Preprint version of article published in:

Cottam, M.P., Harvey, D.W., Pape, R.P., and Tait, J. (eds):
Foresight and Precaution*, Proceedings of *ESREL 2000.
Balkema, Rotterdam. (pp. 1373–1378) 2000.

Assessment of safety functions at an industrial workplace - a case study

Lars Harms-Ringdahl
Institute for Risk Management and Safety Analysis,
Bergsprängargränd 2, S-116 35 Stockholm, Sweden (www.irisk.se)

Abstract

The study is focused on how to model and assess safety at industrial installations. A starting point was the concept of safety function, which is defined as a technical, organisational or combined function, which can reduce the probability and/or consequences of a set of hazards in a specific system. A tentative theoretical framework has been developed. In a case study, a workplace at a process industry was analysed. A number of safety functions were identified and characterised according to the frame-work. The efficiency of these safety functions was assessed, and a few different approaches were tried in this evaluation. A conclusion was that the safety function concept worked well in the practical analysis of the safety in the studied system. It was also clear that there is a need for further improvement of the theoretical framework, and a number of ideas came up during the case study.

1 Introduction

There are many approaches to assessing the safety of a system. One starting point for this paper is a preliminary study with the aim to compare principles for achieving safety in different areas (Harms-Ringdahl 1999a & b). One observation was that there is a varying terminology, sometimes with poorly defined terms. This can be expected to cause confusion and difficulties in many situations. A conclusion was made that "safety functions" was an interesting concept to develop and work further on.

A follow up study has started, and one essential part was to apply the concept on a number of practical case studies. This is done in combination with a theoretical modelling of industrial safety systems. The general purpose is to explore to what extent "safety function" can be a valuable concept in practical analysis of safety properties of a system.

The aims of this case study was to:
a) Make a description of the safety characteristics at a selected workplace.
b) Try a tentative general model of safety functions.
c) Test ideas for the assessment of the "efficiency" for some types of SF.
d) Test if the concept is practically applicable and seen as useful by company management.

The first three aims are related to the testing and improvement of the theoretical approach. The last aim is oriented towards possible practical applications. This paper summarises experiences from the first case study.

2 On the modelling of safety

2.1 Different approaches

There are many approaches to the description of safety characteristics in systems. Some examples are shortly discussed here. Energy models have been used for a long time (e.g. Johnson 1980), and they usually involve technical as well as organisational aspects in the barriers.

Safety within the nuclear power area is well documented in numerous reports. For example, a summary of basic safety concepts in the nuclear power sector 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 e.g. 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 in the modelling of safety characteristics. An interesting example is a framework for modelling safety management systems (Hale et al. 1997). Safety management is seen as a set of problem solving activities at different levels of abstraction, and risks are modelled as deviations from normal or desired process. There is also a number of other interesting alternative approaches for analysing and describing safety characteristics (e.g. Kecklund et al. 1995, Hollnagel 1999).

Many alternative ways of describing the safety characteristics exist. It could be discussed how complex or simplified the model should be made. In this case study, a concrete industrial system should be analysed and a compromise was needed. As expressed by Wahlström (1994): a model should be refined enough not to be trivial, but simple enough to bring forward only the essential characteristics of the real system.

2.2 A framework for describing safety functions

Definition

The preliminary study (Harms-Ringdahl 1999a & b) did not reveal any generally applied description of what a safety function (SF) is. As a consequence, a tentative definition was proposed*: a safety function is a technical or organisational function with the purpose of reducing the probability and/or consequences of a set of hazards.* Human actions should also be considered and was regarded as part of the organisational component.

Parameters

Safety function is a broad concept, and in specific applications it requires more concrete characterisation. This can be achieved using a set of "parameters", and some essential examples are:

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

a) *Level of abstraction* is here divided into four levels. The highest level is called *general function* and is related to the aim. *Principal function* and *functional solution* are less abstract. The concrete solution, e.g. a specific safety relay or an operator's action, is on the lowest level. These levels are not yet strictly defined, but will be improved during the project. Examples on this theme are given in Table 1.

b) *Systems level* describes the level of detail at which the system is studied and modelled. This can concern components, subsystems, larger systems or a whole factory. Here, it concerns the safety functions, but it could be applied also on the system for which safety is wanted.

c) *Type of safety function* describes what is included in a safety function. It can be divided into technical, organisational and human functions. Also functions where safety is not the main objective may have essential safety features. All these can be at different levels of a) and b).

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 corresponding equipment, etc. Organisational conditions of different kinds should be included here. Examples are management of projects, and maintenance. One essential aspect is type of organisation; this can range from a hierarchy with strict rules for decisions to informal and open decision-making.

Safety characteristics and efficiency

A SF could be described by a set of characteristics, which are intended to describe the contribution of a SF to the overall safety, and give the basis for an evaluation of the SF. Examples of characterisations are:

- Consequences of a failure of SF
- Robustness, the vulnerability of the SF to deviations, interruption of procedure etc
- Possibility to verify results of a SF
- "Efficiency" is intended to give a measure of how well a SF can fulfil its aim. A suitable definition has not yet been developed. A tentative description is given in Section 3.3.

Similar terms can be found in a standard from IEC (1998):

- *Functional safety* is the ability of a safety-related system to carry out the actions necessary to achieve a safety state for the "Equipment Under Control".
- *Safety integrity* is the probability of a safety-related system satisfactorily performing the required safety-related safety functions under all the stated conditions within a states period of time.

3 A case study

3.1 The studied system

About the workplace

The case study was made at a section of a pharmaceutical industry. In principle, it is a simple batch production, where different substances are added and mixed following strict procedures. Hygienic demands are high, and cleaning follows specified routines. This type of production is common in pharmaceutical, food and other similar process industries.

A general impression was that the procedures and technical equipment were of good standard. The company has high aspirations of maintaining good working conditions and safety.

In this presentation, a limitation is made to the cleaning function of the system. Between each batch, the production vessel is cleaned following detailed specifications. The cleaning procedure is 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), hot (80 ^{o}C) and cold water.

Selection of the workplace
From the start, the author had used the workplace as an exercise at a training course in safety analysis. This meant that a fairly detailed analysis had been made of the workplace, using the two methods energy analysis and deviations analysis (Harms-Ringdahl 1993).

The workplace was regarded as suitable, because it had some clear hazards, like potentially high pressure, strong lye and hot water. Another reason was that production was carefully regulated with routines and rules that would be easy to distinguish and describe.

3.2 Approach

Different steps
The case study was made in a few major steps:

- Summing up earlier obtained information
- Modelling the safety functions
- Interviews; Assessment of characteristics
- Analysis

Modelling the safety functions
Information about safety functions was collected in a dialogue with an engineer, who knew the system and its design history well. He had also participated in the safety analysis.

The data collection started with a discussion of an accident scenario - the collapsing of the tank due to overpressure. A number of safety functions, which could prevent the accident, where identified. This was followed by a search for functions related to mitigation and emergency activities. Some further scenarios were then debated to achieve more data.

These exercises were followed by a check with the parameters of the general model. This lead to identification of a number of additional SFs not observed before. After that, these were arranged and structured by the author. The result was then checked and confirmed by the interviewed engineer.

Interviews - Assessment of characteristics
In a second round three persons were interviewed. The first was the same engineer as before. Number two was a works manager with responsibility for the workplace, and number three was an operator and also safety representative. Also these had been involved in the safety analysis. It meant that all those interviewed had a good insight in the hazards and the problems of the system.

In the interviews, a check was made, if the description of the safety functions of the system was correct and complete enough. All agreed, but a few extra points usually came up and were added to the description. The main issue was to assess three different characteristics for each identified safety function. These characteristics are described below.

The three interviews, as well as the first modelling discussion, took less than two hours each.

3.3 Classification of characteristics

Characteristics
A safety function can be described by a number of characteristics, and in this case study three were applied:

- Intention
- Importance
- Efficiency

Intention

The intention was divided in 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 the main purpose is something else
3) Intended to give safety - or reduction of consequences

Importance

Importance from safety point of view:

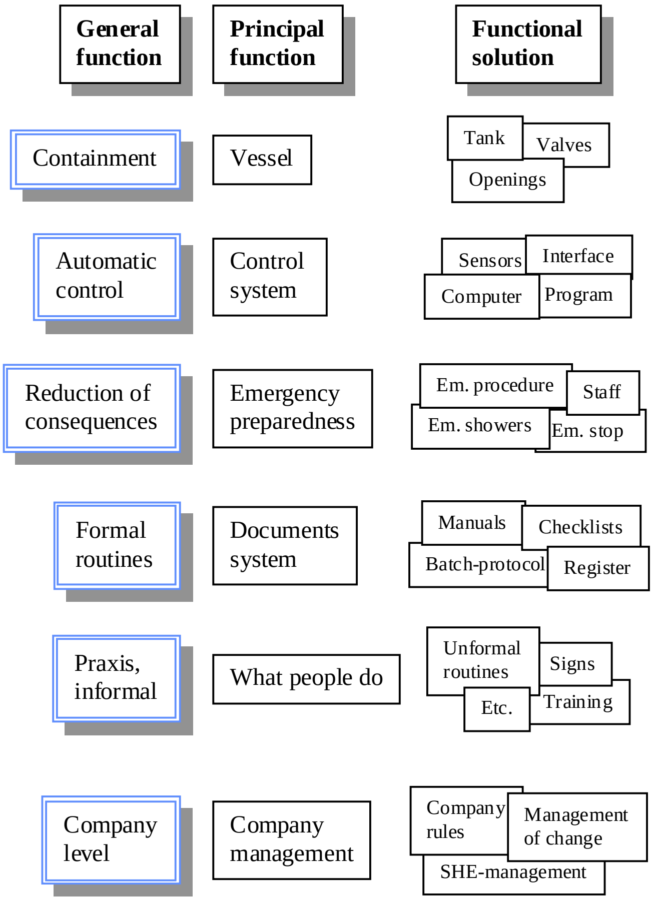
0) No influence on safety
1) Small
2) Rather large
3) Large, closely connected to accidents or size of consequence

Efficiency

The "Efficiency" for each SF should be assessed. A rather straightforward scale of probability for success was used in this test. It was divided in eight sections, starting with A = Less than 1% likelihood of success, up to H with 99,99%. "Success" would have a somewhat varying meaning depending on the type SF.

4 Results from the case study

4.1 Identified safety functions



General function	Principal function	Functional solution
Containment	Vessel	Tank Valves Openings
Automatic control	Control system	Sensors Interface Computer Program
Reduction of consequences	Emergency preparedness	Em. procedure Staff Em. showers Em. stop
Formal routines	Documents system	Manuals Checklists Batch-protocol Register
Praxis, informal	What people do	Unformal routines Signs Etc. Training
Company level	Company management	Company rules Management of change SHE-management

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

The safety functions were structured on different levels of abstraction and systems levels. An overview of the identified safety functions is given in Figure 1. The left part shows the "general functions" of a fairly abstract and general character. The middle part is on a medium level of abstraction and is called "principal function". The right part shows the system at a lower system level and more concrete, which is named "functional solutions".

The lowest row in Figure 1 shows functions on the company level, while the rest is on workplace level. It could be debated if the company level should be included or not, since it probably do not have a direct influence on the accident chain. In this case study it is included, because several SF came up on this theme.

The safety functions were divided in six major groups. In all, 54 safety functions were identified on the level of "functional solution". It was *not* regarded as meaningful to go down to a level of detailed components. The list would then be very long, and difficulties would arise to maintain a comprehensive perspective.

Looking on a detailed level, one could find for example 40 sensors and 30 computer controlled valves. A procedure manual (counted as one safety function) described 40 actions etc.

4.2 Assessment of safety functions

The 54 safety functions were assessed according to three main characteristics. As expected, it was differences between the interviewed persons. A comparison showed that of all the 162 assessments made, only 26% were identical for all three persons.

There are some contributing explanations to the differences. The three persons had different roles and priorities at the workplace. E.g. the design engineer can be supposed to have larger insight about intentions in the design process than the others do.

The first characteristic concerned the "intention" with a SF. Here the variance was rather large, and for around 37% of the SFs it was unclear if it was intended or not. For 33% it was agreed that safety was intended, and 29% that it was not intended.

Table 1 gives an overview of how important the safety functions were considered to be. Four of the safety functions were given a rank of 3 by all the assessors (see Section 3.3). In all, 13 of 54 functions were thought to have no or little importance. It can also be seen that as much as 41 functions were regarded as important by at least one person.

Table 1. The number of safety functions for different scores given on "importance" by three reviewers.

Classification*	0	1	2	3	All 3	Total
A Containment, vessel	2	1	6	0	2	11
B Control system	4	1	4	3	2	14
C Emergency preparedness	0	0	1	3	0	4
D Formal, documents system	4	1	3	0	0	8
E Praxis, what people do	0	0	5	2	0	7
F Company management	0	0	7	3	0	10
Total	10	3	26	11	4	54

Classification*: **"0"** = Only score 0 were given. **"1"** = At least one score 1, but no higher
"2" = At least one score 2, but no 3 **"3"** =At least one score 3 **"All 3"** = All three reviewers gave 3.

Estimates of "Efficiency" were more difficult to give; for around 30% of the SFs a missing estimate could be noted. For some SFs, it was good agreements, which usually was the case when the efficiency was low, or very high.

5 Discussion

Using the concept

One observation was that the concept of safety functions worked as a basis for discussions. It was intuitively understood by all involved, and no long explanations were needed.

The process of identification of SFs was fairly quick. It helped that a safety analysis had been done before, but the used approach supported clearly the work. In the assessment discussions, also ideas for a number of supplementary SFs came up.

In the case study, the modelling was based on a practically oriented collection of data, which was later structured and discussed on a concrete level. A more academic opening with theory and model would probably have worked less well.

Classification and structuring

One aim with the classification and structuring was to get a comprehensive picture of how safety was achieved. The result of the structuring is shown in Figure 1.

In Section 2.2, four different parameters are described. The parameters (a) *Level of abstraction* and (b) *Systems level* were combined in the horizontal dimension to give three columns. Also the vertical dimension had a mixture of parameters: (c) *Type of SF* and *(*d) *Type of object*. This mixed approach was found to give the most comprehensible model of this system.

The four parameters were included in the first interview when SFs were identified. The aim here was to use them as a checklist to widen the scope in the analysis. Around twenty percent more SFs were found by this. The overall experience was that the parameters appeared to be useful, but they needed further development. It could be interesting to also apply other classification models (e.g. Kecklund et al. 1995, Hollnagel 1999) on the collected information.

Assessment

All the SFs had been assessed regarding intention, importance and efficiency. The practical aim was to find which SFs were most important, and also where improvements were needed. This appeared to work fairly well, and a number of essential points for improvement were discovered.

Assessments were made independently by three persons with different positions in the company. However, it was a large variance between the individuals, and they were often undecided which value they should choose.

A general observation is that it was difficult to apply the simple classifications on all types of safety functions in this case study. The classification system needs further evolution, and probably also ways of adaptation to different types of situations.

Difficulties with the "intention"

One difficulty concerned the "intention" with a SF. Here the variance was large between the persons. For example 37% of the SFs were judged differently. One example when the intention was obscure concerned a written instruction, which has many steps. Some of these have essential safety features, but the importance of these was probably not understood when the instruction was written.

It appeared that the concept of intention was a bit more complicated than anticipated from the beginning. If it is used as parameter in classifications, the definitions need to be clarified.

Definition and terminology
However, this difficulty with "intention" also affects the general definition of safety function. It was phrased: " *..... the purpose of reducing the probability ....".* As a consequence of the discussion above, the word "purpose" is not suitable.

There could be a combination of different technical and organisational functions involved in a specific SF. Also actions by individuals in the system are essential for safety, and this could be included in "organisational function".

Based on this, a new definition is proposed:

> *A safety function is a technical, organisational or combined function, which can reduce the probability and/or consequences of a set of hazards in a specific system.*

About the identified safety functions
The analysis of safety functions has improved the understanding of the safety characteristics, both for the company and for the author. The investigation showed a complex pattern of technical and organisational - both formal and informal - functions. It was clear that the "informal" SF were essential both on the operative level and in the system design.

At the intermediate level "functional solution" used in the analysis, 54 SFs were identified. However, going one step towards more detailed levels of systems, the number of SFs would climb to several hundreds or over one thousand. One conclusion is that it is necessary to start on a fairly high level of systems description, if the analysis should not drown in too many details.

6 Summary and conclusions

Although, a complete framework and theory do not yet support the safety function concept, it was useful in practice as a basis for discussions and gave new insights. The safety function concept worked well in the practical analysis of the safety in the studied system. Thus, it appears reasonable that the concept could support a methodology for improvement of safety in technical systems. The reasons are that the concept is rather easily understood, it created ideas, and it helped in the assessment of the safety of the system.

It was also clear that there is a need for further improvement of the theoretical framework, and a number of ideas came up during the case study.

The practical results were:
a) a structured summary of the important safety functions in the system,
b) an identification of a number of weaknesses in the safety system, and
c) ideas for improvements of the safety system

It is a need for improving the theoretical framework, and a number of ideas came up during the case study. Most basic is a proposed new definition:
A safety function is a technical, organisational or combined function, which can reduce the probability and/or consequences of a set of hazards in a specific system.

Acknowledgement
The Swedish Council for Work Life Research has sponsored this research project, which is gratefully acknowledged.

7 References

Hale A.R., Heming B.H.J., Carthey J. & Kirwan B. 1997. Modelling of safety management systems. *Safety Science* Vol. 26, No 1/2, 121-140.

Harms-Ringdahl L. 1993. *Safety analysis - Principles and practice in occupational safety*. Elsevier Applied Science, London.

Harms-Ringdahl L. 1999a. On the modelling and characterisation of safety functions. In G.I.Schueller & P.Kafka (eds) *Safety and Reliability ESREL'99*. Balkema, Rotterdam, 1459 - 1462.

Harms-Ringdahl L. 1999b. Beskrivningar och modeller av säkerhetsfunktioner - en förstudie. Swedish Nuclear Power Inspectorate, Stockholm.

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

IEC (International Electrotechnical Commission) 1998. Standard IEC 1508: Functional safety: safety related systems. International Electrotechnical Commission, 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.* National Safety Council, Chicago.

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 L.Norros (Ed.) *Fifth European Conference on Cognitive Science Approaches to Process Controll*, VTT, Espoo, Finland.

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