Preprint version of article published in:

Schueller & Kafka (eds): Safety and Relibility.
Proceedings of ESREL'99 European Safety and Reliability Conference 1999.
A.A.Balkema, Rotterdam. (pp. 1459-1462) 1999.

On the modelling and characterisation of safety functions

Lars Harms-Ringdahl
Institute for Risk Management and Safety Analysis, Stockholm, Sweden

Abstract

Different theories and applications concerning "safety barriers" and "safety functions" have been investigated. The general aim was to compare principles and terminology in some different areas. Of special interest are applications from the nuclear and chemical-process industries, and a short summary is given. The study is based on a literature review, interviews and discussions.

Only a few theoretical models describing safety functions have been found. This points to the need for further development of models and theories that might provide a basis for improved practical tools to support the design and evaluation of organisational proce dures. A tentative model is discussed. It is based on "safety function elements" and the characteristics needed to describe and assess safety functions, e.g. purpose, efficiency, and reliability.

1 INTRODUCTION

There are usually high demands on the safety performance of systems where the consequences of accidents are large. There are variations between industrial sectors, concerning both the design/assessment of safety equipment and safety management. Conceptions on how to achieve safety are also highly dependent on the background of the people involved. An engineer will often have different priorities from a behavioural scientist or lawyer at a regulatory authority.

Since the concept of safety, and also methodology for achieving it, varies so considerably, a decision was made initially to compare how safety is handled in different application areas. "Safety function" was regarded as a key concept. A tentative definition*: a safety function is a technical or organisational function with the purpose of reducing the probability and/or consequences of a set of hazards.*

The aim of the project was to study principles for achieving safety, and to consider whether safety function might be a fruitful concept to develop. The main parts of the project are intended to:

1. compare some application areas;
2. prepare a summary of how "safety function" or similar expressions are used;
3. design a tentative model to describe and characterise safety functions.

The project is based on information from the literature, interviews and discussions. The paper here is an abbreviated version of a full report published in Swedish (Harms-Ringdahl 1999).

2 EXAMPLES OF SAFETY APPROACHES

2.1 Nuclear power sector

Safety within the nuclear power area is well documented in numerous reports. A summary of basic safety concepts in the nuclear power sector is provided by INSAG (1988). Twelve fundamental safety principles are discussed, and they are divided into three main groups. A compressed overview is given in Table 1. In the report, a set of 50 "specific safety principles" is also discussed. In a later report (INSAG 1996) the characteristics of "defence in depth" in nuclear safety are further described.

Table 1. Summary of general safety principles (from INSAG 1988)

Main groups	Safety principle
Safety management	Safety culture Responsibility of the operating organisation Regulatory control and independent verification
Defence in depth	Defence in depth Accident prevention Accident mitigation
Technical principles	Proven engineering practices Quality assurance Human factors Safety assessment and verification Radiation protection Operating experience and safety research

2.2 Chemical industry sector

The chemical industrial sector also has a long tradition of systematic safety work. A comprehensive overview of safety principles is provided in "Guidelines for Safe Automation of Chemical Industries" (CCPS 1993). It describes both general aspects, and also safety in connection with automated safety and process control systems.

A fundamental term employed is "*protection layer*", although this is not explicitly defined. It "*typically involves special process designs, process equipment, administrative procedures, the basic process control system and/or planned responses to imminent adverse process conditions; and these responses may be either automated or initiated by human actions*".

A figure entitled *"Protection layers"* displays eight levels. These are arranged in order of how they are activated in the case of an escalating accident:

1. Process design.
2. Basic controls, process alarms and operator's supervision.
3. Critical alarm, operator's supervision and manual intervention.
4. Automatic safety interlock system.
5. Physical protection (relief devices).
6. Physical protection (containment devices).
7. Plant emergency response.
8. Community emergency response.

2.3 Automation of technical systems

An essential part of the guideline (CCPS 1993) concerns automation aspects and control systems. A design philosophy for *safety interlock systems* is encapsulated in ten distinct points.

There is also a general standard called "*Functional safety: safety related systems*" (IEC 1998) from the *International Electrotechnical Commission*. The standard covers the aspects that need to be addressed when electronic systems are used to carry out safety functions. It is extensive and contains seven parts.

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. A number of basic terms are employed in the standard:

- *Safety-related system* implements the required safety functions necessary to achieve a safe state for the equipment under control. (A person could be part of a safety-related system.)
- *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 functions under all the stated conditions within a stated period of time.

"*Safety function*" is a much-used term, but it is not defined. Perhaps it is regarded as self-evident. "*Barrier*" is not mentioned at all.

3 DISCUSSION

3.1 Procedures and theories

The literature review reveals that safety aspects of procedures are regarded as essential. They have received considerable attention, especially in the nuclear sector. For example, according to Marsden (1996), the design of procedures has many inherent failure sources: "*Procedures prepared by 'technically qualified' personnel working in isolation are frequently found to be incomplete, incorrect, or generally unrealistic. Critical information can be effectively masked in documentation which is poorly formatted.*" Marsden also quotes investigations where around 70% of nuclear power incidents were found to involve essential procedural failures.

Wahlström and Gunsell (1998) have performed a review of safety work in the nuclear sector. They have discussed a number of parameters and concepts that could be used in the description of safety work. There are a number of methods for the evaluation of safety management. However, the authors note that methods have not been validated in a scientific way; nor are they based on any theoretical model.

Four methods for the analysis of organisational factors in probabilistic risk assessment have been studied (Abramovici & Bourrier 1998). The general conclusion drawn is similar to that of the other study, i.e. the methods do not appear to be based on clear models and scientific theory.

3.2 About safety functions

The term "safety function" is used rather often, but few definitions are given. Beard (1996) has conducted an investigation of how the term is defined in the nuclear sector. Although the research for this investigation was comprehensive, he found only one place where the term *nuclear safety function* is formally defined, and that definition was so general as to be of little value. A further conclusion was that there is a need to improve the usage and content of "Safety Function" statements.

There are also a number of similar terms in use, some defined, others not. One interesting approach utilises the concept of *safety barrier function.* This is defined as a function that can arrest accident evolution so that the next event in a potential chain is never realized (Svenson, 1991). Svenson also offers a related definition of *barrier system*, which encompasses the physical, technical, or human-factors/organisational systems performing the barrier function.

4 A TENTATIVE MODEL

4.1 Characteristics of the safety function

There does not appear to be a generally applied description of what a safety function is. Hence, a tentative definition is proposed here*: 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 are also considered, and 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 "dimensions", which are sketched out below:

- Level of abstraction.
- Systems level.
- Parts of the safety function.
- Type of system.

Level of abstraction starts at the lowest level with the concrete solution, e.g. safety relay or operator's action. The other, higher levels are functional solution, principal function and general function.

Systems level describes the level of detail at which the system is studied. This can concern components, subsystems, larger systems or a whole factory. It encompasses both the system for which safety is wanted and the safety functions.

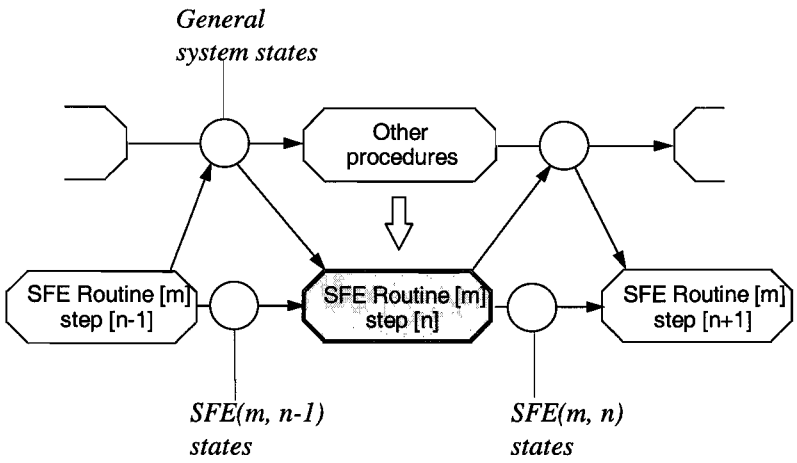
Parts of the safety function describe what is included in a function. They can be divided into technical, organisational and human functions. Further, functions where safety is not the main objective may have essential safety features. All these can be at different levels of abstraction and system.

Type of system 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. Procedures of different kinds should be included here. Examples are management of projects or of operations, and maintenance. One essential parameter is type of organisation; this can range from a hierarchy with strict rules for decisions to informal and open decision-making.

4.2 The safety-function element

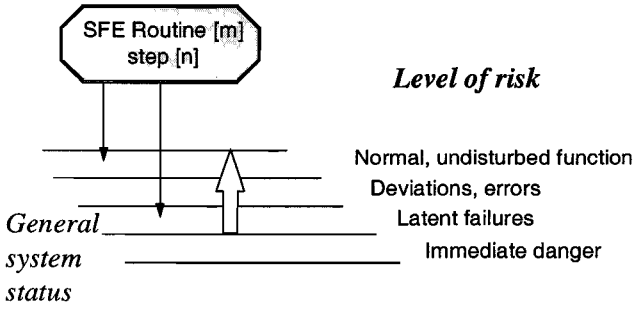
One approach to modelling a "safety function" is to divide the function into a set of *Safety Function Elements* [SFE (m,n)]. In simple form, the set represents an organisational procedure (number m) that is divided into a number of steps (n). Figure 1 symbolises the connections between consecutive SFEs, and also relations to neighbouring procedures.

Figure 1. A model of Safety Function Element, SFE (m,n) and its relation to other elements.



The approach can be used to characterise and analyse each SFE. Figure 1 also indicates a use of "SFE-states" that can be related to a general system state. It also relates to "level of risk" (as broadly indicated in Figure 2). The application of SFE (m,n) can reduce the "level of risk", leave it unchanged, or lead to a deterioration in the situation.

Figure 2. A Safety Function Element, SFE (m,n) influencing the level of risk.



It is planned that this model outline will be applied in a number of practical cases. The first step will be to start with a rather simple industrial installation, and analyse some accidents along the concepts outlined here. The experiences from the case studies will show the practical value of the model.

5 CONCLUSIONS AND SUMMARY

- There is a varying terminology, sometimes with poorly defined terms. This can be expected to cause confusion in many situations.
- The field of safety and safety functions was found to be less theoretically developed than expected.
- This indicates a potential for development of both theory and methodology.
- A simple tentative model is proposed for description and characterisation of safety functions. It is not complete, but should be regarded as providing a basis for ongoing discussion.
- It was found that the safety-function concept is interesting to work on further. In fact, a project directed at safety in common workplaces has already been initiated.

ACKNOWLEDGEMENTS
The Swedish Council for Work Life Research and the Swedish Nuclear Power Inspectorate have sponsored the study, which is gratefully acknowledged.

REFERENCES

Abramovici, M. & Bourrier M. 1998, Beyond the Black Box: Organisational factors in probabilistic risk assessment methods. *Society for Risk Analysis - Europe 1998 Annual Conference*, Paris.

Beard, J.T. 1996. What Does "Safety Function" Mean? Published on the Interment: *http://www3.dp.doe.gov/CTG/authbase/sf_paper.htm.*

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

Harms-Ringdahl L. 1999. Beskrivningar och modeller av säkerhetsfunktioner - en förstudie. (To be published) Stockholm.

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

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.

Marsden P. 1996. Procedures in the nuclear industry. In N. Stanton (ed). *Human factors in Nuclear Safety*: 99-116. London: Taylor & Francis.

Svenson, O. 1991. The accident evolution and barrier function (AEB) model applied to incident analysis in the processing industries. *Risk Analysis* Vol. 11, No 3, 499-507.

Wahlström B. & Gunsell L. 1998. Reaktorsäkerhet; En beskrivning och en värdering av säkerhetsarbetet i Norden. NKS-sekretariatet, Risö forskningscenter, Denmark.