**2**	**19**	**31**
a Further investigation of system	6	0	9	15
b Direct proposal for improvement	4	2	9	15
c Other	0	0	1	1
3 Management	**27**	**0**	**9**	**36**
a Instructions for operators	14	0	5	19
b Routines in the department	8	0	4	12
c Company level	5	0	0	5
4 General or other	**5**	**7**	**7**	**19**
a Hazards with lye, etc	2	4	4	10
b Other	3	3	3	9
Total	47	23	48	118

The classification was based was on areas of responsibility within the company (categories 1-3). The final category, however, contained more general ideas, or items that did not fit into any of the specific categories.

Table 4 provides an overview of the proposals generated by the three rounds of analysis. It is clear that the methods tend to support different categories of improvements. Energy Analysis points especially at workplace design, ergonomics and mechanical hazards. Deviation Analysis generates many proposals for the control system, whereas Safety Function Analysis prompts three times as many suggestions related to management as the two other methods put together.

It should be noted, as stated above, that the Safety Function Analysis did not cover the entire system. This might, for example, explain the lack of proposals in the area of ergonomics.

Overlap between methods

There is an overlap between the methods with regard to proposals made, which reduces the total number of proposals. The set of combinations for all three methods is shown in Table 5, and is shown separately for the four categories of proposals. Following elimination of overlaps, the total number of proposals comes to 94, which means that the number of duplicate proposals was 24.

Only four proposals were generated by all three methods independently. These were connected with emergency equipment, over-pressure in the tank, and the blocking of machine movements. It can also be seen that 16 identical (or similar) proposals were generated by two of the methods.

Table 5. Number of proposed measures for all three methods by category.

Method/combination	Category of proposed measures				
	Mecha-nical	Control system	Mana-gement	General	Total
Deviation Analysis only	8	12	6	4	30
Energy Analysis only	8	0	0	4	12
Safety Function Analysis only	1	4	24	3	32
Two methods only	6	6	3	1	16
All three methods	1	1	0	2	4
Total, excluding duplicates	**24**	**23**	**33**	**14**	**94**
Total, including duplicates	32	31	36	19	118

4.5 Other observations

Several items are included in a safety analysis, and a few additional observations are relevant here. They concern:

- Evaluation of hazards.
- Application in design.
- Preceding analysis.

Evaluations

There were a total of 144 identified items on which to make evaluations, as shown in Table 3. All the evaluations concerned whether a situation or condition was acceptable or not. Around half-an-hour meeting time was devoted to evaluations for each analysis. In total, this meant 1.5 hours for 144 items, giving a mean value of between one and two minutes per item. This rather quick procedure meant that a number of the evaluations could be defective in one sense or another.

At nearly all evaluations, consensus was reached. But this was not compulsory, since it was possible simply to note a dissenting opinion on the analysis record. There was discussion on a few occasions, e.g. with regard to the dependability of the control system. If sufficient information was not available, some kind of investigation tended to be proposed.

Applicability at the design stage

One argument for this type of safety analysis is that it might be useful at the design stage. A simple check was made on this theme. The starting point was the list of measures, which was examined by a safety engineer at the company and the author. A judgement was made, for each proposed measure, if it might have been formulated at the system-design stage or not.

An overall conclusion is hard to draw from this simple test, but it was indicated that 70% of the proposals would have been possible to find out. Management aspects show the lowest rate, at approximately half of all items in that category.

5 Discussion

5.1 Modelling safety features

The general approach to modelling was to identify SFs from the perspective of the workplace. The SFs were combined and structured into a hierarchy (Figure 1). The model was a compromise, needed to obtain a comprehensive perspective. It would have been possible to work at a more detailed level. For example, the control system included 40 sensors and 30 computer controlled valves.

A general question concerns how "useful" the model proved to be. One aspect is that a model should be refined enough not to be trivial, but simple enough to bring forward only the essential characteristics of the real system (Wahlström, 1994). In this case, the main advantages of the model appeared to be that:

- It arranged information about safety features, giving an overview of different items that normally belong to different areas.
- The identified SFs could be treated in a fairly consistent manner.
- The model was easily understandable by the people involved (operator, supervisor, and design engineer).
- The resulting list could be used as basis for evaluation and discussion of improvements.

5.2 Applying Safety Function Analysis

Estimation of characteristics

The description of the method applied (Section 3.3) contains six separate steps. One essential part of the case study was the estimation of three characteristics: *Intention*, *Importance*, and *Efficiency*. The results are summarised in Section 4.2. In the case study, one aim of the estimation round was to test how meaningful these characteristics were, and how different assessors estimated the different SFs.

Of the three characteristics, "intention" appeared to be least useful, since it did not support a better understanding of the safety features. Estimates of "importance" showed that most of SFs (76%) were regarded as important by at least one person. These could be seen as some kind of relevance measure of the model.

The estimates of efficiency were more interesting, revealing several weaknesses in the system. In all, 26% of the safety functions were regarded as having low efficiency – defined as a success rate less than 50%. The estimate was useful later when the need for improvements were assessed. Discussions about how efficiency could be increased helped create ideas for improvements.

About the estimations

As expected, there was discrepancy between assessors. A comparison showed that 23% of the estimates of the three characteristics were identical for three persons. It is not clear whether this should be regarded as poor or satisfactory, considering the large number of combinations of possible estimates. There are some contributory explanations for the differences. One is that the three persons had different roles and priorities in the workplace. Another reason is that the design engineer can be supposed to have greater insight into how the system was supposed to work.

It might be seen as an advantage that the estimates could be made rather quickly – one to two minutes per person and SF. It also reflected different perspectives on the system. One potential purpose of the estimates was to serve as a screening tool, in order to find items to develop further.

Of course, improvements could be made both concerning the scales used and the choice of characteristics to estimate. This will be considered in further development of the method. In practical applications, the estimates could be made as a group process and directly address potential differences of opinion.

5.3 Comparison of methods

Basis for comparisons

In this case study, a number of different methods were used on the same object. Results can be compared in many different ways (e.g. Suokas and Rouhiainen, 1993), and the choice is not self-evident.

The comparisons here are based on two major questions in relation to quality of a safety analysis (Rouhiainen, 1992; see also Section 3.5). The first is concerned with identification of hazards. In Table 3, a comparison is made of "items", including both hazards and safety functions. The other question is related to how the analysis introduced remedial measures. In Table 5, the basis for comparisons lies in the proposals for improvements generated by each method.

There are some problems with such measures. For example, the application of a single method might identify several small hazards but miss a very large one. A number of proposals could be generated, but they might address minor problems or be inefficient.

One way of handling this is to look at identified "items" that are regarded as unacceptable (Table 3). Supplementary information is obtained by comparing the types of improvements suggested by the methods (Table 4). A third approach is to study the overlap between suggested improvements according to method. These two latter approaches address both what is found and what is missed.

Assessment of hazards is exposed to two diametrically opposed problems: acceptance of too dangerous a condition, and demanding a change that is unnecessary (in one sense or another). A systematic check on errors in the evaluation has not been made. Due to the large number of evaluations, some "errors" are likely to have occurred.

Identification and assessment

The three methods used in the case study assessed 92 items to be in need of improvement (Table 3). The number of items per method varied between 21 and 37.

During the assessments, a number of uncertainties had to be treated. Rather than making an estimation that would be a kind a guess, a further investigation was often recommended to deal with uncertainties. Table 3 shows that as many as 41% of the proposals referred to a need for some kind of further investigation.

Comparison of improvements

The analyses generated over a hundred proposals, and they are summarised in Table 4. The methods focus on different aspects of the system, and it is clear that they support different types of improvements. For example, Deviation Analysis generated many proposals for the control system, and Safety Function Analysis gave several suggestions related to management.

In the counting of proposals, also "further investigations" are included. As many as 41% of the proposals referred to a need for some kind of further investigation (Table 3). This gives an overestimation of the number of proposals, but an inquiry might generate one or more further proposals. These might justify this choice of counting. Probably, it would not impact substantially on the comparison between methods.

General comments

The three methods gave clearly different types of results. Some differences have been summarised in Table 5, based on suggested improvements. In particular, the division into four types of improvements clearly demonstrates some of the weaknesses and advantages of the different methods. It supports the apparently trivial but rather important conclusion that you should not expect a single method to handle all types of hazards or safety problems.

5.4 Concluding remarks

This study is based on only one case, and thus the conclusions are tentative. It appeared that the SF concept could be useful in practical applications. One reason for this is that it supported the building of a model and getting an overview of the safety features in the studied system. One further argument is that all people involved in the case study easily understood the basic idea.

The concept also worked as a foundation for Safety Function Analysis as a method. The method with a step-by-step procedure has been practically tested. The main features appeared to have worked satisfactory. One result of applying the method is a model of the safety features of a system. This has improved understanding of the system, and provided a basis for estimations and ideas for improvements.

The application of SFA has added to the quality of overall safety analysis of the system. The reasoning here is based on quality issues (Rouhiainen, 1992), as discussed in sections 3.5 and 5.3. More particularly, SFA has added proposed improvements concerning management issues.

One conclusion is that the approach has several promising features, and that it is attractive to apply and develop further. One clear need is to improve estimations, especially for efficiency, and to make modelling more explicit so as to encompass coupling between functions.

Acknowledgement

The author expresses his gratitude to the persons at the company concerned, who participated in the safety-analysis workgroups. Support from the Swedish Agency for Innovation Systems and Ångpanneföreningen's Foundation for Research and Development is gratefully acknowledged.

References

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

Haddon, W., 1980. The basic strategies for reducing damage from hazards of all kind. Hazard Prevention, 16, 8-12.

Hale, A.R., Heming, B.H.J., Carthey, J., Kirwan, B., 1997. Modelling of safety management systems. Safety Science, 26, 121-140.

Harms-Ringdahl, L., 1999. On the modelling and characterisation of safety functions. In: Schueller, G.I., Kafka, F. (Eds.). Safety and Reliability, ESREL'99. Balkema, Rotterdam, pp. 1459-1462.

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., Tait, J. (Eds.). Foresight and Precaution, ESREL 2000. Balkema, Rotterdam, pp. 1373-1378.

Harms-Ringdahl, L., 2001. Safety analysis – principles and practices in occupational safety (2nd edition). Francis & Taylor, London.

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

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

INSAG (International Nuclear Safety Advisory Group), 1988. Basic safety principles for Nuclear Power Plants. International Atomic Energy Agency, Vienna.

INSAG (International Nuclear Safety Advisory Group), 1996. Defence in depth in nuclear safety. International Atomic Energy Agency, Vienna.

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

Kecklund, L., Edland, A., Wedin, P., Svenson, O., 1995. Comparison of safety barrier functions in the refueling process in a nuclear power plant before and after a technical and organizational change. In: Norros, L. (Ed.). Fifth European Conference on Cognitive Science Approaches to Process Control. VTT, Espoo, Finland.

Kjellén, U., Sklet S., 1995. Integrating analyses of the risk of occupational accidents in the design process. Part I: A review of types of acceptance criteria and risk analysis methods. Safety Science, 18, 215-227.

Lees, F., 1996. Loss prevention in the process industries (2nd edition). Butterworth-Heinemann, Oxford.

Reason, J., 1990. Human error. Cambridge University Press, New York.

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

Rouhiainen, V., 1992. QUASA: A method for assessing the quality of safety analysis. Safety Science, 15**,** 155-172.

Suokas, J., Rouhiainen, V., 1993. Quality management of safety and risk analysis. Elsevier Science, Amsterdam.

Swuste, P., 1996. Occupational hazards, risks and solutions. Delft University Press, Delft, the Netherlands.

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

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