Guide to safety analysis for accident prevention

Lars Harms-Ringdahl

IRS Riskhantering AB www.irisk.se

Guide to safety analysis for accident prevention

Drawings by Nils Peterson
Diagrams and photos by the author

Published by IRS Riskhantering AB,
Bergsprängargränd 2A, Stockholm, Sweden
www.irisk.se

ISBN 978-91-637-3164-8

The updated electronic version can be found www.irisk.se/sabook

Paperback

Also available as paperback: www.shopmybooks.com

In the Nordic countries: www.gmlforlag.se

Contents

Preface

This book is about safety analysis as a tool for accident prevention. The methods can be used to analyse systems and to investigate accidents, and thereby generate knowledge for systematic improvements.

The prevention of accidents is an extensive and complex subject. In the accident prevention arena, many practices and theories exist side by side. There are different traditions involved in explaining accidents, and investigating, and preventing them. The variations are not necessarily problematic, but they suggest that accident prevention in practice is not as efficient as it could be.

The variety is fascinating in many ways, and I have had the opportunity to see it from different perspectives and in various roles. Over the years, I have had the privilege to work with safety in a number of fields. At the beginning, it was in the industrial sector, including paper mills, and the engineering, chemical, and pharmaceutical industries, where the focus was on occupational accidents. In stages, my scope has widened to encompass other areas, and it has been interesting to test the arsenal of industry-based methods in new settings. Examples are:

- Power production
- Railway and other transportation
- Hospital care
- Emergency services
- Safety work at societal level

There are many similarities between safety analyses and accident investigations, and often similar methods can be applied. It is also possible to apply a general methodology that can be efficiently applied in many different sectors. This has been one of my motives in attempting to write a generalised description of safety analysis and how it can be applied.

Safety analysis

Safety analysis is a central concept in this book, and it is here defined as a procedure for analysing systems in order to identify and evaluate hazards and safety characteristics. The definition is wide, and covers many ways of analysing. It includes quantitative and qualitative risk analyses, accident investigations, and also some other applications. The rationale for this wide scope will be discussed further on.

Safety analysis can be used to:

- Support efficient accident prevention.
- Contribute to an understanding of how accidents can occur at the specific workplace under examination.
- Increase awareness and communication.
- Demonstrate systematic safety work.

About this book

The aim of this book is to explain general methods of safety analysis, which can be used for accident prevention in different fields. The idea is to give simple straightforward descriptions, and relate them to practical experiences. The ambition is to promote wider use of the methodology, which offers a potential for better accident prevention.

The book builds further on earlier publications (Harms-Ringdahl, 1987, 1993, 2001), which had a focus on occupational accidents. The material has been developed from the specialised literature, and from the author's own work on the analysis and prevention of accidents. Many important lessons have been learned from teaching on training courses in safety analysis and accident investigation.

The most obvious feature of the new book is that it will be published as an electronic book that is free to download. The reason for this is that it will make for a larger circulation, which will spread the methodology more widely. There will be no economic obstacles to looking at the book, and if it is found useful, it can be applied directly.

There are other advantages to having an electronic version, since you can easily search and jump between pages. The use of links makes it easy to look at other references. But some people prefer paper versions, and it is possible to obtain a print-on-demand version.

General comments

The ambition has been to be general in descriptions, since the principles of many methods can be applied to different types of systems. This might make the descriptions harder to follow, but, on the other hand, it makes the methodology more general applicable.

The book suggests a general framework for accident prevention and safety analysis. Several methods of analysis will be described. Some selected methods are thoroughly described and practical suggestions given – almost like in a cookbook. The intention is that the reader should get sufficient advice to perform a fairly good analysis on the basis of the description.

The general perspective means that the methodology can be applied to a variety of systems and situations where safety is an important issue. They may concern a mechanical workshop, a ward at a hospital, or children in a school. They all have it in common that some kind of organised activity is involved. The word *company* comes up throughout the book, and this should usually be interpreted in a wide sense. It refers to any type of organised activity in the public or private sector.

Safety analyses and accident investigations have many common features, which will be further explained in the framework discussion (Chapter 2). Both approaches can be applied:

- To identify problems and hazards in a given situation, e.g., in a workplace
- To understand how a situation can be made safer
- To develop safety improvements
- To be important tools for safety management within the organisation

The basic idea underlying the book is to show how safety analysis can be practically applied. Its emphasis lies on explaining how different methods work. It is important to consider theories of accident causation, system behaviour, management, human error, and so on. However, they are kept to a minimum in order to limit the number of pages. The reason for this is that the book is mainly intended as a guide for people who would like to employ the methodology. For this reason, there is no stress on theory. A bibliography is provided for those who want to go further theoretically.

Looking in the literature, you will find a large number of different methods, which are more or less thoroughly documented. The book presents a set of methods that are described in detail, and a selection of others that are more cursorily explained. Chapter 4 gives a short overview, and a more extensive one can be found in Chapter 15. The main focus is on qualitative methods, which can be beneficial in large application areas. Quantitative and probabilistic methods are only briefly presented. One reason for this is that there is already a large literature available, which is more directed at technical and/or hierarchical systems.

Sections in the book

The book is built up in four major sections:

1) Background to and framework for analysis
2) Methods of analysis
3) Planning and accomplishment
4) Examples

The framework section concerns the analytic procedure, i.e., the various stages that make up an analysis and how these are related to one another. This section also aims to give a perspective on how you can get an integrated and consistent framework for how different methodologies can be applied.

The method section presents a number of methods. It starts with techniques for risk evaluation, such as the risk matrix. The book describes methods for both analyses of systems and accident investigations. The number of existing methods is large, and a limited selection has therefore been made.

The planning section discusses the practical aspects of an analysis. One basic step is to define the aim of the analysis and the type of results desired. In order to achieve this, careful planning is essential. An analysis should be seen as a supplement to a company's own safety activities. The section also considers quality aspects, as well as arguments for and against specific methods of safety analysis.

The examples section presents case studies of accident investigations and analyses of systems from different application areas.

Use and practical reading

This book is primarily intended for practitioners, but may also be useful for researchers. Persons most interested in practical applications can skip over several of the chapters. An important readership consists of those who intend to do some kind of a safety analysis themselves, such as:

- Safety professionals
- Fire engineers
- Designers
- Consultants in different specialities

Another important group consists of persons who, in one way or another, have an interest in the results of an analysis:

- The customer, who is to commission an analysis and get a sufficiently good result
- The manager, who can use safety analysis to support the planning of a new system
- Other stakeholders, such as employees, whose safety is concerned
- Safety committee members, who want to be able to question management on what methods have been used to assess risks
- Officials from a supervising authority, who need to know if an analysis is accurate enough

For these people, the advice on planning and the methodological overview might be most relevant (chapters 14 and 15).

Web and paper versions

The web and paper versions are intended to be as similar as possible. However, the electronic version can be updated more frequently. Version numbers will be provided to keep track of updates. Positive features of the web version are:

- Contents easily accessible as bookmarks in the left-hand column
- Links to other places in the book and to outside material
- A search function, which can help in finding words and phrases of special interest (accessed by pressing Ctrl + Shift +F)

Acknowledgements

The material in this book has been developed over several years through contacts and collaboration with many people. My thanks go to my research colleagues and friends in Sweden and other countries, and to the many others who have encouraged the application and development of safety analysis in occupational and other contexts. For collaboration in recent years, I would like especially to mention Anders Bergqvist, Celeste Jacinto, and Mattias Strömgren. Also, I wish to thank Jon Kimber for his careful checking of the text.

Many thanks to the Swedish Council for Working Life and Social Research (FAS) for the financial support they have provided for this book, and for some of the projects on which it is based.

My deep appreciation goes to Karin Michal for valuable discussions and positive support over many years.

1 Accidents in a systems perspective

1.1 The accident concept

Common meanings

The meaning of *accident* is often seen as simple and straightforward. A common definition is that accidents are unplanned or unforeseen events causing injury or damage. From a legal perspective, the term accident can mean that the damage was not intended, and/or that the event cannot be regarded as involving a crime.

Definitions vary between different fields, and sometimes over time. One example can be taken from the field of occupational safety (DNBIJ, 2006), which runs: "A personal injury caused by an incident or exposure which occurs suddenly or within 5 days."

Within the medical tradition and in epidemiology, the term *injury* is prevalent, and more common than the term accident. A short definition from WHO (2004) is: "An injury is the physical damage that results when a human body is suddenly or briefly subjected to intolerable levels of energy."

A more comprehensive descriptive definition used by WHO (2004) is: "Injuries are caused by acute exposure to physical agents such as mechanical energy, heat, electricity, chemicals, and ionizing radiation interacting with the body in amounts or at rates that exceed the threshold of human tolerance. In some cases (for example, drowning and frostbite), injuries result from the sudden lack of essential agents such as oxygen or heat." The injuries are divided into *unintentional (accidental)* and *intentional (suicide or violence).*

Definition in this book

Here, however, it can be useful to apply a broad definition, since accidents concern many different fields and also because ideas change over time. In this book, we will apply a general definition:

> *An accident is an event that causes damage or injury, but which was not intended to have a negative outcome.*

Or more briefly:

> *An accident is an event that causes unintentional damage or injury.*

The rationale for this is discussed below, where it is found that the meanings of *unintentional* and *unexpected* have their ambiguities. *Damage* is a broad term, which includes injury to humans; for clarity, it is spelled out in the definition.

Attributes

From the examples above, it is obvious that the concept of accident refers to a number of elements, such as:

- A short time scale – an event
- Unintentional consequence
- Unexpected or unforeseen consequence
- Negative consequence – injury or damage
- A situation in which the accident occurred

The time perspective

The accident event is usually a rather brief and physical occurrence. But, from a broader perspective, the time scale can be fairly long. Exposure to chemicals may have a negative effect after a short time, but it may be a long time before more symptoms are manifested. Another example is working in cold weather, where freeze injuries sometimes take hours to develop.

Unintentional – on the part of whom and how

That an accident is unintentional might at first appear a straight-forward statement. The affected person did not want to be injured, and if he had foreseen the injury, he would have avoided the situation. When a system perspective is adopted, it is obvious that the role of different actors in what happened must be considered. The actor can be:

- The victim (injured person)
- Another person (co-worker, a driver on the road, a patient in the hospital)
- The manager who decides what to do immediately
- The company manager who has overall control and responsibility
- The supplier, designer or similar, who is associated with the performance of the equipment, etc.

We could also examine *intention* and make a list of various types of intentions, such as:

- Acting carefully and considering safety
- Acting normally but not considering safety especially
- Acting confused or unbalanced, but without any intention to cause damage
- Taking risks deliberately but thinking that they are manageable (e.g., driving fast and taking short cuts, knowing that it is dangerous)
- Violation of clear rules
- Intention to cause injury

These intentions can concern the victim or, in general, all the other types of actors. The final points can be seen as covering criminal behaviours.

Unexpected or unforeseen

There are issues over what *unexpected* means in this context. The first concerns the person to whom the event was unexpected, e.g., the victim, a person ignorant of the situation, or an experienced worker. A second concerns degree of expectance, ranging from being completely unexpected to the hazard being well known, which is related to how much foresight you can expect. The general conclusion is that the meaning of *unexpected* is unclear, and the term should not be used as an element in an accident definition.

Range of consequences

Consequence is related both to what is damaged and to the magnitude of the damage. A specific accident can have a number of consequences at the same time. Table 1.1 shows different types of consequences, related to what can be damaged. The magnitudes of the consequences also have a wide span, ranging from major accidents with huge damage, to events with almost negligible effects.

The term *function*, as used in the table, has a general meaning. It can concern operations, work, and services of different kinds, such as health care, and food distribution. Different types of consequences are listed.

Table 1.1 Different types of consequences of accidents

Subject	Consequence	Comments and examples
Persons	Injury	Relatively acute effects; the terminology is usually limited to physical damage. Sometimes lost income is included.
	Mental effects	Acute mental effects, such as shock, confusion and anxiety
	Reduced health	Physical or mental consequences; short or long-term effects over a fairly short time
	Insecurity	Fear, lack of safety, lack of information
Environment	Environmental damage	Poisoning, contamination, harm to biosphere, loss of recreational facilities
Function	Complete loss	Distribution of electricity, telecommunications, or provisions, etc. This can concern persons, companies or the community.
	Insufficient	Quantity and/or quality are insufficient
	Information disturbance	Wide area of application, which can concern distorted or lost data, errors in decision-making, or threats to personal integrity
	Increased vulnerability	There can be secondary effects, which depend on how sensitive the function is to disturbances
Economy	Losses	Direct losses, such as medical care or damaged equipment.
		Damage to housing, production facilities or other properties.
		Indirect losses, such as increased costs, lost profit or opportunities.
Other	Decline in trust	Can affect the authorities, companies and other organisations
	Loss of values	Secondary effects on more intangible values, emotional, aesthetic, and historical, concerning individuals and society

1.2 The size of the accident problem

Accidents are a major health problem in all societies. Here, we will discuss a few accounts of the magnitudes of injuries and other damage. There are statistics from various sources, based on different perspectives, which means that a comprehensive overview is hard to obtain.

WHO statistics

The World Health Organization (WHO) presents statistics on injuries in a program called Violence and Injury Prevention and Disability. It is estimated that 5.8 million people died from injuries world-wide in 1998 (Krug, 1999). This corresponds to a death rate of 0.98 per 1000 persons. A conclusion of the study was that injury is the leading cause of death in all age groups. It should be remembered that, for every person who dies, many more are injured and perhaps permanently disabled. The magnitude of the problem varies considerably by age, sex, region, and income. In 1998, the death rate of males was almost double that of females.

WHO's injury statistics do not identify where injuries occur. This means that the data do not permit comparisons between hazards at work, in traffic, in the home, etc. Information about accidents in different arenas can be obtained from other sources.

Table 1.2 Fatal injuries in the EU by cause of death, all ages (from Eurosafe, 2009)

Cause of death	Comments		Part
Accidents (unintended)	Road traffic accidents	20%	47%
	Accidental falls	17%	
	Accidental poisoning	5%	
	Accidental drowning and submersion	3%	
	Accidents caused by fire and flames	2%	
Suicide	Self-inflicted injuries		23%
Intended	Interpersonal violence		2%
Other causes	Other code or unknown		29%

Occupational accidents – a global perspective

The International Labour Organization (ILO) compiles statistics for occupational accidents and diseases. In a large number of countries, both industrialised and less developed, the frequency of fatal accidents has fallen since the 1960s. A statistical analysis has been performed by Hämäläinen et al. (2006). In the world during the year 1998, the estimated number of fatal occupational accidents was 350 000, and there were 264 million non-fatal

accidents causing at least 3 days absence from work. The study found an average fatal occupational-accident rate of 13.8 per 100 000 workers. However, the differences between different countries are huge. The figures are high, but they are also uncertain – mainly due to missing data.

The public health perspective

The European Association for Injury Prevention and Safety Promotion (Eurosafe, 2009) has presented a summary of injuries in the European Union (EU) over the years 2005 to 2007. The data collection was based on medical records. The study emphasises the scale of the problem, and states that every year more than 250 000 inhabitants of the EU die due to the external causes of injury and poisoning. For all age groups, injuries are the fourth leading cause of death, after cardiovascular diseases, cancer and diseases of the respiratory system. Table 1.2 gives an overview of different causes of fatal injuries (Eurosafe, 2009, p. 27).

Road traffic accidents and falls dominate among accidents, but it can also be seen that suicide is the most important single cause. The data show large variation between countries; a factor of four or even higher between the lowest and highest values can be seen for some causes.

Table 1.3 Fatal injuries and hospital admissions in different sectors (Eurosafe, 2009)

Sector	**Deaths**		**Hospital Admissions**	
	n	Share	n	Share
School			100	1%
Sports			600	8%
Home, Leisure,			4 500	63%
Combined	*122*	*48%*	*5 200*	*72%*
Road traffic	51	20%	1 000	14%
Workplace	6	2%	300	4%
Total unintentional injuries	*179*	*70%*	*6 500*	*90%*
Homicide, assault	6	2%	300	4%
Suicide (including attempted)	59	23%	400	6%
Total all injuries	*244*	*~ 100%*	*7 200*	*100%*

n = number in thousands

The same study (Eurosafe, 2009, p. 7) also shows the sectors in which injuries have occurred, and a summary is provided in Table 1.3. The home, leisure, sports, and school sectors have been clustered together in the deaths columns, but their shares in hospital admissions are presented separately. It

appears that home and leisure accidents and injuries constitute by far the largest arenas in which injuries occur. This is followed by suicides, which also appear to be a very large problem. Road traffic shows high numbers, which might have been expected. In this summary, the number of workplace accidents is high, but they still make up only a small proportion of all injuries.

Medical accidents in hospitals

The risk of accidents in hospital care has been known for a long time, but has only received serious attention during the last ten years. It appears that conventional ways of collecting accident data do not identify accidents in hospitals.

A number of studies in different countries have been based on reviewing medical records. These have shown a high injury rate during hospital treatment due to medical errors, which are often called *avoidable adverse events* in the medical terminology. A study (Kohn et al., 2000) concluded that, in the USA, between 44 000 and 98 000 Americans die each year as a result of medical errors.

A Swedish study (Socialstyrelsen, 2008) of a set of medical records of in-patients found that 8.6% were injured due to avoidable errors. The results can be extrapolated to Sweden as a whole, which gives 3 000 deaths per year, and a mortality rate of around 33 per 100 000 inhabitants.

In 2005, WHO established the World Alliance for Patient Safety, with the aims of coordinating, disseminating and accelerating improvements in patient safety world-wide. In information from WHO (2012), it is stated that:

> "Patient safety is a serious global public health issue. Estimates show that in developed countries as many as one in 10 patients is harmed while receiving hospital care. In developing countries, the probability of patients being harmed in hospitals is higher than in industrialized nations. The risk of health care-associated infection in some developing countries is as much as 20 times higher than in developed countries."

Accident arenas

Clarification of arenas where accidents occur is important from a preventive perspective. Table 1.3 shows that there are many sectors and arenas that must be considered. There is also large variation in the conditions and situations that affect the accident rate, such as:

- Standard of living in the country
- Resources for accident prevention in the country

- Political systems
- Large or small enterprises

It is difficult to make reasonably accurate comparisons between countries and between accidents across different problem areas. The scope, accuracy and availability of the statistics vary a lot, which makes prioritisation problematic. There are, however, many valuable summaries, such as those from which the tables above are taken. Another study (Takala, 1999) shows rates of fatal occupational accidents in the world in eight different main regions. There are differences between low and high values of more than a factor of four.

1.3 Critical accidents

The magnitude of the accident and injury problem is really dreadful. There are an estimated 5.8 million deaths by injury every year according to WHO sources (Krug, 1999). This corresponds to around 30 jumbo jet crashes every day, which would not pass unnoticed. However, most accidents and injuries are seen as "normal", and these everyday disasters do not get much attention.

The statistical information on injuries and accidents is not complete, making overall comparisons highly uncertain. The statistics may look different in different regions, but it is important that accident prevention is directed where it is most needed. Looking at Swedish death accidents, there are about 15 times as many avoidable adverse events in hospitals as there are fatal road traffic events. Therefore, I will make an attempt to make a ranking list of accident occurrence relevant to Sweden and similar Western countries:

1) Medical accidents in hospitals
2) Home and leisure accidents
3) Road traffic accidents
4) Sport accidents
5) Work accidents
6) School accidents

Looking at the broader accident panorama, accident prevention is an issue that calls for greater attention and concern than is expressed today. Finding more efficient ways of preventing accidents and injuries is a real challenge. The use and adaption of systematic methods would be of great benefit.

2 Safety work and accident prevention

2.1 Safety work

The previous chapter has presented a broad perspective on accidents, which has gone beyond some of the traditional perspectives. This section will consider the concepts of *safety work* and *accident prevention* generally. It is based on a study (Harms-Ringdahl, 2007) performed for the Swedish Rescue Services Agency, which was supposed to have an overview of national safety work in Sweden.

Safety work is generalized here to include the prevention of losses and injuries in most situations. In this book, the following definition is used:

> *Safety work consists in activities and measures that can contribute to reductions in injuries and losses.*

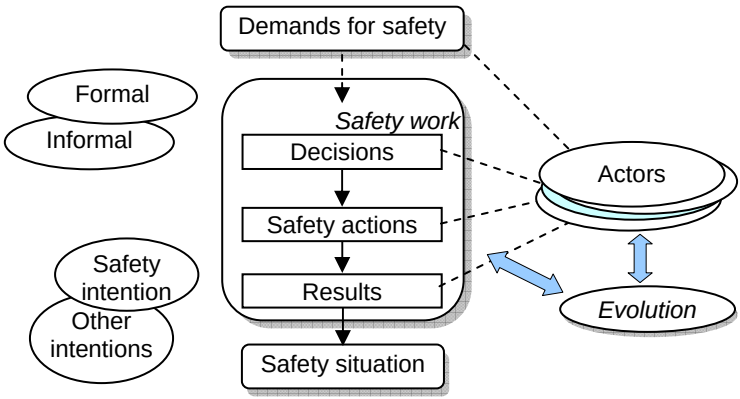


Figure 2.1 A general model of safety work

A simple model of safety work has three major elements: decisions, safety actions, and results (Figure 2.1). Results represent the outcomes of activities that will affect the safety situation. In order to get results, we must assume that one or more actors participate in safety work in some way, such as by taking safety-oriented decisions, or by supporting safety actions. In order to

start the process, there must be some kind of demand for improving the safety situation.

Safety work can be organised in a formal way. It can take place within a hierarchical structure (as in Figure 2.2, Section 2.3), with laws and regulations, policy documents, and clearly defined responsibilities for company management.

However, safety work can also be informal, and voluntary actions from individuals and groups are important in many situations. They may be personal initiatives of different kinds, what people tell each other, and so on.

A safety action is usually intended to achieve safety. However, actions that have another intention can also affect the safety situation. For example, a program intended to reduce the drinking of alcohol for social reasons could also reduce traffic accidents and violence.

The element *evolution* indicates that safety work is a dynamic activity. All the actors concerned can learn and improve their safety work in different ways. Evolution can be preferred as a general term, but *learning from accidents* is a far more widely used expression.

2.2 Elements in safety work

The concept of safety work presented here is general and quite abstract. In practical use, the elements in the model can be specified and adapted to the relevant situation. Examples of elements which can be used to categorize a specific situation are presented in Table 2.1.

Table 2.1 Important aspects of and parameters in safety work

Aspect	**Reference**	**Comments**
Types of consequences	Table 1.1	Different types of injuries and damage
Actors and their roles	Table 2.2	Includes both organisations and individuals
Arenas	Table 2.3	Where activities take place and losses occur
Sources of risk	Table 2.4	Hazards and potential causes of loss
Activities and tools	Table 2.5	What actors do to prevent losses or mitigate consequences
Theoretical models	Section 2.3	Scientific and mental models of risks

Actors and their roles

Actors can include private companies, public services, different kinds of organisations, and also individuals in different roles as employees, at home, and as parents. Furthermore, a specific individual or organisation can have a number of different roles at the same time. Table 2.2 presents examples of different actors and roles. They can be described in several ways, and the table shows complementary divisions. It should be noted that any one specific actor can have several roles, sometimes contradictory.

Table 2.2 Parameters for actors and their roles

	Actors and roles	**Comments**
1	Actors responsible for an activity	The actors who operate the risky activity, such as an employer, the operator of a traffic service, or a car driver
2	Persons at risk	Victims, persons who might be injured or suffer other losses
3	Organisations at risk	Organisations that can suffer direct or indirect losses
4	Official protection bodies	Legislators, national and regional authorities, special organisations
5	Interest organisations	Labour unions, organisations of consumers, of patients, and of victims (e.g., of traffic accidents)
6	Other safeguarding individuals	Engaged individuals, journalists, whistle-blowers, etc.
7	Advancement of knowledge	Statistics, research, investigations and information to the public; consultation can transfer knowledge between sectors
8	Risk increasing	Intentional through rule-breaking or criminal activity; unintentional through negligence or choosing other priorities

Arenas

An *arena* is a place where people stay or perform their activities. It is also the place where they might get injured or where damage occurs. The term is general, and there are overlapping roles in many ways. A certain facility can be used for education during day-time, sports in the evening, and entertainment in the weekends. A ward at a hospital is a workplace for the staff and a place for care of patients. Table 2.3 gives examples of how arenas can be categorised, but note that they overlap.

Table 2.3 Examples of arenas.

Type of arena	Comments
Workplace	In industry, trade, etc., people are employed or self-employed. Actually, most places are workplaces for some people.
Care-taking	Large area with medical treatment, care for the elderly, etc.
Education	The largest segment is publicly provided school, but higher education is also included
Transport	Many types, using both public and private vehicles
Housing	Where people live and stay a large part of their time
Sport and leisure	Voluntary activities, more or less organised
Entertainment	Can be in a large arena, including sports, music, theatre, etc.

Sources of risk

Table 2.4 General parameters for sources of risk

Source of risk	Examples	Comments
Physical or chemical process	Fire Fall Chemical influence Medical influence	Often based on a mechanism through which energies can cause direct injury or damage
Human influence	Physical act of a person Action of a group Psychological influence Influence by threat	The direct, concrete influences of persons or groups. (The intention does not necessarily have to be negative.)
Disturbance to a technical system	Interruption to service Collapse of system Accidents as side-effects	Modern societies are often sensitive to technical disturbances, which can cause numerous problems.
Disturbance to organisational and social functions	Stop in services Shortage of supplies Lost control and panic Open conflict Warfare	A failure in societal functioning can cause difficulties in many ways, but the warning time may be longer.
Disturbance in nature	Flooding Earthquake Loss of provision Ecological loss	These disturbances are natural events, but they might be affected by human actions.

Strategies and means for prevention depend, of course, on the existing sources of risk (hazards) and the types of damage that can occur (e.g., Table 1.1). A general set of parameters for sources of risk is shown in Table 2.4, which describes a mixture of technical, human and social factors. It is essential to take not only technical factors into account, but also the societal functions that need to be considered in a risk panorama.

Activities and tools

A great variety of activities and tools can be employed in safety work. Table 2.5 gives categories and examples of what can be considered. There is overlap, and a particular safety action can concern more than one category. This book focuses on tools for the analysis of accidents and systems. However, there are strong links to many of the other elements in the table.

Table 2.5 Activities and tools in safety work

Type		**Comments**
Society	Politics	Overall and detailed decisions, priorities and allocation of resources.
	Laws	General laws and directives.
	Authorities	General influence and forcible means (rules, permits).
	Checks	Inspections, statistics, safety reports.
	Sanctions	Punishment, fines, economic claims, withdrawal of licences to operate.
	Planning	Planning of operations, infrastructure, and other resources.
	Economy	Economic incentives through charges, grants and rebates Emphasis on economic market principles.
Operators	Risk management	Rules and manuals for operations, safety policies, agreements, risk analyses, etc.
	System design	Technical design gives basic safety characteristics. Robust systems give reduced vulnerability.
Individuals	Personal risk management	Individuals can avoid risky situations, seek information, claim compensation if damage occurs, make agreements, and buy insurance. This concerns both employees and consumers in a broad sense.
	Personal commitment	A personal engagement that goes beyond normal job specifications. Whistle-blowers who highlight unacceptable risks.

Table 2.5 Activities and tools in safety work (continued)

Tools	***Analysis of accidents***	Investigations of accidents and incidents – can be deep or shallow. Compilation of statistics about events that have occurred.
	Analysis of systems	Inspections, supervision, safety analyses, and summaries of results.
	Measuring performance	Monitoring of policies and planned activities.
	Auditing	Independent checks on safety routines and reporting.
	Readiness for crisis	Plans for crisis management, and contingency planning.
General	Learning	Actors can learn and develop their safety work.
	Evaluation and reflection	Define criteria for checks on efficiency and the effects of safety work. Reflection will concern whether the right things are being done.
	Research	Scientific studies of safety work can increase knowledge about what is successful. Research results can be used by different actors.
	Understanding values	Actors have different values. Handling of conflicts can be needed in cases of differing perceptions and conflicting demands.
	Changing attitudes	Attitudes to safety can be made more positive through information, discussion and the development of norms.

2.3 Theories and principles

Theories about accidents and ideas how they can be prevented are numerous. They are essential in the practical world, since they influence safety work in many ways. This may concern the design of management systems, the application of risk analysis tools, or the accomplishment of event investigations.

Earlier in this chapter, a number of fairly concrete elements were discussed. There are several overlaps between the views taken in the chapter, which is natural since many activities appear in different forms in different situations.

Models and theories

Theories about risk and safety come from several research disciplines. There is great variation in the approaches, and various models can be

relevant in defined situations. Many theoretical overviews have been presented (e.g., Kjellén, 2000). Any safety analysis method is based on one or more theoretical models, which might be explicit or implicit. Theoretical models will be discussed only scantily in this book, but they will sometimes appear in presentations of analytic methods. Here are examples of theoretical aspects:

- The natural sciences have many applications in modelling courses of events and their possible consequences.
- The Energy Model (e.g., Haddon, 1963) has become much appreciated in the safety arena (see Chapter 6).
- Statistics and mathematics have an important role to play in many applications, especially in relation to reliability studies. There is a vast literature (see, e.g., Aven, 2008A, 2008B).
- There are psychological theories of human errors and decision-making (e.g., Reason, 1990).
- There are organisational and sociological theories, which consider "normal accidents", "corporate memory" (Perrow, 1984), and group thinking.
- Power, conflicts and negotiations are considered in political science. The actors involved have differing interests, all of which can be seen as legitimate in some sense.
- The term *safety culture* was first used in the nuclear industry (INSAG, 1988). Thereafter, it has been circulated widely and used in different applications, and is sometimes also called *safety climate* or the like. The terms are often used, but they are hard to define precisely (see, e.g., Guldenmund, 2000).
- Various system models, which include feedback and a focus on safety (e.g., Kjellén, 2000).
- Barriers and safety functions provide models for how safety is achieved (see Chapter 11).
- Resilience is related to the capability of a system to tolerate disturbance without collapsing. It has been used in environmental research for a long time.[1] The concept has also been introduced in the safety area (Hollnagel et al., 2006) in recent years.
- "Risk homeostasis" (Wilde, 1982) is a fairly pessimistic theory. It predicts that if safety improvements are implemented, these will be neutralized by a changed behaviour. For example, if car brakes are improved, drivers will increase their speed, leading to a similar risk level as before.

[1] See www.resalliance.org

To this we could add the *common sense* meaning that people (and organisations) have various explanations and *mental pictures* of why accidents occur. These can be simplistic and stereotyped, and even act as obstacles to efficient safety work and collaboration.

Ideological perspectives

In addition, we have ideological perspectives on risk and safety. They can be expressed in parliamentary legislation, which is based on political values, but they can also be seen as reflecting group attitudes and opinions, or the engagement of individuals. Sometimes, such values are explicit and clearly formulated, but they can also be implicit and less obvious. Some examples of values rooted in ideology are:

- Rules of morality and justice, e.g., that an individual should not be exposed to a very high risk that is not voluntarily chosen
- The individual should be aware of his exposure to risk and act upon that
- There should be sustainable solutions and risk concerns, which also consider future generations
- A zero vision for accidents, which has been expressed in the Swedish car traffic sector in relation to deaths and serious injuries
- Economic and market-oriented principles
- The polluter-pays principle
- The demand that people who have suffered a loss should be compensated, e.g., through insurance
- That persons and/or organisations who cause damage should be punished

Strategies and principles

Safety strategy refers to an overall long-term plan of operations that will achieve the safety objectives of the actor concerned. There are several principles involved, and they often overlap; several of these have been listed above. Examples are:

- Laws and directives
- Rules for practical application
- Clarifications and rules for dividing responsibilities within and between organisations, including agreements between actors
- Technical specifications
- Setting demands on individuals (e.g., in the car-driving profession as a car driver, as passenger, etc.)
- Punishment for violations and errors

- Top-down surveillance of companies and individuals by the authorities
- Bottom-up surveillance by consumers, labour unions, safety representatives, etc.
- Information and publicity to change attitudes among the public
- Economic incentives to improve safety
- Insurance, to both protect offenders and compensate victims

System models

All accidents occur within some kind of system. A system can be defined as a group of separate parts that interact in some way. Systems can be addressed in several ways, and various approaches to systems theory have been available in the scientific field for a long time now.

Hale (1999) pointed out that there is a fairly good consensus between the two first "ages" of safety, which are related to technical and human failures, respectively. In the “third age” with concern for complex socio-technical and safety management systems, development is still at an early stage. Although there may be basic agreement in the scientific community concerning technical and human failures, the variation in conceptions of accident causation is very wide.

A simple example of conflicting views can be taken from a workplace. The managers think that the workers are negligent by not following the rules, and that is causing accidents. By contrast, the workers think that the employer just wants to save money by not installing safer machines.

We can find many ways of describing a *systems perspective*; how useful they are depends on what they are to be used for. One example of a systems model, which shows different societal levels of control, is shown in Figure 2.2 (Svedung & Rasmussen, 2002, reproduced with permission of the authors). The model has been applied in an accident investigation method called AcciMap (see Section 13.7). It shows how some of the tools described in Section 2.2 are related.

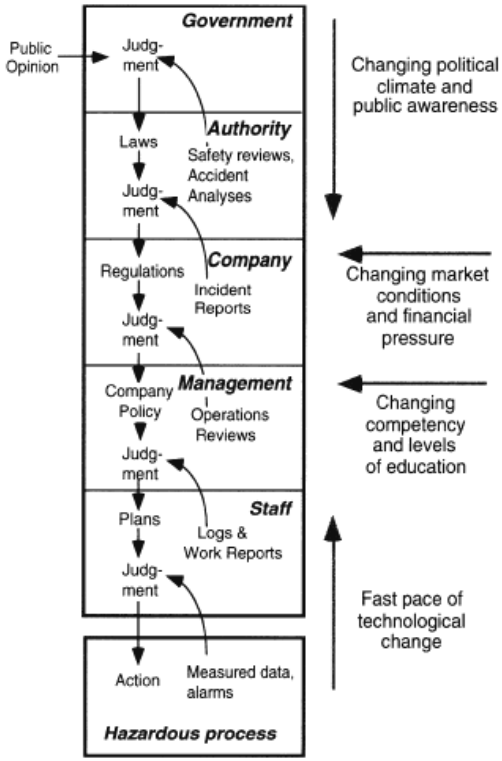


Figure 2.2 Model of decision-making at different levels (Svedung & Rasmussen, 2002)

Human error

There is an extensive literature on the subject of human error, which has grown over the years (e.g., Hale and Glendon, 1987; Reason, 1990; Dekker, 2006). This section will briefly consider some aspects (perhaps, rather arbitrarily).

In practical situations, the question of human error is often disputed. Some people see it as the cause of accidents, while others regard it as a symptom of an underlying problem. It is nearly always the case that human errors lie behind an accident, but the errors can be of many different types. They may be simple, such as when someone hits his thumb with a hammer. But they may also be advanced cognitive errors, as when an important safety system is designed in the wrong way. All people make unintentional

mistakes. Usually, it is only when they have unfavourable consequences that they get attention.

A popular reaction to an accident is to blame it on the *human factor*. Newspapers usually accept this as the main explanation. Often, it is a representative of an authority or a safety manager who couches the explanation in these terms. There is a certain ring to the term, the *human factor*. It implies that accidents are due to irrational and unpredictable elements in a situation, and that nothing can be done about them. Moreover, it is often the person sustaining an injury who is regarded as *the factor*, which is sometimes related to scapegoating, and the attitude of placing the blame on someone else.

People make mistakes, but more often they do things right. Instead of focusing on human error, an alternative starting-point might be to regard the person as a safety resource rather than a hazard. People are supposed to intervene when technical equipment fails, when the computer is stuck, or when organisational rules are just silly. A different approach involves the human being as a problem solver and a safety factor in technical systems.

From the end of the 19th century and onwards, many have sought to understand why people make errors in their thinking and in the performance of actions. Reason (1990) has provided an interesting review of developments over the last hundred years. The most renowned of the pioneers was Sigmund Freud (1914), who found meanings in what were apparently random and day-to-day slips and lapses. Analysis of the errors often permitted the detection of explanations in unconscious thought processes, which had their origins in psychological conflicts.

In cognitive psychology, the idea of *schemata* plays a central role. According to Reason (1990, pp. 34-35):

> "The very rapid handling of information in human cognition is possible because the regularities of the world, as well as our routine dealings with them, have been represented internally as schemata. The price we pay is that perceptions, memories, thoughts, and actions have a tendency to err in the direction of the familiar and the expected."
>
> "The current view of schemata is as higher-order, generic cognitive structures that underlie all aspects of human knowledge and skill. Although their processing lies beyond the direct reach of awareness, their products – words, images, feelings and actions – are available to consciousness."

One model to which reference is often made is based on distinguishing between three different performance levels (Rasmussen, 1980).

1) On a skill-based level, people have routine tasks with which they are familiar and which are accomplished through actions that are fairly direct. The errors have the nature of slips or lapses.
2) On a rule-based level, people get to grips with problems with which they are fairly familiar. The solutions are based on rules of the IF/THEN type. A typical type of error occurs when the person misjudges the situation and applies the rule incorrectly.
3) On a knowledge-based level, people find themselves in a new situation where the old rules do not apply. They have to find a solution using the knowledge that is available to them. On this level, errors are far more complex by nature, and may depend on incomplete or incorrect information, or limited resources (in a number of different senses).

Violations represent a further type of human error. By a violation is meant an intentional action that is in breach of regulations, either written or oral. The intention, however, is not to damage the system. Deliberate intention to harm is better described as sabotage. It is difficult to draw a sharp dividing line between errors and violations. Violations can of course be committed both by people involved in planning and design and by those who work directly in the actual system.

There are many reasons why people act in breach of regulations. Some examples:

1) The person does not know that the action constitutes a violation. He or she may not be aware of the regulation, or may not be conscious that the action in question represents an infringement.
2) The person is aware of the regulation, but forgets it, e.g., if it seldom applies.
3) The regulation is perceived as unimportant, either by the person concerned or by those around him.
4) There is a conflict between the regulation and other goals.
5) The regulation is thought to be wrong or inappropriate, with or without reason.

In safety work, the issue of human errors is important in several ways:

- At the identification stage of a system analysis or accident investigation, human error often comes up as an essential element.
- In the design of safety improvements, a better understanding of human behaviour can provide for more efficient solutions.

2.4 Assumptions and priorities

Parameters for different situations

There is a large spread of application areas and approaches to safety. Take, for example, nuclear installations, aviation companies, and large chemical industries, which are often associated with a potential for major accidents, but also with rigorous safety management systems. On the other hand, you can have more uncomplicated types of systems, where minor accidents are frequent, and safety is managed in a much more relaxed way.

The variety of situations can be described by a set of parameters, and examples are given in Table 2.6 (Harms-Ringdahl, 2004). More items could easily be added to the table. In Group A, there are large companies with strict control and good resources, whereas in group B companies show considerable variety, and sometimes have very limited opportunities to manage their risks.

Table 2.6 Parameters for the management of risks

Parameter	Group A	Group B
Accidents	Large consequences, infrequent	Small consequences, occasional
Organisation size	Large, complex	Small, simple
Regulation	Precise, strictly enforced	General
General management	Structured, formal,	Informal
Safety management	Formal safety management system	Informal handling of safety issues
Economy and resources	Good	Poor
Stability	Good stability	Changes are common
Priorities	Harmony and agreement	Conflicts are common

It should be noted that a specific activity, company or organisation often has parameters in both groups at the same time. For example, a company has a formal safety management system but changes are common, which gives improvisations and informal safety activities more prominent roles.

It is important to be aware of the differences between the groups. If they are not spelled out, it is easy to assume that the A type is the norm for all safety work. My impression is that standards and legislation are often based on this assumption.

In reality, the B type is more important, since B companies employ many more people, and also generate many more injuries and much more damage. This has been shown above (in tables 1.2 and 1.3, and in Section 1.3).

Some attention has been paid to the setting of priorities in the research literature, and an interesting review of published research papers has been presented by Hale (2006). He checked articles in 9 scientific journals in the safety arena. The road safety theme showed the largest number of articles, which was followed by risks in the major hazard sectors of process industry, such as chemicals, energy, oil and gas. Occupational safety received only about half as much attention. Consumer and public safety and the risks of other aspects of life obtained much less attention.

The two faces of Janus

Hale (2006, p. 35-36, cited with permission) formulated the imbalance of interests in a somewhat different way. Instead of groups A and B, he talked about the faces of Janus:

> "My review of the scientific literature showed that the vast majority of the research published has been on the major hazard industries and disaster risks. Only road safety, of the activities which kill their participants in ones and twos rather than in tens or hundreds, has had comparable attention paid to it. Major hazard risks and their prevention are complex and high-tech and hence they are sexy. They require very sophisticated methods and models to understand the interactions and emergent situations leading to disaster. … It is the smiling face of Janus.
>
> "His scowling face is represented by a proportion of the ill-intentioned and ill-equipped small and medium-sized companies, the back street and home based industries, the labour-only contractors, temporary employees and the developing countries to which risky, polluting and unhealthy industry is exported. Progress in improving safety in these would be far more effective in lives saved, … It seems to me urgent that both governments and research funders recognise this scowling face of Janus, give it more priority and adapt their strategies to it.*
>
> "*This is no new viewpoint. Authors such as Carson (1979) have pointed out this divide in safety regulation over many decades."

2.5 A challenge

The first two chapters in this book have discussed accidents and safety work, and have pointed to various paradoxes and challenges. They have shown the existence of great diversity in safety work, which utilises tools that range from the simple to the complex.

The presentations of the theory and applications of safety analysis and accident investigations have, to a large extent, been based on work in fairly advanced companies with good resources. They are what I call *Group A companies*, and which Hale (2006) has called "the smiling face of Janus". However, they relate to only a small proportion of all accidents (less than 1%, I would imagine).

In fact, accidents occur in many different settings and situations (see, for example, Table 1.3 and Section 1.3). The nature of safety work may vary, but a vast majority of cases belong to *Group B companies* (Table 2.6). This can be seen as reflecting what Hale calls the "scowling face of Janus" (see citation above), to which I have claimed 99% of accidents belong.

In my previous book (Harms-Ringdahl, 2001), occupational accidents were my main concern. Since then, I have reconsidered the safety techniques involved and their various applications. Many of the methods can also be useful in many other situations. To do so, however, it is essential to utilise a broad conceptual framework, which is also helpful in avoiding unnecessary, tacit assumptions (cf. Table 2.6).

Learning across different areas of application benefits from a broadened perspective. Methods of safety analysis and accident investigations can also be applied in other areas. Further, it is important to cover the fields of medical mishaps and home and leisure accidents.

Accordingly, my ambition is to broaden the scope of the methods. The challenge is to make the selected methods applicable to a majority of all accidents. This means that definitions need to be fairly general and abstract, and some of the methods need to be expanded to cover a broader range.

3 A framework for safety analysis

3.1 A starting point

Analyses of risks are conducted in a variety of professional arenas, and in various ways. There are international standards that define parts of the terminology for certain application areas. However, the broad field of applications entails that the meanings of a number of concepts vary quite a lot.

A theoretical framework is supposed to help the reader to make logical sense of the meaning of the concepts and factors that have been deemed as relevant and important. It provides definitions of relationships between variables in an attempt to help the reader to understand the interactions between them.

This chapter presents a framework for the analysis of risks, safety, and accidents. It defines some expressions, and it explains basic procedures and types of applications. The framework is not intended to be a theory that connects all the pieces, which would be pointless, since the area we discuss is too broad to be unified. Further, it is a field in ongoing change and development.

Definitions of terms

At first, it might appear easy to find a set of general definitions of terms that would work on most occasions. However, it quickly emerges that there are quite a lot of competing definitions. Just a small selection of the definitions in the safety arena is given here.

There appear to be three general principles for how definitions are formulated. The first type of definition might be classified as descriptive. The other two types are normative – saying how things should be done. They might be influenced by underlying theories and conceptual frameworks. A definition can:

1) Give a simple statement of the meaning of a term
2) Sum up all the elements that are usually included for practical use
3) Include characteristics that must be considered for a perfect result to be obtained

Terms are used differently according to their area of application. In the chemical industry, *risk analysis* is the preferred term for all types of methods. In the nuclear industry, *safety analysis* appears to be more common. Examples of other expressions are *risk assessment* and *hazard assessment*. It is good to be aware of the variety of terms, and that they may have more than one meaning.

The International Organization for Standardization (ISO, 2009A) has published a glossary of terms, which is fairly general. It was preceded by a set of more technically oriented standards developed by the International Electrotechnical Commission (e.g., IEC, 1995). Sometimes, I refer to these as being within the *technical tradition*, which often has a focus on quantitative applications.

Basic terms

A handful of definitions are used throughout this book, and they are summarised here. The intention is to use simple and general definitions that can function in different types of situations and applications. The principle has been to make the definitions descriptive, and thereby avoid unnecessary presumptions. As a consequence, normative statements about how things should be done are avoided.

Accident and incident

First, a short definition of *accident*, and then a somewhat more exhaustive one (from Section 1.1):

> *An accident is an event that causes unintentional damage or injury.*
>
> *An accident is an event that causes damage or injury, but which was not intended to have a negative outcome.*

Second, a short definition of *incident*:

> *An incident (or near-accident) is an event that almost causes unintentional damage or injury.*

Hazard

The term *hazard* is often used to denote a possible source or cause of an accident.

Risk

The word *risk* is used in a variety of contexts and in many senses. In general, it can be defined as the possibility of an undesired consequence. A rather theoretical definition comes from the International Organization for Standardization (ISO, 2009A), which states that risk is the *effect* of

uncertainty on objectives. An *effect* is a deviation from the expected – positive and/or negative. It also states that risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence.

Risk can also have a more technical meaning as "the combination of the probability of an event and its consequence" (ISO, 2001). In everyday speech, the meaning shifts between these different senses.

An example of a highly technical description can be taken from the International Atomic Energy Agency (IAEA, 2007). It states that risk is "the mathematical mean (expectation value) of an appropriate measure of a specified (usually unwelcome) consequence:

$$R = \sum p_i C_i$$

where $\boldsymbol{p_i}$ is the probability of occurrence of scenario or event sequence $\boldsymbol{i}$, and $\boldsymbol{C_i}$ is a measure of the consequence of that scenario or event sequence."

Accident investigation

A simple definition (Harms-Ringdahl, 2004) is:

> *An accident investigation is the collection and examination of facts related to a specific occurred accident.*

Safety investigation of accidents can be used as an alternative. The term indicates that the aim is to identify system weaknesses and to find improvements with no intention of blaming anyone for what has occurred.

Event investigation

The general term *event* can be used to cover accidents, near-accidents, and other types of events. This can be desirable (Freitag, 1999), since different events can be analysed in almost identical ways. A suitable definition is:

> *An event investigation is the collection and examination of facts related to a specific occurred event.*

Risk management

The ISO (2009A) uses the definition given below. It states also that risk management generally includes *risk assessment*, *risk treatment*, *risk acceptance*, and *risk communication*.

> *Risk management [consists in] coordinated activities to direct and control an organization with regard to risk.*

Safety management
Safety management is an alternative term. In light of the discussion in Chapter 2, it seems preferable to have a definition that covers both formal and informal activities and large and small organisations. Accordingly, in this book, we use the definition below (Harms-Ringdahl, 2004):

> *Safety management is a way of managing hazards and risks in an organisation.*

3.2 Safety analysis procedure

Definition

Safety analysis is a central concept in this book. There is no broadly agreed definition of safety analysis, but one is proposed here:

> *Safety analysis is a procedure for analysing systems to identify and evaluate hazards and safety characteristics.*

The definition is wide, and it covers the specific definitions of risk analysis and risk assessment presented below (in Section 3.4). It includes:

- Both qualitative and quantitative methods of risk analysis
- Accident and event investigations
- The generation of proposals for improving safety as a specific step in the analysis.

Here *procedure* is a central concept, which means going through a set of consecutive stages that have been defined in advance. What these procedures can look like is described in the following sections.

The inclusion of accident investigations in this definition is in harmony with international standards. One ISO standard (2009C) and other risk analysis guidelines (e.g., FAA, 2000) include accident investigation applications in their set of tools.

The term *safety analysis* is used frequently in the nuclear industry. In a general glossary (IAEA, 2007), it is defined as “evaluation of the potential hazards associated with the conduct of an activity”. This is fairly well in line with the definition given above.

Basic steps in safety analysis

A safety analysis consists of a number of co-ordinated steps or stages, which jointly make up a procedure. Depending on the approach and purpose of the analysis, there might be variations. Figure 3.1 presents a general model of safety analysis procedure, with six basic stages, which starts with the planning of the analysis and ends with the reporting of results.

Plan the analysis

The first basic step is to plan the analysis. This is discussed in greater detail in other places in this book (sections 3.3 and 14.1). The planning of an analysis involves defining the goals and scope of the analysis, choosing methodology, and so on.

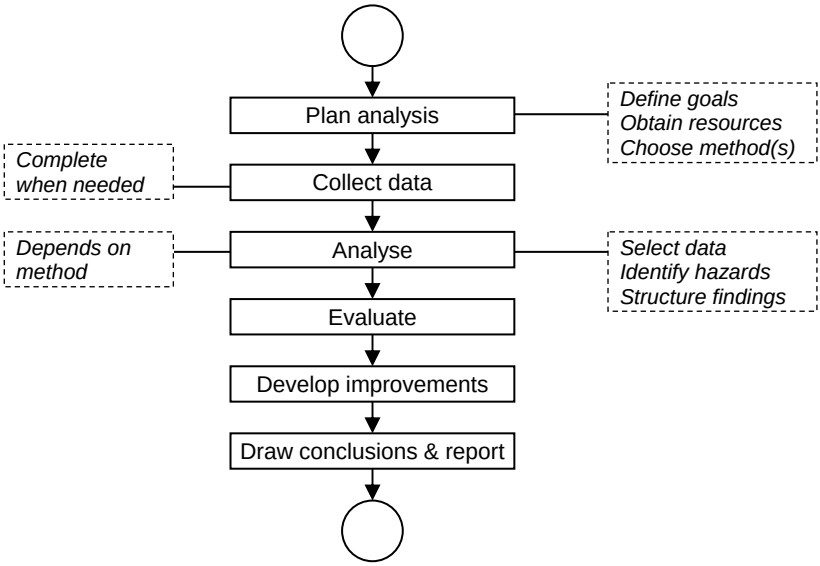


Figure 3.1 Basic steps in a safety analysis procedure

Collect data

Information on the system to be analysed is essential. The need for information is governed by the aim of the investigation, by how detailed the study needs to be, and by the methods to be employed.

Collection of data is performed at the beginning, but supplementary information is usually needed in the course of the analysis to meet the specific needs that come up. Thus, the search for information can be seen as an iterative process.

Useful information can concern technical design, how the system functions, and which activities are undertaken. When the aim is to investigate an accident, information related to that accident is obviously needed. In cases where an installation has been in operation for some time, information is relatively easy to obtain. There are people with different experiences to ask. Useful reports may concern accidents that have occurred, near-accidents, and disturbances to production.

Analyse
How analysis is performed is determined by the methods applied. *Analyse* is a general term, which usually contains several elements. It can concern selection of data to meet the needs of a specific method. In most methods, there is an element called *Identify hazards*, for the finding of hazards and different kinds of problems. An analysis often involves a lot of information, and there is a need to organise and structure the findings.

Evaluate
The identified risks or other properties of the system need to be evaluated. The evaluation is intended to support decision-making about risks and the need for improvements, and also to aid selection of the problems that need further attention. Such evaluation can take different forms (as discussed in detail in Chapter 5). One application of risk evaluation is to judge whether a system is *safe enough*, or whether safety measures are necessary. In a quantitative analysis, the values of probabilities and consequences are estimated, and the evaluation is based on these.

Develop improvements
A safety analysis may include the development of *safety improvements*, which is therefore considered as part of the procedure. However, this stage is not included in all approaches, which means that this block will sometimes be empty (see Figure 3.1). For example, the ISO standard (ISO, 2009C) does not include the improvements stages in either risk analysis or risk assessment. Instead, the standard refers to *risk treatment* as a part of risk management.

In many situations, it is beneficial to include the improvements step in the analytic procedure. The reason for this is that it enables the analysis to create understanding of the system, and of its problems and risks.

Draw conclusions and report
The final basic step is to draw conclusions on the basis of the previous stages and to report the results of the safety analysis.

3.3 Safety analysis in context

There is always a context within which a safety analysis is performed. There are users who have in interest in the analysis, and its results have to be managed properly. Figure 3.2 shows a number of elements to consider in the general planning of a safety analysis. Most of this account might seem self-evident, but experiences have shown that elements are often missing or neglected. A more detailed account of the blocks and of the planning of an analysis is given in Chapter 14.

The general system

Let us take our point of departure in the object that is to be analysed. It is usually a part of a larger organisation or system, and can in principle embrace any type of production or activity. It could, for example, be a mechanical workshop, a chemical plant, a ward in a hospital, a school, or a consulting company.

The system to analyse

The object of the safety analysis might be the whole system, but is more likely to be a smaller part of it, such as a certain activity or a subsystem.

External demands

There are always formal demands on systems, of whatever kind, which are expressed in the laws and regulations of the authorities. Requirements can concern safety and related issues – for workers, for children in school, for patients in hospital, etc. They can also concern products and their safety characteristics, e.g., with regard to consumer safety. Safety demands can determine how the work should be organised, when an accident must be investigated, or when a safety analysis must be conducted.

There are also contractual agreements to consider, e.g., concerning relations between employer and employees, or between buyer and seller. In addition, economic considerations are an important aspect of the demands imposed on production. All in all, there is a complicated web of demands on a production site, of which safety is just one aspect.

Safety work

As discussed in Chapter 2, there are a number of activities related to the achievement of safety. Safety work includes the safety analysis procedure, but it also provides inputs into how an analysis should be performed. This can be more or less formal or systematic.

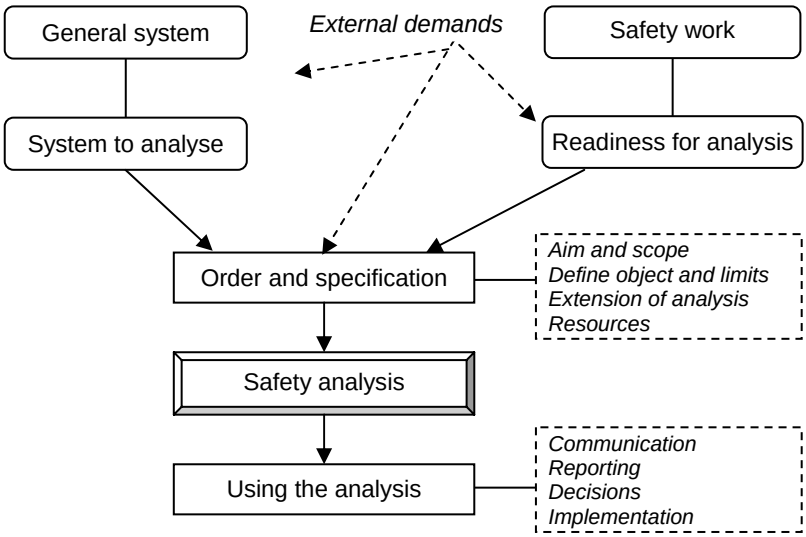


Figure 3.2 The safety analysis procedure in context

Readiness for analysis

A company can be more or less ready to perform an analysis when the demand arises. Readiness means being in a state of preparedness to meet a situation and carry out a planned sequence of actions. Readiness for analysis can concern:

- Criteria for when a safety analysis of a system needs to be conducted
- Criteria for when an accident should be thoroughly investigated
- Availability of personnel who can perform an analysis
- Understanding within the organisation on how to benefit from an analysis
- Suggestions for employing a suitable methodology

Now and again, situations in which there is a need for a safety analysis arise. For example, there are situations where:

- A severe accident has happened.
- A planned change to technical equipment might lead to a deterioration in performance.
- An organisational change is planned.
- A safety problem has been detected and improvements are needed.
- A thorough check on a new design is needed before a decision on it is taken.

In many cases, the organisation is not at all ready to investigate an accident or perform a safety analysis. The block *Readiness for analysis* is not present in such cases, but it can be seen as representing good praxis.

Order and specification

In situations where a need has been addressed, a first step is to decide whether an analysis should be performed or not. This can result in an order to carry out an analysis, from either an external or an internal actor. Then, there is a need to specify the following:

- The aim and scope of the analysis
- A definition of what is to be analysed, i.e., the object and its limits
- Extension of analysis – shall it be superficial or exhaustive
- Resources, in terms of time, etc.

Safety analysis

The steps or stages in a safety analysis are shown in Figure 3.1. How they will be performed is determined by the specification of the analysis, by the methods employed, and so on. Possible outcomes range from making suggestions for changes to a recommendation to keep things as they are.

Using the analysis

The results of an analysis shall meet the demands and specification. A basic step is to communicate the results, which often takes place in a written report. Supplementary ways include engaging a working group, and discussions with decision-makers and other stakeholders. The results can be seen as a basis for making decisions about changes and improvements. If a decision is made to change something, further development and implementation will follow.

Where there is a readiness for analysis, the process can be seen as a *learning system* – from each analysis the persons involved learn something new from the analysis. The stakeholders can be people in production as well as those engaged in safety work. Issues might be:

- Further improvements to the system that was investigated
- Improving the design process
- Learning how to perform better safety analysis and communicate results
- The promotion of communication between different stakeholders and actors

3.4 The probabilistic tradition

Risk analysis and risk assessment has been developed in depth in several technical fields. In the theories and concepts, statistics play an essential role often in combination with reliability theory. There is a vast amount of research literature, and several devoted scientific journals. This field is highly influential, and has an important role to play in many applications. I refer to it as lying within the *probabilistic* or *technical* tradition.

A consistent methodology has been developed, which has generated a number of international standards (e.g., ISO, 2009A; 2009B). These, in turn, are closely related to standards issued by the International Electrotechnical Commission (IEC). Several standards are available, and there are sometimes differences in terminology and concepts.

Often, a combination of different aspects are considered, such as *Reliability*, *Availability*, *Maintainability* and *Safety* (*RAMS)*. For example, the railway industry has adopted this perspective in a standard from the European Committee for Electrotechnical Standardization (CENELEC, 1999).

There are also several other traditions in which terms like *risk analysis* are used, which have a statistical foundation or are based on other perspectives. Kaplan (1996) has reflected over the historical difficulties involved in definitions of the terms related to risk analysis.

A general and fairly broad perspective is adopted in this book. It has several points in common with the probabilistic perspective, but they do not entirely overlap. Accordingly, I give a short account of the probabilistic or technical tradition (as I have interpreted it), and comparisons between some aspects are made further below.

Risk management process

Figure 3.3 gives an overview of the different elements in risk management in the technical tradition. This account is based on two standards from the ISO (2009A, 2009B). A starting point in the process is to establish the context, which defines the basic parameters for managing risk, and also sets the scope of and criteria for the rest of the process. At the risk analysis stage, the level of risk is estimated, which is the magnitude of a risk expressed in terms of the combination of consequences and their likelihood.

There are a number of important definitions in the standards:

- *Risk management [consists in] coordinated activities to direct and control an organization with regard to risk.*
- *Risk assessment is the overall process of risk identification, risk analysis and risk evaluation.*

- *Risk identification is the process of finding, recognizing and describing risks.*
- *Risk analysis is a process to comprehend the nature of risk and to determine the level of risk.*
- *Risk evaluation is the process of comparing the results of risk analysis with risk criteria.*
- *Risk treatment is the process to modify risk. … Risk treatments that deal with negative consequences are sometimes referred to as "risk mitigation", "risk elimination", "risk prevention", and "risk reduction".*

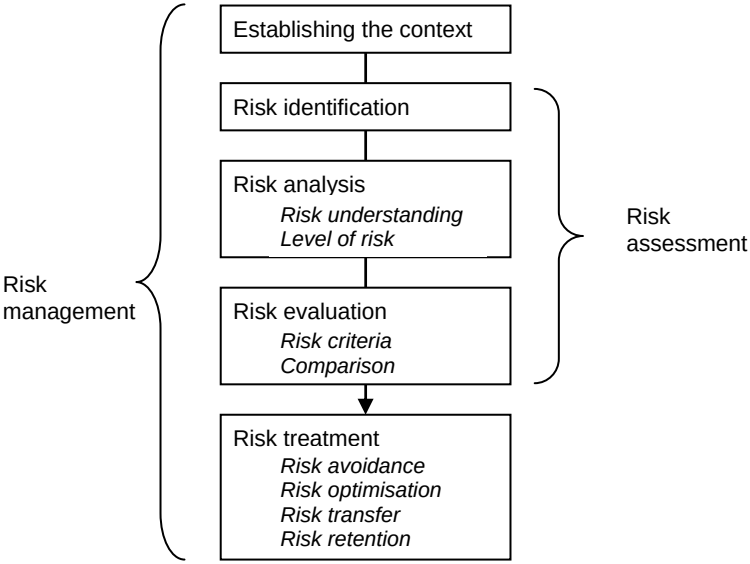


Figure 3.3 Main elements in the probabilistic risk analysis tradition

Comparisons

It is difficult to distinguish between the terminologies, especially since there are differences between the standards, and there are also changes over time. Here, comparisons are made between the terms *risk analysis*, *risk assessment* and *safety analysis*. The two first terms are based on the ISO's Standard Risk Management – Vocabulary (ISO, 2009A), which was referred to above.

Table 3.1 Occurrence of elements in definitions of risk and safety analysis

Element / Term Source	**Risk analysis** ISO, 2009A	**Risk assessment** ISO, 2009A	**Safety analysis** Section 3.2
Identification of risk	No	Yes	Yes
Understanding	Yes	Yes	Yes
Estimate level of risk	Yes	Yes	Included, but not mandatory
Risk evaluation	No	Yes	Yes
Suggest improvements	No	No	Yes
Accident investigation	No	No	Yes

Table 3.1 shows the elements included in the definitions. Risk assessment and safety analysis look similar, and differ only with regard to two of the elements. Estimation of the level of risk is mandatory in risk assessment, but can also be used in safety analysis. Differences are that suggestions for safety improvements are recommended in safety analysis, and also that accident investigations are included within that framework.

On the basis of these definitions, it can be concluded that safety analysis is a somewhat broader concept than risk assessment, and that risk analysis has obtained a much narrower definition.

Shift in thinking

In recent years, there appears to have been a shift in terminology, and probably also in thinking, in the technical tradition. Take, for example, the term *risk analysis*, which in earlier standards (IEC, 1995; ISO, 2001) included both the identification and estimation of risk. Identification has now been placed in a separate block, and estimation is called determination of the level of risk.

The ISO (2009C) has widened the scope of risk assessment, and now describes its purpose as to "provide evidence-based information and analysis to make informed decisions on how to treat particular risks and how to select between options". My original intention was to compare the concepts of *safety analysis* and *risk analysis*. With this shift, it is more appropriate to consider safety analysis in relation to *risk assessment*.

The nuclear industry has another technical tradition, where the term *safety analysis* is preferred. In a general glossary (IAEA, 2007), it is defined as evaluation of the potential hazards associated with the conduct of an activity. The term *risk analysis* is not included at all. On the other hand, the ISO standards (2009A, 2009B) make no mention of the term *safety analysis*.

Although the technical tradition might appear consistent and stable, it is in fact involved in a process of change. There will probably be overlaps between earlier and newer definitions for quite some time. There are also advanced technical fields where there are different ways of thinking, which is reflected in different usages of terms. My impression from many industrial visits is that the term *risk analysis* is usually employed in a broader sense than *risk assessment*. This means that there is still plenty of room for misunderstanding, and also a need for careful definitions of terms and procedures.

3.5 An accident investigation framework

The field of accident investigations

Investigations of accidents and other adverse events make an important contribution to safety work. It is essential to know how and why accidents can occur in order to effectively prevent them. Usually, accident investigation and risk assessment are considered as separate domains, with their own traditions and approaches.

However, there are many similarities between analysing events that have occurred and those that may occur in the future. Accordingly, in this book, accident investigation and the analytic forecasting of systems will be treated in a similar manner. Investigation of accidents and other events is included in our general definition of safety analysis (Section 3.2). One ambition in this book is to highlight the similarities and obtain fairly consistent descriptions. A special chapter (13) is focused on methods for accident investigations.

Accidents can also lead to criminal investigations, where the aim is to establish whether someone has caused an accident intentionally or negligently. This type of investigation is not discussed here.

There is a vast amount of literature on accident investigations, and several guidelines have been published. Some examples are presented below; they are available on the Internet, and may be useful for readers who wish to go further into this specialised domain.

The European Safety Reliability and Data Association (ESReDa, 2009) has published its *Guidelines for Safety Investigations of Accidents*. One of its ambitions was to present best practices that can be useful in different applications. The guidelines take up topics like planning and investigation procedures.

Another guideline comes from the U.S. Department of Energy (DOE, 1999). The focus is on investigating accidents in order to prevent injures to persons (employees and the public) and damage to the environment. The

guide concerns what should be done within the DOE's area of formal responsibility, but it also gives lot of general advice.

A guide from the Energy Institute (2008) discusses how human and organisational factors can be analysed in incidents and accidents. A number of investigation methods with this focus are shortly presented.

Accident investigation procedure

The general safety analysis procedure, which concerns both systems and accidents, is illustrated in Figure 3.1. Concentrating solely on accident investigation can make the model more specific and detailed, as is shown in Figure 3.4.

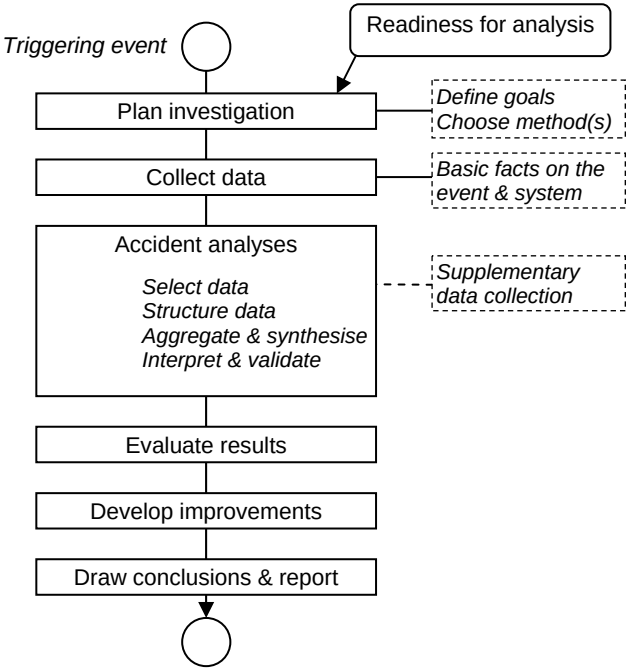


Figure 3.4 Basic steps in accident investigation

The procedure is the same for investigations of accidents, near-accidents and other events. It is closely related to the one proposed by Strömgren et al. (2013), where some features are discussed in greater detail. Figure 3.4 describes a fairly comprehensive accident investigation.

Readiness for analysis
Readiness is discussed in greater detail in Section 3.3. Here, it means a state of preparedness to plan and carry out an investigation when a certain type of accident has occurred (triggering event).

Triggering event
An investigation starts with a triggering event. Readiness includes some kind of rule for determining when an investigation should start. Possible events are:

- An accident causing severe injury to a person
- An incident with potentially large consequences
- The failure of an important safety barrier

Plan investigation
The first step is to plan the investigation, which is based on considerations in the readiness block. Investigations can be performed for various reasons, and it is essential to clarify their objective and specific goals. Planning also covers the scope of the investigation, its time schedule, and the resources needed.

At this stage, the accident investigation method (one or more) is chosen, since it might influence data collection. When more is known about the accident, additional methods might be employed. General planning is dealt with in Chapter 14, while Section 15.3 is concerned with choice of suitable methods.

Collect data
Data collection applies to information about the event and other facts. It is concerned with documentation of the accident scene, relevant objects and technical systems, and also interviews, documents and recorded data. The need for information is governed by the aim of the investigation, which determines how detailed the study should be, and the methods to be employed.

A general check list for data collection can be helpful in order to avoid missing information or the ruining of evidence. Some investigation methods can provide support at this early stage.

Interviews are a main source, and it is important not to influence the answers through leading questions. One way is to pose a few open questions, and then listen carefully:

- What was your role?
- Describe the event and circumstances when it happened?
- Do you think something could have prevented the event?

Accident analysis

Accident analysis is often a complex process, which can be performed in various ways. One or more investigation methods can help at the analysis stage. Chapter 13 presents a number of methods, and Section 15.3 compares these methods.

Analyse is a general term, which usually contains several elements. Figure 3.4 gives some examples of analytic activities:

- *Supplementary data collection*. During the analysis, there is usually a need for supplementary data. How much depends on the methods applied, and whether there are more questions to ask.
- *Select data*. All information might not be relevant to a specific investigation, so a selection must be made.
- *Structure data.* During collection, data come in a rather arbitrary order. Structuring brings order to the information and helps further analysis.
- *Aggregate and synthesize.* Data are combined and analysed to create a description of the event, and explain how it could have occurred. Outputs can take on many forms and are strongly dependent on the investigation method. One procedure is to reconstruct the course of events and the actions involved.
- *Interpret and validate*. This part includes interpretation of and a critical check on the results of the preliminary analysis. It can include examination of data from different sources to identify possible inconsistencies, and also attempts to test whether hypotheses or assumptions are correct.

Evaluate results

Evaluate here refers to making a judgment on the findings, such as identified hazards, safety problems, and other circumstances in relation to the event. The evaluation can concern how important a specific finding is, and whether there is a need for improvements. Principles and methods of evaluation are discussed in detail in Chapter 5.

Develop improvements

An accident investigation may include the development of safety improvements and recommendations. This is of benefit, since the analysis has created an understanding of the system and its risks.

Draw conclusions and report

The final basic stage is to draw conclusions from the investigation and to report on the results. Concluding and reporting concern the course of events, explanations of it, lessons learned, and suggested safety improvements. In addition, a summary should be given of how the investigation has been performed.

3.6 Relationships

Relationships between management, analysis and investigation

Because of the diversity of application areas and concepts, it is hard to define general relationships between accident investigation, safety analysis and risk management. Although the three differ in a number of respects, there are many links between them, as illustrated in the model below (Harms-Ringdahl, 2004).

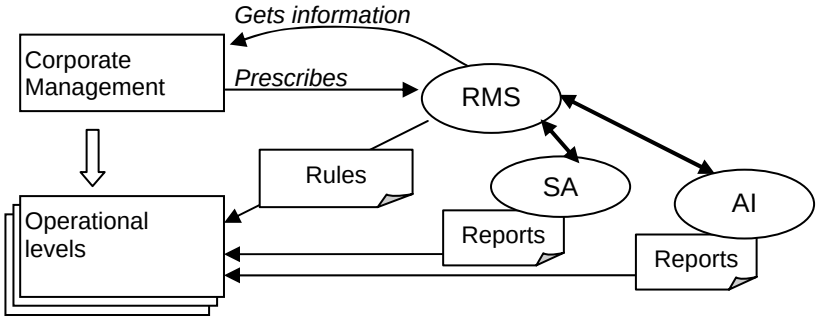


Figure 3.5 Elements and relations in a Group A type of company

In Figure 3.5, we have taken a company that is well organised; it belongs to *Group A*, as defined in Table 2.6 (Section 2.4). The company has an elaborated corporate management with a risk management system (RMS), good stability and economy. In this type of situation, the RMS prescribes when and how safety analyses (SA) and accident investigations (AI) shall be performed. The activities generate reports with observations and recommendations.

The model above assumes a top-down control system. Another perspective is to treat an accident investigation (AI) as a learning process (e.g., Hale, 1999). Then, the scope of the investigation is widened, and there will be a greater emphasis on feedback, learning, and how the system can be improved.

Relations between accident investigation and safety analysis
Especially in complex systems, there are many relations between AI and SA. Some questions that might be raised in an investigation are:

- Has this type of event been studied earlier in an SA?
- Did the SA overlook this event, and, if so, why?
- Can the AI identify the need for an SA to be performed of a specific situation?

From an SA perspective, there are aspects like these:

- Experiences and data from earlier AIs may provide important inputs into an SA.
- An SA might establish that a specific type of event is of essential importance. If such an event occurs, an investigation should be performed automatically.

Environment, quality and security

There are many similarities in the management of risk, environment, quality and security.

In the discussion above, you could often just change a few words, and what is applicable in one area would be applicable in another. Possible collaboration across areas is often advocated, e.g., in the nuclear industry (IAEA, 2007, p. 133). The areas have been discussed from several perspectives in the previous chapters (e.g., in Table 1.1).

Quality management addresses the quality of products and services, and the ability of a company to provide satisfactory production capacity. In short, s*ecurity* is concerned with intentional damage. It deals with the prevention of, detection of, and response to theft, sabotage, unauthorized access and espionage.

The exact interactions between the areas depend on the context, but they have many things in common:

- The goal of preventing damage and other undesired effects
- An organised system for goal achievement
- The need to demonstrate effectiveness and efficiency
- The need for investigation when something has gone wrong
- The use of safety (risk) analysis for the identification of negative future events
- Collaboration with production management

These similarities can be put to use, and synergy effects can be highly favourable. Synergy means that different entities collaborate to the benefit of all in a final outcome. Several of the methods described in this book can be used in similar ways in all these areas.

3.7 In conclusion

A generic framework for safety analysis has been proposed. It bears great resemblance to risk assessment in the technical tradition, as described by the ISO (2009A, 2009B). There are a few differences, with regard to terminology and the application of risk evaluation, but there are no controversies.

The safety analysis framework has been designed with the aim of having a wide area of application. This means that assumptions regarding the situation and organisational conditions are avoided (e.g., a top-down hierarchy is not necessary). Also, the investigation of events that have occurred is included in safety analysis.

Relationships and synergies between fields, applications and types of risks are important to consider. For example, different types of consequences can be treated consistently within one and the same analysis. My experience is that giving a broad scope to safety analysis can facilitate this.

4 A brief summary of methods

4.1 Selection of methods

There are numerous methods of safety analysis, each with its own characteristics. About 50 methods are mentioned in a book I wrote some years ago (Harms-Ringdahl, 2001). In an ISO standard (2009C), 31 "risk assessment techniques" are included, and, in a handbook from the US Federal Aviation Administration (FAA, 2000), 81 different "analysis techniques" are referred to. Clearly, anyone who is to work with safety analysis must choose between the large number of methods available.

Terms are used a bit differently, and precise definitions can be hard to formulate. As a method, safety analysis is more precise than general techniques such as interviewing, brain-storming and the Delphi technique, all of which can be applied to many types of problems.

In this book the definition is:

> *A safety analysis method is a documented procedure used to acquire knowledge about risks and safety characteristics in a system.*

How to choose between the methods available is not self-evident, and the outcome of the choice depends on various considerations. The selection of methods in the book is grounded on a set of criteria, of which the first two are most important.

- The analytic procedure is systematic, and is sufficiently well described for different analysts to work in a similar manner.
- A public description is available, which might be in a book or scientific article, or on the Internet. This criterion will exclude proprietary methods, which means that there are some restrictions in using them. Such methods are mentioned occasionally in this book, but only briefly described.
- The method is fairly easy to understand and apply.
- The analysis can be conducted with a reasonable amount of effort, taking anything from part of a day to one or several weeks.
- The analysis can be conducted even when information on the system is incomplete. For example, an analysis may be conducted of equipment that is still at the planning stage. It may have less accuracy, but is still worthwhile.

Methodology related to probabilistic risk analysis is only briefly described, since it does not meet the two final criteria, and would also make the text more complicated. For the interested reader, there are several textbooks describing such methodology (e.g., Aven 2003) for the reader interested in that field.

This book highlights a set of methods. It is based on the author's own selection. It was guided by the criteria above, and also by a desire to present a range of complementary approaches.

4.2 Types of methods

Parameters

The methods can be categorised in several ways. One possibility is to base the categorisation on the purpose of the analysis. However, a specific method might fall into more than one category, and might, for example, be used for both the analysis of systems and the investigation of accidents. The aims of the methods can be categorised as follows:

A *Risk identification*. The aim is to discover undesired events or problems that might occur in the analysed system.

B *Analysis and understanding*. Assess how an accident could occur and what its consequences might be.

C *Risk evaluation*. Judge whether the risk level and the system characteristics are acceptable.

D *Investigation of accidents* (*events*). Study the events that have occurred in a specific system.

E *Other aims.*

In risk identification, the focus is on what can happen in the future. Typical questions to address are:

- Which problems can arise?
- What could cause an accident to occur?
- Which consequences would there be if X occurs?

Evaluation of risks is included in some methods. However, evaluation can comprise different methodologies which are described in more detail in Chapter 5.

Investigation of accidents and events concentrates on what has happened. The questions usually focused upon are:

- What has happened?
- How could the accident have occurred?
- How can a reoccurrence be avoided?

Methods are sometimes described as *proactive*, which usually means that they are applied in the analysis of a system before an accident occurs, and the aim is to prevent any future occurrence. The opposite term *reactive* has a more negative meaning, indicating that you do things when it is too late. However, accident investigations can also be proactive in that they aim to avoid other accidents. During recent years I have learned that a thorough investigation can be even more powerful than an ordinary risk analysis.

Other characteristics

Methods can be categorised in several other ways, which have greater or lesser utility according to the context.

The technical tradition

In the technical tradition, analyses might be categorised as follows. Such a perspective will lead to a grouping of methods related to the output they deliver.

- Quantitative, which is based on the calculated values of probabilities and consequences, and is sometimes referred to as probabilistic risk assessment.
- Semi-quantitative, which is based on probabilities and consequences in intervals or ranges.
- Qualitative, based on other types of principles.

The systems perspective

Methods can be divided into four more or less distinct groups, which are based on the aspects they consider:

- A technical perspective on how the system works (T)
- A human and psychological perspective (H)
- Organisational aspects (O)
- A combined perspective (THO), which emphasizes interactions between different components and procedures, in a workplace or in other situations.

Safety improvements

In some methods, there are provisions for identifying potential safety improvements. A characteristic would then be whether or not a method supports the development of improvements.

4.3 Examples of methods

A sample of methods

Table 4.1 provides a sample of 15 methods. The grouping is based on the parameters at the beginning of Section 4.2. The first and largest group includes 7 methods, which are used mainly for the identification of risks and problems.

A Risk identification

The first six methods employ a similar analytic procedure. They are the Action Error Method, Deviation Analysis, Energy Analysis, Failure Mode and Effects Analysis (FMEA), Hazard and Operability Studies (Hazop), and Job Safety Analysis. The key steps that these methods have in common are as follows:

1) The object of the analysis is divided into several parts, which in principle means the construction of a simplified model of the system.
2) For each part of the system, sources of risk (hazards) or other factors related to the risk of accidents are identified.
3) Some form of risk assessment is carried out.
4) In most cases, a stage at which safety measures are proposed is included.

The method Preliminary Hazard Analysis belongs to a subgroup that might be called *coarse analyses*. They are used to obtain a quick overview of hazards at a plant or in some kind of activity or installation. Such an analysis represents a compromise between thorough analysis and unsystematic observation (see Section 12.8).

B Analysis and understanding

This group consists of methods that can be useful for analysing logical connections and safety barriers in a system.

C Risk evaluation

Table 4.1 shows two methods of risk evaluation that represent different principles, which are thoroughly presented in Chapter 5.

D Accident investigations

Two examples of methods of accident investigation are given below, and several more are described in Chapter 13. In addition, some of the other methods can be used for investigations, and they are marked with a D in the table.

Table 4.1 Examples of methods applied in system-oriented safety analysis

Method	Comment	Ref	THO	Aux
A Risk identification				
Energy Analysis	Identifies hazardous forms of energy	6	T	
Job Safety Analysis	Identifies hazards in work tasks	7	TH	
Deviation Analysis	Identifies hazardous deviations in equipment and activities	8	THO	D
FMEA (Failure Mode and Effects Analysis)	Examination of components in a technical system	12.2	T	
Hazop (Hazard and Operability Studies)	Identifies hazardous deviations in chemical process installations	9	T	
Action Error Method	Identification of operator's errors in an operational procedure	12.5	H	
Preliminary Hazard Analysis	A coarse analysis	12.8	MT	
B Analysis				
Event Tree Analysis	Logical tree of alternative consequences of an initiating event	12.3	T	C D
Fault Tree Analysis	Logical tree of the causes of an accident	10	T	C D
MORT (Management Oversight and Risk Tree)	Based on a logical diagram of management and potential failures	12.7	O	C D
Safety Function Analysis	Analysis of the safety characteristics of a system	11	THO	C D
C Risk evaluation		5		
Risk Matrix	Acceptability is based on estimated consequences and probabilities	5.4	T	
Direct Evaluation	Several factors are included in a recommendation of acceptability	5.2	TO	
D Accident investigations	Several methods exist	13		
STEP (Sequentially Timed Events Plotting)	Diagram of events in an accident	13.2	TH	
Acci-Map	Relates the accident to the organisation at different levels	13.7	O	
E Other				
Task Analysis	Analysis of people's tasks; it can also be used in risk identification	12.6	H	A
Safety audit	Structured examination of a management system	12.7	O	C

Ref refers to the chapter or section where the method is described in greater detail

THO refers to the main orientation, **T**echnique, **H**uman, or **O**rganisation

Aux shows if the method also can also be placed in another category

Grouping of methods

Methods can be structured in many ways, and one supplementary approach is shown in Figure 4.1. The *risk identification* group (the same as Group A above) contains some methods that *search directly* for potential injuries. Other methods *search indirectly* for e.g., deviations, which might cause injury.

The second group, comprising two methods, focuses on the analysis of safety characteristics and barriers. The third group concentrates on accident sequences and events, which is where the investigation of accidents especially belongs. The fourth group is concerned with evaluations and decisions.

Two general methods – Fault Tree Analysis and Event Tree Analysis – can be useful for applications in the latter three groups. They can also be used to analyse logical interrelations between events, failures, and barriers.

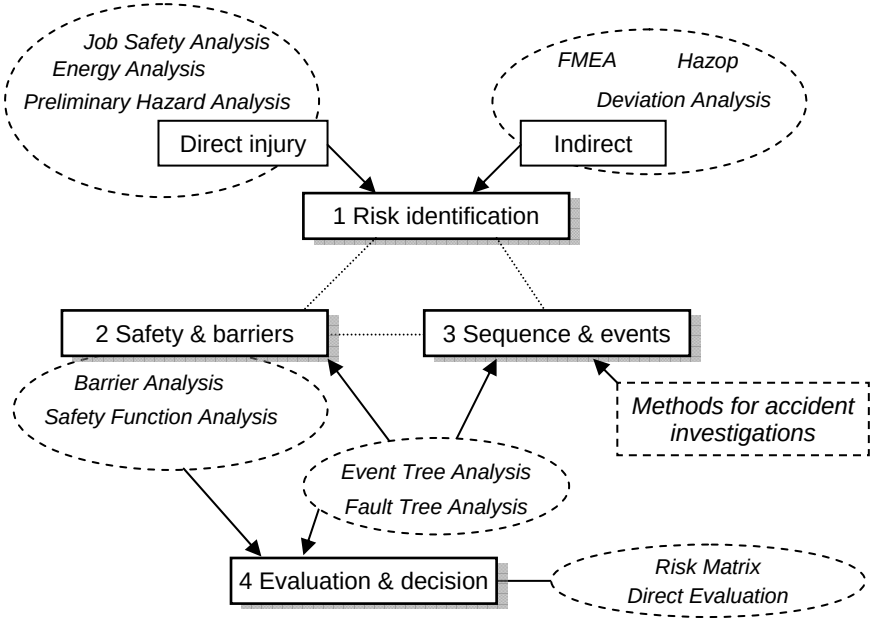


Figure 4.1 An alternative grouping of methods

4.4 Do we need more than one method?

For a newcomer to this field, the diversity of methods can cause confusion. Would it not be enough to have just one?

A complication is that any one specific method will only cover a limited part of the risk panorama. The methods have different applications, with advantages and disadvantages. If you want to conduct a fairly thorough analysis, it can be wise to apply additional methods based on complementary principles.

Figure 4.2 illustrates the coverage of two and three methods. It is based on experiences from a number of courses, where Energy Analysis and Deviation Analysis have been applied to the same object. The two methods identified roughly the same number of hazards, and about one third of these overlapped.

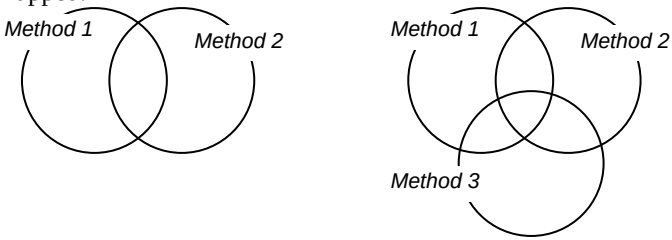


Figure 4.2 Separate methods covering different areas

In another test (Harms-Ringdahl, 2003A) using three methods, Safety Function Analysis was added to the other two. The proposals for improvements were compared, and only 5% were generated by all three methods (discussed in greater detail in Section 16.9).

The answer to the introductory question is: *It is not enough with one method.* At a specific situation you could use one method, but that should be carefully chosen.

One intention of this book is to help the reader to choose the approaches and methods that best meet actual needs. Accordingly, the characteristics, and advantages and disadvantages, of different methods are discussed in several places (especially in Chapter 15).

Choice of approach and method is seldom (completely) rational. It is common, and practical, to carry on as usual with the same method without considering other options. I have come across numerous cases, especially where Failure Mode and Effects Analysis (FMEA) has been used in all situations.

We all have our preferences and biases. There is an old adage: *If you only have a hammer, you tend to see every problem as a nail.* I hope we can get away from this by being more systematic in choosing a suitable methodology. A detailed discussion of how to make a choice is presented in Chapter 15.

5 Evaluation of risks and systems

5.1 Basics of evaluation

Aim and scope

The risk evaluation stage forms an important part of a safety analysis. The seriousness of identified hazards and problems is to be estimated, and the need for improvements to be assessed. This can be done in different ways, and this chapter will give a summary of some approaches to risk evaluation.

Making an evaluation might sound easy, but in theory and practice it is rather complex. Evaluations can be made in many different ways, and descriptions in the literature show large variability. Actually, the subject is difficult for most people.

The general aim of a risk evaluation is to give systematic support for decisions about the design, operation and maintenance of a system. A simple description is in many cases sufficient:

> *The evaluation of a specific hazard is the judgement of the need to take action.*

Risk evaluation has a number of meanings depending on the application area. In this book, the following definition is used:

> ***Risk evaluation*** *is the process of judging the tolerability of identified hazards, problems, and system safety properties.*

This definition is more general than usual, since safety analysis is a broader concept than risk analysis and risk assessment; for example, it includes accident investigations. The definition is similar to one in a standard issued by the ISO (2009A), which defines risk evaluation as the "process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable".

It can be compared with an earlier narrower definition from the IEC (1995): "Risk evaluation is the process in which judgements are made on the tolerability of the risk (based on the risk analysis)".

Changing views on evaluation

In recent years, views on risk evaluation have been changing in a way that clearly goes beyond issues of probabilities and consequences. This can perhaps most clearly be seen in the updated ISO-standard (2009B) for risk management. It states that the purpose of risk evaluation is to assist in making decisions about the treatment of risk and setting priorities.

Such decisions should take account of the wider context of the risk, and should also consider tolerance of the risks borne by parties other than the organisation that benefits from the risk-taking. Further, it is self-evident that decisions should be made in accordance with legal, regulatory and other requirements. In some circumstances, a risk evaluation can lead to a decision to undertake further analysis.

Aims

The basic aim of a risk evaluation is to provide a basis for deciding whether an analysed system is acceptable as it is or whether changes are necessary. Some examples of more detailed objectives are given below. They do not exclude each other, and are usually determined by the general goal of the safety analysis. The objectives can be to:

- Distinguish between important risks and less important ones.
- Suggest which system improvements are needed to increase safety.
- Give an estimate of the *size* of the risk.
- Support the choice between given alternatives, when risk characteristics should be balanced against other features. This might involve making comparisons between technical solutions, or between tenders from companies competing for an order.

Evaluation in accident investigations

Also in accident investigations, there is a need to make judgments on identified problems, deviations and hazards. These have been observed, so they are known already to exist. The aim of an evaluation in such situations is to decide whether or not safety improvements are needed.

Assumptions about the situation

There are many situations in which risk evaluations can be made. To make the account slightly simpler, we assume the following:

- There is a system to be analysed, which might be a factory, a workplace, a hospital ward, technical equipment, or something similar.
- Identification has been performed, which gives a list of hazards, deviations, or problems, depending on the method. The number of items may be quite high (sometimes around a hundred).

- The analyst (together with a work group) is to evaluate each item on the list.

Evaluation as part of the decision process

The overall aim of a safety analysis (SA) is to support decision-making about future actions. After performing a SA, the usual result is information about hazards, system weaknesses, possible improvements, and other circumstances. This information is to be analysed and considered by the decision-maker.

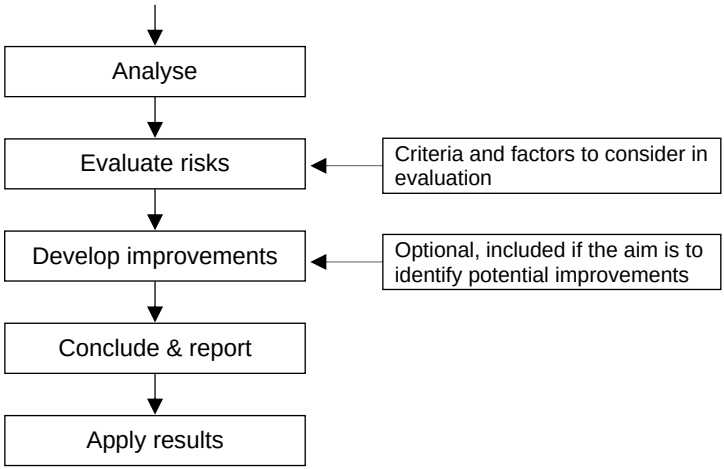


Figure 5.1 The evaluation and decision procedure in safety analysis

The evaluation stage is seen as a part of a general decision process in Figure 5.1, which is an extension of Figure 3.1. The analysis stage provides information about hazards, problems, and also safety characteristics. At the evaluation stage, this information is considered and compared with criteria and rules.

At the concluding stage, information is available about existing hazards and how they have been evaluated, and sometimes there are suggestions for improving the system. The conclusion can be regarded as a recommendation by the analyst and the analysis team.

The whole SA is finally communicated to the end-user, who will make the final decisions, which will also include aspects other than risk and safety. In practice, there is overlap between the stages, which makes the decision process more complicated. The *Evaluate risks* block can be strict and formal, while the final decisions by the end-user are usually more informal.

This perspective on risk evaluation as a decision task is common. Aven (2003) sees decision-making as a process, with formal risk and decision analyses to provide support, which is followed by an informal managerial process that results in a decision. Aven also defines the starting point for a risk analysis as a decision problem, which is often formulated as the task of choosing between a set of alternatives.

Principles and criteria

A decision is basically concerned with weighing advantages against disadvantages. However, the grounds for establishing what to consider are far from self-evident, and many different concepts have been presented in the literature.

It is important to be aware of complexity and of multiple alternatives in making decisions about risks. In real cases, there is often an overlap between and a combination of approaches. Ten examples of principles are presented below. The first three have a probabilistic orientation, and a focus on future accidents and losses.

1. Quantification of expected losses

It is common to base an evaluation on the expected *level of risk*, which is expressed in terms of the combination of consequences and their likelihood (ISO, 2009A). The result is often used to determine whether a hazard is tolerable or intolerable. The quantitative approach is further discussed in Section 5.3.

2. ALARA

ALARA is an acronym for *As Low As Reasonably Achievable.* It is often used when the level of risk lies somewhere between tolerable and intolerable. This is a kind of decision in which level of risk and costs are balanced against each other.

The directives issued by the authorities offer one basis on which accident risks can be assessed. These, however, are mainly general by nature, and do not cover all types of hazards. In some situations, and for certain types of equipment, fairly concrete information can be obtained on whether or not a risk is acceptable. But there are also many formulations of the type: *Protection against injury shall be adequate*, or *Risks should be As Low As Reasonably Achievable (ALARA).* To establish what is adequate or reasonable remains a matter of judgement.

3. Cost-benefit analysis
Cost-benefit analysis (CBA), in a general sense, can be used for making comparisons. In a formal economic CBA, monetary values are assigned to all benefits and all costs. In a safety context, CBA can mean that measures should be applied where the risks and problems are largest. Instead of monetary values, other values can be chosen. They might concern:

- Minimisation of downtime for a certain type of equipment
- Optimisation of product quality and functionality
- Customer satisfaction, and many further issues

4. Compliance with norms
Many organisations want to follow laws and regulations, and those related to safety are of special interest here. The principle is to compare observed problems with formal norms, e.g., directives about machine guards, or exposure limits.

If the aim is to suggest acceptance or rejection of a system, there is a need to compare the risk level with given criteria. These can be sometimes be found in regulations or in other norms. However, the availability of clear and unambiguous norms is the exception rather than the rule.

5. Manage safety
In risk management the goal is to obtain adequate control of the hazards in a system. An evaluation is intended to assess technical and organisational safety features to see whether they are adequate. When an accident has occurred, you can see it as a result of an insufficient safety system rather than as a random event.

6. Compare different alternatives
This type of evaluation is based on a direct comparison between alternatives, where risk is an important factor. Aven (2008A) emphasises this strongly, and states that “if a decision-making situation is not clearly formulated, the analysis should not be carried on”.

7. An integrated perspective
Broadening scope can lead to the integration of different types of consequences. Often in a safety analysis, accidents and injuries to people are the main concern. However, an unwanted event may also cause damage to the environment, hamper or halt production, and result in economic losses. There are advantages to encompassing safety, health, and environmental and production aspects within one and the same analysis (cf. Table 5.1).

8. Safety as a high priority

Safety comes first is a common phrase in discussions about risk, but its exact meaning varies. It has several similarities to the precautionary principle (which can also be interpreted in different ways). Examples are:

- A new system must have at least the same level of safety as the previous system.
- That the safety level is satisfactory must be verified before operations start.
- The system shall be systematically designed and monitored in order to maintain a satisfactory safety level.
- Where there are uncertainties about the situation, these should be clarified before the system is approved.

9. Evaluation as a negotiation between stakeholders

There may be several stakeholders with an interest in a decision. As well as management, there are employees, customers, authorities, insurance companies, etc. They may all value risk and problems differently, and if diverse opinions are not properly handled, conflicts can arise, which result in distrust, unsatisfactory safety, and loss of time and money.

The different perspectives of stakeholders can also be an advantage in many situations. It might take longer to do an evaluation, but the results will be better in the end. One reason is that diversity might attract extra attention to a structured evaluation with clarified criteria and principles.

10. Explicit and implicit values

Often, an evaluation is seen as a mainly technical process. However, decision-making has received attention in many fields, such as economics, philosophy, politics, psychology, and sociology. A large body of literature exists, which makes a quick summary unworkable.

Nevertheless, we cannot disregard the large number of aspects that will influence evaluation and decision-making. When we judge which risks should be accepted, rejected or reduced, we do so on the basis of a set of values. Sometimes, these values are explicit, sometimes implicit and undefined. One example is *transparency*, which means that it must be simple for the persons concerned to see the policies, facts and methodology that have led to a decision. It is also essential to specify the individuals who have provided facts and performed the analysis. There is also a *fairness* perspective, which may concern whether an unreasonable burden is imposed on a group of people by a risky undertaking.

Approaches to evaluation

There are a number of approaches to the evaluation of identified hazards and other system properties, and terminology varies between different fields. The following division can be made:

1) *Direct Evaluations* focus on the need for safety measures for each identified risk (see Section 5.2). The evaluations are based on a number of defined criteria, e.g., the requirements of legislation.
2) *Quantitative* (or *probabilistic*) *evaluations* are based on numerical estimates of consequences and probabilities (see Section 5.3).
3) In a *Risk Matrix*, probabilities and consequences are placed in categories, rather than being given numerical values (see Section 5.4). A comparison is made with rules for which risks should be accepted.
4) *Analysis of barriers* and their adequacy is seen as a special type of evaluation. Barrier and safety functions are discussed mainly in Chapter 11.
5) *Other types of evaluations* are possible such, as those that involve the concepts of *relevance* and *comparison* (see Section 5.5).

Different types of consequences

An accident can have a range of consequences, not only injury to people. Usually, it is beneficial to consider a broad range, meaning that different types of consequences are considered in one and the same safety analysis. The analysis can concern injuries to people, health problems, damage to the environment, loss of property, and production problems. Table 5.1 proposes a classification for such an integrated approach.

Table 5.1 Classification of types of consequences (SHEP)

Code	Description	
S	Safety	Injuries to people in accidents
H	Health	Health problems for people
E	Environment	Environmental problems
P	Production & property	Problems with production, quality, etc., and loss of property

Health is intended to deal with the injuries that occur as a consequence of long-term exposure to chemicals, poor working postures, etc. Injuries due to accidents and exceptional contacts with dangerous substances are seen as consequences of accidents, and fall into the *Safety* category.

5.2 Direct Risk Evaluation

Basic decision

Many methods contain an identification stage, which results in a list of hazards, deviations, problems, or some similar things. The aim at the evaluation stage is to examine each item on the list, and to decide whether or not something should be done to treat it. This basic issue is addressed in most methods of risk evaluation. It can be phrased in many ways. For example, the British Health and Safety Executive (HSE, 2008) writes:

> "Having spotted the hazards, you then have to decide what to do about them. The law requires you to do everything 'reasonably practicable' to protect people from harm. You can work this out for yourself, but the easiest way is to compare what you are doing with good practice."

Principle

A direct-evaluation approach focuses straight away on answering the question of acceptability. The approach is commonly adopted, but seldom described in any detail. The method here is based on an earlier suggestion (Harms-Ringdahl, 1987), and is simply called *Direct Risk Evaluation.*

Figure 5.2 shows the principle and procedure. The hazards are compared with a set of criteria for evaluation. Each identified hazard is directly classified into two main categories: *Acceptable* or *Not acceptable*. In concrete terms, not acceptable means that some kind of action or an additional safety measure is required.

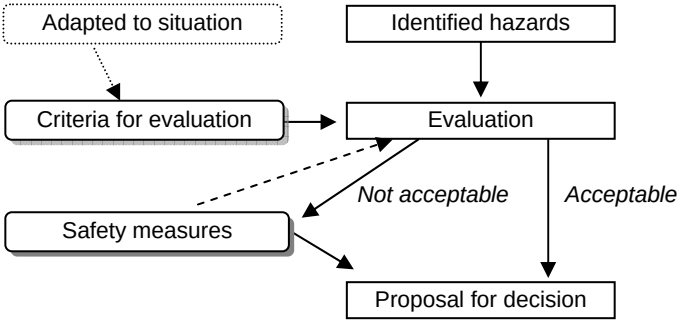


Figure 5.2 Overview of procedure in Direct Risk Evaluation

The risk evaluation scale

The use of only two main categories is too crude in many situations. Instead, a more detailed evaluation scale, such as the one shown in Table 5.2, has greater utility. The codes 0 and 1 correspond to the class *Acceptable* or *Tolerable* (whichever term you like best). Safety measures are usually concrete actions, designed to improve the system. In general, the scale agrees with a British standard (BSI, 2004, p. 50) and also other recommendations.

However, it is beneficial to broaden the concept of a safety measure, and also let it refer to actions such as further investigation. The reason for this is that there are often uncertainties during an analysis, which, for example, can concern the function of a technical system, or whether routines really work. Advantages of the broader concept are that:

1) Uncertainties and lack of knowledge can be handled in a consistent way.
2) The evaluation and the analysis can be concluded fairly quickly, because uncertainties are clearly stated and supplementary investigations can be performed later.

Table 5.2 Risk evaluation scale

Code	Description	
0	No need for improvement	*Acceptable*
1	Safety measure* can be considered	
2	Safety measure is recommended	*Not acceptable*
3	Safety measure is imperative	
4	Intolerable; work should not be started or continued until the risk has been reduced	

*Safety measure also includes improving knowledge and further investigation

Criteria for evaluation

Before the evaluation starts, agreement is needed on which criteria are to be used. As a starting point, the list of criteria in Table 5.3 can be useful, and if needed it can be adapted to the actual situation. The criteria are based on different sources, e.g., the two mentioned above (BSI, 2004; HSE, 2008) and earlier suggestions (Harms-Ringdahl, 1987 and 2001). They also relate to the principles and criteria presented in Section 5.1.

The criteria come in approximate order of importance. They are intended as an aid to deciding when a hazard or problem demands safety measures. The basic rule of decision-making, however, is that if any of

these criteria indicate problems, improvements are appropriate. Nevertheless, the selection of risk values (Table 5.2) is still often a matter of judgement. One reason is that the criteria are general, and there is a need to weigh up their relative seriousness. In addition, if several criteria are met, this gives a higher score.

Table 5.3 Seven criteria for evaluating hazards as unacceptable

	Criteria	**Comments**
1	Breach of directives issued by the authorities	Directives can be more or less clear
2	Deviation from company policy and rules	Policy might be more or less well-defined
3	High values for consequences and/or probabilities	There may be serious potential consequences, or problems that are frequent
4	Deviation from good praxis at similar installations	Good praxis can offer simple solutions to problems
5	Knowledge is uncertain and unsatisfactory.	Evaluation should not be based on inadequate information
6	A suitable solution is available	The risk might easily be reduced.
7	Low system tolerance for errors and faults	A single human mistake or technical fault can trigger a hazardous event

Criterion 1: ***Directives of authorities*** can provide a basis for evaluation, but they are often general and might need interpretation. Sometimes, a directive is sufficiently precise to establish that something must be done. In such cases, a note that refers directly to the directive can be made on the record sheet.

Criterion 2: ***Company policy and rules*** are supposed to be followed. Usually, it is expected that deviations from them are corrected.

Criterion 3: ***High values for consequences and/or probabilities*** are reasons for safety improvements, as in quantitative evaluations (see sections 5.3 and 5.4). For example, serious consequences impose high demands on system safety, and a special check on the system may be needed.

Criterion 4: ***Good praxis*** reflects long experience of how to deal with different kinds of problems, and sometimes gives an indication of what is *reasonably practicable.* The criterion also stipulates that a system shall not be unsafe if reasonable safety systems are available.

Criterion 5: ***Uncertainty*** means that knowledge is inadequate, e.g., on how the system works in practice in particular situations, or what the consequences of an error might be. It is not satisfactory for an evaluation to be based on poor facts, which is especially important when consequences are severe. Four alternative ways of proceeding are suggested:

a) Directly search for more information, and after that complete the evaluation.

b) Improve knowledge, but do that after the analysis. This means proposing a measure that consists in pursuing a deeper investigation or even conducting a complementary safety analysis.

c) Follow the *Safety First* principle, and do something even if it is not necessary from a risk perspective. Especially if there is a simple solution available (Criterion 6), this can sometimes be more cost-efficient.

d) Disregard the uncertainty and lack of knowledge, and do an evaluation anyway. In my opinion, this is both irrational and unethical.

Criterion 6: ***Suitable solution***s are sometimes easily available. They may deal with hazards and problems that do not have to be dealt with according to the other criteria. In such cases, it may be sensible to weigh up costs and benefits.

Criterion 7: ***Low fault tolerance*** means that an accident can be triggered by a simple human error or a single technical fault. The safety level can then be considered unsatisfactory. In some areas, e.g., the railway industry, that a single technical failure can lead to an accident is unacceptable.

Integrated evaluation

An accident can have different types of consequences as discussed in Section 1.1 (Table 1.1). In a Direct Risk Evaluation, integration of them can be fairly easy. This can be done by combining the SHEP codes (in Table 5.1) with the risk evaluation codes (in Table 5.2). Some examples:

- Notation *S3* means that, from a safety perspective, a measure must be taken.
- Notation *E2* means that, from an environmental perspective, a measure is recommended.
- Notation S3 & E2 mean that two types of consequences can occur, and that both have been considered in the evaluation.

Practical aspects

Evaluation as group work

There are advantages in doing evaluation work in a group. The result should then be seen as a recommendation from the group to management (who ultimately decide). One benefit is that such a group can represent different values and experiences, which enables more comprehensive judgments to be arrived at. Another advantage is that the members of the group may get more engaged in the results through participation in decision-making.

The method is based on a set of criteria that often need some kind of interpretation. A good start is to discuss the basis for the planned evaluation. The first evaluation might take some time, but it is a way of preparing the ground for how to proceed. After a while, when people get used to it, it goes much quicker.

Handling of disagreement

Disagreement can be expected now and then, because making evaluations is not an easy task. This should not be seen as something negative in itself, and it can be constructive to compare different perspectives. The analysis leader can support a debate that stimulates better understanding.

Should disagreement arise, it is not necessary for it to be resolved immediately. Divergent views on evaluation can be noted on the record sheet, e.g., *1-2*. This notation informs the reader that there are different perspectives. The measures adopted in such cases are usually concerned with improving knowledge.

However, in practice, disagreement is seldom a problem. In my experience, only a few percent of all evaluations end in disunity, and noting down separate values usually satisfies all participants. Actually, it has happened a few times that participants have felt that they almost are too much in agreement.

Handling uncertainties

Criterion 5 deals with the handling of inadequate knowledge. When there are uncertainties, they must of course be clearly stated, both in the analysis protocol and in the report. This is a practical way of handling such situations, which makes it possible to conclude an analysis fairly quickly. The alternative is to wait for further investigations that might take a long time.

5.3 Quantitative evaluations

General

A quantitative approach to risk evaluation is used in many applications of safety analysis. In a simple sense, this means that the probability of the occurrence of a certain event and the size of its consequences are estimated. A quantitative measure of risk can then be utilised to judge whether or not a hazard is acceptable. In this book, I refer to this as the *quantitative* tradition or the *probabilistic* tradition.

Quantitative assessments are especially used in applications where the consequences of accident are severe. The methodology is common in fields like nuclear power, off-shore , aviation, space flights, and so on. In such industries, safety is an imperative, and large resources have been devoted to developing methodologies for risk assessment. The regulation of chemical plants with a potential for major accidents has generated a large interest in quantitative assessments and acceptance criteria.

This book has a different aim and scope than those in the quantitative tradition. It covers simpler applications and involves less complicated considerations. Quantitative evaluation methodology is therefore only briefly discussed. Section 3.4 briefly describes a framework for quantitative evaluation and the terminology of the probabilistic tradition.

Principles

Probabilistic risk evaluation involves comparing estimated levels of risk with defined risk criteria in order to determine the significance of the level and type of risk. The process of evaluating identified risks has a number of stages, which in the *classical* approach can include:

1) Establish which type of criteria to use. It could concern expected number of deaths, sick-days, induced cancers or some other injury or damage.
2) Define the risk criteria and values for what can be accepted.
3) Estimate the level of risk, involving values of probability and consequence for a selection of the hazards.
4) Do the evaluation, which means that estimated values are compared with defined risk criteria.

The simplest type of risk criterion has a single level to select the risks that need treatment. This is usually too simplistic, and does not consider the uncertainties involved. A more common approach is to divide the frequency of occurrence and the size of consequences into three hazard areas (A, B and C), as shown in Figure 5.3:

A) Low risk area, where the level of risk is regarded as negligible, or so small that no risk-reducing measures are needed.
B) Middle area (or *Grey zone*), where costs and benefits are considered, and advantages are balanced against potential consequences.
C) High risk area, where the level of risk is regarded as intolerable whatever benefits the activity may bring, and risk treatment is essential whatever its cost.

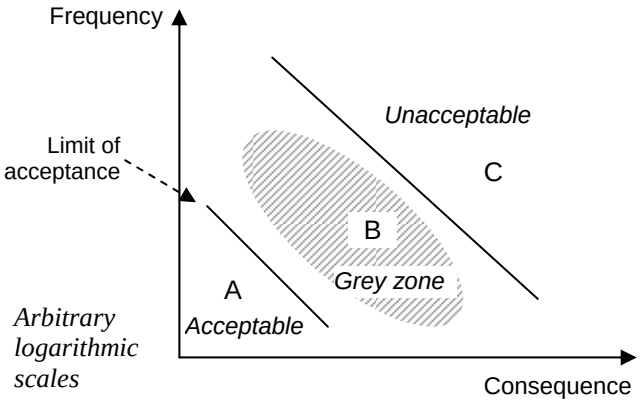


Figure 5.3 Frequency and consequence diagram for the evaluation of risks

Hazard A has a low frequency of occurrence, and a small consequence if an accident should occur. The risk level is low and considered negligible, and is below the limit of acceptance.

Hazard C has a high frequency and large consequence, and is above the limit of what is tolerable. Something needs to be done to reduce consequence and/or probability for the analysed system to be approved.

Hazard B is in the grey zone between the limits for what is acceptable and unacceptable. Should it be accepted or not? This is often a complicated question, especially in large and complex systems. Two general principles are often relevant here:

- ALARP – As Low As Reasonably Practicable
- ALARA –As Low As Reasonably Achievable

Applying the ALARP principle means that the best that can be done under prevailing circumstances must be done. For an identified practicable risk reduction measure, the duty holder should implement the measure unless it can be shown that it is not reasonably practicable. This principle is regarded as valid, for example, in the UK nuclear and offshore industries (Schofield, 1998).

ALARA is similar, but is usually regarded as less rigorous. The risk is reduced as far as is reasonable, rather than as far as possible. One interpretation of the ALARA principle is that the costs of safety equipment are balanced against the values of the increased safety (e.g., Taylor et al., 1989). The two expressions are often confused, and there are somewhat different interpretations.

Risk estimations

Quantitative risk estimates can be made in a number of ways, and also include several parts (e.g., IEC, 1995; ISO, 2009). Frequency analysis gives an estimate of the likelihood of each identified undesired event. Three general approaches can be used separately or in combination:

- Use relevant historical data
- Apply analytic techniques, e.g., Fault Tree or Event Tree
- Use expert judgement

Consequence Analysis estimates the likely impact if the undesired event occurs. In the chemical industry, for example, there are a large number of calculation methods for gas emissions, and also for events related to fires and explosions. A detailed account of this type of estimation is beyond the scope of this book, and the reader is referred to the more specialised literature (e.g., Lees, 1996).

The risk calculations should help to express the risk in suitable terms. Some commonly used measures are:

- Predicted frequency of mortality (individual risk)
- Plot of frequency versus consequence for societal risk, known as the F–N curve, where F stands for frequency and N for the cumulative number of undesired outcomes (e.g., fatalities)
- Expected loss rate, in terms of casualties, economic costs, or environmental damage

There are many uncertainties associated with the estimation of risk, which are also considered in one of the standards (ISO, 2009C). *Uncertainty Analysis* involves the examination of factors that might contribute to variation and imprecision in the result; it is influenced by data, methods and models. *Sensitivity Analysis* is closely related, and involves how the result depends on changes in single model parameters.

Several authors have addressed this type of problem. For example, Aven (2003) has discussed the issue of what constitutes a good probability assignment. Benchmark Studies (see Section 14.5) have shown that estimates can vary widely.

5.4 The Risk Matrix

Principles

The Risk Matrix method is a popular and common approach to evaluation in risk analysis. It is a semi-quantitative method, where probabilities and consequences are categorised, instead of using numerical values. The Risk Matrix is applied in many different areas, and consequently the terminology and methodology vary quite a lot. One perspective is that it is a method or "mechanism to characterize and rank process risks" (Markowski & Mannan, 2008).

Usually, the Risk Matrix is described as a table with categories of consequences in rows, and categories of frequencies or probabilities in columns. The principle is that each cell is associated with a level of risk. For each identified hazard, a categorisation is made of the size of consequence and of the probability of occurrence. This combination defines at a certain matrix cell, which classifies the level of risk of the hazard.

Table 5.4 Example of a Risk Matrix with risk ranking

Probability	**Consequence**			
	Minor	Medium	Large	Catastrophic
Frequent	*Medium*	*Medium high*	*High risk*	*High risk*
Probable	*Medium*	*Medium*	*Medium high*	*High risk*
Remote	*Low risk*	*Medium*	*Medium*	*Medium high*
Very unlikely	*Low risk*	*Low risk*	*Medium*	*Medium*

Table 5.4 gives an example of a Risk Matrix, where low levels of risk are to the bottom-left, and high levels of risks to the top-right. In-between, there is a medium-risk area. The probability scale goes from *Very unlikely* at the bottom to *Frequent* at the top.

This layout is analogous to the diagram in Figure 5.3, and it is similar to the model in an ISO standard (2009C). However, there are other preferences, and the British standard (BSI, 2004) has the opposite order for the probabilities, with *Very unlikely* at the top. You can also find matrices with probabilities in the rows, and consequences in the columns.

Often, the Risk Matrix is used directly to define the limits of acceptable and unacceptable risk. This means that a rule is stipulated for how hazards shall be evaluated. In application to a specific hazard, potential consequence and probability are estimated. The rule then automatically gives an answer to the question of whether or not the hazard is acceptable.

Alternative rules

There are a number of similar semi-quantitative methods. They have it in common that they are based on rules to classify the level of risk. Instead of a matrix, the rules can be based on numerical values.

One way of extending an evaluation is to include more parameters. In *Failure Mode and Effect Analysis* (FMEA) (see Section 12.2), a *Risk Priority Number* (RPN) can be calculated, which is used for prioritising the identified hazards. The RPN is the product of the numerical estimates of *Consequence*, *Probability*, and *Detection*. The *Detection* estimate indicates the degree of ability to detect and remove failures in time. A high detection value means that the failure will escape discovery and consequently is more dangerous, while a low one is easily discoverable.

Risk Matrix procedure

There are many references in which the matrix is explained rather summarily, and the method is generally seen as a flexible, simple and efficient tool. However, it is hard to find a full and general description of how the Risk Matrix should be applied. A more detailed account than usual is provided by the ISO (2009C, pp. 82-86), which calls it a consequence/ probability matrix. Other examples come from a British standard (BSI, 2004, pp. 49-50), and from the web (e.g., Ozog, 2002).

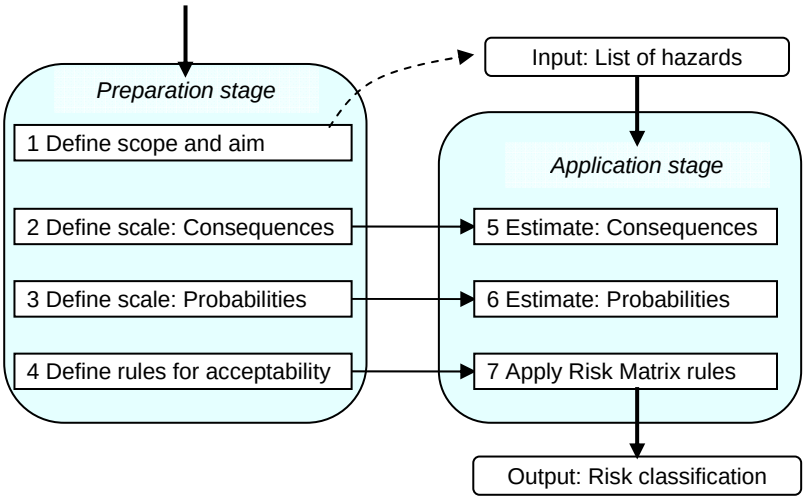


Figure 5.4 Procedure for applying Risk Matrix methodology

This lack of documentation might be explained by the assumption that the Risk Matrix approach is so simple that an exhaustive manual is not needed. Consequently, the Risk Matrix procedure varies a lot betwen different users and areas. This indicates that the application needs to be more systematic if you want reliable and reasonable results.

The block scheme in Figure 5.4 represents my interpretation of what should be considered. It contains two main parts. The *Preparation stage* includes the definitions and decisions that should be performed in advance. The *Application stage* concerns the the estimates and evaluations for each item in the input material.

The account below is a short manual for the application of Risk Matrix methodology. It is based on reviews of a number of applications, in which I have seen quite a lot of difficulties. The statements in the manual are intended to overcome some of these difficulties.

Preparation stage

At the preparation stage, a number of decisions are made concerning how the evaluation should be performed.

1. Define scope and aim

There are several issues that need to be considered before estimation starts:

- Establish whether it is enough just to consider the level of risk, or whether other factors must be included, e.g., legislation.
- Specify the types of problems to be estimated (hazards, quality problems, need for improved safety, etc.).
- Determine whether the estimates shall apply to the ranking of hazards and problems, or whether an absolute categorisation is needed.
- What are the demands for accuracy?
- What are the demands for transparency?
- Specify the source of and justification for the criteria of approval and acceptability.
- Stipulate how uncertainty in the estimates is to be handled.

2. Define scale: Consequences

There are several suggested units and scales for consequences, which might be used, directly or in adapted forms (see Table 5.6):

- Determine the types of consequences that are to be included, e.g., human injury, economic loss, and environmental damage.
- Choose the scale and units to be applied.
- Select the principle for selecting scenarios. Should the worst case be entered into the table, or the most likely outcome, or the whole range of possible negative consequences?

3. Define scale: Probabilities

The scale for probabilities is important. Of relevance are:

- Frequency (occurrences per time unit) or probability (occurrence related to a defined time period).
- The number of units. Should it be one device (or one workplace), or should it concern all devices (or all similar workplaces)? There is a huge difference between considering one item and thousands of items.
- The time period to consider. It can be a single work cycle, or the use of equipment on one occasion. A longer time perspective might be a year, or the several years that are linked to the entire life of the equipment.
- How an estimate of probability is to be obtained (from statistics, an educated guess, or something else).

4. Define rules for acceptability

Defining rules for acceptability has three major parts. The first is to choose categories of *risk statements*, examples of which can be found in tables 5.5, 5.8 and 5.9. The second defines the rule for how each combination of consequence and probability is to be obtained. The basic approach is to determine a level of risk for each cell in the matrix shown in Table 5.4.

A common alternative is to create a *risk value* by a mathematical rule, usually by multiplication of the scores for consequence and probability. The obtained value is compared with a numerical limit for what is acceptable. This means that the matrix format is not needed.

From a theoretical point of view, this can be seriously misleading if it is not done correctly. The reason is that the scales are often logarithmic, and you do not get the expected level of risk by multiplying logarithmic numbers (as some users might believe). The correct way is to add the logarithmic values so as better to represent the level of risk.

Application stage

At the application stage, the estimates are based on decisions made at the preparation stage. The items (usually hazards) are treated one by one.

5. Estimate: Consequences

It is fairly easy to define possible consequences, but when there is a range of alternative outcomes, it becomes more difficult. If you have to make a choice here, it is an advantage to note down the assumptions you have made.

6. Estimate: Probabilities

The estimation of probabilities is more problematic. Data are usually missing, which means that educated guesses have to be made on the basis of the available information. Assumptions about the situations involved have a major impact on the results, and they should be noted down when needed. An example is a specific human error that might have a serious effect. For example, you can assume that a job is done:

- By a specialist operator, or
- By anyone reasonably familiar with the task, or
- By a summer trainee

The estimate will be more complicated when the inputs to the evaluations are deviations or other problems, which is the case for FMEA (Section 12.2), Hazop (Chapter 9), and Deviation Analysis (Chapter 8). Then there is a triggering event, which might initiate a chain of subsequent events, and the outcome will also depend on which barriers are in place.

7. Apply Risk Matrix rules

In principle, this is the easy part, since the rules are clear and the estimates have been made. The output is an estimate of the level of risk of all the hazards, and also includes comparisons with limits for acceptability. It can be used in different ways:

- In a Risk Matrix, in which the identity numbers of the hazards are plotted. This gives a quick overview of the results (see the example in Table 5.5)
- In an analysis protocol, which shows the risk statements for each item (Low, Medium, etc.).
- In a ranking list of hazards based on their risk statements.

Table 5.5 Risk Matrix with plotted hazard identity numbers (1–12)

Probability	**Consequence**			
	Minor	Medium	Large	Catastrophic
Frequent	12	1		2
Probable	11			
Remote		3, 4		7, 8, 10
Very unlikely	5		6	9

Scales and categories

In applying the Risk Matrix principle, there is a need to establish suitable scales for the estimates. There are a number of published scales, and some might be useful directly. In the Preparation stage, an adaptation of the scales to the actual situation will be made.

Consequence categorisation

Table 5.6 provides examples of scales for consequences if a certain mishap or event occurs. It should be noted that some scales start with a low level of consequences, others with a high level.

- Example A is designed for occupational hazards, and is divided into six classes.
- List B has four classes, as suggested in a military standard (DoD, 2000). It is almost identical to a standard for railway safety (CENELEC, 1999), where *Insignificant* is used instead of *Negligible* for Category IV.
- Example C comes from an occupational health standard (BSI, 2004, p. 49), and has three classes.

Table 5.6 Examples of the categorisation of consequences

Example A	
Code	*/ Category*
0	Not harmful or trivial
1	Short period of sick leave
2	Long period of sick leave
3	Disablement
4	Fatality
5	Several fatalities, major disaster

Example B	
Code	*/ Category*
I	Catastrophic
II	Critical
III	Marginal
IV	Negligible

Example C
Severity of harm
Slight harm
Moderate harm
Extreme harm

Types of consequences are also relevant, and it is most common to consider human life and health (examples A and C). It is also possible to include disturbance to production, monetary loss, and damage to the environment or property (compare with Table 5.1). Example B has been used in cases with several types of consequences.

Frequency categorisation

Another type of estimation concerns the likelihood of occurrence, and there are a number of published categorisations. Table 5.7 shows two examples of scales, one starting with high probabilities, the other with low.

Table 5.7 Examples of the categorisation of frequency of occurrence

Example D	
Code /Category	
Frequent	Likely to occur frequently. The hazard will be continually experienced.
Probable	Will occur several times.
Occasional	Likely to occur several times.
Remote	Likely to occur sometime in the system life cycle.
Improbable	Unlikely to occur, but possible.
Incredible	Extremely unlikely to occur. It can be assumed that the hazard may not occur.

Example E
Likelihood of harm
Very unlikely
Unlikely
Likely
Very likely

Example D is a slight simplification of a military standard (DoD, 2000), which is similar to the railway standard (CENELEC, 1999). In both standards, the recommendation is to make estimates for the whole system, such as the frequency of occurrence of a hazardous situation in a railway system. The DoD (2000) has defined two columns: one for a *Specific Individual Item*, the other for a *Fleet or Inventory*.

The other example (E) is based on an occupational health standard (BSI, 2004, p 49), and has four classes. Note that this example has a rising order in contrary to the other.

Factors in probability estimates

The European Standard (EN 1050, 1996), Safety of machinery – Principles for risk assessment, suggests a more detailed way of estimating probabilities. The standard states that:

> "The risk associated with a particular situation or technical process is derived from a combination of the following elements:
> - the severity of harm;
> - the probability of occurrence of that harm, which is a function of:
>
> a) the frequency and duration of the exposure of persons to the hazard;
>
> b) the probability of occurrence of a hazardous event;
>
> c) the technical and human possibilities to avoid or limit the harm (e.g., reduced speed, emergency stop equipment, enabling device; awareness of risks)."

These factors are key components of risk, but no scales or values are recommended, and it is not described how estimates should be made.

Evaluation output categories
The Risk Matrix has a number of outputs, which we can call evaluation categories. The simplest set is:

- Acceptable (or Tolerable)
- ALARA (As Low As Reasonably Achievable)
- Unacceptable (or Intolerable)

A similar example (Table 5.8) can be taken from the rail industry (CENELEC, 1999), which has four categories. It is interesting to note that the Railway Authority is given a key role in the evaluation of risk.

Table 5.8 Categories of actions based on risk information (CENELEC, 1999)

Risk evaluation	Risk reduction/control
Intolerable	Shall be eliminated
Undesirable	Shall only be accepted when risk reduction is impracticable*
Tolerable	Acceptable with adequate control*
Negligible	Acceptable without any agreement

* and with agreement of the Railway Authority

Another way of proceeding is to evaluate whether or not a safety improvement is needed. An example was presented in Table 5.2, which is based on a work environment standard (BSI, 2004). Another (Table 5.9) is taken from a guide for shipping operations (IACS, 2004), which has a similar classification.

Comments on the Risk Matrix

The Risk Matrix has obtained great popularity in many areas. There are several ways of applying the methodology, and it is difficult to find a clear and complete guide in the safety arena.

The method is usually regarded as simple, but can often be complicated and difficult. This is discussed further in Section 5.6. The Risk Matrix is useful in the right circumstances, especially when there is a clear source of risk and a fairly straightforward path to injury and damage. When there are demands on quality and trustworthiness, you need to plan thoroughly before you start.

Table 5.9 Categories of actions based on risk information (IACS, 2004)

Risk level	Action
Trivial	No action is required
Tolerable	No additional controls are required. Monitoring is required to ensure control is maintained.
Moderate	Efforts are required to reduce risk. Controls are to be implemented within a specified time.
Substantial	New work not to start until risk reduced. If work in progress, urgent action to be taken. Considerable resources may be required.
Intolerable	Work shall not be started or continued until the risk has been reduced. If reduction is not possible, the activity shall be prohibited.

5.5 Other evaluation approaches

In this chapter a number of evaluation principles have been described. Two alternative approaches are presented in this section, which can be useful in certain situations.

Compare systems

Assume a situation where an existing system is to be replaced by a new or redesigned one. This is common since we know that changes take place all the time. One application is in a situation where a safety criterion is that the new system shall be at least as safe as an earlier or comparable system.

The aim of a comparison evaluation might be to judge whether or not the new system is safer. The general methodology has four steps:

1) Select the functions and/or characteristics to be compared.
2) Compare the risk level of each item in the new and the old system.
3) Evaluate the results and draw conclusions.
4) Propose possible actions if needed.

The selection of items to be compared can focus solely on the parts that might be affected by the changes. An alternative is to use the comparison judgements in a common method, such as Energy Analysis or FMEA.

The comparison can be based on estimates of probabilities and consequences. An alternative is to use a simple scale to make a combined judgment:

a) Decreased risk
b) Same risk
c) Increased risk

Relevance judgement

In the planning of a new system, or when changes are foreseen, the information may be flimsy or very uncertain. Only a coarse specification might be available, and the knowledge of the system and its future might be limited.

Even in situations of this kind, it can be useful to perform a safety analysis in order to identify future risks. One approach is to evaluate the relevance of potential risk sources. The aim is to indicate the hazards and problems that need to be carefully considered in future planning and design, so that they do not have serious consequences in the final system.

Assume a project development. A number of potential hazards and serious problems can be expected, but it is hard to know how they will appear in the future system. As a first step, a coarse analysis is performed. A number of risks are identified, and these are summarised in a *risk list*. Each item in the list is judged according to whether it should be considered in the detailed design later in the project. A categorisation can be made, as in Table 5.10. A high score for an item means that it should be considered throughout development.

Table 5.10 Scale for the categorisation of relevance

Code	Relevance	Comment
0	No relevance	Risk is negligible
1	Low	No special checks are needed
2	High	The item shall be checked when important decisions in the project are made
3	Very high	The item shall be considered carefully throughout the project

The relevance principle is oriented towards risk management and control. It was first developed for road construction, which has a planning period of many years (Hult & Harms-Ringdahl, 2000). The methodology has also been applied for risk identification and risk control in a large railway project in northern Sweden (Hult, 2000).

5.6 Critical issues

General

The aim of this section is to discuss problems with and the practical applications of evaluation. In the scientific literature, probabilistic approaches are well-described, and there is extensive development and debate (e.g., Aven, 2008B). This book will not go in depth into this specialised field; instead, we adopt a more general perspective.

The term *risk* was briefly defined in Section 3.1. The concept has several meanings, which are applied differently among users. This can cause problems in evaluation situations, if they are not clarified.

A general view is that a risk is acceptable if it is balanced by a larger advantage (cf. the ALARA principle). One difficulty here is that the party exposed to risk (person, group, or organisation) may be different from the party gaining the advantage. This is reflected in a recent standard (ISO, 2009B) for risk management.

The actors who do the evaluation will be influenced be their specific interests. This means that different values among the parties concerned are natural, and also may give rise to conflicts. If decisions are to be fair and sufficiently correct, an evaluation needs good quality and transparency. This can be aided by a good logical structure and a well-defined evaluation process.

An important issue is that evaluation is usually limited to a function of probabilities and consequences, which represents an estimate of a future loss. In reality, there are many other aspects to consider (as discussed in Section 5.1).

Estimates of frequencies and consequences can be helpful, but my experience is that the majority of hazards lie in the intermediate zone between clear acceptance and obvious danger. This means that the ALARA principle, or something similar, needs frequently to be applied.

Evaluation failures

Evaluation is a difficult task, and two general types of failures are rather obvious:

- ***Underestimating the risk.*** This entails that the hazard is rated too low, and risk-reducing countermeasures are not taken.
- ***Overestimating the risk.*** The hazard is rated too high, which entails that resources for countermeasures are used in an inefficient way.

Uncertainties in the data

In strict quantitative assessments there are techniques for handling uncertainties. Also, in semi-quantitative estimates, uncertainties and insufficient information can be major problems. As far as I can see, accounts of the Risk Matrix technique have not given any advice on how to handle uncertainty. In Direct Risk Evaluation (see Section 5.2), the issue of uncertainty is specifically addressed.

Problems with the Risk Matrix

Initial reflections

In technical publications (standards, regulations, descriptions of praxis) the Risk Matrix approach predominates. The Risk Matrix is the most common method of risk evaluation, and seems to be regarded as simple and reliable. However, it does have some difficulties, which have not received much attention. It is important to be aware of them when an evaluation method is chosen.

I have studied a number of applications of the Risk Matrix, and my general impression is that most users apply the method without referring to any manual or guidelines. They rely on implicit assumptions, which they presume to be shared by everyone. This means that the practical way of making the estimates seldom was clarified. Lack of motivation in arriving at estimated values is more the rule than the exception. There are few or no explanations of:

- How the method was used
- The meaning of the scales for probability and consequence, and their origins
- The criteria for tolerable and intolerable, and who has determined them

Another implicit assumption in using the Risk Matrix is that only probability and consequence values are considered. Sometimes, this limitation is clearly formulated (e.g., ARA, 2009, p. 100): “Low – the risk is acceptable without restrictions”. A number of other factors are described in Section 5.1, some of which cannot be disregarded. If you do disregard them, the evaluation will sometimes be completely misleading.

Small and large risks

Some problems are related to how *size* is considered in the evaluation:

- Level of detail in the analysis
- Range of consequences
- Addition of small risks
- Wrong conclusions

The level of detail of the analysis will affect the results (ISO, 2009C, Annex B). A detailed analysis will give a larger number of scenarios, each with a lower probability. This will underestimate the actual level of risk. The way in which scenarios are grouped together in describing risk should be consistent, and defined at the start of the study.

A specific event or failure can result in a range of potential scenarios with varying consequences and probabilities. The selection of scenarios will strongly affect the result of the evaluation. Alternative scenarios are more fully described in the description of Event Tree Analysis (Section 12.3).

Another aspect is that several hazards can be categorised as having a minor level of risk, but jointly they might add up to be an important source of damage.

A worrying observation is that evaluators sometimes instinctively assume that a large consequence is automatically related to a low probability, as if that is a law of nature. It is not. This is just wishful thinking, and it can be really dangerous in situations where a large consequence is feasible.

Carvalho and Melo (2013) have compared results from a set of hazard scenarios using the Risk Matrix approach. Around 40 people independently estimated consequences and frequencies. It was found that there was little agreement between them, which means low *inter-rater reliability*. Different analysts can attain varying results and draw contradictory conclusions, due to difficulties in making objective judgements, which supports the recommendation that estimates should be made as a form of teamwork.

"What's Wrong with Risk Matrices?"

This is the title of an article by Cox (2008). He states that little research has rigorously validated the performance of risk matrices in improving risk management decisions. The article explores the mathematical and logical qualities of risk matrices as sources of information for risk management, decision-making, and priority setting. Cox (2008) found limitations related to:

- *Poor resolution.* Typical risk matrices can correctly and unambiguously compare only a small fraction (less than 10%) of randomly selected pairs of hazards. They can assign identical ratings to quantitatively very different risks (*range compression*).
- *Errors in assigning ratings*. For risks with negatively correlated frequencies and severities, they can be "worse than useless".
- *Suboptimal resource allocation.* Effective allocation of resources to risk-reducing countermeasures cannot be based on the categories provided by risk matrices.

- *Ambiguous inputs and outputs*. Categorisations of level of risk cannot be made objectively for uncertain consequences. Inputs to risk matrices (e.g., frequency and consequence categorisations) and resulting outputs (i.e., risk ratings) require subjective interpretation.

This is severe criticism, and Cox (2008) suggests that risk matrices should be used with caution, and only with careful explanations of embedded judgments.

Summary of problems
A number of weaknesses have been mentioned in this section. Table 5.11 presents a summary of these.

In conclusion

On many occasions, the Risk Matrix can be a useful tool, which is reflected in its great popularity. However, this section has also demonstrated a number of problems central to the Risk Matrix approach.

A conclusion is that risk matrices should be used with caution, and with careful explanations of procedure, assumptions and facts. If this is not done, the results can sometimes "be 'worse than useless' leading to worse-than-random decisions" to cite the forceful conclusion of Cox (2008).

Sometimes, unformulated foundations and unclear work procedures will cause quality and reliability problems. Section 5.4 on the *Risk Matrix procedure* represents a simple attempt to deal with some of the problems that may be encountered in applying the Risk Matrix method.

There appears to be a need for more extensive research and development in the field. The validity and reliability of risk matrices and other evaluation techniques have not been studied enough. How a Risk Matrix is used will have a large impact on safety and system performance in numerous workplaces and systems.

Table 5.11 Summary of Risk Matrix problems

	Problem	**Comments**
1	Limited scope in only considering probabilities and consequences	Can, for example, lead to regulations being neglected (see Section 5.1).
2	Unreserved recommendations for use by, e.g., authorities	The results might be approved without criticism, which sometimes is problematic.
3	Performance of the Risk Matrix has not been generally validated	Little research has rigorously scrutinised the theoretical basis, and practical results.
4	Mathematical weaknesses limit the results	See results from Cox (2008) above. Can entail ineffective allocation of resources.
5	Over-confidence in results from the Risk Matrix	Results can sometimes be seen as the truth, or even as scientific by unaware users. The status of mathematical science has been undeservedly assigned to the application.
6	The working procedure is usually unsatisfactorily defined	Can give varying ways of working and unreliable results. The procedure is in reality fairly complex (see Section 5.4).
7	User bias in the estimates influences the results	Such bias can be conscious or instinctive; it is not always obvious.
8	Errors in estimates might be common	Sometimes, excessive risks are accepted, or small risks rejected (meaning that resources are spent inefficiently).
9	The treatment of uncertainties is unclear	There is no self-evident way of dealing with uncertainties in estimates of consequences and probabilities.
10	Low inter-rater reliability	Different analysts can generate divergent results and different conclusions, due to subjective judgements.

6 Energy Analysis

6.1 Principles

Energy Analysis is based on a simple idea: for an injury to occur, a person must be exposed to an injurious influence – a form of *energy*. This may be a moving machine part, electrical voltage, etc.

In using this method, the concept of energy is treated in a wide sense. Energy is something that can damage a person physically or chemically in connection with a particular event. An injury occurs when a person's body is exposed to an energy that exceeds the threshold of the body. The purpose of the method is to obtain an overview of all the harmful energies in an installation.

The approach of seeing energy as a cause of injury was first developed by Gibson (1961) and Haddon (1963). The concept has proved useful, and has been further developed and discussed in many books and reports (e.g., Hammer, 1972; Haddon, 1980; Johnson, 1980). An additional suggestion is how the analytic procedure can be broken down into a number of defined stages (Harms-Ringdahl, 1982).

Thinking in energy terms is based on a model that contains three main components:

1) *That which might be harmed*, usually a person but it could be equipment or industrial plant.
2) *Energies*, which can cause harm.
3) *Barriers*, which prevent harm from being caused, such as safeguards for machinery.

In the model, an injury occurs when a person or object comes into contact with a harmful energy. This means that the barriers have not provided sufficient protection. Harmful energy can take on many forms, such as an object at a height (from which it may fall) or electrical voltage, i.e., energies in a traditional sense. Table 6.2 provides a summary of different kinds of energies.

One essential part of the energy model is the concept of barriers. These will prevent the energy from coming into contact with the person and/or cause injury. Table 6.3 shows various safety measures that might prevent accidents from occurring due to the release of energies. These measures can also be seen as barriers.

6.2 Energy Analysis procedure

An Energy Analysis has four main stages, and also involves preparing and concluding the analysis (see Figure 6.1). It is usually best to complete each stage before moving on to the next. As an aid to analysis, a specially designed record sheet can be used.

Prepare

Before embarking on the analysis itself, a certain amount of preparation is required. This concerns a delimitation of the object, which may be a single machine, a workplace, or a whole factory. During preparation, other clarifications may also be needed, e.g., concerning what assumptions should be made about the machine. Such preparation is similar to that used in other methods of safety analysis (as discussed in Chapter 3).

One essential aspect is to obtain information about the installation being considered. For Energy Analysis, this can consist of technical drawings and photographs. If the installation already exists, you can just go round and look at it.

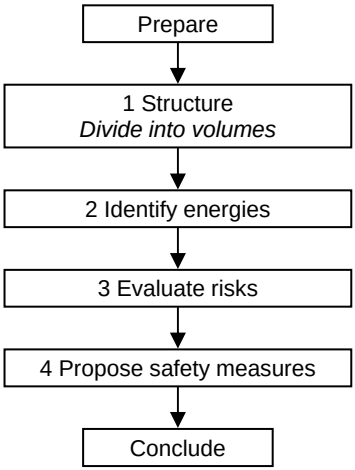


Figure 6.1 Main stages of procedure in Energy Analysis

1 Structure

The purpose of the structuring stage of the analysis is to divide the system into suitable parts, which are then analysed one at a time. In this method, structuring is performed in accordance with the physical layout of the installation under study. In principle, the plant or equipment is divided into *volumes* (spatial segments). If the analysis is applied to a production line, it

is appropriate to go from one end of the line to the other. The installation can be envisaged as being divided up into boxes.

After structuring, a check should be made as to whether any component has been omitted or forgotten in some way. Good praxis is to have a general volume, called something like *General*, *Surrounding area*, or the *Whole room*. This volume might also be associated with the energies that affect most volumes, such as electricity, pressurised air, and traffic.

2. Identify energies

For each box or volume, sources and stores of energy are identified. The checklist of energies shown in Table 6.2 can be used as an aid.

3. Evaluate risks

Each identified source of energy is evaluated. This can be done in different ways, as discussed in Chapter 5. The method itself does not prescribe what kind of evaluation should be made. A simple approach is to apply *Direct Risk Evaluation* (Section 5.2). Table 6.1 shows an adaption of the principle for Energy Analysis.

An alternative is to apply the *Risk Matrix* (Section 5.4). In any such evaluation you need to consider that a specific energy may have a variety of consequences, and you need to decide how to handle this. There is also a need to consider the presence and effectiveness of barriers, which will affect the seriousness and likelihood of injuries.

Table 6.1 Direct risk evaluation scale applied in Energy Analysis

Code	Description	Comment
0	No need for improvement	Energy cannot cause any significant injury
1	Safety measure* can be considered	Energy can cause injury, but barriers are adequate
2	Safety measure recommended	Energy can cause injury and barriers are inadequate
3	Safety measure is imperative	Serious consequences and inadequate barriers
4	Intolerable, correct before start	Serious consequences and immediate danger

*Safety measure includes improving knowledge and further investigation

4. Propose safety measures

At the next stage, a study is made of the energies for which safety measures are required. Questions are raised how risks can be reduced. Table 6.3 shows a methodology that can help in finding safety measures. Can a particular energy be removed or reduced? Can safety devices be installed? It is good to be able to suggest a variety of solutions, since it is not certain that the first will be the most effective.

Conclude

The analysis is concluded by preparing a report, which summarises the analysis and its results. It might contain descriptions of the limits and assumptions of the analysis, the most important energies, and proposals for safety measures. Sometimes, a record sheet might suffice.

Energy checklist

Table 6.2 shows a checklist§ of different types of energies. It is designed for use as an aid to identification. For most categories, the link between energy and injury is obvious. But some types of energies may require further comment.

Chemical influence (Category 8) is treated as an energy that might give rise to injury. In some cases, it is possible to conceive of this influence in terms of the chemical having a micro-level effect on human cells. *Asphyxiating* chemicals are gases or liquids that are not poisonous in themselves, but which restrict or eliminate access to air. This subcategory might refer to the possibility of being exposed to a suffocating gas or of drowning in water.

The final category on the checklist is headed *Miscellaneous*. It is included to provide an additional check on the identification of hazards – and it goes a little bit beyond the pure energy concept. *Human movement* might involve the risk of falling, stumbling, colliding with protruding objects, etc. *Static load* may help to identify work situations where a person is operating in a poor ergonomic position.

The *Sharp edge* and *Danger point* subcategories can be seen in terms of energy concentrations when a person or piece of equipment is in motion. *Enclosed space* can be used as an extra check. There might be overpressure, toxic gases, etc., which are not normally dangerous but could be under unusual circumstances.

The energy list contains a few deliberate inconsistencies. Some categories do not refer to energies in a physical sense, but they have a clear relationship with them. For example, *Collapsing structure* (under Category 1) may apply where the object under study is a heavy installation (such as a liquor tank). The energy in question is the potential energy of the tank, but

the keyword is related to a consequence. Similarly, the subcategory *Handling, lifting* is used to cover the potential and kinetic energy of a manually handled object. The idea is that problems related to the handling of materials can also be treated at the identification stage.

Table 6.2 Checklist for Energy Analysis

1. POTENTIAL ENERGY	**6. HEAT & COLD**
Person at a height	Hot or cold object
Object at a height	Liquid or molten substance
Collapsing structure	Steam or gas
Handling, lifting	Chemical reaction
	Condensed gas (cooled)
2. KINETIC ENERGY	**7. FIRE & EXPLOSION**
Moving machine part	Flammable substance
Flying object, spray, etc.	Explosive: material, dust, gas, or steam
Handled material	Chemical reaction, e.g., exothermic
Vehicle	combinations or impurities
3. ROTATIONAL MOVEMENT	**8. CHEMICAL INFLUENCE**
Machine part	Poisonous
Power transmission	Corrosive
Roller/cylinder	Asphyxiating
	Contagious
4. STORED PRESSURE	**9. RADIATION**
Gas	Acoustic
Steam	Electromagnetic
Liquid	Light, incl. infra and ultra
Pressure differences	Ionised
Coiled spring	
Material under tension	
5. ELECTRIC	**10. MISCELLANEOUS**
Voltage	Human movement
Condenser	Static load on an operator
Battery	Sharp edge
Current (inductive storage and heating)	Danger point, e.g., between rotating rollers
Magnetic field	Enclosed space

Energy-based safety measures

One important advantage of Energy Analysis is that it gives systematic support for developing safety measures (Haddon, 1980; Johnson, 1980). Table 6.3 provides a strategy in ten points for finding safety measures based on the energy model.

Table 6.3 Checklist for safety measures using Energy Analysis

Safety measure	**Examples**
The energy	
1. Eliminate the energy	Work on the ground, instead of at a height Lower the conveyor belt to ground level Remove hazardous chemicals
2. Restrict the magnitude of the energy	Lighter objects to be handled Smaller containers for substances Reduce speed
3. Safer alternative solution	Less dangerous chemicals Handling equipment for lifting Equipment requiring less maintenance
4. Prevent the build-up of an extreme magnitude of energy	Control equipment Facilities for monitoring limit positions Pressure relief valve
5. Prevent the release of energy	Container of sufficient strength Safety railings on elevated platforms
6. Controlled reduction of energy	Safety valve Bleed-off Brake on rotating cylinders
Separation	
7. Separate object and energy:	
a) in space	One-way traffic Separate off pedestrians and traffic Partition off dangerous areas
b) in time	Schedule hazardous activities outside regular working hours
8. Safety protection on the energy source	Machine safeguards Electrical insulation Heat insulation
Protection of the object	
9. Personal protective equipment	Protective shoes, helmets.
10. Limit the consequences when an accident occurs	Facilities for stopping the energy flow Emergency stop Emergency shower facilities Specialised equipment for freeing a person (if stuck)

6.3 Example

In this example, a tank for the storage of sodium hydroxide (lye) is to be acquired. There is a desire to make a preliminary assessment of the hazards involved. A starting point is a sketch of the installation, which provides the basis for a simple Energy Analysis.

System description

Concentrated lye is to be stored in a stainless-steel tank. At lower temperatures the lye is viscous, and heating equipment using an electrical current is needed. The tank is filled using a tube equipped with a valve. On top of the tank there is a manhole and a breather pipe. Under the tank there is a pit. A ladder has been permanently installed to provide access to the tank. Not visible on the sketch (see Figure 6.2) is a tube with a tap, used to evacuate the liquid.

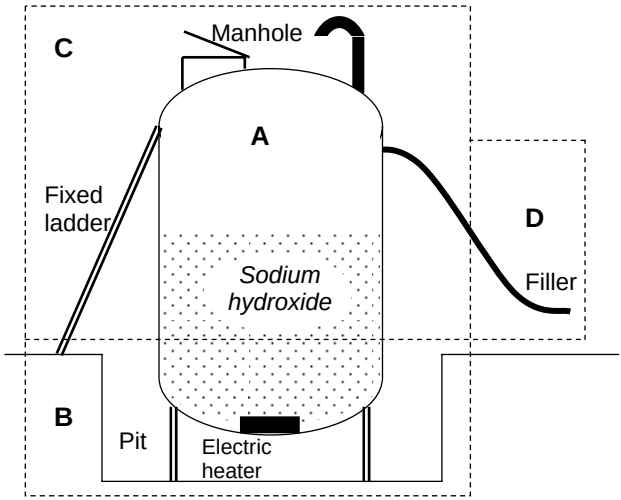


Figure 6.2 Liquor tank

Preparing

Our start material consists of the sketch and the description above. The limits of the system are set by what is visible on the sketch. The aim of the analysis is to get an overview of potential hazards based on the outline of the system. The result will be used in the detailed design in order to obtain an installation that is sufficiently safe. Table 6.4 shows an excerpt from the record sheet used.

Analysis

1. Structure

A classification is made into four volumes, as shown in Figure 6.2:

A. The tank
B. The pit (the space under the tank)
C. The area surrounding the tank
D. The filler tube and its surroundings

2. Identify energies

Let us start with the tank (Volume A) and follow the checklist (Table 6.2). First, there is *Potential energy* (1).

- *Person at a height* will be relevant when someone is working on the tank and also goes down into the tank for servicing.
- The level of the liquid is above that of the tapping-off tube. If the valve is opened or if a connecting tube fails, the lye will run out.
- The tank has great mass. It requires stable supports (*Collapsing structure*).

Then, *Stored pressure* (4) may be relevant. If the ventilation system fails, there will be high pressure when lye is pumped in, and the whole tank might burst. This could occur if the manhole and the ventilation pipe on top are closed. When tapping-off lye there may be low pressure, but this is usually not harmful. (The pressure of liquid was earlier treated as a form of potential energy.)

Electric (5) refers to the electric-power supply to the heating element. Insulation failure is hazardous. Lye is electrically conductive.

Heat & cold (6) applies to the heating element. Over-heating might occur if the liquid level is low, or electric power is not turned off correctly

Chemical influence (8) is obviously relevant because lye is highly corrosive. It is certainly the most obvious and the greatest hazard in the system.

The *Miscellaneous* (10) category provides an opportunity for a variety of items to be taken up. It is not necessary to think strictly along energy lines. For example, one might wonder about the manhole. It has to be large enough, and there must also be space for a ladder.

Then we continue with Volume B (the pit) and the remaining volumes.

3. Evaluate risks

The risks are evaluated, and the approach with Direct Evaluation was chosen. The scale in Table 6.1 is used. The assessments are shown on the record sheet (Table 6.4), and the judgement in this example reflects the thoughts of an imaginary study team.

4. Propose safety measures

In proposing safety measures, you can go through the record sheet line by line (Table 6.4). For each item evaluated as *2* or *3*, one or more proposals can be made. The checklist in Table 6.3 can support a systematic approach to getting ideas for improvements.

An alternative is to first group similar energies in categories, and then work with each category. One example is lye, which comes up at several places in the analysis. The different proposals can be combined in to a "lye package", which includes technical and organisational suggestions.

It can be difficult to make concrete safety proposals for some hazards. In such cases, it might then be stated, for example, that job routines must be established or that a further investigation needs to be carried out. An important alternative is to note that no solution has been found, but that the problem still requires attention.

The list below shows the results after the checklist for safety measures has been applied. It starts with three questions that ought to be discussed before the final decision on design.

Safety measure rule	**Concrete solution**
1. Eliminate	Can lye be removed from the process?
2. Restrict	A smaller tank?
3. Safer alternative solution	Can the lye be replaced by another chemical, or can a diluted mixture be used?
4. Prevent build-up	Safety guard to prevent over-filling
5. Prevent release	Secure connection for hose on filling Method for emptying the filler tube after use
6. Control reduction	Overflow facilities in case of over-filling
7. Separation	Prohibit unauthorised entrance and fence off the area
8. Safety protection on the object	Keep the filler tubes in a locked cupboard
9. Personal protective equipment	Protective clothing

10. Limit the consequences	Emergency shower facilities Water for flushing Draining facilities Emergency alarm First-aid facilities Make the pit under the tank sufficiently large

Concluding
After completing the analysis, a summary is prepared. In this case, it will contain a list of recommendations to be applied during continuing design and planning. In writing the final report, it may be attractive to combine the various proposals in order to get a structured set instead of taking them one by one.

Remarks
The results of the analysis are not remarkable, but they provide a more complete picture than otherwise would have been available. In this example, it would have been possible to stare blindly just at the hazards created by the lye itself. As a consequence, only some of the problems would have come to light. A more extensive analysis would have dealt with situations that arise in the course of re-filling the tank, etc. Therefore, in this case, a supplementary method should be employed.

6.4 Comments
A simple method
The method is straight-forward, and, with a little experience, it is simple and quick to use. Two checklists (tables 6.2 and 6.3) provide support for the identification of hazards and the creation of ideas. After some practice, the lists can be used more freely, and are not needed for every detail.

The identification stage can be completed in just one or a few hours, even with quite large systems. Examples of pitfalls when using Energy Analysis:

- Some *volumes* are missed, especially energies just outside the studied object.
- Too much time is spent on details, e.g., trivial energies.

One issue is to determine the lowest level of energy with which the analysis should be concerned. In principle, anything that can lead to an injury to a human being could be included. There is a trade-off between comprehensive coverage of hazards and the avoidance of trivia.

Using a record analysis sheet helps in performing the analysis. It is advisable to use the concrete words with which a specific energy is concerned. Simply repeating the names of categories on the checklist should be avoided. For example, *lye* and not just *corrosive substance* should be written, and *tool at a height* should be entered rather than *object at a height*. It is also good to note the magnitude of the energy, e.g., how many metres, or weight in tons. This will help in the assessment of risks.

The most practical way of proceeding is to identify energies in all volumes before embarking on the next stage of the analysis. This permits a better overall picture to be obtained and a more consistent form of risk evaluation to be applied.

Ideas for safety measures

In order to generate ideas for safety measures, it is best to think freely and try to come up with as many as possible. The checklist is designed as an aid to the imagination and a means of getting away from rigid lines of thinking. It is meant to provide different angles of approach. When a body of ideas has been built up, then the process of sifting through and improving the ideas can begin.

Energy magnitudes

In many cases, it is possible to specify the magnitude of an identified energy e.g., in terms of its height, weight, or speed. This provides a more concrete basis for the assessment of risk. Let us look at some examples.

Person at a height

A person working at a height can fall down and get injured. The consequences can vary a lot depending on the circumstances. I have seen rules stating that protection or railings should be used above a certain height. However, the height has ranged from 0.5 to 2 metres depending on the source and the situation.

Speed

High speed can easily cause injuries. One simple approach is to transform the energy of the moving object into its equivalent height (h_e). Based on velocity (v), and standard gravity (g), we get $h_e = v^2/2g$. A speed of 10 km/h will then correspond to a height of 0.4 metres, and 30 km/h is equivalent to 3.5 metres.

Rotation

The energy in a rotating object can cause great damage if it comes loose. Again, the energy can be converted into height. The basic parameter is the

circumferential velocity (v_c), in metres per second. For a cylinder with most of the mass on its periphery, the equivalent height is $h_e = v^2/2g$. For a solid cylindrical object, the height (h_e) is half of that.

What does this mean? Let us take the example of a paper-rolling machine. Paper is wound onto a reel, which may be rolled at a speed of 2000 metres/minute. The equivalent potential energy is that of mass at a height of 28 metres, and a reel can weigh up to several tens of tons.

Explosions

Chemicals can contain considerable amounts of energy. At some installations, the risk of explosions is critical, and it should be detected and kept under strict control. The task of Energy Analysis is to identify the existence of materials with the potential to cause explosions. If they do exist, good risk control is needed. The role of the evaluation would then be to assess whether the control is adequate.

For *flammable gases*, small leakages are enough to cause a problem, and for example propane, the lower limit of ignition is around 30 mg per litre of air.

A *dust explosion* can occur when a combustible material is spread as small particles or dust. A small amount of dust (around 1 mm thick) might cause an explosion if it is mixed with air. A rule of thumb is that, if you cannot distinguish the colours under a layer of dust, there is a potential danger.

Table 6.4 Part of record sheet from the Energy Analysis of a tank with lye

Volume / Part	**Energy**	**Hazard /** *Comments*	**Evalu-ation**	**Proposed measures**
A. Liquor tank	Person at a height (4 metres)	Falls down / *During service*	2	Routines for service
	Level of lye	Contact with lye / *Lye can run out*	3	"Lye package"
	Weight of tank (10 tons)	Falls or collapses / *If damaged or poor design*	1	(Standard construction)
	Excessive pressure	Tank rupture / *On filling*	0	(Good ventilation exist already)
/Heating system	Electric (380 volts)	Shock / *If poor insulation, lye is conductive*	2	Check proposed installation
	Heat	Burn injury	1	
/General	Lye (10 tons)	Injury to eyes and skin, corrosive	3	"Lye package"
B. Pit	Height (2.4 metres)	Falls	3	Railings and fixed ladder
/Heating system	See above	–	-	
C. Outside tank	Person on platform or ladder	Falls	3	Suitable design of platform, railings and fixed ladder
	Tools and equipment at a height	Fall on people below	2	As above
D. Filler tube	Level of lye	Contact with lye remaining in tube	3	"Lye package", routines, and lock

For the evaluation scale, see Table 6.1.

7 Direct Hazard Analysis

7.1 Principles

One approach to analysing a task or a procedure is to focus directly on the injuries or damage that might occur. This straightforward principle underlies what is here called Direct Hazard Analysis, which includes a few different methods. These methods are not based on any explicit model of how accidents occur. The object of an analysis can be almost any type of activity, e.g., a job at a factory, nursing at a hospital, or children studying in school. Such an activity is here called a *procedure*; it is usually organised in one way or another, but this is not an essential requirement.

The best known example in this category is Job Safety Analysis (JSA). Actually, this chapter describes a generalisation of this method, involving the extension of JSA to other applications. JSA and other examples are described below.

Analytic procedure

A complete Direct Hazard Analysis has four main stages, plus a preparatory and concluding part. The procedure for analysis is shown in Figure 7.1.

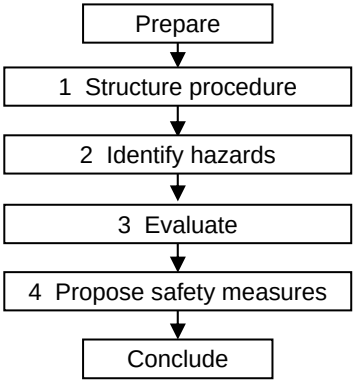


Figure 7.1 Main stages of procedure in Direct Hazard Analysis

Prepare

It is essential clearly to define the object to be analysed, and specify what the analysis shall include and exclude. The preparation stage also includes formulation of the aim of the analysis.

1 Structure procedure
The aim of the structuring stage of the analysis is to describe and clarify the procedure. It includes a division of the procedure into suitable parts, which are then analysed one at a time. The result is a list of activities to be analysed further.

2 Identify hazards
The aim is to identify hazards that might cause injuries, and the result is a list of potential injuries. The method can be extended to the identification of other types of damage, such as halts to production, damage to equipment, and so on.

Table 7.1 Checklist for types of injuries (after EU, 2002)

Type of injury	**Example**
Fall	- at same level - from height
Hit by contact with	- moving object (vehicle, etc.) - static object - person (intentional or unintentional) - animal
Crushing and cutting	- pinching or crushing - cutting or clipping - tearing - bite/sting by animal/human/insect
Suffocation	- drowning - other suffocation
Chemical effect	- corrosion - poisoning
Thermal-effect injuries	- hot object, liquid, steam - open fire, flames - cold, cooling
Electricity and radiation	- electricity - light - sound - vibrations - other radiation (ionising and non-ionising)
Acute overexertion of body	
Mechanism of injury, other	

At the identification stage, each activity on the list is investigated. A checklist of hazards or types of injury is useful. The content of such a list might vary, depending on what is being investigated. A general checklist is

shown in Table 7.1, which is a simplification of a taxonomy for the coding of home and leisure accidents (EU, 2002).

There, the reference is to "Mechanism of Injury Codes", which appear to combine medical aspects and energies. One advantage is that injury statistics are often based on a similar classification, and these statistics can be used at the evaluation stage. An alternative, which can be seen quite often, is to use a checklist of energies, such as the one shown in Table 6.2.

3. Evaluate

The list of hazards might be long. The aim of the evaluation stage is to set priorities and judge which hazards need special considerations. Each hazard on the list is evaluated, which can be done in different ways, as discussed in Chapter 5. The method does not presuppose a specific solution for this. A simple approach is to apply *Direct Risk Evaluation* (Section 5.2).

One way is to apply the *Risk Matrix* (Section 5.4). The scale for classification of consequences in Table 5.6 can then be used. When using the matrix, the likelihood of injuries also needs to be estimated. The matrix approach is more motivated when the analysis deals with a fairly general object, such as *children in school* or *football training*. Statistics on injuries may then be useful.

4. Propose safety measures

At the next stage, a study is made of the hazards for which safety measures are required. For Job Safety Analysis (Section 7.2), there is a checklist that can be used for finding improvements, and which might be useful in other applications. A common experience is that when a safety problem is well-defined, it is fairly easy to find improvements, especially if a work group has been engaged.

Conclude

The analysis ends with a summary of results and a set of conclusions. Usually a written report is the best way to distribute findings and get results in form of safety improvement activities.

Comments

In the analysis, the list of hazards may be long, and it might be practical to use a record sheet. One example, for Job Safety Analysis, is shown in Table 7.2.

The Direct Hazard Analysis method is generic, and the principle that underlies it can easily be adapted for special applications. In particular, the checklist for identification needs to be tailored to suit the situation.

7.2 Job Safety Analysis

General

Job Safety Analysis (JSA) is one of the oldest and best known methods for the analysis of hazards. Several descriptions of the method have been published (e.g., Grimaldi, 1947; McElroy, 1974; Heinrich et al., 1980). Several variants are in circulation, and nowadays a number of descriptions are available on the web. Sometimes, it is called Work Safety Analysis instead. The method is not based on a clear accident model. However, its perspective is fairly close to that of the energy model, and some descriptions of the method contain checklists of different energies.

In Job Safety Analysis, attention focuses on the job tasks performed by a person or group. The principle is to divide a job into a number of tasks, and then identify hazards in each task. The production system is seen from the perspective of either the worker or the job supervisor.

In the workplace, responsibilities and legal requirements are defined, which makes the whole situation more organised. This method is most appropriate when tasks are fairly well-defined. One advantage of the method is that it is straight-forward and relatively easy to use.

Analytic procedure

The method has a well-defined analytic procedure, which is the same as that of the general procedural model shown in Figure 7.1. It consists of four main stages, plus a preparatory and concluding part. In Job Safety Analysis, these stages are specially designed.

Prepare

The preparation stage includes formulation of the aim of the analysis, and also defining and setting the boundaries of the job tasks to be analysed. Information about the job is collected, and it is useful if written instructions exist. For the analysis, a special record sheet is used. An example is given in Table 7.2.

For this type of analysis, it is beneficial to involve a team of people in the workplace. The team might include someone familiar with the method, a job supervisor, and a person who knows the job in practice and its potential problems. The main reasons for engaging a team are:

- Getting better information about the job and its conditions
- Obtaining a broader perspective on risk assessment and proposals for measures
- Improving circulation of results
- Having better confidence in the results obtained

1. Structure procedure

The purpose of the structuring stage of the analysis is to obtain a list of work tasks. A suitably detailed list of the different phases of the work under study is prepared. Good basic material consists of standard job instructions, but these should be regarded just as a starting-point. Usually, they cannot be assumed to be either complete or correct. It is important to take account of exceptional tasks and those that are only seldom undertaken. The following items should be considered:

- The standard job procedure
- Preparations for starting and finishing off the work
- Peripheral and occasional activities, such as obtaining materials, cleaning, etc.
- Correcting the disturbances to production that might arise
- The job as a whole, including descriptions, planning and other related tasks

Depending on the type of work, the following two components may also be included:

- Maintenance and inspection
- The most important types of maintenance and repairs

2. Identify hazards

The aim is to identify hazards which could cause injuries. The tasks on the list are gone through one by one. A number of questions are posed in relation to each of these:

- What types of injuries can occur?
  - Pinch/squeeze injuries or blows, moving machine parts, objects in motion or at a height, etc.
  - Cuts or pricks/stabs, sharp objects, etc.
  - Falls, working at a height, etc.
  - Burns
  - Poisoning
- Can special problems or deviations arise in the course of the work?
- Is the job task difficult or uncomfortable?
- Is the task usually performed in a different way than prescribed, or are there incentives to deviate from regular procedures?

The first point is a variant on the checklist of injuries above (Table 7.1). The three other points widen the perspective, and are intended to facilitate the identification of problems. It is advantageous not to restrict the analysis to accidents alone. Contact with chemicals, ergonomic problems, etc. may also be included, which can increase the benefits of the analysis.

3. Evaluate

Each identified hazard or problem in the list is evaluated. The purpose is to distinguish the ones that call for improvements. It is common to apply the *Risk Matrix* (Section 5.4) in using this method. However, the user should be careful in application; otherwise, the results might be misleading (Section 5.6). One alternative is to apply *Direct Risk Evaluation* (Section 5.2), which also needs to be applied with care.

Engaging a team in the analysis can be of great help at the evaluation stage. The different perspectives of team members facilitate the making of good judgements.

4. Propose safety measures

The next stage of the analysis is based on the hazards regarded as serious. When going through the record sheet, an attempt is made to propose ways of reducing risks. Such measures may apply to:

- Equipment and task aids
- Work routines and methods (Can the work be carried out in a different way?)
- Elimination of the need for a certain job task
- Improvements to job instructions and training
- Planning how to handle difficult situations
- Safeguards on equipment
- Personal protective equipment

This stage of the analysis principally concerns the generation of ideas. It is of benefit if ideas for several alternative solutions are produced. Several measures may be required to reduce a given risk. A particular safety measure may be hard to implement, so an alternative might be needed. Several different items that are similar in one way or another may be merged into one, e.g., if the hazards have similar causes or if a common safety measure is required.

Conclude

The analysis is concluded with a summary of results. In simple cases, the record sheet itself may be used to report the results. The list of job tasks and the record of the analysis may also be used, fairly directly, to produce an improved set of job instructions.

Practical use of Job Safety Analysis

Simplicity

The method is easy to learn. One of its advantages is that it is based directly on ordinary job tasks, which are easy to visualise. It is also based on commonly accepted ideas regarding safety and regular safety work. For this reason, it is easy to teach the method and get it accepted for direct use by job supervisors and work teams. Simple analyses can be conducted with little preparation and only a small amount of effort.

Applications

The method is useful when applied to more or less manual jobs. These could be machine operating in an industrial workplace, building work, doing repairs, etc. It is less suitable for automated production, when teams have to co-operate with each other and with computers, and for other complicated tasks.

One suitable application of the method is in job planning. A supervisor may consider a repair that has to be made. He goes through his list of what is to be done with the repair team. This enables them to identify hazards at various work phases and to determine which safety measures are needed.

Such an analysis is informal, and the records of the analysis, etc. are not so important. A decision can be made immediately, and people are then appointed to take responsibility for implementation. The extra time required for the analysis may be about an hour. Quality of the analysis may not be so high, but the reduction in risk can still be significant.

Information materials

Information is needed to prepare the list of work phases, and to identify hazards. Where systems have been in operation for some time, there is a body of experience available. Generally, this is possessed mainly by those who work directly with the equipment and by job supervisors. This knowledge can be accessed through discussions in a suitably composed study team. The information needed can also be obtained from:

- Interviews
- Written job instructions (sometimes incorrect, always incomplete)
- Machine manuals
- Work studies, if these are available
- Direct observations, the observer simply standing and watching
- Photographs, both to depict problems and to facilitate discussions within the study team
- Video recordings, which are especially valuable for tasks that are only seldom undertaken
- Accident and near-accident reports

List of phases of work
An important part of the analysis consists in producing a list of job tasks. Sometimes, this can take longer than the identification of the hazards themselves. Only brief descriptions of the different phases are needed. It is more important that the list is sufficiently complete.

One common dilemma arises when there is a major discrepancy between job instructions and how the job is carried out in reality. This can be a serious problem, which needs careful consideration. The method itself does not solve this problem, but it can be of good help in identifying discrepancies and the hazards to which these give rise.

Time taken by the analysis
The time taken by an analysis may vary considerably, but the method can be regarded as relatively quick to apply. How much time is needed for any one analysis depends on:

- The magnitude/diversity of the task to be analysed
- The efficiency with which the analysis is conducted and participants are trained

A rule of thumb is that the identification of hazards takes 5 minutes per phase of work. The number of work phases may come to between 20 and 50. The identification stage of the analysis may therefore be expected to take between one hour and half a day. The author's personal experience is that it takes roughly the same amount of time to produce a list of work phases, and the same time again to conduct discussions on safety measures. In total, the analysis may take between half a day and two days.

7.3 Example of a Job Safety Analysis

In this example, a redesign of a paper mill was planned. A part of the planned changes concerned a rolling machine, which had been in operation for a number of years. This type of machine is known to be hazardous, and the redesign of the workplace gave an opportunity to make improvements.

System description

The system to be analysed was a machine for the rolling and cutting of paper, and the working area around it. In principle, standard production at the machine consists of three basic operations. First, there is the unrolling of a wide reel of paper; then, the paper passes through a set of rotating knives; finally, a set of narrower reels are wound. Figure 7.2 shows work at such a machine, and Figure 7.3 demonstrates a difficult working situation.

Figure 7.2 Part of paper rolling machine

Preparing

The object of the analysis was the work done at the machine and in the area around it. The aim of the analysis was to obtain an overview of potential hazards, and its results were to be used in the redesign of the workplace. The machine was in operation and information could be obtained through observations and interviews. The experience of the operators was important, and they were invited to join the analysis team.

Analysis

1. Structure

The job was first subdivided into four main tasks (1-4), which made up the regular planned work. However, many other things were done at the machine, and three other items were added to the list:

1) Removal of produced reels and transportation to store room
2) Preparation of machine for new production cycle
3) Installation of new base reel in machine
4) Operation of machine
5) Tasks at start and end of workday
6) Corrections and cleaning
7) Other transport of materials

The three final tasks were more loosely planned, and they vary quite considerably by nature. Table 7.2 shows an extract from the record sheet. It concerns Task 2, *Preparation of machine for new production cycle.*

2. Identify hazards

Figure 7.3 Work at paper-rolling machine (part of job task 2.4 in Table 7.2)

Hazard identification was quite easy, and the operators provided much useful information. In practice, they answered questions like: *What can happen to a novice worker at this task?* Figure 7.3 illustrates part of job task 2.4, where an operator feeds new paper into the machine. It can be advantageous to break down tasks in even greater detail in the case of difficult or dangerous situations. In the table, this is indicated by a slash "/Correction of disturbances".

3. Evaluate risks

The risks were evaluated, and the approach with Direct Evaluation was applied. The scale shown in Table 5.2 was used. The evaluations were made by the study team and noted on the record sheet (Table 7.2).

4. Propose safety measures

The ideas in the checklist for proposals were sometimes useful. However, when a problem had been identified as important, the team had no problems in suggesting improvements. Some examples can be seen in the record sheet.

Concluding

In this case, it was clear that improvements were needed, and the report became a very short summary. The proposals were directly incorporated into design work by the chief engineer, who was a part of the analysis team.

Comments

In this case, the analysis was simple and straightforward, and could be performed in just a couple of hours. Record sheets for JSA can be designed in several ways, but here the sheet had five headings. The Comments column is intended for explanations, so that the reader can understand what might happen, why it is dangerous, etc. Alternative extra headings in a record sheet might be Causes, Consequences, and Responsible for measure.

Another example of a JSA is presented in Section 16.6.

Table 7.2 Extract from the record sheet of a Job Safety Analysis

Job task / Part	**Hazard**	**Comments**	**Eval**	**Proposed measures**
2 Prepare machine for new production cycle				
2.1 Removal of old base reel	Reel falls down	Rather heavy (40 kg). The reel can get stuck, or the operator can lose grip	2	Lifting equipment and adjustable holding facilities
2.2 Taking away packing band on new reel	Cutting injury	Sharp steel band Packing band recoils, due to tension Erroneous method (knife)	2	Use of proper tools Include this task in instruction manual
2.3 Installation of new base reel	Reel falls down	Heavy (2 tons). Mistake in operating lifting equipment is hazardous	3	Improve instructions
	Squeeze injury	Moving machine parts	3	Improve machine guards
2.4 Feeding new paper into machine	Operator falls, if paper tears	Heavy task, if brakes are not completely off, or if base reel is oval	2	Improve design for releasing brake pressure
	Squeeze injury	Paper reels and steel rollers rotating with great force	3	Develop automatic paper feeder, or change work routines (use the previous sheet of paper to pull through a new reel)
/Correction of disturbances	Squeeze injury Cuts from roll knife	Disturbances often occur	3	Improve automatic control system Develop safer correction methods Include in manual and during job training

Eval = Evaluation codes from Table 5.2: SM = Safety measure

0 = No improvement 1= SM can be considered 2= SM recommended 3=SM is imperative

8 Deviation Analysis

8.1 On deviations

The deviation concept

Systems do not always function as planned. There are disturbances to production, equipment breaks down, and people make mistakes. There are deviations from the planned and the normal. Deviations can lead to defective products, machine breakdowns, and injuries to people.

It is fairly easy to understand intuitively what deviations are and why they are important. There are a large number of terms used to denote deviations of one type or another. Some examples are disturbance, breakdown, fault, failure, human error, and unsafe act. In the analysis of hazards, a strict definition is not always necessary. Nor may it always be desirable. The need for precise definition is greater in some cases, e.g., when a statistical classification is to be made.

The deviation concept is a common element in a number of different theories and models. There are a variety of areas of application and definitions (Kjellén, 1984 and 2000). At a general level, a system variable is classified as a deviation when its value lies outside a norm. Some system variables are:

- Event or act, i.e., part of a procedure or a human action
- Condition, i.e., state of a component
- Interaction between the system and its environment

Examples of the types of norms that appear in the literature include:

- Legal – a standard, rule or regulation
- Adequate or acceptable
- Normal or usual
- Planned or intended

Consequences of deviations

Many kinds of deviations can arise within a system. Consequences will be of different types, some leading to increased risk, others being harmless. They can be characterised in many ways, and Table 8.1 gives one example

Table 8.1 Classification of deviations by type of consequences

Consequence	Comments
1. Direct accident	The deviation leads directly to an accident. For example, the wing of an aeroplane falls off in mid air.
2. Accident under certain conditions	In addition to the deviation itself, certain other conditions must be met for an accident to occur.
3. Increase in the probability of an accident	The deviation increases the probability of other deviations, or leads to a weakening of a safety function.
4. Latent failure	A hidden error impairs the safety functions of a system.
5. Not dangerous	The deviation does not lead to an increased risk.

Consequences of Type 1 lead directly to an accident; however, they are usually preceded by several other deviations. Types 2, 3 and 4 increase risk in the system. A *latent failure* can exist within a system for a long time without it being noticed, but when the function is needed it does not work. One example is a defective fire alarm; if a fire starts, the alarm is of no help.

Other aspects of deviations can be important when potential effects are concerned. It is important to consider:

- Detection of the deviation, which lies in a range from immediately observable to almost impossible to detect
- Possibilities to correct, which concern the extent to which deviations can be corrected so that the system can be returned to a safe state

One simple view is to consider a series of deviations, one leading to another until an accident occurs. This perspective is sometimes referred to as the Domino Theory (Heinrich, 1931). In reality, the relation between deviations and the occurrence of accidents is usually complex. A more realistic approach is to consider a (large) number of simultaneously existing deviations, which might combine to cause an accident. An important feature of some safety analysis methods, such as Fault Tree (Chapter 10) and Event Tree (Section 12.3), is the examination and clarification of relations between deviations.

Deviation methods

The concept of deviation is used in a number of methods for safety analysis such as:

- Deviation Analysis of systems (Section 8.3)

- Deviation Analysis (Investigation) of accidents (Section 13.9)
- Failure Mode and Effects Analysis – FMEA (Section 12.2)
- Hazop (Chapter 9)
- Human Error Identification (Action Error Method, Section 12.5)

In general, the principle underlying these methods is that they identify deviations that might cause injury or damage. An important feature is that they develop a model of the analysed system. Such a model can be represented in a flow diagram of actions or a technically oriented description. The methods adopt somewhat different approaches to both modelling and deviations. The modelling issue is considered further in Section 15.2.

8.2 Principles of Deviation Analysis

Aim and definition

Deviation Analysis is used to study a system and the activities within it. The approach can be used in two applications. The first is a *system-based* analysis starting off with the properties of the system that is to be analysed. The second is an *accident-based* analysis investigating an accident or critical event.

In both applications, the aim is to identify and analyse deviations that can cause accidents or other problems. The method includes the development of preventive measures. This section describes the characteristics and features that are common to both applications.

In this context, the term *deviation* has a general definition:

> *A deviation is an event or a state that diverges from the correct, planned or usual function. The function can be a process, a technical function, or a human or organisational activity.*

This general characterisation may sometimes lead to dispute over what is the correct function, etc. However, this does not have to create a problem, and it can be solved by:

- Seeing the dispute as positive, and treating it as a deviation in itself: "unclear what is the correct way to do this job", or
- Applying an even wider definition that takes into account possibly divergent opinions:
  A deviation is an event or a state that diverges from the correct, planned or usual function, ***according to at least one participant in the analysis****.*

Remember that the purpose of discussing deviations in an analytical context is to discover conditions that might lead to hazards. It is not important to make correct classifications, unless you are collecting data for some kind of statistics.

Background

The method has its roots in work within the Occupational Accident Research Unit (OARU) of the Royal Institute of Technology in Stockholm. An accident model was developed and tried out in several applications; a first English description was published by Kjellén and Larsson (1981). The original model has two major parts: the accident sequence, which is described as *a chain of deviations*; and, underlying *determining factors*. These are relatively constant properties of the system that influence the accident sequence. Over the years, the model has been used in many different applications, and a number of variants have been developed (Kjellén & Hovden, 1993).

The model has been adapted to be suitable as a tool for risk analysis (Harms-Ringdahl, 1982, 1987). The experiences of a number of studies of system-based analysis and of accident investigation have given rise to a simpler model. The major simplification was that the concept of *determining factors* was abandoned. This was compensated for by introducing a wider concept of deviation that includes both events and constant problems.

Basic ideas

The basic ideas underlying Deviation Analysis can be summarised in a few simple statements:

- Accidents are always preceded by deviations.
- Deviations can increase the risk of accidents, but the cause-consequence relationships can be complex.
- Knowing the potential deviations in a system enables better understanding of the causes of accidents.
- The risk of accidents can be reduced if deviations are identified and can be eliminated or controlled.
- The system to be analysed is seen as a combination of technical, human and organisational elements.
- Deviations are of several kinds; it is essential to consider technical, human and organisational deviations.

Applications

There are two kinds of applications of Deviation Analysis methodology. They have similar aims, which are to identify and analyse deviations. The major difference is how the identification is made.

A *system-based* analysis is based on the production process and the activities it involves. The process is divided into a number of blocks, and deviations related to the different blocks are identified (see further in Section 8.3). One specific aim of this approach is to anticipate what might go wrong.

An *accident-based* analysis uses information from an accident, a near-accident or a critical event (see further in Section 13.9). When applied in this way, the analysis is sometimes called Deviation Investigation. One aim here is to find deviations that have influenced the course of the accident event and its consequences. A further purpose is to anticipate what might go wrong in the future.

As an aid to identification, the special checklist of deviations shown in Table 8.2 can be used. It can be employed in both applications, but is especially important in system-based analysis. The number of identified deviations can be large. There is a need to distinguish the most important ones, and both applications contain a defined stage for evaluation. A further common feature lies in support for finding safety measures based on deviations.

To sum up, the main difference between system-based analysis and accident investigation is how deviations are identified. However, there are several similarities:

- Identification of deviations
- An identical checklist to support identification (Table 8.2)
- Evaluation of the importance of deviations
- Development of safety measures based on deviations

Checklist for Deviation Analysis

The checklist (Table 8.2) can be used both for analysis and for accident investigation. It is designed as an aid for the identification of deviations, and considers technical, human and organisational functions. The list is based on functions of the system, giving examples of what can go wrong. It is not intended to be a categorisation or taxonomy of deviations, and there are overlaps between categories.

This checklist is general, and other more specialised methods, such as *Hazop* (Chapter 9) and Action Error Method (Section 12.5), employ other checklists for types of deviations.

Table 8.2 Checklist for system functions and deviations

Function	Deviation
Technical	
T1. General function	Departure from the normal, intended or expected functioning of the system
T2. Technical function	Failure of component or module, interruption to energy supply, etc.
T3. Material (in a wide sense)	Deviation from the usual, unusual size, wrong delivery date, poor quality, wrong quantity, etc.
T4. Environment	Poor light, bad weather, unusual temperature, waste; any temporary disruptive state of the environment
T5. Technical safety functions	Safety devices are missing, defective or inadequate, such as interlocks, monitors, and machine guards
Human	
H1. Operation/movement	Slip or misstep in manual tasks
H2. Manoeuvring	Lapse or mistake in control of the system
H3. Job procedure	Mistake, forgetting a step, doing subtasks in the wrong order
H4. Personal task planning	Choosing an unsuitable solution, violations of rules and safety procedures and risk-taking
H5. Problem solving	Searching for a solution in a hazardous way
H6. Communication	Communication error with people or the system, on either sending or receiving a message
H7. General	Inconsistency in system demands on personnel, concerning skills or knowledge

Comments on technical deviations

T1 *General function.* These are deviations from the normal, intended or expected functioning of the system. The system does not work as expected, and there can be different kinds of disturbances. Deviations related to automatic functions and computer controls are also included in this category. Examples include a failure to achieve a desired final outcome, that the operation stops unexpectedly, or that a machine runs too quickly.

T2 *Technical function.* These are deviations of a technical nature, e.g., technical failure of a component or module, or interruption of electric power supply.

Table 8.2 Checklist for system functions and deviations (continued)

Function	**Deviation**
Organisational	
O1. Operational planning	Non-existent, incomplete or inappropriate
O2. Personnel management	Inadequate staffing, lack of skills
O3. Instruction and information	Inadequate or lacking, e.g., no job instructions
O4. Maintenance	Inadequate or routines not followed
O5. Control and correction	Inadequate or routines not followed
O6. Management of change and design	Inadequate routines for planning, checking and following-up
O7. Competing operations	Different operations interfering with one other
O8. Safety procedures	Missing, inadequate, disregarded

ST3 *Material*. Material should be seen in a broad sense. It concerns the *object* of production, which can be a piece of steel that is to be welded, or a patient who is to be treated in a hospital. It also applies to that which is used in the system, and also to transport and waste. Deviations can concern unusual characteristics, poor quality, wrong quantity, wrong delivery time, etc.

T4 *Environment*. This refers to abnormal or troublesome conditions in the indoor or outdoor environment. Examples include faulty or dim lighting, bad weather, the accumulation of waste, and other temporary environmental states that give rise to difficulties.

T5 *Technical safety functions.* These are fulfilled by devices designed to reduce risk, such as machine guards, interlocks and various types of technical monitoring equipment. Examples of deviations include safeguards that are defective or inadequate and equipment that has been removed or disconnected.

Comments on human deviations

Since human errors are nearly always more complex by nature than technical failures, it is more difficult to provide a simple classification of human deviations (see also Section 2.5). This means that certain types of human deviations, e.g., *forgetting something*, or *failing to take adequate safety precautions* can be placed in several categories. For this reason, flexible use should be made of this part of the checklist.

H1 *Operation/movement*. This applies to errors in the direct handling of material and equipment. They include simple errors of various types, e.g., slipping, falling over, missteps, etc.

H2 *Manoeuvring*. This category refers to the indirect handling of objects, using a machine or control system. Deviations include misreading an indicator, error of judgement, choosing the wrong control button, moving an object in the wrong direction, etc.

H3 *Job procedure*. This applies where a normal task procedure exists or is expected. Deviations comprise various types of mistakes (errors of judgement), such as forgetting a step, doing subtasks in the wrong order, misinterpreting signals, etc. Also, a person may totally abandon the normal job procedure and work by means of stage-by-stage improvisation.

H4 *Personal task planning.* Most jobs allow several degrees of freedom, and provide scope for several types of deviations. An unsuitable solution may be chosen for a variety of reasons, such as inadequate knowledge or a lack of instructions. Violations, such as breaching regulations and risk-taking, may have many different explanations. Not using personal protective equipment is a special case of this, and deserves special attention.

H5 *Problem solving.* This is a complex activity, when the individual has to take several decisions. Interesting here is to identify situations where there is room for a person to try to solve a problem in a hazardous way.

H6 *Communication.* This is an important component of many systems and job tasks. The category is used to identify situations where individual communications errors can be hazardous. It covers missing information, misunderstanding, and misinterpretation, and is closely related to category O3, which concerns communication in the organisation.

H7 *General.* A company might have inconsistencies in the demands imposed on personnel. These can concern required physical or cognitive skills, or special knowledge needed for the job. The limitations of human beings may cause problems, either for themselves or for the functioning of the system.

Comments on organisational deviations

Not only human but also organisational failures are highly complex by nature. For this reason, flexible use should also be made of this part of the checklist. Organisational failures can be seen as the *root causes* of many technical and human failures – since it is decisions made during planning that generate the preconditions for other failures. One way of using the organisational part of the checklist is to begin with technical and human failures. For the most important ones, a check is then made to study which organisational issues may have affected these failures.

O1 *Operational planning.* This is a general category that, in principle, also covers the points below. Planning can involve a variety of problems. It may simply be non-existent, or it may be incomplete or misguided.

O2 *Personnel planning.* This is a matter of having the right person in the right place. Problems include a lack of staff, staff without the required skills, and a lack of plans for training or recruitment.

O3 *Instruction and information.* The people who do the job must have adequate information on how to do it in the right way and according to plan. This might apply to manuals for equipment or to job descriptions for occasional tasks. Problems include a lack of instructions, and instructions that are inadequate, out-of-date or simply incorrect.

O4 *Maintenance.* This is an important function in making the system work well. Problems include a lack of maintenance plans, plans that are not followed, important routine subsections that are missing, the unavailability of spare parts, and a way of working that is unsatisfactory.

O5 *Control and correction.* These are operations designed to ensure that equipment and activities function as planned. If they fail, the system should be returned to its *normal state*, or plans should be modified as appropriate. Deficiencies in correction can cause a steady reduction in the safety of both technical and organisational functions.

O6 *Management of change and design.* Inadequate routines for planning, checking and following-up when systems are changed can result in reduced safety. For example, safety routines and responsibilities might be lost when a new organisation is set up.

O7 *Competing operations.* This category refers to situations where different operations can have a disruptive effect on one another. The operations may be quite independent, or they might compete for the same resources. For example, the number of cranes on a construction site is limited. If demand is great, a crane may not be available, prompting workers to resort to hazardous manual lifting.

O8 *Safety procedures*. These are designed to ensure that hazards are identified and controlled in accordance with the norms that prevail in the workplace. Safety management systems fall under this heading. The problem may be that safety activities are generally lacking or inadequate. Other possible deficiencies include low or misguided priorities, unclear areas of responsibilities, poor routines and weak implementation.

Development of improvements

Deviation Analysis includes a simple but systematic method for the generation of ideas for safety measures. To increase the safety of a system, improvements should be based on deviations that have been identified as hazardous. Efforts are made to generate measures that can:

1) Eliminate the possibility that a certain deviation will arise
2) Reduce the probability that it will arise
3) Reduce consequences if it does arise
4) Enhance readiness for deviations

Eliminate the possibility that a certain deviation will arise is the first approach. This might mean a change in activity or device to remove the possibility. This type of measure is effective but often difficult to implement.

To r*educe the probability* that a deviation will arise is closer at hand. Technical failures can be handled by better choice of components, maintenance procedures, etc. Human errors might be avoided with better man-machine interfaces, enhanced training, improved instruction manuals, etc.

The third type of strategy is to *reduce the consequences* of a deviation. This might involve a technical solution, e.g., the installation of an interlock, or improving opportunities for the operator to recover the system if he or she should make a mistake in the sequence.

The fourth approach is to enhance *readiness for deviations*. The idea is to support early identification of the deviation and provide for plans on how it should be corrected in a safe and effective manner. This might be most essential since many deviations cannot be avoided. A minimum requirement is that operators know how to act when the deviation appears.

The checklist (Table 8.2) of system functions, particularly its organisational section, can also be used as an aid. Ideas are noted in the analysis record sheet. These are then sifted through, and what emerges is put together into a proposal containing a number of different safety measures.

8.3 Deviation Analysis procedure

General

Deviation Analysis is used to study a system with the aim of identifying deviations that can cause accidents or other problems. The analysis usually includes a stage where proposals to increase safety are generated.

The method can be applied to many different kinds of systems, and to major as well minor arrangements. A small system might be a workplace or a specific repair workshop, whereas a large one might be a whole factory. The principle is the same, but the approach to structuring and hazard identification will vary according to type of object.

Steps in the procedure

Deviation Analysis proceeds in a manner that is similar to Energy Analysis and Job Safety Analysis, and involves the same basic stages. The main stages in the analytic procedure are shown in Figure 8.1. In principle, each stage is performed before the next is started, but in practice there is often an overlap between them. Each stage is briefly described, and practical information can also be found in Section 8.5.

Prepare

Before the concrete analysis starts, planning and preparations need to be done. The method is highly flexible, which makes it important to reflect over what is to be achieved and how it should be done. During preparation, there are some issues to consider:

- *Aim.* The aim of the analysis and what it is to deliver should be stipulated. The analysis might concern the identification of deviations with potential to cause harm, and suggestions for safety improvements.
- *Scope.* The analysis can focus on accidents, or its scope can be widened to include other consequences, such as disturbances to production, poor product quality, and damage to the environment.
- *Defining the object* involves specifying which parts of the system are to be covered by the analysis, and also clarifies the operational conditions that are supposed to apply. It also determines what is *not* to be included in the analysis. A general piece of advice is not to be too restrictive in making this definition.
- *Depth of analysis* can range from a detailed study to a coarse overview.
- *Resources.* It is important to estimate what resources are needed, which can apply to support from persons in the organisation, number of working hours, and time needed for the whole analysis.

- *Practical issues.* There are also a number of practicalities, such as determining whether a working group is desirable, and ensuring that the requisite information will be available during the analysis. As an aid to analysis, a record sheet can be used, such as that shown in Table 8.5 which you will find at the end of Chapter 8.

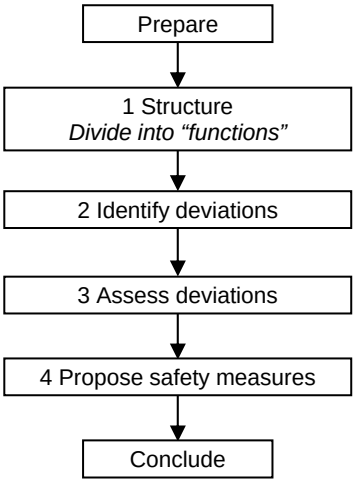


Figure 8.1 Main stages of procedure in Deviation Analysis

1. Structure

The aim of structuring is to make the system *analysable*, which means preparing a summary of the functions in the system. Its purpose is to make a division into more elementary functions, which are analysed one by one. At the same time, modelling helps to ensure that the entire system is covered in the analysis. The result of the structuring is often a flow chart, which is then regarded as a model of the system. It shows what is included, and also the system boundaries. Structuring is an important part of the analysis. It needs to be done with care, and a sufficient amount of time should be allowed for it.

This structuring is intended to model activities and functions in the system – what is happening. The starting point is a description of operations. These are divided into blocks of an appropriate size. Here are some examples of how a structure can be established:

- On a production line, a number of production steps are taken in sequence. The different links in the production chain can be followed, and these can be divided up into different sections.

- For a transport system, a classification can be made in accordance with the various types of conveyors used.
- A series of actions needs to be taken (a procedure). One example from everyday life is that of preparing a meal. A structure is obtained simply by listing the various actions required.

Usually, there are certain self-evident main activities. On the other hand, there may be a number of subsidiary activities, which are not immediately apparent. Examples of subsidiary activities include maintenance, the transportation of packaging material and the handling of waste. It is important to include these activities in the block diagram. One reason is that they might have been overlooked in the conventional planning and in work descriptions. These activities may be hazardous, and have enhanced risk, since they have not been considered properly.

A good habit is to add a block denoted by a heading such as *General*, *Planning* or *Organisation*. This acts as a reminder to pay attention to the activities that might be missing, and also to organisational aspects.

A block diagram can easily be too detailed and cluttered, making it difficult to see the totality. A rule of thumb is to have between five to ten major blocks. When needed, a block can be further divided into sub-functions. Some further aspects of structuring are treated in Section 8.5.

2. Identify deviations

The aim of this stage of the analysis is to find essential deviations. It is not possible to take up all conceivable deviations, since the total number can be very large. The stage generates a list of deviations to be considered.

The block diagram is the foundation in this stage. Identification can involve:

1) *Teamwork*, where the activities in the model are scrutinized one by one.
2) *Interviews* with persons familiar with the process. The model is used as a check that all parts are covered.

For each block, an attempt is made to identify deviations that can lead to accidents or have other negative consequences. A good starting point is to describe the purpose of the particular section under study. In searching for deviations, the checklist shown in Table 8.2 can be used as an aid.

It is fairly easy to find technical problems and situations where human errors can occur. When such a deviation is critical, the organisational conditions are of special interest. For example, if a certain component is important, the analysis can continue by looking in particular at *Maintenance* (O4) and *Control and correction* (O5).

Another example is where there is an operation with many possibilities for people to make errors, and the skill of the operator is relevant to safety. Then, it can be important to look at *Personnel management* (O2), *Instruction and information* (O3), and perhaps also at *Control and correction* (O4).

In addition to follow the block diagram, identification can be done through other interviews, with a focus on occurred problems and general experiences. *Searching in documents*, such as accident records, information on incidents, production reports, etc., can be very useful.

It should be remembered that a deviation does not have directly to lead to damage. Alternatively, it might lead to the increased likelihood of other deviations, making the system more vulnerable to damage, or to something else (see Table 8.1). The identification stage is further discussed in Section 8.5.

3. Evaluate deviations

The next step is to evaluate the importance of the identified deviations. The aim of this stage is to judge whether safety improvements are needed, and also to give help in setting priorities among the deviations. The principles for this are discussed in Chapter 5. The method itself does not prescribe what kind of evaluation should be performed.

In this method, deviations that can cause damage to production and the environment can also be included. This is discussed in Section 5.1, and Table 5.1 can be used for the classification of types of consequences.

In some cases, it is possible to obtain information on how frequent or serious the deviations are, which can support the evaluation. Data on this can be obtained through interviews, from records of operations, and from notes about repairs. From accident investigations, information can be gathered on deviations that have involved a high level of risk.

4. Propose safety measures

The aim of this stage is to deliver a set of suggestions on how the system can be improved. The stage is not compulsory, but it is sensible to take advantage of the analytical situation. The analysis has given a fairly deep understanding of problems in the system, which facilitates the generation of suggestions. The deviations assessed to be most important should be considered first.

At the end of Section 8.2, there is an account of a systematic approach to how safety measures can be found. If an analysis team is employed, ideas for improvements come quite easily. At this stage, it is best to think as freely and creatively as possible, so as to develop a variety of ideas that can then be sifted through and modified.

At the end of the stage, the various proposals can be organised in a suitable way. They might be summarised in *packages*, which address specific areas for improvement (see more in Section 14.3.)

Conclude
As usual, the analysis is concluded by preparing a summary. In Deviation Analysis, it can contain an overview of deviations and hazards, and the safety measures proposed. The analysis protocol can be used as an annex.

8.4. Examples

Deviation Analysis can be applied to many types of systems and problems. This section provides two simplified examples of how an analysis can be performed. They are just outlines, since going into the complexities would take up too much space here.

Example 1: A conference

This example is taken from an environment that is not particularly hazardous. A conference involves a *procedure* with which many are familiar. Most people will also have come across various examples of the disturbances and deviations that can arise.

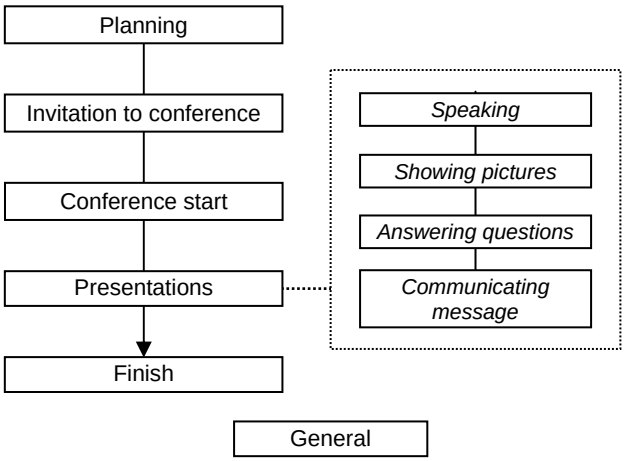


Figure 8.2 Block diagram of a conference

Suppose that an important conference is to be arranged. The conference organiser is concerned that everything will go well, since several previous

conferences have gone badly. The aim of the analysis is to identify what might go wrong in order to prevent further problems. The chosen method is Deviation Analysis.

The first step is to describe the major parts of the conference. It is divided into five major blocks in the left part of Figure 8.2. It starts with planning of the conference, followed by *Invitation to conference*, which involves attracting the interest of the target group. An important aspect is to obtain an overview of the whole conference. This is solved by adding the block *General*, although, at the beginning, is not clear what should be included in it.

It would be possible to perform a rough analysis solely on the basis of the simple diagram. In this case, however, it is important to be careful and look at the details. Each block can be divided into further activities. The figure shows a division of the block *Presentations* into four phases, where the first is *Speaking*. One aim of the presentations is to impart knowledge and facts to the audience, which is explicitly described as *Communicating message*.

Table 8.3 Examples on deviations during a conference presentation

Function	Deviation	Code
SPEAKING		
Public address system	Does not work (see below)	T1
	Oscillates, howls	T1
	Failure of a microphone	T2
	Faulty adjustment	H3
Managing the system	No checks on the sound equipment	O5
	No-one appointed to manage the sound	O2
	Sound management not planned	O1
	Inexperienced sound manager	O2
Speaker	Cannot cope with the microphone	H1, O3
	Too weak a voice	H7
	Has a difficult dialect	H7
General /Other	Presentation takes too long	H4, O5
	Disturbance from drilling in an adjacent room	O7

Code refers to the classifications in the general checklist (Table 8.2)

The diagram can now serve as a base for the identification of deviations. Let us consider analysis of the subphase *Speaking*. The conference hall is large, so a public address system is needed. A number of deviations are easily

found, and they are summarised in Table 8.3. The checklist in Table 8.2 can be used as a help, and the right-hand column (Code) in Table 8.3 shows how deviations relate to Table 8.2. However, in a practical analysis, I would exclude that information, since it complicates things.

It quickly emerges that the list becomes rather lengthy, and it can be practical to divide the function *Speaking* into a few groups. Going through all the blocks will make the number of deviations will be large, and the evaluation stage is important to set priorities. This is not shown in this example. A general advantage with this analysis is that it provides an overall picture of possible problems, which provides an opportunity for better planning of the conference.

Example 2: Work with an automatic lathe

The next example concerns work with a computer-controlled lathe of a fairly conventional design. Production batches are small, so the product to be manufactured changes from time to time. This means that lathe settings are adjusted, and tools and computer programmes exchanged quite often. There are a number of energies that can lead to serious injuries.

The aim of the analysis is to identify deviations that might cause accidents or production problems. In addition, ideas for improvements should be proposed. This account covers structuring of the work (Figure 8.3) and examples of deviations (Table 8.4). Further, an extract from the record sheet is presented (Table 8.5).

1. Structure

A block diagram of work with the machine is shown in Figure 8.3. The procedure is divided into six main phases. At the *Setting-up* phase, the operator will tool the lathe, change settings, read in the computer control programme, etc. At the *Testing settings* phase, the lathe is run for one part of the programme sequence, and then stops. The operator makes certain checks on the settings, and adjusts the control parameters if needed. When the entire job cycle has been tested, automatic operations can then be set in motion.

The block *Genera*l was added to include general activities and functions, and at first it was not evident what it should contain. However, after a while it became clear this block should include many important functions, such as maintenance, change of product, and development of software.

In fact, all the blocks proved to include several activities. The right-hand side of the figure shows the testing phase, which contains several subphases.

2. Identify deviations

In this case, the primary identification was made at interviews with operators of the machine. Table 8.4 provides examples of different deviations that had occurred during the activities *Setting-up* the lathe and *Testing settings*.

A few comments: A *settings sheet* shows how the lathe should be set up, and which tools and computer programmes should be used. The deviation *Select wrong settings sheet* means that the machine will be set up for the wrong type of manufacturing. Such errors are difficult to detect in advance, since instructions are listed in coded form on the works order. An error can be made by the operator, or it might have been introduced earlier, at the planning stage.

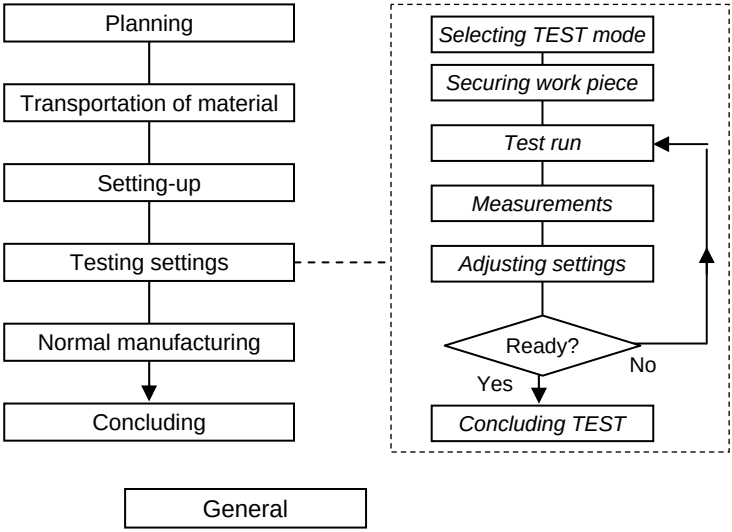


Figure 8.3 Working with an automatic lathe

Some deviations can lead to accidents, while others either cause defects in the finished product or mean that extra time must be taken to complete the work. Table 8.5 shows how a Deviation Analysis record sheet can be filled in.

3. Evaluate deviations

After the identification step, the deviations are evaluated. In this case, *Direct Evaluation* was chosen, and the scale in Table 5.2 was used. In addition, production problems should be considered, and therefore Table 5.1 with a classification of different types of consequences (SHEP) was also used.

Table 8.4 Deviations when working with an automatic lathe

Activity	**Example of Deviation**
SETTING-UP	
Studying works order and settings sheet	Select wrong settings sheet Wrong number on the settings sheet
Fitting cutting tools and accessories	Select wrong tool Fit tool in wrong place Fit tool incorrectly Defective or worn-out tool
Removal of tools	Leave the old tool in place
Loading computer programme	Error in loading procedure Data transmission failure Select wrong programme (for another product) Select out-of-date version of programme
TESTING SETTINGS	
General	Omit entire test procedure
Selecting TEST mode	Wrong indication of mode (lamp faulty) Press wrong button
Securing work piece	Inadequate fastening (technical or manual error)
Test run	Excessive pressure of tool on work piece Work piece comes loose Speed of rotation too high (error in earlier installation, or technical failure) Work with safety hood open Operator puts head in machine to see better Unexpected machine movement (for the operator) Unwanted stop, e.g., with no READY signal
Control measuring	Incorrect measurement
Adjusting settings	Wrong calculation Enter values incorrectly
Ready? (Continue test)	Finish the test before the entire cycle is completed (may depend on unclear information from the system)

Table 8.5 Extract from a Deviation Analysis record sheet for a lathe

Function / Part	**Deviation**	**Consequence /** *Comments*	**Eval***	**Proposed measures**
Testing settings /General	Omit the whole procedure	Work piece can come loose at full speed during later operation	S3, P2	Extra interlock to avoid omission Instruct the operators on the hazards of omitting the procedure.
/Selecting TEST mode	Wrong mode indication Press wrong button	Work piece can loosen at full speed / *Broken lamp gives a faulty indication*	S3, P2	Change design of indicator
/Securing work piece	Inadequate fastening	Work piece can come loose / *Many possible reasons; technical or manual failures*	S3, P2	Conduct a Fault Tree Analysis to summarise possible failures and errors
/Operation, one phase at a time	Work with safety hood open	Operator squeezed by tool or caught by rotating work piece / *Interlock installed*	S2	Improve interlock with e.g., dead man's grip when hood is open
	Disturbance, problem with sensors	Unwanted stop Squeezed / *If starts unexpectedly*	P1, S2	Develop safety correction routines Interlock with e.g., time out function for unwanted stops
/Control measuring	Incorrect measurement	Normally no danger, but the whole product batch can be destroyed	S1, P3	Instrument which is easier to use Better illumination
/Adjusting settings	Wrong calculation Enter values incorrectly	See above	S1, P3	Better training of operators and good calculation facilities
/Continue test	Finish too early	Work piece can loosen / *Possibly hazardous consequences at next stage*	S3, P2	Clearer indication from the system when test procedure is completed

Eval* = Evaluation codes from tables 5.1 and 5.2: SM = Safety measure

S = Safety H = Health E = Environment P = Production

0 = No improvement 1 = SM can be considered 2 = SM recommended 3 = SM is imperative

In the fourth column (Table 8.5), the evaluations are shown. The first deviation was classified as S3 and P2, indicating that the situation was not acceptable from either a safety or a production perspective. The deviation *Incorrect measurement* was judged as S1 and P3, which meant that safety was not affected, but that there could be a serious production problem.

In this part of the record sheet, no deviation was judged as leading to health or environmental problems. This could have been shown by putting a H0 and E0 in each row. However, it is often practical just to make the entries that indicate a non-acceptable situation.

4. Propose safety measures

In the record sheet (Table 8.5) a number of measures are proposed. Several of these are aimed at reducing the probability of deviation.

Conclude

One observation in the study was that there are several types of deviations that might cause a work piece to come loose. The consequences of this might be serious, and a deeper study is recommended. *Fault Tree Analysis* was regarded as a suitable method for this. A general conclusion was that operations at the lathe should be improved in order to improve the safety of both workers and production.

8.5 Comments

General

Deviation Analysis is a generic method and can be applied to different types of problems, and in various situations and systems. Many undesired events are preceded by deviations. For example, the principles are applicable to interruptions to production, accidents leading to environmental harm, and fire and explosion hazards.

In the examples above, the situations have been related to well structured and organised activities. This approach can also be useful in freer and looser contexts, such as doing outdoor sport, preparing food, or planning a public event. The method can be used for a detailed study or for a coarse analysis at general level. How this is achieved depends mainly on how the structuring is performed.

Sometimes, the freedom offered by the method makes it more demanding to apply. Usually, Energy Analysis and Job Safety Analysis are seen as easier than Deviation Analysis. However, applications can be adapted to the skills of the analyst, meaning that an analysis can range from simple to advanced.

All production systems are more complex than they seem at first sight. In this method, both functions and deviations are studied, which adds to the complexity. The handling of information is essential, and data can be obtained from:

- Direct observations of what is happening
- Written descriptions and drawings
- Interviews
- Accident reports, operations records, etc.

A practical way of conducting an analysis is to form a study team. The team should contain people acquainted with technical functions and the organisation of the work. It is also important to be aware of how the work is carried out in practice. In that way, the analysis will be supported by adequate information on both the system and its problems.

The working time to perform an analysis ranges from around a day to a week or more, depending on the situation and the thoroughness requested. The number of conceivable deviations in a system can be considerable. In practice, there is often only time to study a limited number of deviations, which means that good capacity to discern and distinguish is needed by both the analyst and the team.

Structuring

Structuring and making a functional model of the system are essential features of Deviation Analysis. The result of structuring can be depicted in a flow chart representing a model of the system.

Also in several other methods, development of a model is an important step. A short comparison with other methods is presented at the end of Section 15.2. Task Analysis is a group of methods (see Section 12.6) which are designed for modelling some types of work processes. The approach can be employed as an alternative to the structuring stage in Deviation Analysis.

People trying out the method for the first time often regard structuring as difficult. Some of the difficulties are that:

- There is seldom a ready-made structure available at a suitable level of detail. It is the job of the analyst to divide the system into functions.
- Descriptions of system functions are often incomplete.
- There are often several different ways of modelling the system.

In addition, it can be hard to estimate in advance the degree of detail required. On some occasions, descriptions of general functions are enough; on others, details are needed. In the two examples given in Section 8.4, a general classification is made first, and then some of the categorised functions are broken down in greater detail.

This means that the task of describing and structuring a system can take longer than the identification part of the analysis. However, the results of a careful structuring can be of benefit in applications other than analysis. It can be used for the design of job instructions, or for general descriptions of the system as a whole.

Rules of thumb

I have a few suggestions on how you can work with structuring, especially if you are the leader of the analysis:

1) Acknowledge structuring as an important part of the analysis, although sometimes difficult.
2) See it as a trial-and-error process. You can start with a brainstorming session, and then successively improve the model.
3) Do not be too detailed in the block diagram. Around five to ten major blocks is usually appropriate.
4) When needed, the blocks can be further divided into sub-functions.
5) Always include a block called *General* or something like that.
6) Remember that the borders and interfaces between the blocks are often important.

The block *General* represents items and activities that are common to the whole system. It can include functions related to other parts of the analysed system and/or auxiliary activities. One practical tip is that the functions that appear in two or more blocks can often be transferred to this general block. One example is instructions, which contain descriptions of how the work should be done. Another is planning, which prescribes how the job shall be done in the actual situation. My experience is that this block will quickly become filled with a range of items. It is often the case that the most interesting findings and important hazards are associated with this block.

In a way, the situation is simpler when a system is at the planning stage. Then, it is possible to work on the basis of the plans alone. In the case of systems that already exist, there are discrepancies between what is planned and what takes place in practice.

Identifying deviations

Especially when you are new to the method the checklist of deviations (Table 8.2) can be a good help. Remember that the purpose of the list is to support identification. It is not meant as a template or model that should be rigidly applied. In practice, there is no time to ponder over each item at great length.

My experience is that users familiar with Deviation Analysis do not make extensive use of the checklist. It becomes natural for them to observe

and search for deviations without it. In certain situations, e.g., concerning materials or procedures, the checklist used in Hazop (Table 9.1) can be a complementary aid.

Information on deviations that have occurred in relation to previous accidents is valuable. One or more accidents can be studied using Deviation Investigation (Section 13.9). This provides a list of deviations that are related to accidents, and which can be used at the identification stage. It might also increase the motivation of the study team.

Obviously, there are many types of deviations, and they can have different consequences (compare with Table 8.1). Some lead directly to a serious event, but depend in turn on other deviations having previously occurred. Others affect the likelihood of the appearance of further problems. At the end of an analysis, the material can be structured so that related deviations are merged. If the number of deviations is large, and their connections are complicated, a supplementary analysis could help.

One outcome of the analysis is a list of different deviations, which can be seen as a one-dimensional description. Sometimes, it is of interest to further study the logical relationships between the deviations. In such cases, Fault Tree Analysis (Chapter 10) or Event Tree Analysis (Section 12.3) can be used for further investigation of the results.

9 Hazop

9.1 Principles

In the chemical process industry, there is often a potential for major accidents. There is also a tradition that hazards are identified systematically, and that control measures are taken. In the chemical industry, Hazop has become the most established method for safety analysis. It is an acronym for Hazard and Operability Studies. Extensive guidelines have been prepared on how the technique should be employed (CISHC, 1977; ILO, 1988; Taylor, 1994; Lees, 1996). There are also numerous texts about Hazop on the Internet. This chapter therefore gives a fairly short guide to the method.

The method is purely technically oriented, and the basic principle is that a systematic search is made for deviations that may have harmful consequences, such as damage, injury or other forms of loss. Hazop's characteristic elements are defined as follows.

INTENTION	A specification of *intention* is made for each part of the installation to be analysed. The intention defines how that part of the installation is expected to work.
DEVIATION	A search is made for deviations from intended ways of functioning that might lead to hazardous situations.
GUIDE WORD	Guide words are employed to uncover different types of deviations.
TEAM	The analysis is conducted by a team, comprising people with a number of different specialisations.

The first section in this chapter provides an account of guide words, while the second describes the stages of procedure used for Hazop. In Section 9.3 a simple example is provided. The chapter concludes with some comments and tips, principally obtained from original Hazop specifications.

Guide words

One of the most characteristic features of Hazop is the use made of *guide words*. These are simple words or phrases, which are applied to the *intention* of either a part of an installation or a process step. Guide words can be applied to:

- Materials
- Unit operations
- Layouts

Table 9.1 Guide words in Hazop

Guide word	Meaning
NO or NOT	No part of the intention is achieved; nothing else happens
MORE	Quantitative increase, e.g., in flow rate or temperature
LESS	Quantitative decrease
AS WELL AS	Qualitative increase. The intention is fully achieved, plus some additional activity takes place, e.g., the transfer of additional material (in a conveyance system).
PART OF	Qualitative decrease; only a part of the intention is achieved
REVERSE	Logical opposite of intention, e.g., reverse direction of flow
OTHER THAN	Complete substitution; no part of the original intention is achieved. Something quite different happens

An example

Assume we have an installation with liquid, which is to be pumped into a pipe. The first three guide words are immediately and easily understandable. NO means that nothing is pumped, MORE that more liquid than intended is pumped, LESS that less than intended is pumped.

AS WELL AS means that something in addition to the intended pumping of the liquid takes place, and it might refer to:

- The liquid containing some other component, e.g., from another pipe
- The liquid also finding its way to a place other than that intended
- A further activity taking place at the same time, e.g., the liquid starting to boil inside the pump

The guide word PART OF means that the intention is only partially realised. If the part of the installation under study is designed to fulfil more than one objective, perhaps only one of these is met:

- A component of the liquid is missing.
- If the liquid is to be supplied to several places, only one of these receives its supply.

REVERSE denotes that the result is the opposite of what is intended. In the case of liquid, this might be that flow is in the reverse direction.

The guide word OTHER THAN means that no part of the original intention is realised. Instead, something quite different occurs. The guide word may also mean *elsewhere*. In terms of the example, OTHER THAN might be due to:

- The pumping of a liquid other than the liquid intended
- The liquid ending up somewhere other than intended
- A change in the intended activity, e.g., that the liquid solidifies (or starts to boil) so that it cannot be pumped

9.2 Hazop procedure

The literature referred to above gives extensive descriptions of the Hazop procedure, but there are a number of variations. A rather simplified description is provided here. Figure 9.1 gives an overview of the consecutive stages in an analysis. An example of the special record sheet used for Hazop analysis is shown in Table 9.2.

Prepare

The aim and scope of the analysis have to be specified. The objective may be to examine the proposed design of an installation, or to study the safety of an existing plant for generating improved job instructions. The types of problems to be considered can concern hazards faced by people at the installation, product quality, or the influence of the plant on the surrounding environment.

A boundary for the analysis is set by specifying which parts of the installation and which processes are to be analysed. A team is appointed to conduct the analysis. As usual in safety analysis, preparation also involves the gathering of information and planning for the implementation of the study.

1. Structure

The technical installation is divided into different units, such as tanks, connecting pipes, etc. The later steps in the analysis are then applied separately to each unit, one at a time.

2. Specify intention

The intention of each part to be analysed is defined. This specifies how it is envisaged that the part will function. If the designer participates, he or she can provide an explanation. Otherwise, it will be the person most familiar with the installation.

3. Identify deviations
Using the guide words, an effort is made to find deviations from the specified intention. The guide words are applied one at a time.

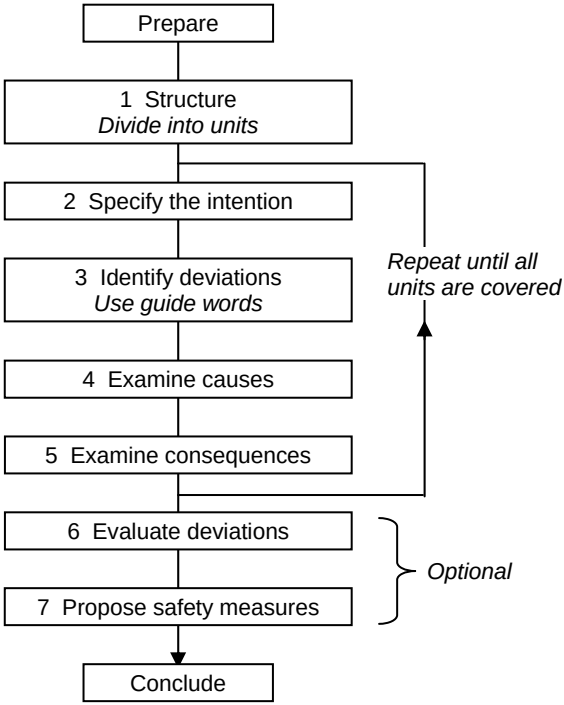


Figure 9.1 Main stages of procedure in Hazop

4. Examine causes
For each significant deviation, an attempt is made to find conceivable causes or reasons for its occurrence.

5. Examine consequences
The consequences of the deviations are examined. The possible seriousness of these should also be assessed.

Repeat the procedure
When analysis of a unit of the installation is completed, this is marked on the drawing. The next unit is then analysed, and the procedure continues until the entire installation has been covered.

OPTIONAL STAGES
In many manuals, the analytic procedure stops here. However, it can be advantageous to take the analysis a bit further and also include the two stages below.

6. Evaluate deviations
Matters of evaluation and grading of consequences are not taken up in traditional Hazop manuals. It is possible, however, to use the types of evaluation discussed for other methods (see Chapter 5).

7. Propose safety measures
In descriptions of the method, the development of safety measures is often not explicit. However, it might be suitable to discuss this during the course of the analysis. The finding of safety solutions can be conceived of in terms of two extremes. In practice, there will be a compromise between the two:

- A solution is produced after each source of risk (hazard) is discovered
- No solutions are produced until after all the guide words have been applied

To obtain ideas for improvements, the same strategy as in Deviation Analysis might be used (Section 8.2). Safety measures may apply to:

- Changing the process (raw materials, mixture, preparation, etc.)
- Changing process parameters (temperature, pressure, etc.)
- Changing the design of the physical environment (premises, etc.)
- Changing routines

Conclude
The analysis is concluded by preparing a summary, but further follow-up might be needed. This might include liaising with those responsible for control measures, further development of safety proposals, etc.

9.3 Hazop example

The Hazop analysis illustrated in Figure 9.2 is a simplified version of an example originally presented by the UK Chemical Industry and Safety Council (CISHC, 1977). It concerns a plant where the substances A and B react with each other to form a new substance C. If there is more B than A,

there may be an explosion. This is a highly simplified example. It is not specified whether a continuous or batch process is involved, how the quantities of A and B are controlled, etc.

We begin with the pipe, including the pump, that conveys Material A to the tank. The first step is to formulate the INTENTION for this part of the equipment. Its aim is to convey a specific amount of A to the reaction tank. In addition, the pumping of A is to be completed before B is pumped over.

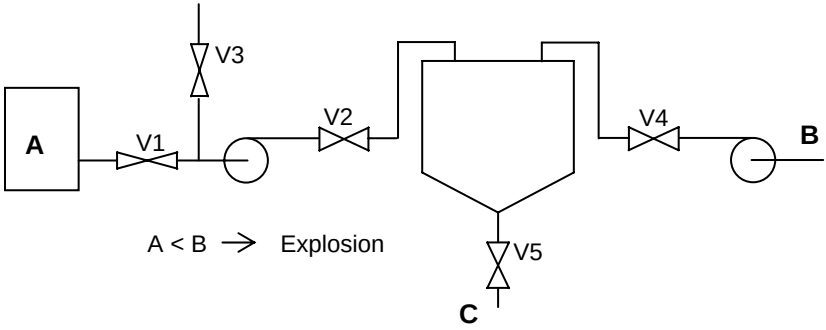


Figure 9.2 Schematic description of an installation

We apply the first guide word, NO or NOT. The deviation is that no A is conveyed. The consequence of the deviation is serious, and involves the risk of explosion. Possible causes of this are sought for, and it is easy to come up with several conceivable explanations:

1. The tank containing A is empty
2. One of the pipe's two valves (V1 or V2) is closed
3. The pump is blocked, e.g., with frozen liquid
4. The pump does not work, for one of a variety of possible reasons. The motor might not be switched on, there might be no power supply to the motor, the pump might have failed.
5. The pipe is broken

The next guide word is MORE. The deviation means that too much A is conveyed. Consequences will not be as serious this time. But Substance C can be contaminated by too much A, and the tank can be overfilled. Reasons for this might be that:

1. The pump has too high a capacity
2. The opening of the control valve is too large

The third guide word is LESS, meaning that too little A is conveyed. The consequence may be serious. Reasons for this might be that:

1. One of the valves is partially closed
2. The pipe is partially blocked
3. The pump is generating a low flow, or is operating for a shorter time than intended

The fourth guide word is AS WELL AS. The deviation is that A is conveyed, but that something else happens. The consequence of the different deviations is that *too little A* is conveyed, meaning the risk of explosion. Examples of such deviations are that:

1. A further component is pumped through the pipe, which might be due to Valve V3 being open, resulting in another liquid or gas entering the flow. Or that there are contaminants in the tank.
2. A is pumped to another place as well as to the tank. This might result from a leak in the connecting pipe.
3. Another activity is taking place which competes with the pumping. Would it be possible for A to boil in the pump?

The fifth guide word is PART OF. The deviation is that just a part of the intention is fulfilled. It might be that a component of A is missing, although this does not appear to be possible in this case.

The sixth guide word is REVERSE. This would mean that liquid is conveyed from the reaction tank to the container for Material A. The consequence can be serious. Conceivable deviations include:

1. The pump is operating in reverse. This would occur if the power supply was wrongly connected to the motor.
2. Liquid is running backwards from the reaction tank or the connecting pipe due to gravity.

The seventh guide word OTHER THAN means that no part of the original intention is fulfilled. Instead, something quite different occurs. Some examples of such deviations are:

1. A liquid other than the intended liquid is pumped.
2. The liquid finds it way to some other place.
3. There is a change in the intended activity. It might be that the liquid solidifies or starts to boil, so that it cannot be pumped.

Table 9.2 shows a part of the analysis summarised on a Hazop record sheet. Such sheets can be designed in quite different ways. For example, the first column with guide words may be regarded as unnecessary. If evaluations of identified hazards are made, a column for writing the evaluation score is needed.

Table 9.2 Extract from a record sheet for a Hazop analysis

Guide word	**Deviation**	**Possible causes**	**Consequences**	**Proposed measures**
NO, NOT	No A	Tank containing A is empty V1 or V2 closed Pump does not work The pipe is broken	Not enough A, explosion	Indicator for low level Monitoring of flow
MORE	Too much A	Pump has too high a capacity Opening of V1 or V2 is too large	C contaminated by A Tank overfilled	Indicator for high level Monitoring of flow
LESS	Not enough A	V1, V2 or pipe is partially blocked Pump gives low flow, or runs for too short a time	Not enough A, explosion	See above
AS WELL AS	Other substance	V3 open, air is sucked in	Not enough A, explosion	Flow monitoring based on weight
PART OF	–			
REVERSE	Liquid pumped backwards	Wrong connection to motor	Not enough A, explosion A is contaminated	Flow monitoring
OTHER THAN	A boils in pump	Temperature too high	Not enough A, explosion	Temperature (and flow) monitoring

9.4 Hazop comments

Time taken by the analysis

For most installations, a Hazop analysis is time-consuming. For this reason, proper scheduling is required. The average period of time required by an analysis is 10 to 15 minutes, either per component or per activity covered by a job instruction. This means one to three hours for each main unit, e.g., a reactor with several connecting pipelines. For an analysis to be effective, study meetings are recommended, but they should last three hours at most.

Thus, if the object to be analysed is a large one, careful planning is required. Planning involves the following:

- Finding time for the entire object
- Getting through the meetings in a reasonable amount of time
- Having the necessary information material available at meetings
- Ensuring that time is available for the control measures and follow-up activities decided upon at the meetings

To complete the analysis in a reasonable time, several teams working in parallel may be needed. One of the team leaders should then adopt the role of co-ordinator.

When is Hazop used?

Hazop can be used in different situations:

- At the planning stage, before detailed design and construction decisions are made
- Before system start
- For an existing installation

The greatest benefit is obtained if an analysis is conducted in conjunction with the design of the installation. It can be meaningful to conduct a Hazop analysis even when the installation has been nearly completed. The reasons why an analysis is justified at this stage are:

- Important changes have been made.
- Operating instructions are critical to safety.
- The new installation is similar to one that already exists. The changes primarily affect the process and not the equipment.

An installation where safety was adequate at the time operations were started may deteriorate over the years. A series of changes may have meant that different types of hazards have arisen. This particularly applies if safety issues were not carefully considered when the changes were made. It may also be that sufficient attention was not paid to safety at the design stage, or that requirements for operational safety have become stricter over time.

Information

The literature on the method stresses the importance of the availability of a sufficiently detailed documentary base for an analysis to be conducted. This means, that a Hazop analysis can only be performed when detailed documentation is available.

Drawings and instructions must be up-to-date and correct. Drawings often need to be updated, which can require a substantial amount of effort. In the case of existing installations, it is often found that information is incorrect.

The study team

Guidelines for Hazop stress the importance of working as a team. This applies to team composition, skills and attitude. Hazop is no substitute for knowledge and experience. The work requires continuity, so members should only be replaced in cases of emergency.

The role of the team leader is important. He or she must be familiar with the Hazop method, capable of leading the discussions, and able to ensure that the schedule for analysis is followed. The task of the leader also involves producing the documentation needed for the study. It is sufficient for the leader alone to have thorough knowledge of the method.

The leader must ensure that proceedings at meetings are efficient, and agendas kept to. There must not be so many delays that the members get bored with the analysis. The leader summarises results when each unit in the study has been completed. He or she also marks the drawing after, for example, a pipeline is ready.

Analysis of batch production

The Hazop literature sometimes contains supplementary advice for the study of installations where batch production takes place. In addition to drawings of the plant, information is needed on the sequence in which the production procedure is carried out. It may be either automatically or manually controlled. The information material may consist of job descriptions, flow sheets, etc. A summary description of the settings of valves, etc. may be needed for the different situations that can arise

The analysis can be structured so as to follow a job procedure rather than different parts of an installation. The same guide words as before are employed, although they can be re-formulated as appropriate. For example, EARLIER, LATER and WRONG ORDER may be employed for time or job sequences. When applied in this way, the method is similar to Deviation Analysis in certain respects.

Miscellaneous

Taylor (1979, 1994) has suggested a variant of Hazop in which the emphasis is on physical variables. The analysis is then based on a checklist that covers temperature, pressure, etc., and a simplified set of guide words is applied to these.

If a lot of changes are made after a Hazop study, a new round of analyses may be required. The additional study would be designed to discover whether new problems had been introduced by the changes already implemented.

Experience has shown that problems of start-up, close-down, etc. are often neglected by over-specialised design groups working in isolation. Sometimes, the guide word MISCELLANEOUS is employed to capture deviations or problems that have not been identified using the other guide words. The category is primarily designed to cover occasional activities that can lead to problems. Examples include starting up and closing down the plant, inspection, testing, repairs, cleaning, etc. This guide word does not have a natural place in Hazop, but can be valuable for the detection of further problems.

10 Fault Tree Analysis

10.1 Introduction

A fault tree is a diagram showing logical combinations of causes of an accident or an undesired event – *the top event*. This can be an explosion, failure of equipment, the release of toxic gas or an interruption to production. *Fault Tree Analysis* (FTA) is used to identify combinations of faults that can lead to the top event. It can also be used to estimate the probability of the top event.

FTA might be the best known method employed in safety analysis. It started to be used in the 1960s. There is an extensive literature on the method (e.g., Vesely et al., 1981; Kumamoto & Henley, 1996; Lees, 1996; Stamatelatos et al., 2002). This chapter will present some features of the method. It will show how simpler kinds of fault trees can be generated, and only briefly discuss probabilistic estimates. The account also presents suggestions for how broader approaches can be adopted.

The method is of greatest value in high-risk sectors with complicated technical systems, where accidents can have serious consequences. The method is fairly difficult to apply, and is generally used by specialists, especially in quantitative applications.

However, FTA can also be useful in regular safety work and outside its traditionally strict applications. Examples of this are not uncommon, and there have been trials including softer aspects, such as organisational issues.

The fault tree methodology can be applied for a variety of purposes, which are not mutually exclusive. Some examples are:

a) *Top-down analyses* of how a top event can occur (involving a strict combination of events and system states).
b) *Probabilistic estimates* for a specific top event.
c) *Bottom-up analyses* that compile a logical summary of the results of other analyses, such as Hazop or Deviation Analysis. A tree can be used to make a transition from a (one-dimensional) list of deviations to a representation of their logical connections and relations.
d) *Bottom-up analyses* of an occurred accident; the aim is to understand how a combination of faults has contributed to the course of events.
e) *Means of communication*; the compact description offered by a fault tree emphasises the overall picture, not particular details.
f) *Illustrations* of how failures, and also management factors, may influence the safety situation.

10.2 Principles and symbols

The binary approach

In Fault Tree Analysis a binary approach is adopted. Either an event occurs or it does not. An event statement can then be designated as *true* or *false*. This can also be expressed in terms of the logical values *1* and *0*, meaning that binary logic and Boolean algebra can be applied.

Symbol	Designation	Function
	Basic event	Basic event or failure
	Event	Event resulting from more basic events
	Undeveloped event	Causes are not developed further
	AND gate	Output event C occurs only if all input events (A and B) occur simultaneously
	OR gate	Output event C occurs if any one of the input events occurs
	Transfer symbol	Indicates that the tree is developed further in another place
Not standard	*Extended fault tree*	*Suggested for the handling of non-binary influences (see Section 10.5)*
	*Influence arrow*	*Events above are influenced in some way, e.g.,increasing probability*
	*Influencing event*	*Event or circumstance influencing higher events; not of the binary type*

Figure 10.1 Symbols used in Fault Tree Analysis

Events, states and logic gates are basic concepts. In designing a fault tree, a number of different symbols are sed. There are several variants of these (see e.g., Stamatelatos et al., 2002), and a limited selection of symbols are shown in Figure 10.1

The first three refer to *failure events* that describe a fault of some kind. They can be events in a strict sense, i.e., something that happens, but may also refer to a faulty state, e.g., a component that has failed. The *AND gates* and *OR gates* are used to provide logical connections between the various events in the tree.

A fault tree can be large, and there is often a need to divide a tree into several smaller ones. The *transfer symbol* (triangle) is used for connecting a lower tree to a higher level tree.

FTA presumes a strictly formal binary approach. However, its logical format makes it appealing to use it in other application. These could be called *soft fault trees*. In order to handle this consistently and clearly, two additional symbols are proposed. The principal aspects of this are discussed in Section 10.5.

Example of a fault tree

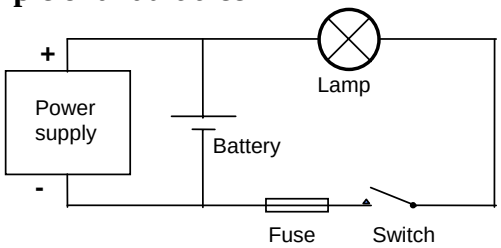


Figure 10.2 A lamp circuit

The appearance of a fault tree can be illustrated by a simple example. A lamp is connected into a circuit, as shown in Figure 10.2. A power supply feeds the lamp, and there is a battery to provide reserve power in case the power supply fails. A fault tree is wanted to analyse the case where the lamp does not light when switched on.

The top event is that the lamp does not light. This is because there is no current through the lamp. In turn, this may be due to the lamp being faulty or there being no power supply to the lamp. The power feed will fail if both the power unit and the battery fail to operate (AND gate).

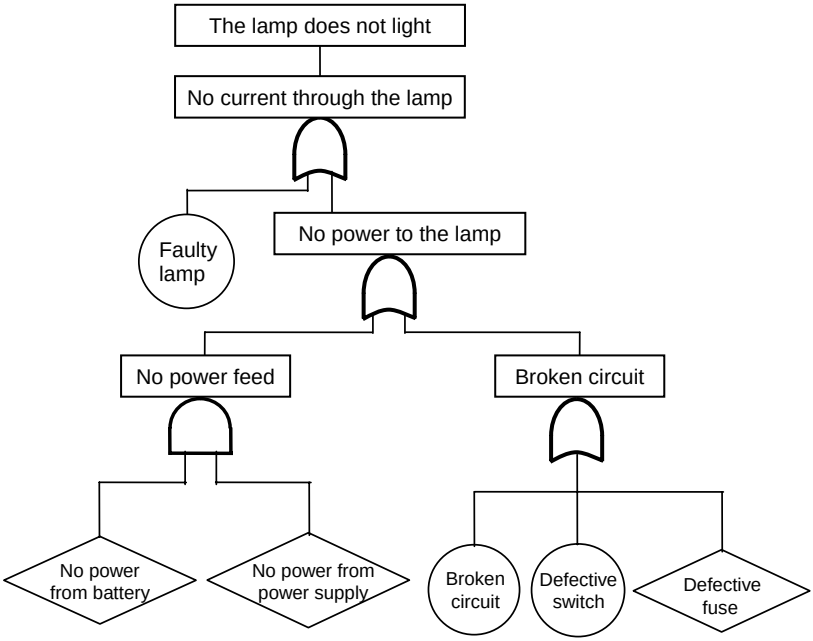


Figure 10.3 Fault tree for a lamp circuit

The tree contains three basic events, and there are also three *undeveloped events*. That the fuse is defective may be due to ageing or some other reason. It might have been overloaded as a result of a temporary short-circuit. It should be possible to develop this further. Similarly, it should be possible to investigate why power is not coming from the battery or the power supply.

10.3 Fault Tree Analysis procedure

A Fault Tree Analysis cannot be conducted in such a direct manner as the analyses described in the previous chapters. Success depends much on the ability of the person performing the analysis. There are various suggestions for how a tree should be constructed (e.g., Kumamoto & Henley, 1996; Stamatelatos et al., 2002). One suggestion, with emphasis placed on the construction stage, is shown in Figure 10.4.

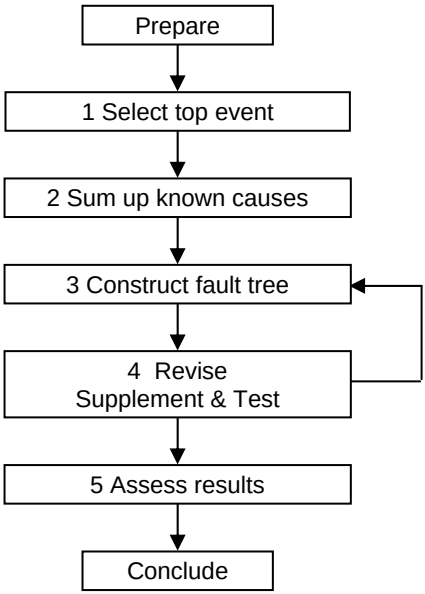


Figure 10.4 Main stages of procedure in Fault Tree Analysis

Prepare
As is usual with safety analysis, the aim and scope of the analysis need to be defined before its starts. Constructing a fault tree involves detailed analysis and may require an extensive set of assumptions, in particular about the operational conditions that are supposed to prevail.

1. Select top event
An important step is to select the undesired event to be analysed. This should be carefully defined.

2. Sum up known causes
When constructing a fault tree, existing knowledge of faulty states and failure events can be utilised. Sometimes, faults identified in a FMEA, Hazop or Deviation Analysis can be used. Also, the results of an accident investigation can be utilised. The result of this step is a list of faults that might contribute to the occurrence of the top event will have been obtained. This material can then be used to construct part of the tree or, at the end, to check the completeness of the tree.

3. Construct fault tree

Construction of the tree begins with the top event. The first step is to consider whether it can occur, independently, in more than one way. *If so*, the system has to be divided up using OR gates. The analysis continues by moving downwards, searching for more basic causes. The advice in Table 10.1 can be used for the design of the tree.

4. Revise, supplement and test

Construction is a trial-and-error process. Progress towards a better and more complete tree is made in stages. One essential step is repeatedly to check whether the tree is logically faultless, and whether it needs to be corrected. Table 10.1 gives some advice. It is hard to know exactly when a tree should be regarded as complete. No important causes of failure should be omitted. A first check is to see whether the items on the preliminary list have been covered.

5. Assess results

The completed tree is then assessed, and conclusions drawn. Depending on the purpose of the analysis, a number of different steps can be included at this stage. Some of these are discussed more extensively in Section 10.4.

- *Direct judgement of the result.* The tree provides a compressed picture of the different ways in which the top event might occur. It also provides a picture of the barriers (safety features) that exist. A check can be made if some failures can directly lead to the occurrence of the top event.
- *Preparation of a list of minimum cut sets.* As shown in Section 10.4, a *cut set* is a collection of basic events, which together can give rise to the top event. A *minimum cut set* is one that does not contain a further cut set within itself.
- *Ranking of minimum cut sets.* Combinations of failures to which special attention should be paid can be evaluated and ranked on the basis of the minimum cut sets.
- *Estimation of probabilities* is the *classical* application of a fault tree. If information on probabilities for bottom events is available, or if these can be estimated, the probability of the occurrence of the top event can be calculated from the list of minimum cut sets.

Conclude

The analysis is concluded with a summary, which gives information about assumptions. It is not enough with just the tree, which might be difficult to understand and interpret. Probably a number of conclusions can be made based on the analysis.

Rules of thumb

In constructing a fault tree, the rules of thumb shown in Table 10.1 can be utilised. Rules 1–7 are applied in the course of constructing the tree. Rules 8–10 are used from time to time to test whether the tree has a valid logical structure. The list of rules is partly based on the account provided by Henley and Kumamoto (1981). A further source is the author's experience of problems encountered by beginners when they first embark on Fault Tree Analysis. Complementary rules can be found in, for example, Stamatelatos et al. (2002).

Table 10.1 Rules of thumb for constructing and testing a fault tree

	Constructing
1.	Work with concrete events and states that are faulty. The statement shall be precise, and also be of a binary nature (true or false).
2.	Develop an event into a further event that is more concrete and basic.
3.	Can an event occur in different ways? Then, divide the event into more elementary events (OR gate).
4.	Identify causes that need to interact for the event under study to occur (AND gate).
5.	Link the triggering event to the absence of a safety function (AND gate).
6.	Frequently create subgroups, preferably making divisions into pairs.
7.	Give a heading to every gate.
	Checking
8.	Check that no non-explicit assumptions or preconceived opinions are included.
9.	Check the logic and structure of the tree. Make sure that the relation between cause and effect is not confused.
10.	Test the logic of the tree from time to time during construction. Start from events at the bottom of the tree, and assume that these will occur. What will the consequences be?

Figure 10.5 provides examples of these rules of thumb. Rule 1 is essential in a strict FTA, and it is important to remember that a fault tree deals with faults. Rules 6 and 7 are closely related, and one aim is to help the reader (and constructor) to see the logical reasoning behind the construction. Figure 10.5b shows one OR gate with four inputs, which is divided up into more gates. It looks different, but the tree still has an identical logical function. This becomes important if an OR gate contains many inputs which might look confusing. The disadvantage is that the diagram takes up more space. Rule 7 is sometimes called the *No-Gate-to-Gate* rule.

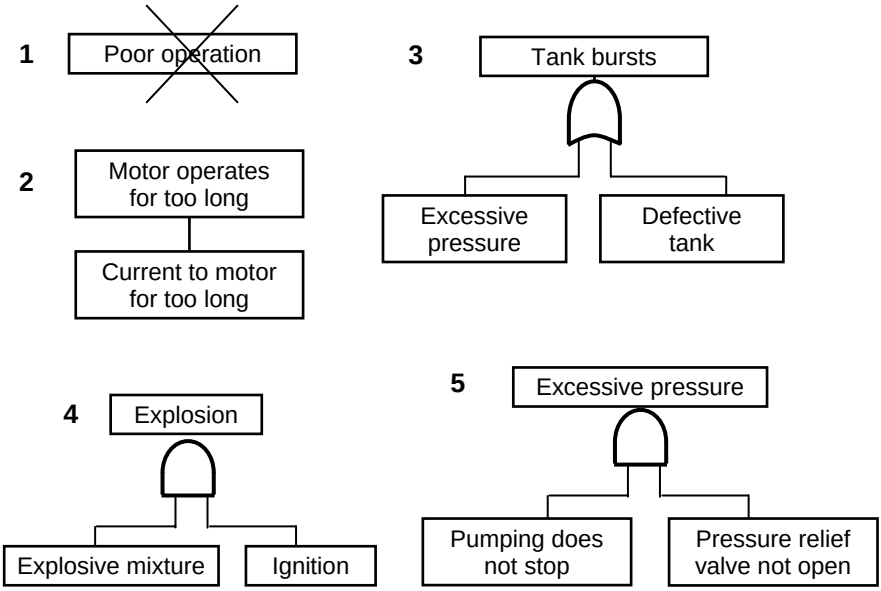


Figure 10.5a Example of the application of rules of thumb in Fault Tree Analysis

The example of Rule 8 reveals a line of thought that has been neglected. That the machine starts unexpectedly will only lead to an accident if a person is directly in the danger zone.

The example of merged rules 9 and 10 shows a case of confusion of cause and effect. Suppose that the motor operates for too long. This does not lead to current flowing for a long time. In this case, the sequential error is obvious, but in more complicated contexts it is easy to perform such logical somersaults. Remember that causes start at the bottom.

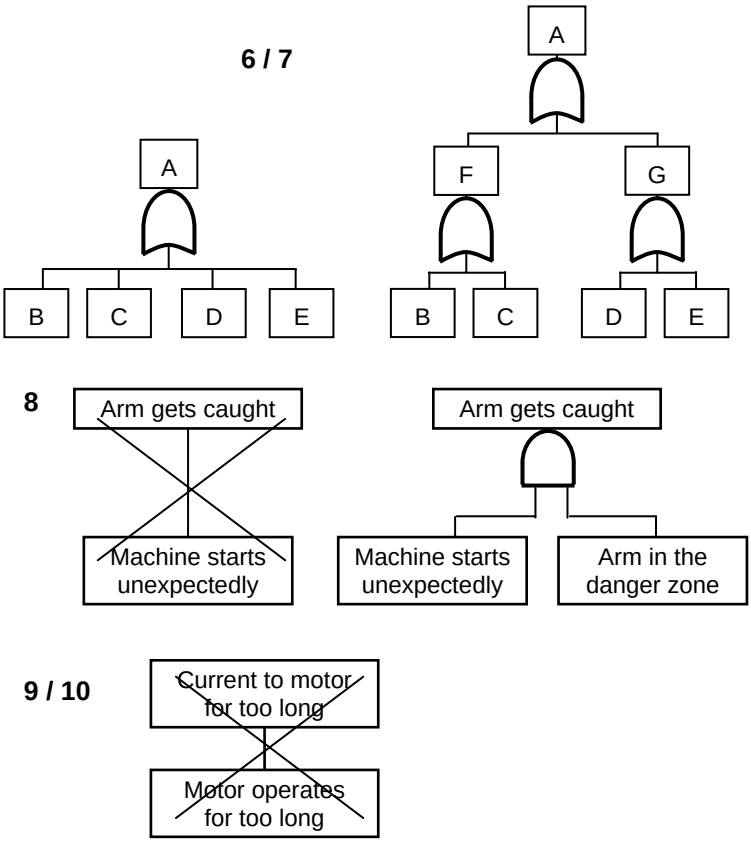


Figure 10.5b Example of the application of rules of thumb in Fault Tree Analysis

10.4 More on Fault Tree Analysis

General

The construction of a fault tree is a combination of art and science. Two analysts will not construct identical trees. (But this also applies to safety analysis in general as soon as you go beyond a superficial level.)

Large numbers of computer programmes of different types are available as aids for the construction of fault trees. For a beginner, it seems best to start by constructing a tree by hand. Otherwise, there is a substantial risk that the task of managing the programme will be predominant, and analytic thought neglected.

On the use of logical symbols

The most important symbols are shown in Figure 10.1 above, but they can be presented in alternative ways. The functions can also be expressed in the form of a set of logical expressions or as truth tables. Figure 10.6 shows how these different forms of presentation are related.

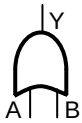
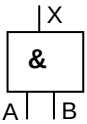
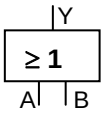
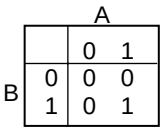
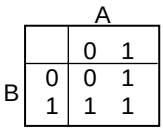
Function	AND	OR
Symbol		
Alternative symbol		
Function denotation	X = A B X = A & B (X = A ∩ B)	Y = A + B (Y = A U B)
Truth table		
Probability	p(X) = p(AB) = p(A) p(B)	p(Y) = p(A + B) = p(A) + p(B) – p(A)p(B)

Figure 10.6 Different ways of describing logical relationships

A truth table shows how a logical function depends on the input variables. This can be explained through the examples given in Figure 10.6:

- The AND gate (X) has two inputs. For A = 1 and B = 1, X = 1. For other combinations of A and B, X = 0.
- The OR gate (Y) has two inputs. For A = 0 and B = 0, Y = 0. For other combinations of A and B, Y = 1.

Fault Tree Analysis is frequently employed to provide a basis for probabilistic calculations, and two basic formulas are included in the bottom row. The probability that A will occur within a certain time interval is denoted as p(A). The probability that A will not occur is 1 – p(A). For the formulas for p(X) and p(Y) given in Figure 10.6 to be applicable, it is assumed that A and B occur independently of each other.

Things that break

That an installation breaks is simply because its load is greater than its strength. Normally, installations are designed and constructed so that there is a margin between lowest strength and highest load. If a failure occurs, this may be because the margin is too narrow. Let us take a bridge as an example.

This is illustrated in Figure 10.7. The load is not constant but varies over time. Sometimes there are a lot of vehicles on the bridge, at other times there are only a few. The curve on the left shows the probability (p) of the bridge being exposed to a certain load.

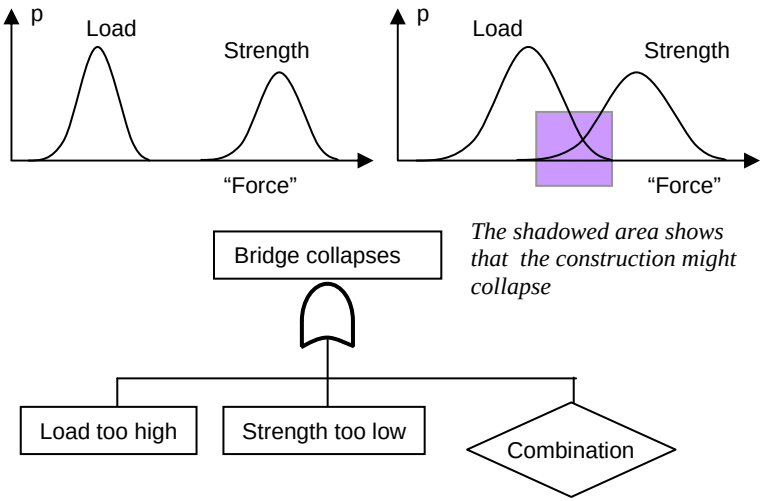


Figure 10.7 Relationship between probability and strength

Nor is the strength constant. The bridge can rust, or extreme cold may mean that it is weaker at certain times. Even if a large number of identical bridges have been built, it is not certain that all have equal strength. Construction errors or material defects can arise.

In the case of the left of the two curves, there is a margin between load and strength. How large the safety margin should be is decided at the design stage. For example, the relation between maximum permissible load and strength might be set at a factor of ten. The right curve shows a situation where the margin is insufficient. Sooner or later, the bridge will collapse.

A fault tree can be marked to denote that load is high relative to a certain specified value, or that strength is lower than this value. A combination of these faults can also arise. Sometimes, it can be difficult to distinguish between the two cases.

Component failures are often classified as primary failures, secondary failures and command faults (linked using OR gates). Primary failures occur during normal operating conditions, e.g., from the effects of natural ageing. Secondary failures occur when a component is exposed to conditions for which it is not designed. Command faults refer to functions where the component does work but where its function cannot be fulfilled, e.g., as a result of signals that are faulty or absent.

Other types of trees

Relationships between different functions can be described by various types of trees, not just fault trees. It is easy to confuse different types of trees. An organisation can be illustrated in the form of a tree, and a *hierarchical* tree can show the order of relations between departments. Such trees can also be used to describe technical systems.

A classification into subgroups or classes can also be illustrated by a tree. The word taxonomy is used to describe the classes created when there is a strict classification. Such a tree is not a fault tree, but can form part of one. It can be used to distinguish between different events that may have the same final result.

A success tree can be used to describe what is required for an installation to work. Such trees are also described as logic-flow or function diagrams. In a sense, they are the opposite of fault trees, which show what is required for something not to function.

Simple preliminary evaluation

A fault tree can be used as a basis for making probabilistic estimates, but it is also possible to draw direct conclusions from studying the tree. Some of the questions raised in such an evaluation are as follows:

- Are there only OR gates in the tree? This might mean that the tree is of poor quality, or perhaps not a fault tree at all. Or it might mean that the system is highly vulnerable, since all faults will lead to an accident.

- Are there basic events that directly lead to the top event? This means that a single basic failure will lead to an accident.
- Are the system's safety barriers included in the tree? These will appear as AND gates.
- Can the level of safety be increased? The tree can suggest where a safety barrier may be useful, e.g., by showing when a single failure can cause an accident. Symbolically, such barriers will appear as AND gates.
- Are assumptions clearly specified? Or are important assumptions implicit, e.g., that electrical power will be supplied the whole time?
- Can *common cause* failures be a serious problem? This means that faults that are supposed to be independent are in fact triggered by the same event. Examples include loss of electric power, and several human errors arising in sequence as a result of poor instructions or the misinterpretation of a situation.

Ranking of minimum cut sets

As a basis for further evaluation, the tree is often divided up into minimum cut sets (MCS). A cut set is a collection of basic events that can give rise to the top event. A minimum cut set is one that does not contain a further cut set within itself. In the case of simpler trees, a division into cut sets can be carried out by hand. However, there are a number of computer programmes available that can provide assistance in both identifying cut sets and making probability calculations.

Table 10.2 Ranking of importance of cut sets in a fault tree

Combination	**Comment:** The top event can be caused by
HE	One specific human error (HE)
AC	One active component failure (AC)
PC	One passive component failure (PC)
HE & HE	Combination of two human errors
HE & AC	Combination of one HE and one AC
HE & PC	Combination of one HE and one PC
AC & AC	Combination of two ACs
AC & PC	Combination of one AC and one PC
PC & PC	Combination of two PCs
HE & HE & HE	Three independent human errors are needed
HE & HE & AC	Etc.

MCSs can give a ranking of which basic events make the greatest contribution to the occurrence of the top event (e.g., Brown & Ball, 1980). The ranking is based on the number of basic events in a MCS and on the type of fault, which can be divided into three categories.

Table 10.2 shows a suggestion for the ranking of cut sets according to their importance. If a single fault can cause an accident, this is a serious safety problem. Human errors are ranked high, since they are seen as most likely. That a single fault in an active or passive component can cause an accident comes next in rank. After that, there are different combinations of double faults.

Probabilistic estimates

A fault tree can be used for estimating the probability of the occurrence of the top event. Estimates of probabilities for all the bottom events of the tree are needed for this. Advice on probabilistic methods in FTA is given in a large specialised literature (e.g., Kumamoto & Henley, 1996; Lees, 1996; Stamatelatos et al., 2002). There are various computer programmes available, which will help with the calculations. The greatest general problem is finding failure data of sufficient quality on the various components of the system.

An approximation of the probability of the occurrence of the top event is derived by summing the probabilities of the minimum cut sets. This presupposes that these probabilities are low.

An alternative calculation procedure involves working directly from the bottom events in the tree, moving upwards stage-by-stage, and applying formulas for the AND and OR gates (see Figure 10.6). This provides a clearer picture of which types of faults make the greatest contribution to the occurrence of the top event. The correctness of the result depends on two conditions: that bottom event failures are independent of one another, and that each bottom event appears in only one place within the tree.

Probabilistic estimates have a number of benefits. However, there are also a number of difficulties. Lees (1996) summarises some of the problems involved in using Fault Tree Analysis as a tool for risk estimation:

- The fault tree may be incomplete; there is no guarantee that all faults and all logical relationships will be included.
- Data on probabilities may be lacking or incomplete.
- Estimates for systems with low failure probabilities are difficult to verify.

10.5 Strict and informal fault trees

Different types

A fault tree is a useful representation, which is used in various applications. This is explained by the attractive format and characteristics of fault trees, which show relations between variables and how they can contribute to accidents. The tree format is often easy to grasp, and gives an intuitive feeling of the whole situation.

At first, variants of fault trees look similar, but there may be significant differences between them. Types of trees can be divided into two major groups:

- Strict and formal
- Informal or soft

The *strict type* emanates from reliability and mathematical theory. Features of this group are:

- Well-defined events
- Binary event – with the values true or false
- Events are negative, expressing a fault
- Connections between events are based on strict binary logic in the form of gates
- Strict cause-consequence relations are assumed
- Probability values can (in principle) be associated with the events

Informal trees

An *informal tree* is characterised by the absence of one or more of these features. The degree of informality can vary a lot. Informal trees have been used in various applications, such as cause-consequence diagrams and accident investigations (see sections 12.4 and 13.11).

Accident investigations

The aim of using a tree is to show how various contributions combined so that an accident occurred. The advantage of using a tree is that a quick overview can be presented. Usually, such a tree consists only of AND gates, since all the elements are needed for the accident to occur. In many cases, general and vague descriptions of events and conditions are used. Sklet (2002, p. 38) has recounted a railway accident investigation, which described events in general terms, such as “human error (engine driver)”, “sabotage”, and “engine failure (runaway train)”.

A "fuzzy extended fault tree analysis" has been proposed by Celik et al. (2010). The aim is to combine the effects of organisational faults and shipboard technical system failures in a risk assessment schema. From an accident investigation report, the fault tree defines three main failure states, which are technical failures, operational misapplications, and legislative shortages.

MORT - Management Oversight and Risk Tree (MORT) (Johnson, 1980) provides a third example of a tree structure used in accident investigations (see further in Section 12.7.)

Combining fault tree with organisation

In a study from the railway area, a fault tree showed different causes of how a safety system could fail (Albrechtsen & Hokstad, 2003). The tree is composed of OR gates, and the events at the bottom of the tree are linked to *risk influencing factors*. These are relatively stable conditions that affect the risk of an activity (Rosness, 1998), examples being the design of the trains, maintenance, and operational procedures. Aims were to provide a ranking of the most critical factors, and show how risk reducing measures should be prioritised.

Master Logic Diagram

This is an example of a top-down approach, which can be used to identify events that can trigger accidents in chemical installations (Papazoglou & Aneziris, 2003). It is a logic diagram that resembles a fault tree but without the formal mathematical properties of the latter. The principle is to start with a top event, e.g., *Loss of containment*, and decompose it into simpler contributing events. Such a tree will consist only of OR gates. Events at the bottom can be fairly well technically defined, or specified more generally, in terms like earthquake, flooding, snow, or ice.

Extended fault trees

It is obvious that informal trees can also be valuable in safety analysis. There are many suggestions for how the fault tree concept can be expanded, especially in the mathematically oriented literature.

In this book, I would like to suggest an extension based on the concept of *Influencing event*. This denotes an event, state or circumstance that can have a wide range a meanings and is not binary by nature. This event can influence higher events in some way, but a strict cause/consequence relation is not essential.

For this purpose, two additional symbols are needed. An *Influencing event* is symbolised by a hexagon. The symbol *Influence arrow* indicates that the events above are influenced in some way, e.g., by increasing the probability of occurrence. These two symbols are included in Figure 10.1.

Figure 10.8 illustrates how these symbols can be used, which represents an expansion of the fault tree in Figure 10.7 showing how overload might cause a bridge to collapse. The possibility of excessive load on the bridge is affected by increases in the maximum weight of trucks over time. Strength can be reduced by poor maintenance, and/or by inadequate attention at the design phase.

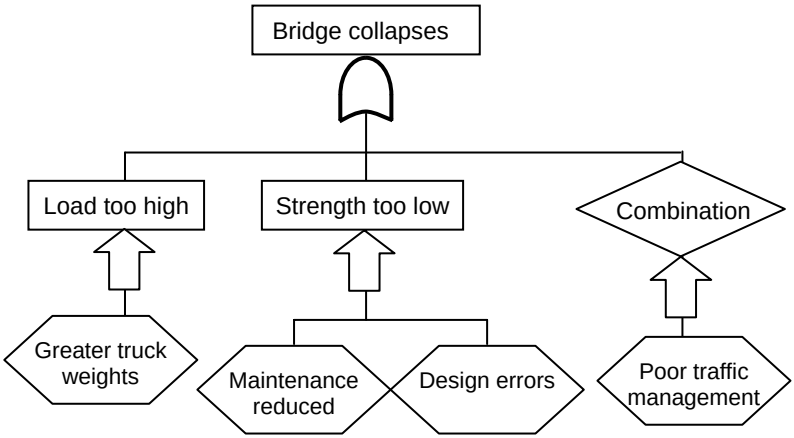


Figure 10.8 Fault tree with influencing events and influence arrows

An advantage of the influence symbol is that it is possible to mix strict and informal trees without creating confusion. The concept can be used in different ways. One approach is first to develop a strict tree, and then indicate the influencing events. You can also start with an informal tree, and either keep it that way, or formalise some parts of it wherever possible.

10.6 Example of a fault tree

System description

A part of equipment for chemical processing (Figure 10.9) is taken as an example. In the tank, two chemicals react with each other over a period of 10 hours and at a temperature of 125°C. When the reaction is complete, the contents are tapped off into drums through the opening of a valve. One hazard in the system is that poisonous gas is formed if the temperature exceeds 175 °C.

The two chemical ingredients are pumped over from two other tanks. The volumes pumped are read off on two special instruments. The contents of the tank are heated by a coil controlled by a relay. The temperature rises at a rate of approximately 2°C per minute when the heating device is connected, and falls at roughly the same rate when it is off.

The temperature is measured using a sensor. The signal from the sensor is linked to the relay and forms a part of the temperature control circuit. If the temperature is lower than required, the relay switches the heating on. If the temperature is too high, the heating is turned off.

As an extra safety feature, the signal from the sensor is also connected to an alarm that is activated if the temperature exceeds 150°C. If the alarm sounds, the operator is supposed to switch off the power feed manually.

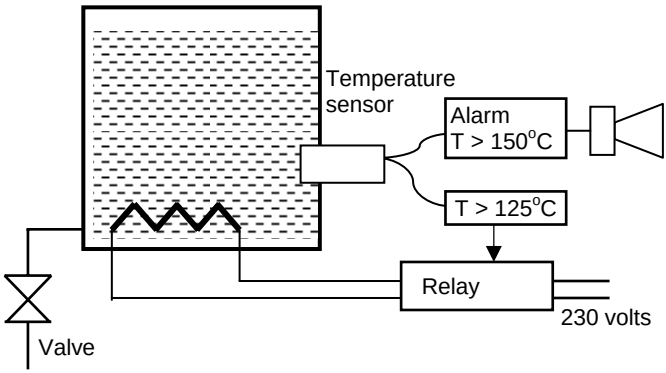


Figure 10.9 Reaction tank with heating and alarm facility

Preparing the analysis

A fault tree is required for the event that poisonous gas is formed, which can occur if the temperature exceeds 175 °C. The level of accuracy of the description is low, but it is sufficient for a preliminary analysis. The

situation is that a proposal has been made, and that the analysis shall be used to evaluate this proposal.

Selecting the top event
The proposed top event *Poisonous gas* can be used directly.

Summing-up known causes
No previous investigation has been made. A Hazop or Deviation Analysis could have been used, which would have given a number of deviations to include in the tree. It can be seen directly that there are some possible faults, which may be hazardous. These include:

- Sensor out of order, giving a low temperature reading
- Temperature circuit controlling the relay function not switching off the power
- Alarm circuit failure

Constructing the fault tree
We start with the top event and see that it is caused by the heating element operating for too long. The upper part of the fault tree is shown in Figure 10.10, which includes two transfer symbols pointing to sub-trees 1 and 2. The tree is divided into two branches combined by an OR gate:

- The temperature sensor system gives too low a value, meaning that the temperature of the liquid will be too high
- The control and alarm system does not work (despite receipt of a correct signal), causing switch-off

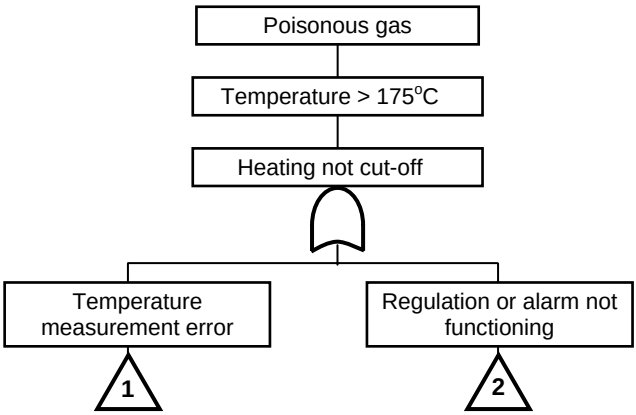


Figure 10.10 The upper part of the fault tree

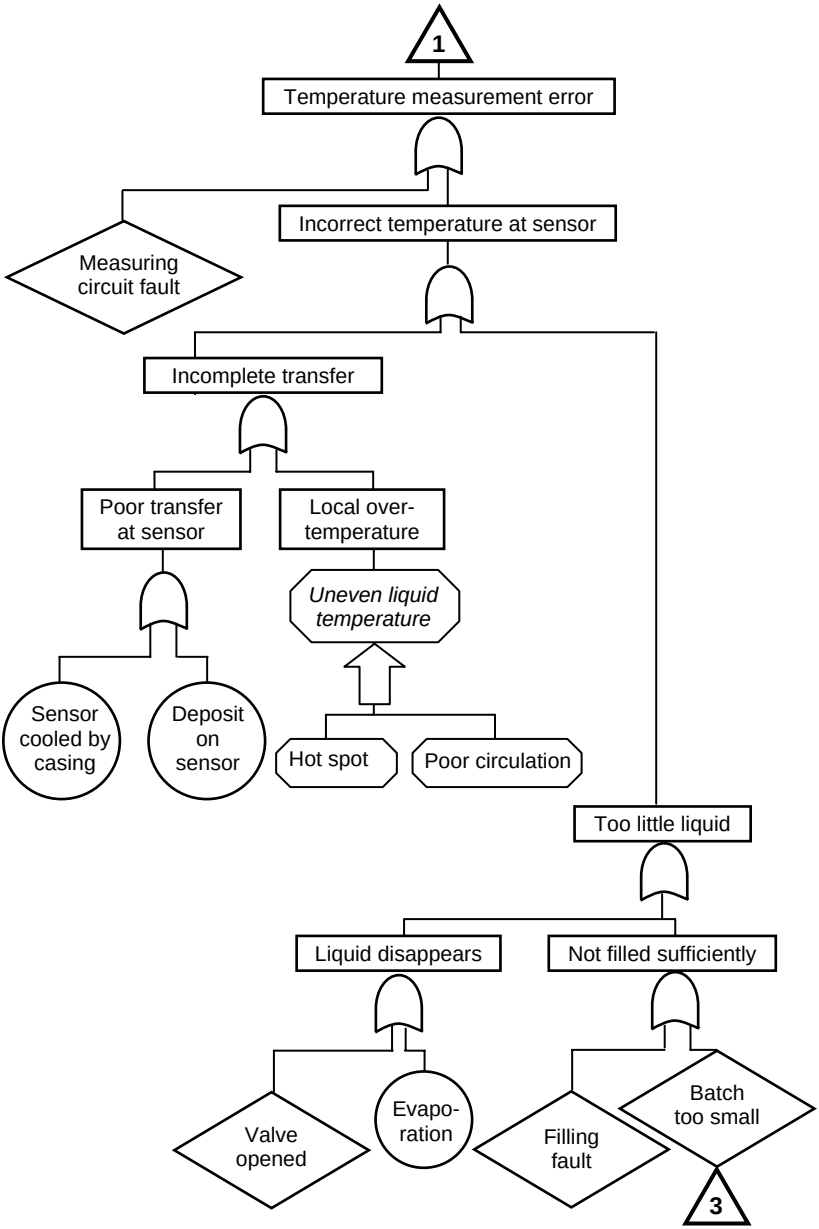


Figure 10.11 Branch 1 of the fault tree

Branch 1 (Figure 10.11) explores how *temperature measurement error* might occur, possibly due to a fault in the measuring circuit. However, no details of the circuit are available, and therefore a rhombus is used to mark an undeveloped event.

That the measured temperature at the sensor is incorrect can depend on that transfer of heat from the liquid is incomplete. Another possible reason is that there is not enough liquid in the tank, meaning that the sensor cannot measure the temperature.

Branch 2 (Figure 10.12) shows how a failure to cut off the heating device may arise. There is not much information on the technical design, and on how the alarm should be used. Accordingly, the fault tree is small, and merely indicates what might be included.

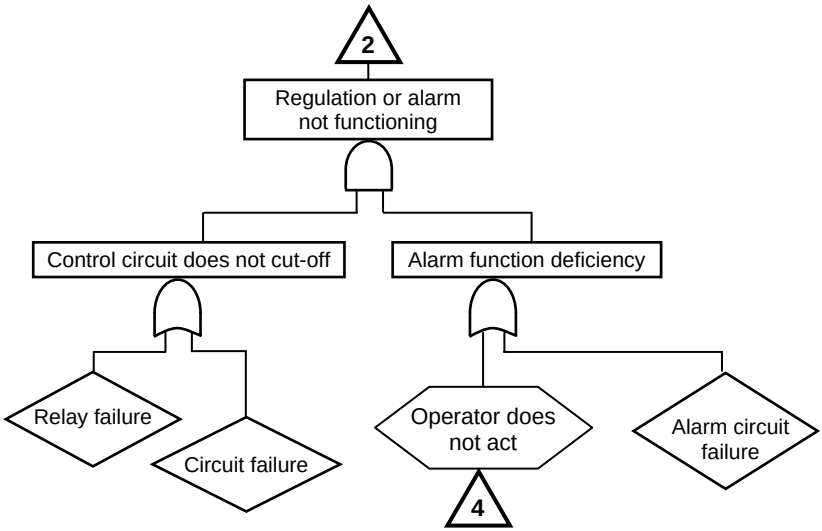


Figure 10.12 Branch 2 of the fault tree – for cutting off heating device

Branch 3 (Figure 10.13) goes deeper into problems of small batch size (less than a certain defined volume), which are related to the technical design and to the filling instructions. These are not binary events; instead, they are symbolised as *influencing events* (states).

Branch 4 (Figure 10.13) concerns the possibility that the operator might do a check and make a correction if there is not enough liquid at the sensor. This branch is also modelled in terms of influencing events.

These two informal trees draw attention to the roles of the operator and management. The influence arrows show that there is some kind of influence, but not how. In *Branch 3*, it is a combination of sensitivity and poor routines, which is associated with an AND function. In *Branch 4*, the relations are rather vague.

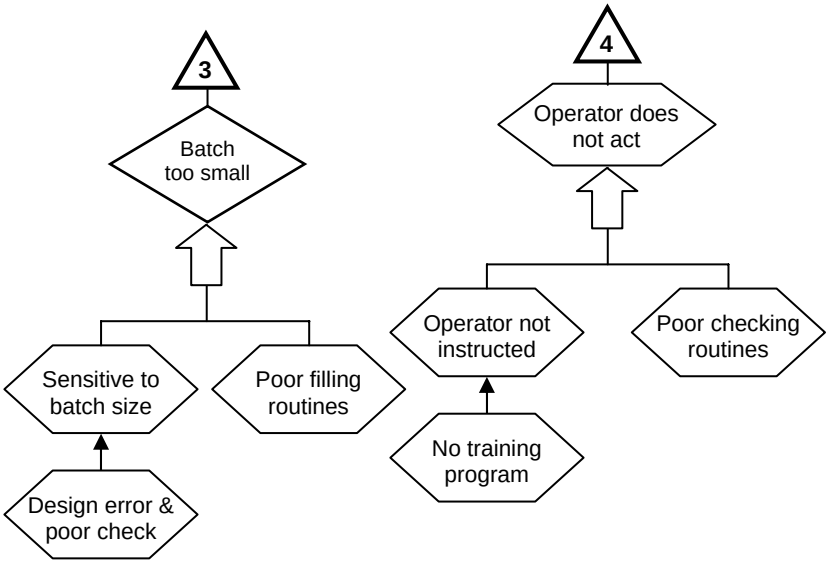


Figure 10.13 Branches 3 and 4 of a fault tree for influencing events

Revising, supplementing and testing

The tree has been developed though a process of revision and supplementation. In this case, there was a need to redefine and rephrase many of the events for them to be sufficiently descriptive. The text in the tree is short, and the meaning of each event is clarified, at least to some extent, by its context and by events. Since temperature measurement errors affect both temperature regulation and the alarm function, it is advantageous to find a solution in which the same errors do not appear twice in the tree.

Assess results

A simple assessment is to inspect the tree. *Branch 1* contains only OR gates, which means that any of the eight events at the bottom lead directly to the top event. There are no safety features to prevent this, which would have been seen AND gates in the tree.

The conclusion that can be drawn from the tree is that any one of eight single-failure events may lead directly to the occurrence of the top event. The safety level has to be regarded as unacceptable. It is also important to have well-developed routines for operations and maintenance.

The installation requires radical re-design and an increased level of safety. The new design and construction proposal will require analysis. Both what precedes and what follows the heating phase must be considered.

Comments

The tree can be seen as providing a first general overview. If there is a demand to go further and attempt to estimate the probabilities, the tree must be more stringently constructed. Some of the bottom events must be defined more precisely, and the relations between them further specified.

Although the tree appears large enough, it is still not complete. For example, the situation where the tank has not been emptied completely is neglected. If the heating is switched on by mistake, the temperature will be too high. Such a situation might to some extent be fitted into *Liquid disappears*, but it is still not fully covered. This is because the analysis only treated the system during continuous operation.

There are three kinds of bottom events, with the traditional *Basic event* (ring) and *Undeveloped event* (rhombus,) and the new *Influencing event* (hexagon). However, it is not always obvious which bottom symbols should be chosen, and several of the ringed sections could be further analysed in further branches. The informal parts of the tree (Figure 10.13) indicate the role of management and operators.

In total, there are 14 bottom events in the tree. However, this number could easily be doubled if a more thorough analysis was conducted. Even in a case as simple as this, a fault tree can become very large. In retrospect, it can be said that the range of the analysis was too narrow.

10.7 Comments

Pro and cons

Fault Tree Analysis is the most difficult of the methods presented so far. After proper training it is not difficult to conduct an analysis, but it requires effort and may take a long time.

The length of time it takes to learn the method obviously depends on the level of ambition and previous knowledge. It may be fairly easy for electronic engineers and computer programmers who are trained in the handling of logical circuits and functions.

Some of the advantages of Fault Tree Analysis are:

1. It is an aid for identifying risks in complex systems.
2. It makes it possible to focus on one fault at a time without losing an overall perspective.
3. It provides an overview of how faults can have serious consequences.
4. For those with a certain familiarity with the analysis, it is possible to understand the results fairly quickly.
5. It provides an opportunity to make probabilistic estimates.

Some of its disadvantages are:

6. It is a relatively detailed and, in general, time-consuming method.
7. It requires expertise and training.
8. It can give an illusion of high accuracy. Its results appear advanced and, when probabilistic analyses are conducted, these can be presented in the form of a single value. But, as with most methods, there are many possible sources of error.
9. It cannot be applied mechanically, and does not guarantee that all faults are detected. In general, different analysts will produce a variety of different trees. But a tree can have different forms and still have the same content.
10. Its implementation generally requires detailed documentary material to be available.

Some problems

One problem is that a tree may be large and require a large amount of time to develop. A second problem is that an analysis may have too sharp a focus on technical failures. Human and organisational factors may be neglected in this type of method. For this reason, immediate concentration on technical failures alone should be avoided. If technical aspects prove to be extremely important, they can be studied in greater depth at a later stage of the analysis.

A simplified picture

A fault tree is a simplification of reality in many senses. One concerns the adoption of the binary approach; an item either works or does not, and nuances in-between are disregarded. Another simplification is that the analysis is restricted to strict logical connections between events, which means that a lot of information must be excluded.

Checking existing trees

Sometimes, a fault tree is already available, and the analyst has the task of evaluating and interpreting it. What might have been overlooked? Some of the questions to address are as follows:

- What assumptions about and simplifications to the system have been made?
- Are only technical failures included?
- Does the tree follow the *rules of thumb*? (The ones given in Table 10.1 are in no way generally accepted or applied, but they do provide some sort of measure of quality.)
- Are there only OR gates? If all failures lead to the occurrence of the top event, the system is dangerous. However, there are also grounds for wondering whether the tree is correct.
- Are there only AND gates? If that is the case, the tree might describe only a very specific accident.

A fault tree can be seductive, encouraging the belief that it is complete and has been well thought through. Therefore, it is worthwhile to do an independent check on the tree, especially if it is the ground on which important decisions will be made.

11 Barriers and safety functions

11.1 The analysis of safety

So far, this book has described methods for safety analysis that are oriented towards the identification of hazards, failures and problems. In this chapter, the focus is on the safety characteristics of a system. This has some potential advantages:

- A comprehensive description and analysis of the safety features of a system is useful.
- Judgements on whether a system is safe enough can be supported by a systematic evaluation, based on assessments of whether the safety functions have sufficient coverage and efficiency.
- Safety functions (both technical and organisational) can be appropriately designed from the beginning on the basis of a suitable analysis.

In accident investigations, the main goal is usually to explain the course of an event. In most systems, there are several safety arrangements in place to prevent accidents from occurring. A basic question is then how the event could have happened despite the safety features. Accordingly, an essential aim of any investigation is to analyse how the safety system failed.

For a long time, there has been considerable interest in the modelling and analysis of safety features and accident prevention. However, concepts and terminology related to safety features vary. There are a number of analytic methodologies, which more or less explicitly include barriers and their roles in the course of an accident.

Interest has been especially great in the off-shore, chemical, and nuclear industries, and research has been heavily oriented towards complex technical installations with advanced control systems (e.g., Harms-Ringdahl, 1999; Hale, 2006; Sklet, 2006). There are many challenges in areas with complex technical and organisational settings, which require sophisticated methods.

However, this represents only a small fraction of the field of accident prevention. Common workplaces, and to an even greater extent out-of-work

situations, produce many more injuries and fatalities than major hazard industries (see sections 1.2 and 2.4). Despite this, these types of situations have received less attention in the analysis of barriers and other safety features.

The transfer of methods from high-risk areas is not uncomplicated, since they represent different kinds of conditions (Harms-Ringdahl, 2004). Many diverse elements contribute to the safety level in the workplace, with both technical and organisational safety features functioning together. *Safety culture*, social factors and informal behaviour can also make essential contributions.

Such considerations have made me interested in exploring the possibilities of obtaining a consistent framework, which could combine technical and organisational – formal as well as informal – safety features. This has also been a major motive for further developing barrier concepts and methodologies that can also work in fairly simple situations.

This chapter presents concepts and methods related to barriers and safety. *Safety functions* have received special attention, since the idea of a safety function was developed also to be useful in informal and relatively simple systems. The concept can be used for the analysis of systems and for accident investigation.

11.2 Barrier concepts and methods

General

There are many approaches to the description of safety characteristics in systems, and terms like barriers and defences are often used to describe them. Energy models have been used for a long time, and they usually involve technical as well as organisational barriers. Johnson (1980) defines barriers as physical and procedural measures to direct energy in wanted channels and control unwanted release. Examples are the containment of a chemical substance, and the maintenance procedure for the container.

Barriers to accidents can be seen from various perspectives, and there are several types of definitions and categorisations. Hollnagel (2004) has presented a number of classifications, e.g., a division into *physical*, *functional*, *symbolic*, and *incorporeal barrier systems*.

A common term is *defence*, which is defined by Reason (1997) as "various means by which the goals of ensuring the safety of people and assets can be achieved". In simple terms, defences shall prevent hazards from causing losses. A distinction has been made between *hard* defences, such as physical barriers and alarms, and *soft* defences, e.g., regulations, procedures, and training, which can combine in several layers.

A defence can be weakened by *active failures*, e.g., unsafe acts, or by *latent conditions*, such as poor design. A combination of active failures, latent conditions, and *local circumstances* might cause an accident to occur. Defence is a wider concept than that of barrier

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

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

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

In these definitions, the barrier function describes the purpose of safety barriers, and it should have a direct and significant effect. A barrier function should preferably be defined by a verb and a noun, e.g., *Close flow*. These definitions emphasize the intention and the planning.

According to this set of definitions, a function that has an indirect effect is not classified as a barrier function, but as a *risk influencing factor/function*. Sklet (2006) points out that the definitions refer to major hazard installations and well-defined systems, which are carefully planned and designed.

The nuclear power sector

Safety within the nuclear power sector is documented in numerous reports. The IAEA (2006) has provided a summary of 10 basic safety principles, which are to guide the industry. The fundamental safety objective is to protect people and the environment from the harmful effects of ionizing radiation. The safety principles are:

1. Responsibility for safety. The prime responsibility for safety must rest with the person or organisation responsible for facilities and activities that give rise to radiation risks.

2. Role of government. An effective legal and governmental framework for safety, including an independent regulatory body, must be established and sustained.
3. Leadership and management for safety. Effective leadership and management for safety must be established and sustained in organisations concerned with, and facilities and activities that give rise to, radiation risks.
4. Justification of facilities and activities. Facilities and activities that give rise to radiation risks must yield an overall benefit.
5. Optimization of protection. Protection must be optimized to provide the highest level of safety that can reasonably be achieved.
6. Limitation of risks to individuals. Measures for controlling radiation risks must ensure that no individual bears an unacceptable risk of harm.
7. Protection of present and future generations. People and the environment, present and future, must be protected against radiation risks.
8. Prevention of accidents. All practical efforts must be made to prevent and mitigate nuclear or radiation accidents.
9. Emergency preparedness and response. Arrangements must be made for emergency preparedness and response for nuclear or radiation incidents.
10. Protective actions to reduce existing or unregulated radiation risks must be justified and optimized.

Defence in depth

Safety Principle 8 is based on the concept of *defence in depth*. It is the primary model for preventing, and mitigating the consequences of, accidents. It is implemented through the combination of a number of consecutive and independent levels of protection that would have to fail before harmful effects could occur. If one level of protection or barrier should fail, the subsequent level or barrier should be available. When properly implemented, defence in depth should ensure that no single technical, human or organisational failure could lead to harmful effects, and that the combinations of failures that could give rise to significant harmful effects are of very low probability. The independent effectiveness of the different levels of defence is a necessary element of defence in depth.

The chemical sector

The chemical industry also has a long tradition of systematic safety work. A comprehensive overview of safety principles is provided in the “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 systems
5. Physical protection (relief devices)
6. Physical protection (containment devices)
7. Plant emergency response
8. Community emergency response

Other aspects

Organisational aspects are highly relevant to the performance of safety systems. An advanced 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. Safety tasks are modelled using the Structured Analysis and Design Technique (SADT).

Automation and control arrangements are fundamental to safety in most industrial and transport systems. There are several guidelines and standards that concern such applications, e.g., *safety interlock systems.*

One example of this is the extensive standard on the functional safety of electrical/electronic/programmable electronic (E/E/PE) safety-related systems from the International Electrotechnical Commission (IEC, 2001, Part 4, page 17). It covers the aspects that need to be addressed when electronic systems are used to carry out safety functions. The standard is technically oriented, and defines safety function as follows:

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

Methods for the analysis of barriers and safety

The list below summarizes a number of methods that are oriented towards barriers and safety functions. They can be used for the analysis of systems and/or investigations of accidents, and are presented in different sections in this book.

- *AEB.* The *Accident Evolution and Barrier Function method* (Svenson, 1991; 2000) can be used for analysis of accidents and incidents (see Section 13.4).
- *MORT. Management Oversight and Risk Tree* (Johnson, 1980) can be used for the analysis of systems and accidents (Section 12.7).
- *SADT. Structured Analysis and Design Technique* (Hale *et al*., 1997) can be used for the analysis of safety management systems (Section 12.7).
- *Safety Barrier Diagrams* (Taylor et al., 1989; Taylor, 1994; Duijm, 2009) offer a way of presenting and analyse barriers to accidents (Section 12.4).
- *Safety Function Analysis* (Harms-Ringdahl, 2000) can be used for the analysis of a system or in an accident investigation (sections 11.4 and 13.10).

Other examples of methods that include barriers in some way are:

- *Energy Analysis*. Barriers are a fundamental part of the method (Chapter 6).
- *Event Tree Analysis*. One common application (Rouhiainen, 1993) is to check a safety function to see whether or not an event gives rise to damage (Section 12.3).
- *Fault Tree Analysis* can show how barriers and safety features might prevent an accident (Chapter 10).
- *MTO-analysis* is used to investigate accidents; a summary of barriers is included in the method (Section 13.6).

11.3 Concept of safety function

Different terms

As shown above, the terminology used to describe safety features varies considerably. Some examples:

- *Barrier*; the term is used in many ways.
- *Barrier function*
  (a) can arrest accident/incident evolution so that the next event in the chain will not happen (Svenson, 1991, 2000)
  (b) is a function planned to prevent, control, or mitigate undesired events or accidents (Sklet, 2006).

- *Barrier function systems* perform the barrier functions (Svenson, 1991, 2000).
- *Barrier system* has been designed and implemented to perform one or more barrier functions (Sklet, 2006).
- *Defences* (Reason, 1997).
- *Protection layer* (defined by example) (CCPS, 1993).

Often, the methods and terms emanate from advanced technical systems, with strict managerial control and well-defined conditions. The role of management for safety is widely acknowledged. However, the importance of informal behaviour and the handling of rules is easily overlooked. It is therefore of interest also to consider these aspects systematically in an analysis.

The following sections describe a methodology that is designed to achieve the consistent handling of different kinds of situations and safety features. As a basic idea, the concept of *safety function* has been used. It has been gradually developed and tested over the years (e.g., Harms-Ringdahl, 1999, 2001, 2003A, 2003B, 2009).

Definition of safety function

Safety function (SF) is a rather common term, which is used in different situations and with various meanings. There are no general definitions in the literature, which has a broad scope. For use in a general methodology, there is a need for a clear definition. A simple description runs as follows:

> *A safety function contributes to reducing risks in a system.*

I have suggested a more explicit definition (Harms-Ringdahl, 2009):

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

Quite deliberately, safety function is defined as a broad concept. One basic idea is to avoid unnecessary assumptions, and instead focus on the functions that might make a system safe. In principle, it covers all the definitions and concepts presented earlier in this chapter. In specific applications, it requires more concrete characterisations, and a number of parameters can be used for them.

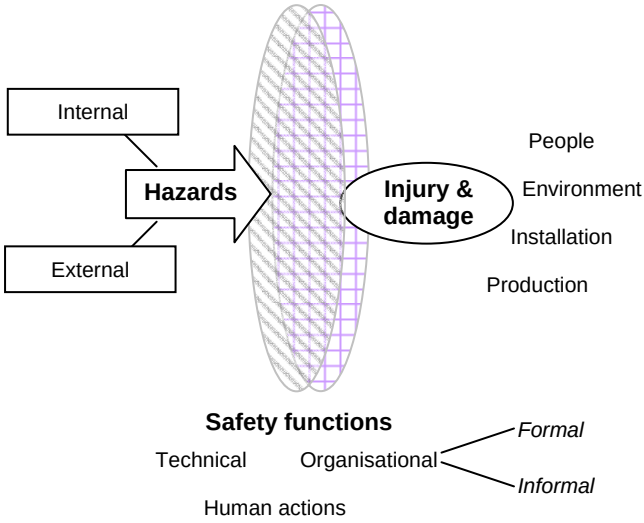


Figure 11.1 A general model of safety functions

The concept and its basic components are symbolised in Figure 11.1. The model might represent a company subject to a number of different hazards. The hazards include energies, and different kinds of internal or external disturbances, which can cause different kinds of injury and damage. In order to prevent these, there is a set of safety functions.

Safety function parameters

The generic SF concept needs to be more concrete in practical applications. The general approach is to let the SF be described by a set of parameters, which may include:

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

a) ***Level of abstraction*** goes from a theory to a concrete solution, e.g., a safety relay or a temperature guard. Table 11.1 gives examples at different levels.

Table 11.1 Level of abstraction for safety functions

	Level of abstraction	**Example**
1	Theory	Explodes if hot
2	General function, e.g., aim	Limit temperature
3	Principal function	Monitor temperature – one of several options
4	Functional solution	Thermometer – checked by operator or electronically
5	Concrete solution	Action by operator or by safety relay

b) ***Systems level*** is related to the systems hierarchy; from the bottom, it could go from components, subsystems, machines, departments up to a whole factory. Table 11.2 gives examples that include five levels, from the railways and from medical services.

Table 11.2 System levels for safety functions

	System level	**Example 1**	**Example 2**
1	General system	Railway traffic in Sweden	Medical services in Sweden
2	Specific system or establishment	Railway company AB	Hospital in city CD
3	Department, or part of system	Train services around city E	Maternity ward, or a children's ward
4	Activity, or subsystem	Railway wagon	Administration of medicine
5	Component, or sub-operation	Wagon wheel, or safety relay	Drug prescription by doctor

c) ***Type of safety function*** describes what is included in a safety function. It can be divided into technical, organisational and human subfunctions, and combinations of these. It may be valuable to distinguish between formal and informal organisational issues.

d) ***Type of object*** characterises the object under study (or under evaluation), i.e., the system that is to be safe. This may be a technical system, software, control room, related equipment, etc. Organisational conditions of different kinds can be included here. Examples include the management of projects and maintenance.

In addition to the parameters above, other characteristics can be used to describe or judge a specific SF. Characteristics can, for example, concern importance, efficiency, and intention. These can be subject to evaluation, as further discussed in Section 11.5.

Web of safety functions

I have used SF methods in many different applications, and there has always been overlap between different SFs. Even at companies with a formal approach to safety, it has been obvious that the systems contained formal and informal elements side-by-side.

Such overlaps can be seen as safety redundancy, which makes a safety system less vulnerable to change. It might be better to describe such a system as a safety web rather than referring to a distinct set of barriers.

A web structure of this kind might contribute to the preservation of safety, or improve the safety resilience of the system in other ways (see, e.g., Hollnagel et al., 2006). The SF concept may be an aid to exploring how organisations can maintain or develop their safety work, and might be a complement to or substitute for organisational audits.

11.4 Safety Function Analysis

About the method

Safety Function Analysis (SFA) is a method based on the concept of safety function. It is generic, and can be applied to most types of systems and unwanted events. The methodology has gradually been developed during the last ten years (see, e.g., Harms-Ringdahl, 2001, 2003A, 2009). The general 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

SFA has two general applications, which are quite similar. The first takes the system, e.g., a workplace, and its hazards as a starting point. The aim of such an analysis is to cover the entire system, more or less thoroughly.

The second concerns accident investigations. The method can be used to draw conclusions about SFs and their properties on the basis of an accident or near-accident. This application and its features are described in the chapter on accident investigations (Section 13.10).

Since the method is generic, the final results can have quite different appearances. Dependence on procedure and the analyst's skill is greater than for more traditional methods. For example, structuring and estimates

can be made and presented in various ways. Therefore, it is important that the analytic procedure is clear and transparent.

SFA procedure

The analysis is based on a defined procedure with a set of stages. Like other methods, it includes a preparation phase, where aim, scope, assumptions, etc. are defined. There is also a concluding phase for the reporting and use of results. Apart from this, an analysis contains five specific main stages (see Figure 11.2).

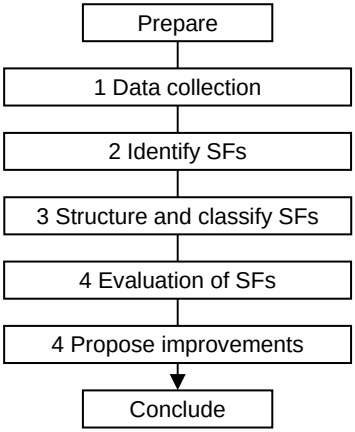


Figure 11.2 Main stages of procedure in Safety Function Analysis

Preparation

Before an analysis can be conducted, its aim and basic conditions need to be defined. This may concern:

- Specific aim and scope of the analysis – a general analysis or an accident investigation
- A clarification of the object of the analysis, the boundaries of the system under study, and what shall be included in the analysis
- The types of hazard for which the safety functions shall be studied, which may include not only accidents, but also production disturbances or environmental damage
- The operational conditions that are supposed to prevail
- Planning of the analysis, in terms of the time and resources available
- Employing a working group

A working group can be effective, both for collecting data on safety features and for evaluating the functions. This is important, in particular if informal safety features are included in the analysis.

1) Data collection

The data collection stage can vary a lot. Possible sources are written materials, such as:

- A summary of existing safety activities
- A previous safety analysis from another type of method, usually showing problems
- A report from an accident investigation, usually showing problems
- Technical documents concerning production processes, equipment or facilities, and also drawings, manuals, and maintenance records

Interviews give valuable information, especially about informal SFs, which are seldom obvious in official documentation. The identification of SFs (see next stage) can be directly included in the interviews.

2) Identification of safety functions

Approaches to the identification of SFs can be placed into five partly overlapping groups. The results will be at a fairly concrete level, with the identified SFs listed in a table. This is the output of Stage 2. The approaches are:

a) Text analysis
b) Interviews
c) Hazard oriented analysis
d) Sequence oriented analysis
e) Comparison with a given set of SFs

a) Text analysis is usually based on documents. It can be a description of the safety features of the system, of an accident, or of other related circumstances. The analyst follows the text, and tries to identify the words or phrases that directly or indirectly indicate a safety function. A practical way of doing this is to use a marker pen to indicate relevant words or phrases. If it is an electronic document, the cut-and-paste commands can be used.

b) Interviews and discussions give additional information and also greater freedom in the search. One procedure is to pose open questions about what might happen, what might prevent an accident from occurring, etc. By listening carefully, the analyst can pick up what can be understood as SFs. This is similar to text analysis.

c) Hazard oriented analysis can start from a specific accident scenario or from a set of hazards. The following kinds of questions are posed:

- 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?

d) Sequence oriented analysis can be practical in investigating an occurred accident, or in the study of an accident scenario. In principle, it follows the course of events, preferably starting with the accident and going backwards. If rescue and amelioration are of interest, a complementary round going forwards can be performed. The search can be guided by a set of questions, such as:

- What technical means (could have) prevented the event/state X?
- What human actions (could have) prevented the event/state X?
- What organisational routines (could have) prevented the event/state X?

e) Comparison with a given set of SFs is a special category of identification. One approach is to start with a structured checklist of general safety functions, and to identify the ones that are relevant. This application can be attractive when several earlier investigations have been performed of similar systems, and the time for analysis is limited.

3) Structuring and classification

The identification stage has generated a list of SFs, in a more or less arbitrary order. The aim of structuring is to sort the SFs in a logical way to facilitate a further analysis. You could see the structuring stage as making a model of the safety features in the system. This stage should be seen as an iterative process, which improves the structure bit by bit. It may look tricky, but you should be aware that there is no unique solution.

The first step is to select two or three categories that can describe the material. The choice depends on the data you have. You could try:

- Types of SFs, such as technical, organisational, human, or other
- Organisational aspects, such as how they are related to actors and the organisations to which they belong.
- Steps in the accident sequence, such as how the SFs are related to starting phases, acute phases, emergence actions, or mitigation.

Each SF is classified on the basis of these categories. The next step is to sort the SFs according to the classification. Practically, this can be done by arranging the material in a table, using a program like Excel or Word. This will make the sorting fairly easy, and different sorting orders can easily be

tested. After the sorting, the material might be in fairly good order. Otherwise, another categorisation can be tried instead.

After sorting, it is useful to check the material, and perhaps rephrase some items to get a more consistent set of SFs. In this way, duplicates or almost identical SF can be found and merged.

The next structuring step has the aim of grouping the SFs at a higher systems level. The parameters in Section 11.3 might be of help in finding a suitable solution. The way of structuring such material is difficult to describe, and some readers might find it more useful to look at examples. Some can be found in sections 11.7, 16.2, 16.3 and 16.9.

In some cases, it is helpful to create sub-classes under the main heading. One simple example is to divide a set of *technical SFs* into *electrical elements, mechanical elements, containment of chemicals*, or things of this kind.

4) Evaluation of SFs

The aim of this stage is to characterise the SFs and evaluate whether changes are needed. Different approaches are described in the following section (Section 11.5).

5) Propose improvements

Usually, the results of the evaluation show that there is a need for improvements of some SFs. The purpose of this stage is to generate proposals for how to do this. As usual, it is valuable to employ a working group. Support for developing improvements is given in Section 11.6.

Concluding

The analysis is concluded by making a report. This summarises the analysis, and gives assumptions, results, conclusions, and a basis for assessment.

11.5 Evaluation of SFs

Basic considerations

Evaluation is an important step in the SFA procedure. The general aim is to characterise the SFs and to evaluate whether changes are needed. Different approaches can be used for the evaluation, and here we show alternative ways of proceeding. The stage can be divided into two steps. At the first, each SF is evaluated separately. At the second, a systems perspective is adopted to see how the different SFs work together.

When the method is used for accident investigation, the actual performances of the SFs are estimated. This is more thoroughly discussed in Section 13.10, which deals with how the method can be applied to event investigations.

Set of estimates
There are a number of characteristics that can be valuable in estimating an individual SF. Examples are:
A) Importance of the SF
B) Efficiency of the SF
C) Intention of the SF

These give a foundation for the valuation of system performance:
D) Need for improvement of the SF

Simple evaluation

The characteristics A to D are presented briefly below, along with suggestions on how they can be classified. One way is for the analyst (or working team) to make the estimates. An alternative is to interview people in different positions in the organisation, and get their independent judgements. In one test (Harms-Ringdahl, 2003A), the different perspectives proved to give valuable input into the analysis.

At the estimation stages, one option is to include *Not estimated* as an option (where, especially in the case of interviews, it means *No opinion*). This option has not been included in the examples below.

A) Importance
Importance can be categorised into four types from a safety point of view (see Table 11.3). The first type (0) means in practice that the SF could be removed without affecting the probability and potential consequences of an accident.

Table 11.3 Scale of importance for SFs

Code	Importance
0	SF has no or very small influence on safety
1	Small influence on safety
2	Rather large influence on safety
3	Large influence on safety

B) Efficiency of SF
The efficiency of an SF is the ability to perform its (intended) function when needed, which can be described in the form of a probability. It ranges from 0% for a function that always fails, to over 99.99% for a function that works well.

Sometimes, *success rate* or *probability to function* is a suitable term. Looking over a specific time period, *frequency of error* might be more relevant and can be seen as the negative expression of efficiency. Examples of coarse scales for efficiency are given in Table 11.4. One alternative is to make probabilistic estimates.

Table 11.4 Scales of efficiency for SFs based on probability or frequency of error

Code	***Efficiency***	*Probability to function*	*Error frequency*
0	Very low	<50%	-
1	Low	>50%	<100 times/year
2	Medium	>90%	<10/year
3	High	>99%	<1/year (>0.01)
4	Very high	≥99,99%	<0.01/year

C) Intention

The *intention* of an SF can be included in the estimation. Table 11.5 suggests a classification of intentions. The first two categories are concerned with the influence on safety. Sometimes it is hard to know the original intention; instead of guessing, the code 9 could be used.

Table 11.5 Classification of intentions and degree of planning

Code	**Description**
0	No intended SF, and no influence on safety
1	No intended SF, but influence on safety
2	Intended SF, but main purpose is something else
3	Intended to provide an SF
4	Intended to provide an SF through a formal system
9	Uncertain intention

Intention is not an essential or necessary parameter. This is actually one important feature of the SF concept, which makes it possible to handle both intentional and unintentional safety issues. However, the intention can give important information on how the SF works, and how it can be managed.

One reason to include intention is that it might clarify responsibility for a specific SF, which can be both formal and informal. This can be valuable when major changes are planned; otherwise, important safety features might get lost.

Simple evaluation

After identification of SFs and estimating some of their characteristics, it is time to draw conclusions and perform the evaluation. The basic aim is to evaluate each SF, in order to decide whether something needs to be done to reduce or control the hazard, or whether no improvement is needed. A simple way of doing this is to apply the Direct Evaluation principle described in Section 5.2, and to use Table 11.6 (similar to Table 5.2).

Table 11.6 Evaluation scale for the acceptability of safety functions

Code	Description	
0	No need for improvement	*Acceptable*
1	Improving* SF can be considered	
2	Improving SF recommended	*Not acceptable*
3	Improving SF is imperative	
4	Intolerable, work should not be started or continued until the risk has been reduced.	

Improving* also includes further investigation

Advanced evaluation

Using the safety function concept it is possible to perform fairly advanced evaluations. This is interesting in systems where the consequences of accidents may be serious. In such situations, it is advantageous to have procedures and defined rules that can make for a transparent and traceable evaluation.

One further aim may be to support engineers with good knowledge of the system, but without experience of risk assessment (Celeste Jacinto,[1] personal communication, 2009). Based on these ideas, an evaluation principle was developed and is described here. This has also been tested in a study with favourable results (Jacinto et al., 2013).

This solution requires the inclusion of three more characteristics:

E) Wanted efficiency, i.e., the setting of a target for the level of efficiency
F) Needs for monitoring of the function
G) Monitoring status, i.e., an automatic or manual check on whether the SF works satisfactorily

[1] Universidade Nova de Lisboa, Portugal

Efficiency – wanted and estimated

The efficiency of an SF is important, and scales to estimate it are presented in Table 11.4. One parameter is *Wanted efficiency* (WE), which is a target for what should be achieved. It can be seen as a more or less formal specification. Normally, when an SF has high importance, it also requires high efficiency. A complementary parameter is *Estimated efficiency* (EE), which is an estimated value of the actual efficiency of the studied SF.

Monitoring as an additional characteristic

Monitoring is an additional characteristic. The aim is to check whether the SF operates well enough. This is essential, since the efficiency of an SF might degrade over time, and a monitoring system can support sustainable functioning. The monitoring can consist in a manual checking routine, or be performed automatically by an electronic system.

One parameter is *Monitoring needs* (MN), which is a target. This is a judgement based on how the *Wanted efficiency* should be maintained. Monitoring status (MS) is based on a comparison between needs and what is actually present. Table 11.7 shows different levels of monitoring, and also a scale for estimating performance status.

Assessing MN and MS is an important part of the evaluation. If MN is low (0 or 1) there is no need for monitoring, which means that monitoring requirements are met automatically.

Table 11.7 Scales for monitoring needs and judgements on status

Code	Monitoring needs		Code	Monitoring status
MN4	Monitoring is essential	}	MS2	Meets the requirement
MN3	Monitoring is necessary, at least periodically		MS1	Exists, but does not fully meet the requirement
MN2	Monitoring is of interest, but not a critical issue		MS0	Monitoring function does not meet the requirement
MN1	Of low interest	}	MS2	OK, no need for monitoring
MN0	Not needed or irrelevant		MS2	OK, no need for monitoring

Evaluation process

In this detailed evaluation, the starting material is a structured table of SFs. For each SF, the evaluation team should assign values to the parameters. The table contains columns for the parameter values. When the parameters are estimated there is a set of decision rules, which determine whether the SF is acceptable as it is, or whether improvements are needed.

The parameters needed for the decision rules are:

a) *Importance* (IMP: 0–3; Table 11.3).

b) *Wanted efficiency* (WE: 0–4; Table 11.4). WE is a target for what should be achieved. It is a judgement. Normally, high importance requires high efficiency.

c) *Estimated efficiency* (EE: 0–4; Table 11.4) is a judgement on the actual efficiency of the existing system.

d) *Monitoring needs* (MN: 0– 4; Table 11.7) are a target. It is a judgement based on the actual SF and how the wanted efficiency (WE) should be maintained.

e) *Monitoring status* (MS: 0–2; Table 11.7) is a comparison between needs and what is actually present.

f) *Acceptability* is obtained by applying the decision rules, as suggested in Table 11.8. The output consists in the values in Table 11.6, showing whether or not improvements are needed.

Decision rules

The values of these characteristics are the input to the decision rules, and generate an answer to the question of whether or not improvements are needed. An example of a set of rules is given in Table 11.8, where the three first columns are used for the input of the values, and the fourth column gives the output.

The general principle is that important SFs must be efficient, and that monitoring is an essential tool for achieving this. When the rules are established, they can be formulated as logical expressions, which can be used in computer programs, such as Excel, and then automatically give results after entering the input characteristics.

Table 11.8 Example of decision rules for SFs

Importance IMP	**Efficiency** Estimated / Wanted	**Monitor MS**	**Accep-tabilty**	**Comments on improvements**
0 Very small	EE ≥ WE	–	0	Improvement is not needed
	EE < WE	–	1	- can be considered
1 Small	EE ≥ WE	–	0	- not needed
	EE < WE	0	2	- recommended *Prevent degrading of SF*
		1-2	1	- can be considered
2 Rather large	EE ≥ WE	0-1	2	- recommended *Prevent degrading of SF*
		2	0	- not needed
	EE < WE	0	3	- imperative
		1-2	2	- recommended
	EE << WE	–	3	- is imperative
3 Large	EE ≥ WE	0	3	- imperative
		1	2	- recommended
		2	1	- can be considered
	EE < WE	0	3	- imperative
		1	3	- imperative
		2	2	- recommended
	EE << WE	0-1	4	Intolerable situation
		2	3	- imperative

– = Any MS value

System evaluation

The descriptions above have concerned how individual SFs are judged. In any evaluation, there should be a special step looking at the totality. Here, the analyst should apply a systems perspective and consider how different SFs and parts work together.

This is more difficult to accomplish. The structuring stage has usually sorted the SFs, and grouped them at higher levels. The system evaluation can concentrate on these higher levels. As an aid, evaluations of the lower SFs can be used to make a more general judgement. Table 11.9 shows two examples (for the principal functions 3 and 5).

11.6 Improvements to safety functions

General

When the evaluation has been performed, there may be a number of SFs that need upgrading. The aim of the improvement stage is to increase the reliability or to widen the range of the SFs. The development stage is both questioning and creative at the same time. Improvement should be seen as an iterative process that continues until the result is satisfactory.

When the problems are clearly evident, it is sometimes easy to suggest solutions. The SFA-method includes support for finding improvements. There are some general principles that might be useful to apply, both at a detailed subsystem level and for the entire system.

After the evaluation, the record sheet contains a list of individual SFs that need improvement. These can be taken one by one, and the list of general principles can be of good use.

However, it is the entire SF system and its performance that are most important. The system might have developed and changed over time a bit at random, especially in the case of more informal functions and situations. It can therefore be valuable also to look for major improvements, such as:

- *Simplify or remove*; too many detailed or repeated control actions can take time and effort, and draw attention away from more important issues.
- *Supplement* with critical areas that are not covered.
- *Apply the general principles* also on the entire system of SFs.

Principles for improvements

From the technical field there are several principles that can be employed to improve reliability. When they are slightly reformulated, they can also inspire improvements in organisational and human functioning. Such a reformulation might involve preferring *item* to *component*. Some general principles are:

- *Good design* of equipment, rules, and management. It is best to do right from the beginning. There is lots of advice on design in different areas.
- *Use of reliable elements.* The reliability of a system depends on the reliability of its components and subsystems.
- *Maintenance* is self-evidently needed in technical systems. But organisational routines and the competences of people also need *preventive maintenance* to keep them working well.

- *Regular testing* of system functions. Planned routines for testing are especially important if latent and hidden failures can occur; otherwise, they might only be noticed when it is too late.
- *Continuous monitoring.* A variable (e.g., temperature) is monitored, and abnormal values indicate that something might go wrong. This can also be applicable to routines and actions.
- *Redundancy* is an addition that improves the probability that a function will work. It can refer to two systems (functions) in parallel; if one should fail, the other can take over.
- *Awareness of common cause failures*. The presence of common cause failures can drastically reduce reliability. A technical example is when several components are exposed to an unsuitable environment; then, they might all deteriorate. An organisational change might affect several people, and reduce the quality of a number of routines.
- *Readiness to observe and act.* If something tends to go wrong, a system with failure reporting and feedback might give an early warning, giving opportunities for reducing negative effects.

As a complementary aid, the key phrases below may be useful:

- Increase the probability of the SF functioning.
- Enhance effectiveness.
- Modify the SF by simplification or by complementary addition.
- Eliminate the need for a specific SF.
- Step up the level of abstraction, which means focusing on the wanted function.
- Step up the systems level, aiming at responsibilities, how rules are written, and instructions designed.
- Consider informal safety work, which can entail supporting engaged individuals and stimulating suggestions from staff.

11.7 Example

Background

In this example, an existing production system was analysed. The aim of the analysis was to obtain information that can support the design and planning of new similar workplaces. This example is also discussed later in this book (Section 16.9), and has been reported upon in an earlier article (Harms-Ringdahl, 2003A).

The studied system

The technical part of the production system (depicted in Figure 11.3) consists of five similar production tanks, each with a volume of about 3 m^3. These are used to mix various compounds, and no chemical reactions should occur. The site also accommodates a cleaning system using lye and hot water, which are governed by a computer-control system.

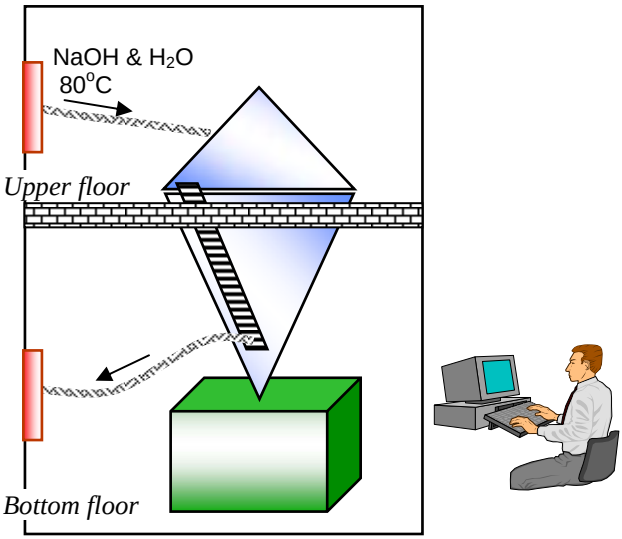


Figure 11.3 Principal layout of the workplace with a lye cleaning system

Batch production is involved, where different substances are added and mixed following strict procedures. Hygienic demands are high, and cleaning procedures are essential. A key part of the work is manual, guided by formal instructions 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.

The analysis

Preparation

The workplace and its surroundings were studied. Both technical equipment and organisational aspects were included, but not down to a very detailed level. The cleaning system was analysed, with a focus on the hazards posed by lye (pH 13.5) and hot water (80^{o}C), which both could cause serious burn injuries.

Data collection

Information about hazards was available from an earlier safety analysis. Information about safety functions was collected in dialogue with an engineer familiar with the system and its design history. He had also participated in earlier safety analyses.

Identification of safety functions

Identification was based on a few accident scenarios, which were discussed with the engineer. The first was the collapsing of the tank due to over-pressure. SFs that might prevent such an accident were identified. This was followed by a search for functions related to mitigation and emergency activities. Supplementary identification came from a check against the parameters of the general model. Ultimately, a list of about 50 SFs was obtained.

Structuring and classification

The identified SFs were structured into six general groups, which are discussed below. The SFs noted on the record sheet (see Table 11.9) were rearranged in accordance with the obtained structure.

Evaluation of SFs

The evaluation followed the *simple procedure* referred to above. In this case, the estimates were based on interviews with people in different positions in the organisation. For each SF, the parameter *Importance* was judged on basis of the scale in Table 11.3. *Efficiency* was estimated in terms of success rate (probability of functioning). For this, numerical values between 0 and 1 were assigned.

After that, the analysis team evaluated each SF on the list. Each judgement concerned whether the SF was acceptable, or whether improvements were needed. The scale in Table 11.6 was used for simple evaluation.

Evaluation of the entire system showed that that the coverage and scope of the safety system in general were insufficient. The conclusion drawn was that improved functions were needed, at both a detailed and a general level.

Proposing improvements

Proposals were made for the SFs that were not approved. In several cases, direct concrete solutions were found. Quite often, information was not sufficient, and the proposal simply consisted of a request for a further check. In particular, this concerned the computer control system, where the design was not transparent enough to allow any adequate proposal.

Concluding

The analysis was summarised in a report, which described the results, the recommendations, the assumptions, and the basis for assessments.

The results

Model of safety functions

One essential part of the results was the summary of the SFs related to the workplace. An overview is shown in diagrammatic form in Figure 11.4. More detailed information was given on the record sheet (extract shown in Table 11.9).

How the structuring should be performed was not obvious at first. It was found appropriate to start with the parameter *Type of safety function*, with a division into technical and organisational functions. These were further divided into six main groups, which are identified in the rows in the model (Figure 11.4):

1. *Containment* refers to mechanical systems that separate the hazards (hot water, lye, and mechanical movements) from operators during normal operations.
2. *Automatic control* starts and stops movements, and includes the prevention of overpressure, a number of interlocks ensuring that openings in the tank are closed, etc.
3. *Reduction of consequences* refers to technical devices, e.g., emergency showers, and related organisational activities.

4. *Formal routines* are regulated in a system of documents, which are carefully worked out, formally approved, and supposedly strictly followed.
5. *Informal routines* include what operators do in their daily work, and also verbal and written 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 safety policy and the system for safety management.

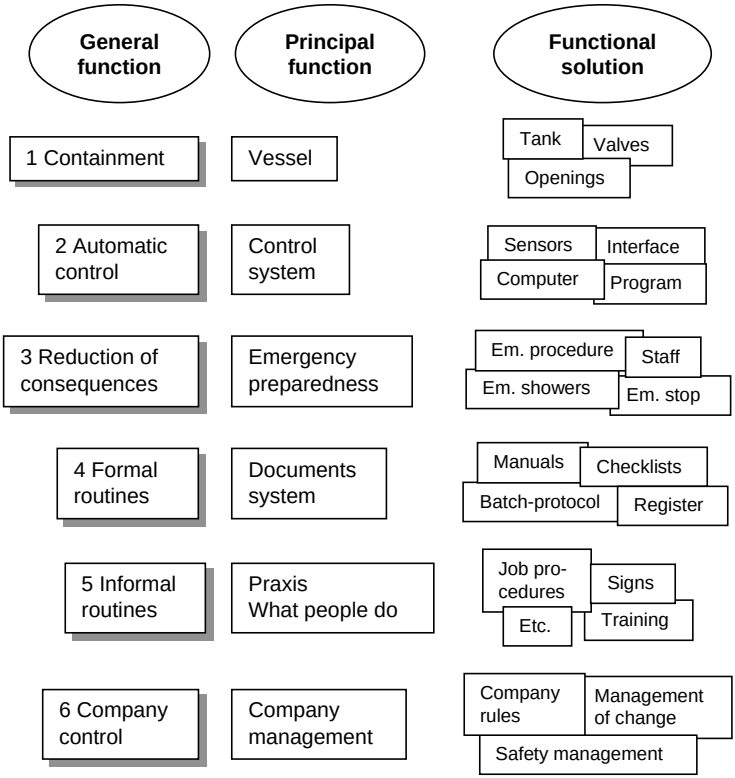


Figure 11.4 Model of safety functions in the workplace

The second part of structuring had the intention of giving an overview without loosing track of the concrete SFs. A solution was to combine the abstraction and systems levels. Four labels were chosen to describe these:

1. *General function* is related to the aim of the SF and is at a highly abstract level.
2. *Principal function* shows concrete functions, technical and organisational.
3. *Functional solution* describes the functions in greater detail, and is at a lower systems level.
4. *Concrete solutions*, e.g., a specific safety relay or an operator's action, are at a lower systems level. These are not shown in the figure, but were listed on the record sheet (Table 11.9).

Comments on the results

Parts of the record sheet are shown in Table 11.9, which includes block 3, *Reduction of consequences*. Three items are shown: emergency stop-buttons, emergency showers, and emergency procedures. They were all estimated as very important, but their efficiency was very low – at between 0% and 20%. For example, the emergency showers were rated low, because they were too far away, and people were not aware that they had to use them quickly. A number of improvements were suggested and summarised in an *Emergency package*.

Several informal organisational routines had been identified and gathered together in block 5, *Informal routines* (lower part of Table 11.9). The investigation showed that they had an important role. An example: *Written instructions* are labelled as informal when they are used without being checked and approved by the control system. The item *5.1.d*, *Instructions for control system*, was ranked as very important, but they were hard to understand and follow. Hence, efficiency was low (10%), and the instructions needed to be completely rewritten.

As a whole, the analysis revealed several weak points, and pointed to many possible improvements. The case is discussed as an example of safety analysis in Section 16.9, where further information about results and analytic procedure are given.

Table 11.9 Extract from the record sheet of a Safety Function Analysis

Principal function / Functional solution	**Concrete solution**	**Assessments***			**Proposed measures**
		Imp	Eff	Ev	
3 Emergency preparedness		3	-	3	Sum up and clarify responsibilities
3.1 Emergency stop-button	Emergency-stop buttons	3	0.2	3	Include pumps & Emergency package
3.2 Emergency showers	a) Shower (1 in the workplace)	3	0.1	3	Emergency package
	b) Eye showers (3)	3	0	3	Emergency package
3.3 Emergency procedure ----------	Persons with special training	2	0.2	3	One person available on all shifts
5 Informal routines		3	-	3	Investigate and clarify responsibilities
5.1 Written instructions	a) Information	1	0.5	2	Improve, investigate needs
	b) Instructions for special activities	2	0.5	2	Include safety aspects
	c) Instructions for machines	2	0.3	3	Check and improve
	d) Instructions for control system	3	0.1	3	Rewrite completely, make user friendly
5.2 Oral instructions	a) "*If disturbance, ask for help*"	2	0.5	3	Include in 5.1.a
	b) "*If cleaning in operation, do not ente*r"	3	0.5	3	Include in 5.1.a
5.3 Information signs	Sign: "*Cleaning in operation*"	2	0.5	3	Investigate to find better system
5.3 Training	a) General	1	-	1	
	b) Disturbances to control system	2	0.1	3	Include in improved instructions 5.1.d

Assessments: Importance, Efficiency, and Evaluation (see tables 11.3, 11.4, and 11.6). Efficiency is expressed as the probability of functioning.

12 Some further methods

12.1 Introduction

There is a wide range of methods for analysing system risks and safety properties. The previous chapters have contained descriptions of some selected methods, but they represent only a part of all the methods available. Further, they are the choices of the author. Others might well have made a different selection.

The aim of this chapter is to broaden the picture and provide an overview of additional methods (see Table 12.1). They have been chosen to represented different ideas. However, one condition is that descriptions of them are publicly available in English. Rather brief accounts are given here, but references are provided to enable the interested reader to go further. The methods are arranged into five categories. However, there is overlap between areas, and some methods belong to more than one of the categories.

Consequence-oriented methods

There are many types of methods that are oriented towards estimates of consequences of unwanted occurrences. They can concern:

- Fires and explosions
- Release of toxic gases
- Determination of toxic effects
- Effects on the environment and eco-systems
- Economic and social consequences

Usually, these phenomena are complex, and require advanced considerations and calculations that go beyond the scope of this book.

Table 12.1 Methods presented in this chapter

Method	Section	Comment
1 Technically oriented		
FMEA	12.2	Failure Mode and Effects Analysis
Event Tree Analysis	12.3	
Cause-Consequence Diagram	12.4	Sometimes called Bow Tie diagram
Safety Barrier Diagram	12.4	
2 Human oriented	12.5	
Human Error Identification		For example, the Action Error Method
Human Reliability Assessment		A group of methods
THERP		Technique for Human Error Rate Prediction
3 Task Analysis	12.6	
Hierarchical Task Analysis		A group of methods
4 Management oriented	12.7	
Audits – in general		Many different approaches
MORT		Management Oversight and Risk Tree
ISRS		International Safety Rating System – *a commercial product*
5 Coarse analysis	12.8	
Preliminary Hazard Analysis		
What-if		
Coarse Energy Analysis		
Coarse Deviation Analysis		
Checklists		Many different approaches

12.2 Failure Mode and Effects Analysis

Failure Mode and Effects Analysis (FMEA) is a well-established method, which has been utilised since the beginning of the 1950s. The simple principle for FMEA is that each component in a system is examined separately one after the other. Two basic issues are raised:

- Failure mode, the ways in which a component might fail
- The effects and consequences that might arise

The method is well-documented, and several descriptions of its use are available (e.g., Hammer, 1972; Taylor, 1994; Aven, 2008A). A number of standards have been published. There are variants of the method, some with a special name. Consequently, just saying FMEA does not define exactly what an analysis will look like.

One common variant is *FMECA – Failure Modes, Effects and Criticality Analysis*. Criticality is a function of the failure effect and the frequency, which are usually included in FMEA in any case. This means that the difference between an FMEA and an FMECA is not always apparent (see Aven, 2008A), and the shorter name FMEA will be used here.

The method is usually employed for analyses of technical systems. FMEA can also be used at different system levels – from individual components to larger function blocks. Sometimes, the term *Functional FMEA* is used to indicate that the analysis works at a higher level.

Analytic procedure

Since there are so many manuals for FMEA available, the account here will be kept summary and short. The details of the analytic procedure will vary quite a lot, since there are several different applications. Usually, the following main stages are included in an analysis:

1) Aim, scope and assumptions are defined.
2) The system is divided up into different units, often components, but sometimes functions modelled in a block diagram.
3) Failure modes are identified for the various units, one by one.
4) Conceivable causes, consequences and frequencies of failure are estimated for each failure mode.
5) An investigation is made into how the failure can be detected.
6) An estimation of severity is made.
7) Recommendations for suitable control measures are made.

The assumptions made at the beginning are important, since it usually is large analysis of a complicated system. Examples of assumptions are that

there is only one failure mode at a time, and that all inputs are at nominal values.

The FMEA record sheet

In practice, the control document is the FMEA record sheet, for which information is filled in for each unit. There are many variants, and several software FMEA templates can be found. An FMEA form has a set of columns, which can be quite numerous (up to 20). The headings of these columns may include:

1) Unit identification, designation and function
2) Failure mode
3) Failure cause
4) Failure effects
5) Failure frequency
6) Failure detection
7) Evaluation and severity ranking
8) Suggested improvement; this is included sometimes, and can be combined with a new estimate of severity if the improvement is introduced.

The columns 4–7 above can contain estimated values that are based on predefined scales (see Chapter 5). Evaluations based on the Risk Matrix (Section 5.4) appear to be most popular. In FMEA, the parameter *Failure detection* is sometimes used. If a failure immediately can be observed when it happens, then it can be corrected, and the chances are smaller that it will lead to an accident. A failure that is easy to detect will then get a lower severity ranking.

One way to estimate risk is to calculate a Risk Priority Number (RPN) (Rausand & Høyland, 2004). The principle is to rank three basic parameters, each on a scale from 1 to 10. These are frequency, severity, and the probability of detecting the failure. An RPN is obtained by multiplying the ranking values, giving a maximum score of 1000. A smaller RPN is better than a large. There are several variants of this kind of estimation.

Comments

A system can contain a large number of components, which can fail in different ways. A detailed analysis may be extensive, and the amount of documentation may be large. One main disadvantage of FMEA is that all components are analysed and documented, also the failures with small consequences (Aven, 2008A).

Another aspect is that many systems have redundant safety functions, which means that a combination of failures is necessary for an accident to occur. It is essential for this to be considered at the evaluation stage (related to columns 4–7 above). Otherwise, FMEA will be unsuitable for analysing systems with much redundancy.

12.3 Event Tree Analysis

Event Tree Analysis can be used to study the potential effects of an event that might be dangerous. Depending on the situation, there may be a range of consequences that might occur – from the worst case to no injury at all.

The method is used to study the alternative consequences of a defined event. It considers barriers and the course of events in a logical framework. The result is a logical tree, which starts with an initiating event showing the relations between alternative consequences. The method is binary, which means that an event is assumed to happen or not happen, and a barrier is assumed to work or fail.

Several descriptions of the method are available (e.g., CCPS, 1985; Lees, 1996; Rausand & Høyland, 2004). Often, the trees are technically oriented, but an event tree can also include human actions.

Analytic procedure

An event tree starts with an initiating event, e.g., a gas leak, and then describes the potential consequences of this event. The procedure for Event Tree Analysis has five general steps, and one optional step:

1) Define aim, scope and assumptions.
2) Start out with an initiating event, which has been considered important, e.g., from a previous FMEA.
3) Identify branching points where alternative outcomes are possible. An example is safety equipment designed to deal with hazards related to the initiating event.
4) Construct the event tree.
5) Describe the accident sequences.
6) Calculate accident frequency (optional).

Example 1

The principle is most easily explained through examples. Figure 12.1 shows an event tree where a dust explosion is the starting point. This might lead to a fire, and the tree shows alternative outcomes given two safety functions –

a sprinkler system and a fire alarm. Frequencies of the events H1 to H5 can be calculated if estimates are available for the frequency of an initiating explosion and the reliabilities of the sprinkler and the alarm.

Event trees can be designed differently. Often, the design starts on the left, which gives a horizontal tree, but in Figure 12.2 the tree starts from the top (appearing as a standing tree). What the trees have in common is that they, more or less strictly, show how events evolve over time.

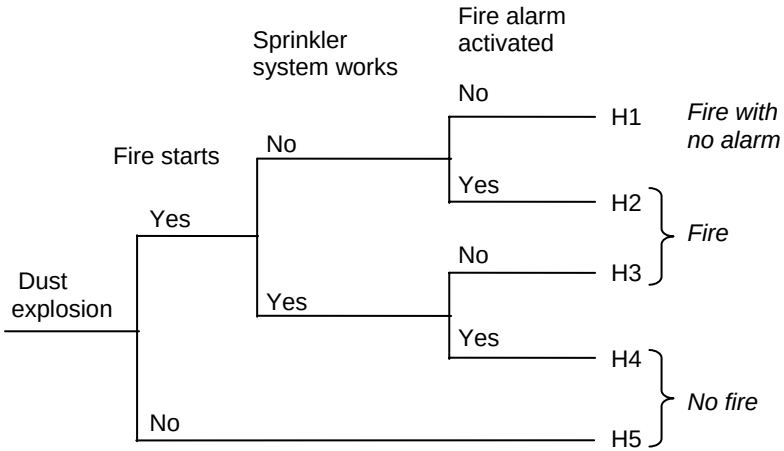


Figure 12.1 Event tree for a dust explosion (adapted from Rouhiainen, 1993)

Example 2

Another example is of a tank for toxic gas and a person working in a control room nearby. In this example, we include probability estimates. Since the tank might leak, a gas detector has been installed. In the case of a leak, an alarm bell should sound, prompting the person to rush out of the premises.

Figure 12.2 illustrates an event tree for the gas leak. Four safety functions have been identified, which gives four branching points. A common simplification is that every part of this sequence contains the possibility of either success or failure. This means that there are two possible end consequences: injury or no injury.

The first branching point is related to where the leak occurs. All leaks will not necessarily lead to gas being present in the workplace. The second branch indicates whether or not the gas reaches the detector. Other branches are related to the functioning of the alarm, and to evacuation of the operator.

An event tree can be used for making quantitative estimates. The initial event is expressed as a frequency (events per year). The branch-off points are expressed as probabilities of success. Figure 12.2 provides an example of how an estimate can be made. For purposes of clarification, rather high frequency and failure probability values have been used. On the basis of these values, the frequency of injury to a person resulting from a gas leak is around 0.2 times per year (0.1 + 0.04 + 0.072).

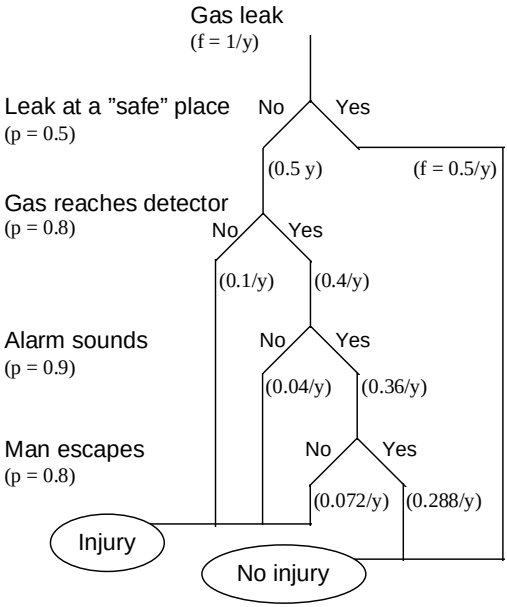


Figure 12.2 Example of an event tree for the consequences of a gas leak (f = frequency, y = year)

Comments

The method is suitable for the study of intermediate events with potential to cause accidents. The advantages of event trees are that they clearly visualise event chains and the roles of safety barriers. It is also fairly easy to make numerical estimates, which are sometimes important. Only one initiating event is studied at a time, which might be time-consuming if many events are to be investigated.

12.4 Cause-Consequence Diagrams

A group of methods focus on critical events in an accident chain and barriers related to that chain. The result is presented in a diagram, where the left part shows the causes of the critical event, and the right part its possible consequences. A common name is *Bow Tie Diagram*, since the diagram is like a bow tie in shape. There are a number of variants of this technique, and three examples are given below.

Cause-Consequence Diagrams

Cause-Consequence Diagrams are related to both Event Tree and Fault Tree analyses. The aim is to examine selected events or states that are important from a risk perspective, usually called critical events. Such events may have been identified in earlier analyses. Descriptions of the method have been provided by Nielsen (1971, 1974) and Taylor (1974, 1994).

The analysis starts with a selected critical event in the system. Possible causes of the event are then investigated, as in Fault Tree Analysis. Consequences are also investigated with the event tree methodology. The method can also be used as a basis for making probabilistic estimates. The principle underlying the method is indicated in Figure 12.3.

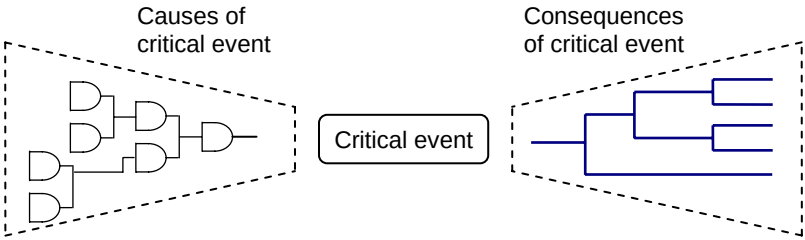


Figure 12.3 Schematic view of a Cause-Consequence Diagram

Safety Barrier Diagrams - Version 1

An approach called *Safety Barrier Diagrams* is a way of presenting and analysing barriers to accidents (Taylor et al., 1989; Taylor, 1994). The term *safety barrier* is used to describe a safety device or other measure that can prevent, reduce, or stop a given accident sequence. A more detailed definition (Taylor, 1994) is:

- Any wall, shield, switch, bolt, interlock, software or operational check which is intended to prevent a signal or activation from reaching a place where it can cause an accident
- A mechanical barrier which can prevent external influences from causing an accident

- A mechanical barrier which can prevent a release of energy or poison from having adverse consequences
- Distance from the source of hazard

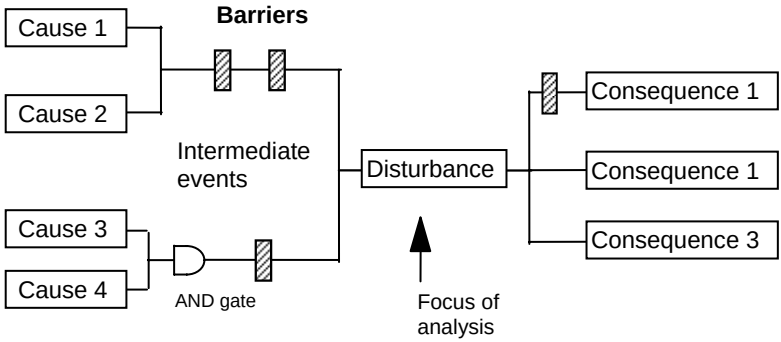


Figure 12.4 Principles of the Safety Barrier Diagram approach (adapted from Taylor et al., 1989)

A *safety configuration* is defined as a combination of safety barriers. Figure 12.4 illustrates the basic structure of a Barrier Diagram. A safety diagram is constructed with the disturbance as its centre point. Possible consequences are shown to the right, and causes and initial events to the left.

As in fault trees, an AND gate is used to show if two or more causes need to occur simultaneously. If one cause is sufficient, the lines are simply combined (instead of using an OR gate). The safety barriers are then shown in the diagram, which should show the possibility of an accident if all the safety measures along an event sequence fail.

There are different ways of proceeding in constructing such a diagram. One way (Taylor, 1994) is to start with concentrations of energy (hazard sources). The safety barriers surrounding each hazard source are listed. In addition, the intended combinations of safety barriers for each operational state are summed up. In the analysis, the reliability of a barrier and the possibilities of bypassing it are investigated. The analysis also includes a check that criteria for *good* barriers are fulfilled. Such criteria are also given in the references to the method.

Safety Barrier Diagrams – Version 2

The concept of a Safety Barrier Diagram has received increasing attention in recent years. Duijm (2009) has presented a further development, which might be called Version 2. This has a more developed syntax, which can support the calculation of probabilities and the use of software in the

analysis. The new version has also established a useful coupling between barriers and management factors.

One further difference is the emphasis on dynamics. Instead of focusing on causes, the new version starts with events, which are also illustrated through the use of arrows (see Figure 12.5).

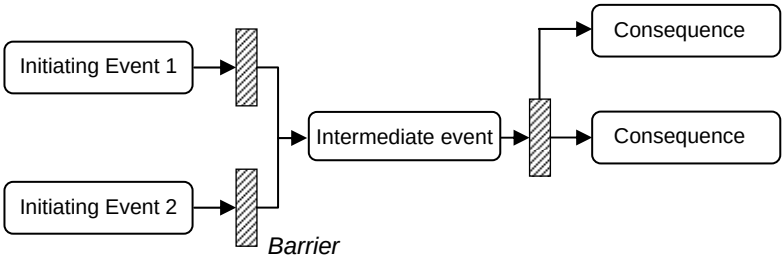


Figure 12.5 Barrier Diagram Version 2 (adapted from Duijm, 2009)

Comments

In principle, Cause-Consequence Diagrams and Barrier Diagrams are more or less identical, since a barrier can be symbolised by either an AND gate or a barrier symbol.

A practical dilemma is that there are often a large number of potentially hazardous critical events (or disturbances) in any one system. This means the construction of a large number of diagrams unless the number of disturbances to analyse can be reduced by suitable grouping.

12.5 Human error methods

There are a large number of techniques available for analysing human errors and tasks. In a review (Stanton et al., 2005), around 200 methods related to human factors were identified. After a screening process, over 90 methods remained and were reviewed by the authors. Clearly, the general field of human error analysis has become a specialist area in a large literature. Only a short orientation is provided here.

In general, the aim of such analyses is to predict human errors in defined tasks, such as specified operations in a control room, and then consider what can go wrong. This section presents brief accounts of some methods in the area:

- Human Error Identification (the Action Error Method)
- Human Reliability Assessment
- Technique for Human Error Rate Prediction (THERP) – an example of a quantitative method

A short summary of a fairly general methodology called *Task Analysis* is provided separately (Section 12.6). One of its applications is to provide inputs into a form of human error analysis.

A general problem is that the number of potential human errors can be immense, especially if multiple errors and advanced faults (e.g., in problem solving) are included. Strategies for prioritising and limiting the number of potential errors become essential. Usually, the human tasks to be analysed need to be precisely defined in any practical analysis.

The analysis of human errors is highly complex, and becomes even more complicated if calculating the probability that actions will go wrong is envisaged. A number of doubts have arisen concerning such calculations. Hollnagel (1993, 2000) points to the assumptions that have to be made. Examples are that actions can be considered one by one, and that it is possible to determine a basic probability for a characteristic type of action. There is a question mark over how well such assumptions accord with reality. One view is that human performance cannot be understood by decomposing it into parts, but only by considering it as a whole, embedded in a meaningful context (Hollnagel, 1993).

Human error identification

There are a number of related methods aimed at the identification of human errors (e.g., Embrey, 1994; Kirwan, 1994). The methods are best suited for use in installations where there are well-defined procedures, e.g., in some processing industries. If there are no well-established routines, it is difficult to find a basis on which an analysis can be conducted. In general, the aims are to identify steps that are especially susceptible to human errors, and to assess the consequences of such errors.

One example is the *Action Error Method*, described by Taylor (1979). The stages in this analysis are:

1) Making a list of the steps in the operational procedure. The list specifies the effects of different actions on the installation. It must be detailed, containing items such as *Press Button A* or *Turn Valve B.*
2) Identification of possible errors at each step, using a checklist of errors.
3) Assessment of the consequences of the errors.
4) Investigation of conceivable causes of important errors.
5) Analysis of possible actions designed to gain control over the process.

The checklist includes various types of human errors:

a) Actions not taken
b) Actions taken in the wrong order
c) Erroneous actions
d) Actions applied to the wrong object

e) Actions taken too late or too early
f) Too many or too few actions taken
g) Actions with an effect in the wrong direction
h) Actions with an effect of the wrong magnitude
i) Decision failures in relation to actions taken

Taylor (1994) later developed a more detailed version of the Action Error Method. There are several other methods in which similar approaches are adopted.

Human Reliability Assessment

One specialised area is concerned with the probabilistic aspects of human errors, and is usually referred to as *Human Reliability Assessment* (HRA). It involves reliability engineers and human-factor specialists, and is applied mainly in the nuclear power domain (see e.g., Kirwan, 1994; Gertman & Blackman, 1994).

The focus is usually on quantification, and results are used in probabilistic safety assessments. The objective of HRA is to find the probability that an activity is successfully completed (or that it fails). Kirwan (1994) has described the HRA process in terms of eight principal components:

1) Problem definition
2) Task Analysis
3) Human error identification
4) Representation of this information in a form that allows quantitative evaluation of the error's impact on the system
5) Human error quantification
6) Impact assessment; calculation of the overall system risk level
7) Error reduction analysis
8) Documentation and quality assurance

However, there are a great number of human reliability methods with different procedures. Hollnagel (1993), for example, has published a list of 27 different HRA techniques.

THERP

Technique for Human Error Rate Prediction (THERP) is a method for analysing and quantifying the probabilities of human error, which is mainly used in the nuclear field. There is a handbook in which the method is extensively described (Swain & Guttman, 1983), and descriptions are also contained in other publications (e.g., Bell & Swain, 1983). The method has been developed steadily over a number of years. The main stages of the technique are:

1) Identification of system functions that are sensitive to human error
2) Analysis of the job tasks that relate to the sensitive functions
3) Estimation of error probabilities
4) Estimation of the effects of human errors
5) When applied at the design stage, utilisation of the results for system changes, which then need to be assessed further.

The handbook also contains tables with estimates of error probabilities for different types of errors. These probabilities may be affected by so-called *performance shaping factors*, meaning that the analyst makes adjustments to the values in the light of the quality of the man-machine interface, experience of the individual operator, etc.

Other examples

The extended Hazop approach

The principles of the Hazop method (Chapter 9) are attractive for application to human errors, and there are some examples of different ways of proceeding (e.g., Kirwan, 1994). One way is to examine a process involving human actions, and apply the Hazop guide words to that. An alternative is to apply Hazop to a technical object, but also include human errors.

One example lies in the proposal made by Schurman and Fleger (1994) to incorporate human error into a standard Hazop study. The analytic procedure is similar to a pure technical application, and human-factor aspects are simply added. The major change lies in the incorporation of human-factor guide words and parameters.

The guide words are additions and reformulations of the standard Hazop set. They include *Missing*, *Skipped*, and *Mistimed*. The new/revised parameters include *Person*, *Action*, *Procedure*, etc. By combining guide words and parameters, meaningful and essential deviations can be detected. Schurman and Fleger state that the major adjustment needed is to the thinking of the analysis team. Operators and maintenance workers should be regarded as subsystems in the process.

Deviation Analysis

Human errors have also been included in Deviation Analysis (described in Chapter 8). The approach is to treat human errors at the same time, and in a similar manner, as technical faults. This means that human actions are studied in less detail than in the more specialised methods. As support for the analysis team, there is a list comprising seven categories of errors. Even though this approach is quite simple, it offers a way of including human errors in an analysis in a practical and fairly simple manner.

12.6 Task Analysis

Task Analysis is a methodology that covers a variety of human-factor techniques. There are a large number of methods, which may sometimes confuse potential users. One survey (Annet & Stanton, 2000) has identified more than 100 task-analysis-related methods. Only a brief overview is given here.

There are a number of fairly extensive reviews (e.g., Kirwan & Ainsworth, 1993; Annet & Stanton, 2000; Stanton et al., 2005). Developments have largely come from the field of psychology. Originally, the methods focused on the tasks of individuals, especially manual workers and process operators, and sometimes also a team of operators. A division can be made into:

- *Action-oriented approaches*, which give descriptions of the operator's behaviour at different levels of detail, together with indications of the structure of the task.
- *Cognitive Task Analysis* (CTA), which focuses on the mental processes that underlie observable behaviour, and may include decision-making and problem-solving. Application of the methodology is more problematic, since the causes of cognitive errors are less well-understood than those of action errors.

Task Analysis has applications in many domains. For example, it might be used for improving the design of operational procedures in a control room. Some of the methods can be applied more generally and outside the psychological domain. In such cases, *task* will denote a procedure involving organisations and software.

Task Analysis in itself is not a methodology for the identification of risks, but it can provide an input into other safety analyses. The structured description of tasks can be useful in Human Error Analysis in general, and also fits in well with Deviation Analysis.

Hierarchical Task Analysis

Hierarchical Task Analysis (HTA) is perhaps the most widely used kind of Task Analysis. It is a generic method for analysing how work is organised (Annet et al., 1971). The outcome is an extensive description of the task and the activities involved. Results are usually presented as a diagram, but can also be shown in a tabular format.

HTA starts with a clear definition of the task that is to be analysed. The next step involves the identification of the overall goal of the task, which is then broken down into a handful of sub-goals. These are divided into further

lower-level sub-goals and activities, which are arranged in a hierarchy of operations. The procedure continues until a suitable level of detail is achieved.

Constraints associated with goals and task elements are analysed, which may influence the outcome of the task. If the task is critical, potential problems might be reduced by re-design, training, and so on.

Figure 12.6 shows a part of an HTA for the computer-controlled lathe presented in Section 8.4. The task is divided into three major parts, which are then further broken down. This figure can be compared with Figure 8.3, which also shows modelling of this kind. The diagrams look different, but they contain the same main elements.

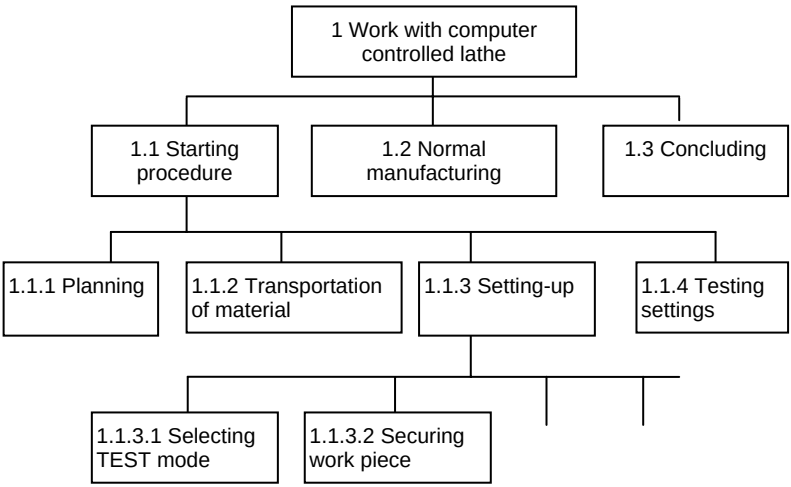


Figure 12.6 An HTA of work at a computer-controlled lathe

Advantages of HTA are that the method is simple and generic (Stanton et al., 2005), which means that it "can be applied to any task in any domain". The results can be used as input to more risk-oriented methods, such as FMEA, Deviation Analysis, and various human-error techniques.

Disadvantages are that the results are mainly descriptive, and that an HTA might be laborious and time-consuming in the case of complex systems. A principal problems lies in the strict hierarchical approach, since, in the real world, there are lots of direct relations between elements lower down in the hierarchy. Such relations can be both planned and informal, and, if they are disregarded, the results might be misleading.

12.7 Management-oriented methods

General

The quality and focus of organisational activities are of decisive importance for the level of risk. They govern how an installation is designed, how work is carried out, who works at the plant, what safety routines there are, and so on.

For this reason, it is essential to have methods for the analysis and assessment of the safety work of organisations. At the same time, it is a difficult subject for a variety of reasons. Organisations and activities are not tangible objects, and it is not easy to get a grip on them. Written documentation reveals only a part of the reality. What gives rise to difficulty is that there are informal decision-making paths, involving people with diverse views on what is relevant, etc. (see Section 2.4).

Analysis of management is quite a complicated area. Some methods are based on practical experiences and ideas, which are organised in a structured manner. Others depart from a more theoretical perspective.

This section takes up examples of methods for examining the organisational characteristics of a company. Approaches such as auditing and MORT (Management Oversight and Risk Tree) are shortly presented. At the end of this section, there are accounts of some further methods.

Auditing

Audit has become a commonplace term, but it does have a variety of meanings. In this section, it concerns the examination of a company management system to see whether it conforms to some kind of (external) norm. An international standard (ISO, 2009A) provides one definition:

> "Risk management audit is a systematic, independent and documented process for obtaining evidence and evaluating it objectively in order to determine the extent to which the risk management framework, or any selected part of it, is adequate and effective."

Another definition of audit is given in a standard related to occupational health and safety management systems (BSI, 2004, page 2):

> "Audit is a systematic and independent process for obtaining evidence and evaluating it objectively to determine the extent to which specified criteria are fulfilled."
>
> "NOTE Independent does not necessarily mean external to the organization."

This standard gives some general advice about audits. Compared with routine monitoring, an audit should enable a deeper and more critical

appraisal of all the elements in a health and safety management system. The approach should be tailored to the size of the organisation and its hazards.

There is plenty of material covering the field of auditing safety management. One example lies in the "Guidelines for Auditing Process Safety Management Systems" (CCPS, 2011), which is extensive (900 pages) and tailored to suit that type of industry. More general recommendations are provided by various organisations, such as the International Labour Organisation (ILO, 2001).

In short, a safety management audit should determine whether the management system is effective in meeting the organisation's safety policy and objectives. In general, an audit should comprise the following stages:

1) Decide aim and scope of the audit, and which parts of the management system should be included.
2) Define the norm (and standard) that the management system should achieve.
3) Compare systematically the elements in the system. A specified methodology may help by providing a scoring system and a structured way of working.
4) Evaluate and compile the results.
5) Communicate conclusions and results.

Quite often, auditing also includes safety, health and environmental aspects, since the management of these is similar and sometimes also integrated. Variation concerning which elements should be included is large. One example from the ILO (2001) describes an audit of the organisation's occupational safety and health (OSH) management, which might include the system elements below (or a subset of these):

a) OSH policy
b) Worker participation
c) Responsibility and accountability
d) Competence and training
e) OSH management system documentation
f) Communication
g) System planning, development and implementation
h) Prevention and control measures
i) Management of change
j) Emergency prevention, preparedness and response
k) Procurement
l) Contracting
m) Performance monitoring and measurement
n) Investigation of work-related injuries and diseases

MORT

Management Oversight and Risk Tree (MORT) has become a classic method for the analysis of safety organisations and the investigation of accidents. Development of the method dates from 1970. A detailed guide and an account of the reasons for using MORT have been prepared by Johnson (1980). In recent years, interest in the method has grown and the Noordwijk Risk Initiative Foundation(NRI, 2009) has published a revised description (free on the web at www.nri.eu.com). The new manual primarily addresses accident investigations. The basic idea is that:

> "MORT emphasises that when an accident reveals errors, it is the system which fails. People operating a system cannot do the things expected of them because directives and criteria are less than adequate. Error is defined as any significant deviation from a previously established or expected standard of human performance that results in unwanted delay, difficulty, problem, trouble, incident, accident, malfunction or failure" (Johnson, 1980).

The energy model (Chapter 6) is an important element in MORT. Another feature is that the MORT logic diagram can be seen as a model for an ideal safety programme. It can be used for:

- The investigation of an accident
- The analysis of an organisational programme for safety

The MORT tree

The MORT logic diagram provides a general problem description. It is rather like a fault tree, and the same symbols are used. A small part of a MORT tree is shown in Figure 12.7.

The *top event* may be an accident that has occurred. This can be due to an *assumed risk* or to an *oversight or omission*, represented by the two main branches of the tree, or both.

For a risk to be *assumed*, it must have been analysed and treated as such by company management. Thus, the combination where a certain type of accident tends to occur and no specific control measure has been taken is not sufficient for the hazard to be counted as assumed.

The other main branch – *Oversights and omissions* – takes up organisational factors. It has two subsidiary branches, one of which is called *Specific control factors* and focuses on what occurred during the accident. This is further divided into the accident itself and how its consequences are reduced, e.g., through fire fighting, provision of medical treatment, etc. The second subsidiary branch treats *Management system factors* and focuses on the question *Why?* It is divided into three further elements: policy, implementation, and risk assessment systems.

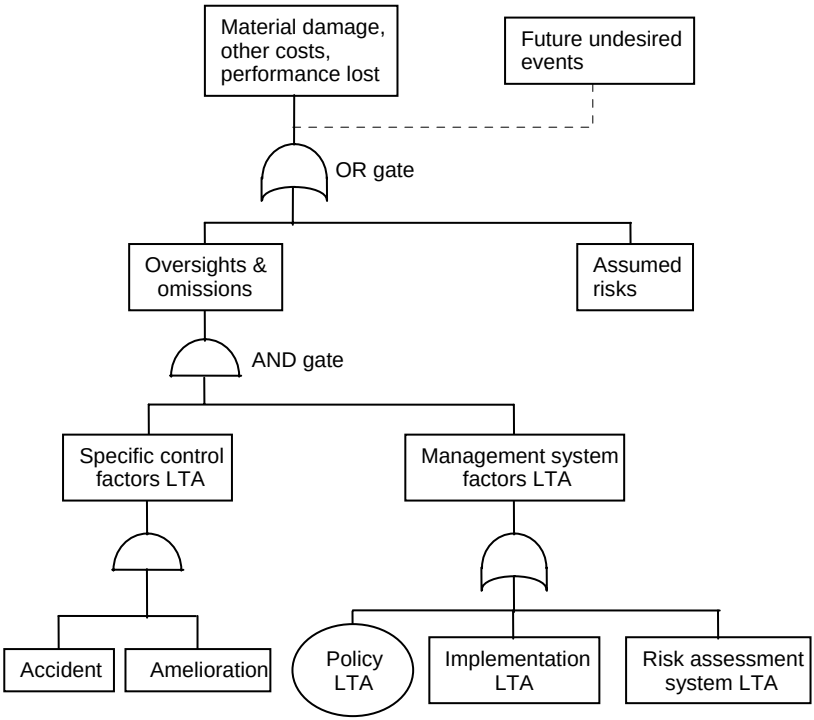


Figure 12.7 The top of a MORT tree (adapted from Johnson, 1980)

The various elements in the tree are numbered. The numbers refer to a list, which is provided as a complement to the tree. For each element, there are specific questions that the analyst should pose. The tree contains around 200 basic problems. However, if it is applied in different areas, the number of potential causes it describes can rise to 1500.

Assessment – Less Than Adequate

Analysis involves going through the elements in the tree and making an assessment of each. There are two assessment levels: *Satisfactory* and *Less Than Adequate* (*LTA*). Assessments are in part subjective; that is, people may make different judgements. Nevertheless, the availability of a list of specific, and often concrete, questions for each element reduces the degree of subjectivity.

Analytic procedure
The analysis is conducted by following the MORT chart, first in general and then in greater detail. Questions are marked directly on the chart. Colours are used to code the answers; green means OK, red LTA, and blue that no answer to the question has been obtained. Irrelevant questions are crossed out. The analysis is completed when all elements have been covered.

Comments
The method allows a large number of problems to be identified. Johnson (1980) mentions that five MORT studies of serious accidents led to the identification of 197 problems, i.e., about 38 problems per study. He describes the method as simple. It is extensive, but each element is easy to understand. However, many regard the method as impracticable, perhaps because there are so many different items to keep track of.

Johnson suggests that the analysis of an accident can be conducted in one or a few days. However, experiences from Finnish applications of MORT to maintenance work (Ruuhilehto, 1993) indicate that an analysis will require up to eight man-weeks.

MORT makes use of penetrating questions based on an ideal model of an organisation. Where the actual organisation deviates from the ideal, there can be far too many negative answers, which analysts may find difficult to handle. This indicates that MORT might be difficult to use in organisations that lack a strict hierarchical management, and where informal elements are common.

More methods

A number of methods consider management aspects systematically, but they have a wider scope. Therefore they are not classified as *management-oriented methods* here. Examples of this are Deviation Analysis, MTO Analysis (Section 13.6), and Safety Function Analysis.

There are several further methods and concepts concerned with the analysis of safety management and safety culture, some of which were initially developed for the nuclear industry. The list can be made long, and only a few examples are given here:

- ASCOT – Assessment of Safety Culture in Organisation Team (IAEA, 1994)
- CHASE – Complete Health and Safety Evaluation (Both et al., 1987)
- Five Star System (British Safety Council, 1988)
- ISRS – International Safety Rating System (see below)
- MANAGER – MANagement Assessment Guidelines in the Evaluation of Risk (Pitbaldo et al., 1990)
- PRIMA – Process Risk Management Audit (Hurst et al., 1996)

- SADT – Structured Analysis and Design Technique (Hale et al., 1997)
- TRIPOD (Wagenaar et al., 1994; Reason, 1997)

International Safety Rating System (ISRS)
ISRS is a commercial audit system, which has a long history (from the 1970s), and with an eighth edition in 2009. The full manual is not public, but there are shorter descriptions available. Due to the widespread use of ISRS, some evaluations have been based on it (e.g., Eisner & Leger, 1988; Guastello, 1991; Chaplin & Hale, 1998).

The objective of an ISRS audit is to obtain a measure of the effectiveness of a company's safety activities compared with a set of criteria developed for the ISRS. A further aim is to offer a system to guide the development of an effective safety programme.

An ISRS audit consists of around 600 questions, which are divided into 20 elements. Each question is given a score for compliance with a given procedure or practice. Scoring guidelines are provided in the audit manual. Examples of the 20 elements include:

- Leadership and administration
- Management training
- Planned inspection
- Task analysis and procedures
- Accident/incident investigations
- Planned task observation
- Emergency preparedness

12.8 Coarse analyses

Why perform a coarse analysis?

Even simple and quick analyses are of value, and provide information on existing hazards. A simple analysis can be justified in many situations such as:

- Presence of major safety deficiencies. If it is already known that there are a large number of safety problems, no detailed analysis is needed for these to be identified.
- Unclear picture of hazards. It is not known whether a thorough investigation is justified.
- Lack of resources. A full analysis cannot be conducted because of lack of people or time.
- Absence of documentation on the existing system or planned changes. There is insufficient information available for a proper analysis to be conducted.

A coarse analysis tends to have the following features:

- It is quicker to conduct than a normal safety analysis.
- It is less systematic, the methodology is often more free, and results are more difficult to repeat.
- It has limited coverage, meaning that only certain aspects of the system are considered, or that only specific types of hazards are investigated.
- It is usually intended to cover an entire system (which is an advantage).

Several of the methods already described can be used in a *coarse* or *quick* manner to cut down the time taken by an analysis. A short summary of a variety of approaches is provided below. Sometimes, the methods will overlap, so that one approach can contain some of the elements of another. Examples are:

- Preliminary Hazard Analysis
- What-if
- Use of checklists – based on summaries of known problems
- Inventories of documented hazards
- Inventories of known hazards
- Comparisons with similar installations
- Comparisons with directives and norms
- Coarse Energy Analysis
- Coarse Deviation Analysis

Preliminary Hazard Analysis

Preliminary Hazard Analysis (PHA) has been around for a long time, and an early description was presented by Hammer (1980), who also introduced the name. It has become a popular method, which also means that there are several ways of performing an analysis.

The aim of using the method is to identify hazards in a system, and it usually includes an estimation of the risk level. My interpretation is that the word *preliminary* indicates that the purpose is to get a first overview of the hazards. If needed, a more detailed analysis is performed later. However, PHA sometimes signifies a rather large analysis, where *preliminary* has a different meaning.

A PHA often includes the following steps:

1) Define the aim and the parts of the system that are to be included in the analysis.
2) Identify hazards. The method does not prescribe how this is done, and it can be based on different principles, such as brain-storming, division into functional blocks, or a checklist.
3) Often, a ranking of the risk is included, which is usually based on the principles of the Risk Matrix (Section 5.4).
4) Recommendations and suggested improvements.

A fairly detailed record sheet is often used to support the analysis. It can contain columns for:

- Hazards
- What might happen (consequences)
- Possible causes
- Estimates of consequences
- Estimates of probabilities
- Ranking of risks
- Suggestions

The method is often regarded as simple, and is often used without a manual; it is mainly the columns in the record sheet that guide the analysis. Since the analytic procedure is not precisely prescribed, the result depends much on the analysis leader and the team.

What-if Analysis

What-if Analysis is a popular technique in processing industry. It is not a specific method with a standardised application, but varies according to the user. The basic idea is to pose questions such as:

- ***What*** happens ***if*** Pump A fails?
- ***What*** happens ***if*** there is an interruption to the electrical power supply?
- ***What*** happens ***if*** the operator opens Valve B instead of Valve A?

If the right questions are posed to a skilled team, good results can be obtained. However, success using this method is much dependent on the extent to which the approach is systematic and on the skills of the users. This method can also be fairly extensive.

Checklists and inventories

Use of checklists

One general approach to identifying hazards is to go through a list of potential sources of risk, and then determine which points on the list are relevant. Checklists have been developed for a variety of situations and specific industrial sectors. The quality and utility of any analysis largely depend on the checklist.

Checking against directives and norms

Directives issued by the authorities can sometimes be treated as checklists. They represent a summary of knowledge obtained over a lengthy period of time. For example, a standard concerned with the safety of machinery (EN 1050, 1996) provides a long checklist of hazards, related to energies, deviations, missing protection, etc.

Comparisons with similar installations

If there is a similar installation where hazards have been thoroughly investigated, this can be of good help. An analysis is performed of whether the same hazards exist at the object under study. This form of analysis may be appropriate when a new installation is planned, or when changes are made to an existing installation.

If several similar installations are to be studied, a more thorough analysis can be performed on the first. The results from that are then used to make a special checklist for the remaining installations.

Other

A number of other methods can be used more quickly. Two examples are:

Coarse Energy Analysis

An Energy Analysis (see Chapter 6) can easily be simplified to provide a simple hazard survey. Simplification involves dividing the system into just a few sections, and only considering energies that can lead to fatal or serious injuries.

Coarse Deviation Analysis

Deviation Analysis (Chapter 8) can also be simplified. This means that the division into functions (the structuring) is done rather crudely. Only deviations with relatively major consequences and important planned changes are considered.

13 Methods for event analysis

13.1 Introduction

Investigations of accidents and events are important tools for accident prevention. Here, they are regarded as a type of safety analysis. They differ somewhat from other applications, which is why a general framework for event analysis was presented in Section 3.5.

The general term *event analysis* is used here, and it concerns an analysis of something that has already happened. It includes accident investigations, and also the study of near-accidents and other events. The aim of this chapter is to provide an overview of the methods that are suitable for such investigations.

A thorough analysis can provide a profound understanding of how the accident could occur and about the system in which it took place. This will provide a basis for the effective prevention of further accidents. The disadvantage from a methodological perspective is that the starting point for an investigation is a more or less randomly selected single event.

There are several methods that can be used in the investigation of a specific event. There is a large specialized literature on this subject, and there are a number of summaries of methods.

For example, the U.S. Department of Energy (DOE, 1999) has published a manual that gives general advice and describes a set of methods. The Energy Institute (2008) has selected methods for analysing human and organisational factors. Another study (Sklet, 2002 & 2004) has focused on methods suitable for the analysis of major accidents. If we consider these overviews, and also the material in this book, we can find more than 50 methods for the investigation of events and accidents.

A selection of methods

There are many ways of characterising and selecting methods (see, e.g., DOE, 1999; Kjellén, 2000; Sklet, 2002). The selection here is based on the considerations referred to in Chapter 4.2. In short, this means that three criteria should be met:

1) A defined analytic procedure
2) Availability of a published manual, which excludes proprietary methods
3) A method that is fairly easy to apply

Table 13.1 Examples of methods for event analysis

Method	Sect.	Asp*	Comment
Specific to event analysis			
AcciMap	13.7	a c	Combines accident sequence and organisational levels
AEB (Accident Evolution and Barrier Function)	13.4	a b	Combines accident sequence and barriers
Change Analysis	13.8	c	Compares situations with and without the accident
ECFA (Events and Causal Factors Analysis)	13.5	a c	Combines sequence and root causes
MTO Analysis (Man–Technology–Organisation)	13.6	a b c	Combines sequence, causes and barriers
STEP (Sequentially Timed Events Plotting)	13.2	a d	A detailed method for sequence analysis
Simple Event Mapping	13.3	a	A simplified approach to sequence analysis
Also for system analysis			
Deviation Analysis	13.9	c	Identification of deviations related to the event (also Chapter 8)
Safety Function Analysis	13.10	b	Search for safety functions and barriers (also 11)
Event Tree	13.11	a d	Logic diagram of barriers and alternative consequences (also 12.3)
Fault Tree	13.11	d	Logic diagram of faults explaining the accident (also 10)
MORT	13.11	b d	Logic diagram with organisational aspects (also 12.5)
Only briefly described			Outside the criteria described above
CREAM	13.1		Cognitive Reliability and Error Analysis Method
SCAT	13.1		Systematic Cause Analysis Technique
STAMP	13.1		Systems –Theoretic Accident Model and Processes
Tripod	13.1		

Asp* = Aspects a–d described in text below

A selection of 16 methods is presented in Table 13.1. They are divided into three groups. The first contains methods that are specialised in event analysis. The second includes methods useful for both system analysis and accident investigation. Finally, there are examples of methods that are important but fall outside the three criteria. They are briefly summarised at the end of this section.

Different aspects are represented in the table, for the reason that employing different perspectives on an event will give a more complete analysis. Examples of aspects of an investigation technique are:

a) Sequence of events
b) Barriers
c) Contributing factors, causes, deviations, etc.
d) Logical connections

Root cause analysis is a common name, but it is not included in the table. This is because it is not a unique method; rather, there are several published variants. I prefer to see it as a generic term, almost synonymous with accident investigation. The same reasoning applies to *Barrier analysis*.

Other methods

Among the large number of accident investigation methods, many do not fulfil the criteria given above. Four examples are listed in Table 13.1, and are briefly presented below

CREAM – Cognitive Reliability and Error Analysis Method

CREAM is based on a model and classification scheme that can be used for accident investigation and for the prediction of human performance. One essential assumption in the model is that a person tries to maintain control of a situation. The actions taken are determined more by the actual situation than by any internal psychological mechanisms that might underlie failure.

An extensive description of the theory and method has been published (Hollnagel, 1998). In brief, CREAM is based on the following principles:

- The probability of human error depends on situation and context. Human errors cannot be analysed as isolated events.
- The probability that an error leads to an accident depends on the functions and state of the system.
- Prediction of future accidents and errors should be based on analysis and understanding of earlier incidents. A similar methodology is needed for near-accident investigation and predictive analysis.

One variant has been developed for the analysis of road traffic accidents (Wallén Warner et al., 2008). It is called *DREAM*, which stands for the Driving Reliability and Error Analysis Method.

SCAT – Systematic Cause Analysis Technique

SCAT is based on a *loss causation model*, which has been proposed by Bird and Germain (1985). The model is based on five components:

- Lack of control
- Basic causes
- Immediate causes – substandard acts and conditions
- Incident
- Loss – people and property

Accident causes are identified using a number of lists related to the model. The result is intended to point to shortcomings in the work environment, performance factors and management systems. SCAT has been published in part, but the more elaborate descriptions are proprietary. There are a few shortened descriptions available (e.g., Sklet, 2002).

Tripod

The *Tripod model* was initiated at the end of the 1980s, and it has been further developed since (Reason, 1997; Groeneweg, 1998). A basic idea in the Tripod model is to highlight the importance of organisational failures as causes of accidents. The name tripod alludes to the fact that the model has three legs:

- General failure types (GFT)
- Unsafe acts
- Negative outcomes

An important characteristic is that the number of GFTs is limited to eleven, which are supposed to cover all situations. The GFTs are:

1. Design
2. Tools and equipment
3. Maintenance management
4. Housekeeping
5. Error enforcing conditions
6. Procedures
7. Training
8. Communication
9. Incompatible goals
10. Organisation
11. Defences

The model has provided a foundation for a few proprietary methods. One is *Tripod-Delta*, which is briefly described by Reason (1997). *Tripod-Beta* is a computer-based instrument for the investigation of accidents.

STAMP Systems-Theoretic Accident Model and Processes
A fourth example is *STAMP* (Leveson, 2004), which has its roots in the same model as *AcciMap* (see Section 13.7), and is based on a hierarchical systems perspective. In this kind of systems theory, systems are viewed as hierarchical structures, where each level imposes constraints on activity at the level beneath it.

In STAMP, systems are viewed as interrelated components that are kept in a state of dynamic equilibrium by feedback loops of information and control. Safety management is seen as a continuous control task that imposes the constraints necessary to limit system behaviour to safe changes and adaptations.

There is a published example of an investigation of an outdoor accident based on STAMP (Salmon et al, 2012). The same accident was also analysed using AcciMap, which provides an interesting benchmark comparison.

13.2 STEP

Sequentially Timed Events Plotting (STEP) is a well-established method for the investigation of accidents. An extensive manual describes the method (Hendrick and Benner, 1987), and also gives lots of advice on how to conduct an investigation. There are several brief summaries available, e.g., by Sklet (2002).

The principle is to identify the events that are related to the accident sequence. These events are arranged in a time sequence and associated with individual actors. The result is a diagram presenting the sequence in relation to different actors.

Investigation procedure

The investigation procedure has a number of stages. In the somewhat simplified description presented here, it contains:

1) Preparation
2) Data collection
3) Identification of events and actors, which are recorded as *building blocks*
4) Organising building blocks in a STEP worksheet with time on one axis and actors on the other

5) Showing the connections between the different events using arrows
6) Testing the STEP worksheet
7) Proposing improvements
8) Summing up the results

1) Preparation

The investigation starts with the establishment of scope and aim, and resource planning. The original description recommends that the time limits – the beginning and end of the accident sequence – are defined during the preparation stage. My view is that it is too early to do this before the investigation has started. Instead, preliminary time limits should be specified, which can be corrected later if needed.

2) Data collection

Data collection is performed by interviewing witnesses, studying documents, etc. One part of this is to establish a list of actors (see below) who are relevant to the accident.

3) Identification of events and actors

An event is an action performed by an actor, which can be a person or an item that influences the accident process. Events are the basic *building blocks* in the investigation, and each event should be documented carefully. The documentation covers:

- Time of the event
- Duration
- Actor
- Action data
- Source of information

4) Organising building blocks

The building blocks are positioned on a STEP worksheet, which in principle is a matrix with time on one axis and actors on the other. Figure 13.1 shows the basic layout. The sequence has been assumed to start at time t_0, and you should note that the time scale does not have to be linear. Each event is related to a specific actor, and is positioned at the time it occurred. The left side of the event square indicates the start time.

5) Showing the connections between the events

Arrows are used to show how the events are related. According to Hendrick and Benner (1987), only direct (causal) relationships should be relevant. However, it is rather common that indirect effects are also included.

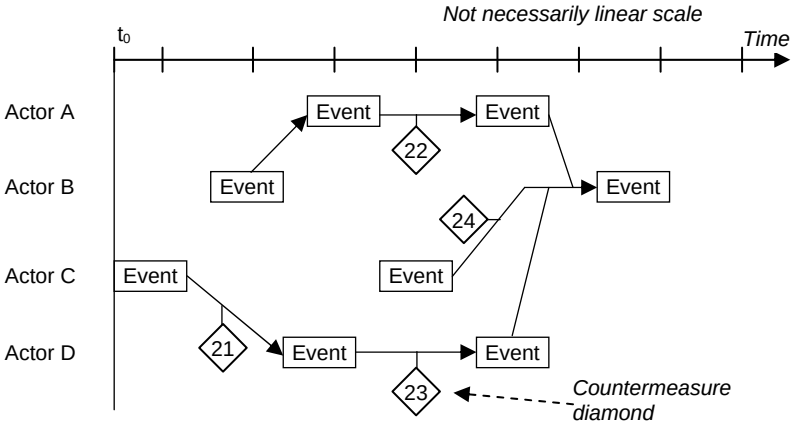


Figure 13.1 The STEP worksheet

6) Testing the STEP worksheet

One feature of STEP is that it involves a systematic check on the worksheet, which can lead to additional events or corrections. This test stage has four parts.

The first is called ***BackSTEP***, which is used to determine what happened during a gap or time interval with uncertain information. The principle is to start with a block to the right of the diagram, and ask questions about what could have led to that.

In the ***row-test***, the focus is on one actor at the time. The aim is to discover if some information might be missing. In doing this, the "First law of accident investigation" (Hendrick and Benner, 1987) is useful: *Everyone and everything is always someplace doing something during an accident.*

The ***column-test*** checks the sequence of events and timing by analysing the placing of each event. To pass the test, the studied event must have occurred after all events to the left in the diagram, and before all to the right. Furthermore, all elements in the same column should occur at the same time.

The ***necessary-and-sufficient*** test is used to check couplings between the events. One question is whether an earlier action was sufficient to produce a later event, or whether other actions were also necessary. This might lead to more events being needed to explain what happened. Another issue is whether there are too many arrows entering a building block, or whether unnecessary events are in the diagram. Hendrick and Benner

(1987) state that the goal is for an event to be preceded only by as many events as are necessary.

7) Proposing improvements

STEP includes a scheme for the identification of safety problems and the development of safety recommendations. This involves an inspection of all blocks and arrows in order to find safety problems, as revealed by the effects on later events. The problems are converted to statements on the need for corrective actions. These are marked as diamonds in the STEP worksheet, and refer to a separate list in which the suggested countermeasures are described.

Comments

A slightly different variant has been proposed by the Foundation for Scientific and Industrial Research (SINTEF) in Norway (Sklet, 2002). In this, a triangle is used to mark safety problems on the worksheet, which are further studied in a separate analysis.

The STEP method assumes situations with strict relations between cause and consequence, and other influences are not included. This is a simplification of the accident scenario, which means that important information might be disregarded. Already at the planning stage of a STEP analysis, the starting point of the accident should be assumed. However, I think that this is hard to establish too early, and will be rather arbitrary.

Multilinear Events Sequencing

A number of other methods are directed at the chronological sequence of an accident. Another example is *Multilinear Events Sequencing*, which has been extensively described by Ferry (1988). It has several similarities with STEP, such as a diagram with events and actors. One additional feature is that the conditions that influence the events can be inserted into the diagram.

13.3 Simple Event Mapping

One of the first issues in an investigation is to find out what happened, and STEP can be used for that. However, the method can sometimes be seen as too time-consuming and rigorous, if all elements in the method are applied. If you say that you use STEP, it is essential that you follow the procedure; otherwise, it is misleading.

In practical investigations, many people, including myself, have often adopted a simplified approach as an alternative. It might be called *Simple Event Mapping (SEM)*, or even STEP Light. The aim of SEM is to give an

overview of the sequence of events. The principle is to identify actors and events related to the accident, and then present them in a time diagram.

A basic idea underlying the SEM approach is to start the investigation by getting an overview of what happened. Explanations and causal relationships are explored at a later stage. The method is intended to be used in combination with one or more other methods for accident investigation. In Section 16.2, an example is given of the event mapping of an incident in a hospital.

The method has a restricted aim compared with STEP. A simplification is that strict cause–consequence relations are not implied by the arrows. This allows for less strict coupling between the events, which also means that the testing of the sequence is less rigorous. Another simplification is that improvements are not suggested, since it is assumed that this will be done later in the investigation using some complementary technique.

Investigation procedure

The analysis should contain the following stages:

1) Planning and preparation
2) Data collection
3) Identification of events
4) Analysis of events
5) Summary of results

1) Planning and preparation

When SEM starts, it is usually uncertain how complex the accident is, but some simple planning is needed. The first thing is to establish which witnesses and documents should be considered. After the first round of identification, a better understanding of the accident and its complexity will be obtained, and then the planning can be revised

2) Data collection

This stage involves interviews with witnesses and the collection of documents.

3) Identification of events

The collected data might be extensive, and include many statements. The data have come in a rather arbitrary order, depending on the sources. The aim of this stage is to identify the essential events and make a list of them. A practical approach is to create a table for the recording of events. The table can have columns like:

- Event
- Actor

- Time of the event
- End time of the event, which can also be a more or less permanent change of state (e.g., something breaks)
- Description of the event
- Source of information

The identified events are noted in the table. It is not necessary that they had a direct influence on the accident. At a later stage, the essential information to be used in the final presentation can be established. The identification of events can be supplemented later, if data are found to be missing.

4) Analysis of events

The aim of this stage is to arrange the events in a suitable order. An analysis can be performed in different ways, depending on the situation and requirements. In a complex case, it can be advantageous to base the initial analysis on a table of events.

Working with the table

Simple sorting is based on the table of events. The events can be arranged in time order, e.g., by using the sort facility in your word processor. They can also be sorted by actor, or by a combination of actor and time.

Separate time phases

An accident investigation usually describes the immediate course of events, often in a rather short time perspective. However, it is not obvious how far back in time the investigation should seek to go. It might be valuable to understand when and how the risks arose. The collection of data might reveal a long prehistory, in which many explanations can be found.

Likewise, you can ask when the accident has come to an end. It might be when the injury occurred, when emergency action is ended, or when the system is back in normal operation. The quality of emergency services and the efficiency of restoration will often considerably influence the consequences.

Thus, a wide time perspective might be valuable, both for getting the full picture and for effective safety improvements. The history can be divided into:

- Prehistory
- Acute phase
- After – emergency action and restoration

At the different time phases, there are often different actors involved. Therefore, a practical approach is to present these phases in separate diagrams or tables. Figure 13.2 demonstrates the principle of merging three time diagrams into one; however, it is often better to have three separate diagrams.

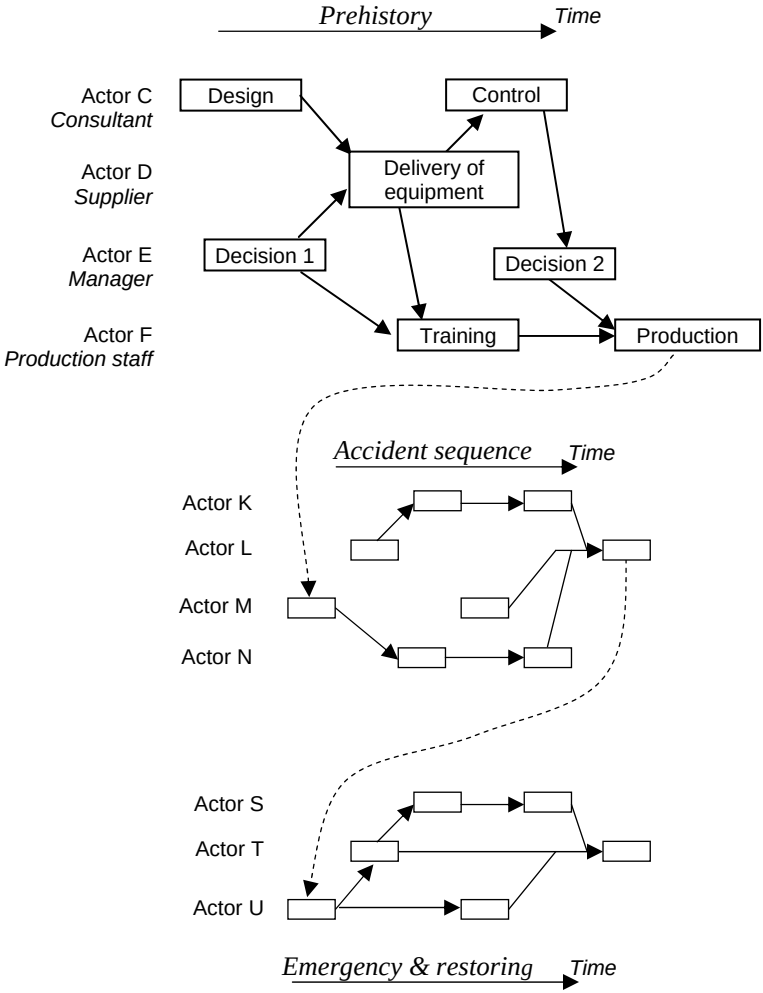


Figure 13.2 Condensed diagram with three time phases in an accident

Diagram
In the next stage, a diagram with actors and events can be created. It is an attractive format and easy to understand. Information for this can be taken directly from the table. Such a diagram could look like a STEP worksheet (see Figure 13.1), although the symbols for suggested countermeasures will be missing.

Checks and corrections
During the analysis stage, the course of events becomes clearer. Examination of the results can uncover errors in time statements, missing information, etc. By using the table, it is rather easy to analyse time information and detect the needs for correction. Quite often, there are uncertainties in time statements, and information from different sources might be conflicting.

This might lead to the introduction of additional events and corrections. If, for example, the time of a specific event is critical, possible contradictions must be sorted out. When uncertainties remain despite extra study, this should be made clear in the report.

Comment
Simple Event Mapping (SEM) is an alternative if a formal STEP investigation cannot be performed. If it is found later that a more thorough analysis is required, the results of the SEM can still be useful.

13.4 The AEB method
The *AEB method* is based on the *Accident Evolution and Barrier Function (AEB)* model (Svenson, 1991). An extensive manual for applying the method has been published (Svenson, 2000). The method can be used for the analysis of accidents and incidents. An accident is modelled as a sequence of human and technical errors, which can be stopped by *barrier functions*.

The AEB method is related to safety barriers and functions, as discussed in Chapter 11. A central concept is *barrier function*, which is a function that can interrupt the evolution of an accident so that the next event in the chain will not happen. A barrier function is always identified in relation to the system(s) it protects, has protected, or could have protected.

Barrier function systems are the systems that perform the barrier functions. A system might consist of an operator, an instruction, a physical separation, an emergency control system, or other safety-related systems.

The aims of an AEB analysis are to give a description of accident evolution, to identify broken barrier functions, and to suggest how the functions can be improved.

Analytic procedure

The analysis is performed in eight steps according to the manual (Svenson, 2000). A quick summary is given here:

1) Data collection and a detailed description of the accident.
2) Select one error event, which can be an important event in the middle of the chain.
3) Develop the flow diagram by identifying error events that both precede and follow the selected event. Also, barrier functions that failed to stop the sequence should be identified.
4) The flow diagram is completed with barrier functions that could have stopped the accident evolution chain.
5) Each existing barrier function is analysed according to specific guidelines.
6) Characteristics of the technical, human factors and organisational systems that may change the strength of each existing barrier function are identified.
7) Proposals are made for new barrier functions, and what is needed for their maintenance.
8) Report with recommendations.

Diagram and barriers

The result of an AEB analysis after Stage 4 is a description of the evolution of the accident in the form of a flow diagram, which shows human and technical errors (Figure 13.3). A division is made into the *Human factors system* and the *Technical system*. The diagram also shows the barrier functions related to specific errors. If a particular accident or incident occurs, all the barrier functions in the sequence must have been broken or ineffective.

One feature of AEB is that it only models errors, which means that it does not provide a conventional event sequence description. The error event boxes are connected by arrows in order to show evolution in an approximate chronological order. The general rule is that one arrow leads to an error box, and one arrow comes out of the box.

The flow diagram (Figure 13.3) also shows barrier functions. The first failed and did not stop the sequence continuing to *Human error event 2*, while the second prevented the potential accident from occurring.

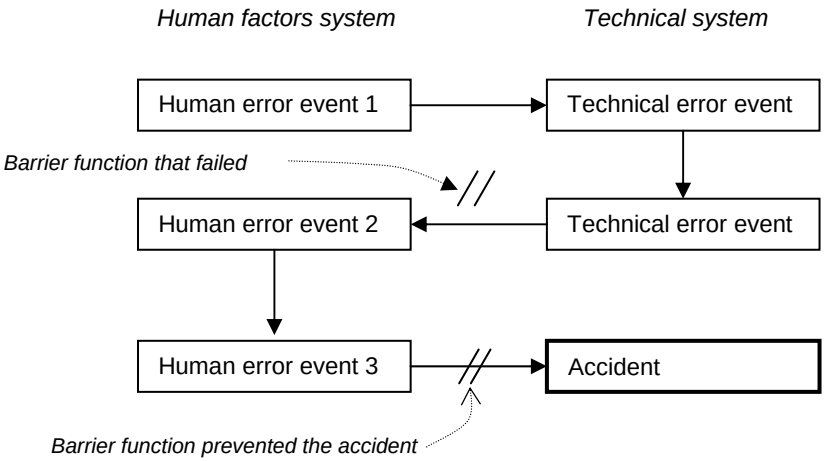


Figure 13.3 Example of an AEB flow diagram

One important purpose of an AEB analysis is to identify broken barrier functions and suggest how they can be improved. They are divided into three main categories:

- Ineffective barrier functions, in the sense that they did not prevent the development of an accident or incident.
- Non-existent barrier functions; if present, they would have stopped the accident or incident evolution.
- Effective barrier functions, which actually prevented the progress towards an accident or incident. These are normally not included in an AEB analysis, since the AEB model is based on errors.

Svenson (2000) points out that the organisational and technological context provides the framework for an accident. Therefore, an AEB analysis includes questions about the context in which the accident took place. Two questions in the method deal with this:

A) To increase safety, how is it possible to change the organisation in which the failure, incident or accident took place?

B) To increase safety, how is it possible to change the technical systems context in which the accident took place?

Comments

The method focuses on a sequence of errors, and on how barriers can prevent accidents from occurring. It should be noted that only events representing errors are shown, which means that it is not a common sequence model.

One potential drawback is that the method reduces the course of events to a single sequence. Consequently, analysis will be difficult in the case of accidents with several parallel chains of events.

13.5 Events and Causal Factors Analysis

Events and Causal Factors Analysis (ECFA) is an example of a technique that combines an accident sequence with an investigation of root causes. The method is described exhaustively in a handbook from the U.S. Department of Energy (DOE, 1999), which is also available on the web.

The aim of an ECFA is to determine causal factors by identifying the significant events and conditions that led to the accident. A key concept in this method is *causal factors*, which are defined as the events and conditions that produced or contributed to the occurrence of the accident (DOE, 1999). There are three types of causal factors:

- *Direct causes* of an accident are the immediate events or conditions that caused the accident.
- *Contributing causes* are events or conditions that, alongside other causes, increased the likelihood of an accident, but they did not individually cause the accident.
- *Root causes* are the causal factors that, if corrected, would prevent recurrence of the same or similar accidents. Root causes may encompass several contributory causes. They are higher-order, fundamental factors that address classes of deficiencies, rather than single problems or faults.

The first stage in ECFA is called *Events and Causal Factors Charting*, and it is mainly used early in the investigation.

Events and Causal Factors Charting

Events and Causal Factors Charting is used to obtain a graph of the sequence of the events in combination with conditions related to the accident. The method can be used manually or with computer support. In short, the steps in the analysis (see DOE, 1999) are:

1) Identify events and conditions related to the accident.
2) Arrange these in time sequence.
3) Construct the primary chain of events that led to the accident.

4) Add secondary events on a line above the primary chain.
5) Place the conditions that affect the events above the events.

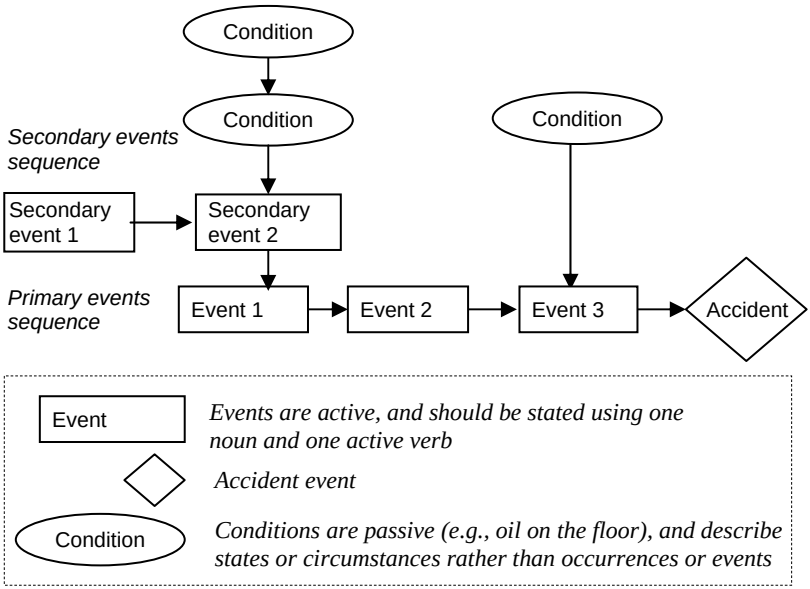


Figure 13.4 Simplified Events and Causal Factors Chart (after DOE, 1999)

Figure 13.4 shows the principles of the chart. The baseline is the primary events sequence at the bottom. Secondary events are added above with arrows showing their connections to the basic chain. Conditions affecting the events are placed in the chart in suitable positions. In a real case, such a chart can be complex and contain many elements.

The causal analysis stage

At the analysis stage of ECFA, the aim is to identify the accident's causal factors. Results from the Events and Causal Factors Chart and from other methods are used. The analytic process is quite complex and guided by a set a questions and rules (DOE, 1999).

When the causal factors have been identified, the final stage in the analysis is to determine the *root causes* of the accident (as defined above). An analysis of root causes can be performed in several ways. ECFA can be used as input. A root cause analysis is then used to refine the list of causal factors and categorize each according to its significance for the accident.

The DOE (1999) writes that there may be more than one root cause of a specific accident, but probably not more than three or four. This statement helps a bit in understanding what the DOE means by root cause. Examples are deficiencies in *Management responsibility* and *Safety policy implementation*.

13.6 MTO Analysis

Introduction

In the Swedish nuclear power industry and in the Norwegian offshore industry, accident investigations based on MTO have become popular. MTO is an acronym for Man–Technology–Organisation, which was introduced by the Swedish Nuclear Inspectorate, mainly as a synonym for Human Factors. According to a summary by Rollenhagen (2011), another source of inspiration was an accident investigation method called the *Human Performance Enhancement System* from the Institute of Nuclear Power Operations.

An accident investigation method often labelled MTO Analysis has been applied in different fields in the Scandinavian countries. Actually, it is not a specific method, but rather a set of related methods. A number of descriptions have been presented, by, e.g., Bento (1999) and Rollenhagen (2003) in Swedish. An English version has been published by Evenéus and Rollenhagen (2007), and the description of the investigation procedure below is mainly based on that. An alternative short description is provided by Sklet (2002).

MTO concept lies within the human factors tradition, but also includes an organisational perspective. The result of an analysis is a diagram, an *MTO event investigation chart*, which describes the accident at three levels. The first level shows the basic event chain and the barriers. The second level presents causes and conditions that have affected the event chain, and the third level demonstrates the influence of the management system. The method is systems-oriented in the sense that accidents are understood as a result of complex interactions between people, technology, and the organisational context.

Analytic procedure

The investigation procedure can be summarised in five steps:

1) Describe the chain of events
2) Search for causes and conditions
3) Identify barriers
4) Analyse consequences
5) Develop recommendations

1) Describe the chain of events

The aim of this step is to explain what happened. Key events are identified through interviews, etc., and are then placed in time order on a single line. The method does not require strict causality between events.

2) Search for causes and conditions

The aim of the second step is to explain why the event happened. There are two elements:

- Conditions that may explain an event, such as working conditions, technical characteristics, procedures and instructions.
- Actions, including a lack of action that are not a part of the basic chain of events, but might have affected the chain.

When such elements are identified, they are represented by oval symbols with explanations, which are then put at suitable places in the diagram. These elements are named causes. In general, *cause* is a term that can be interpreted in many ways, and, in this method, is deliberately treated as a general and vague concept.

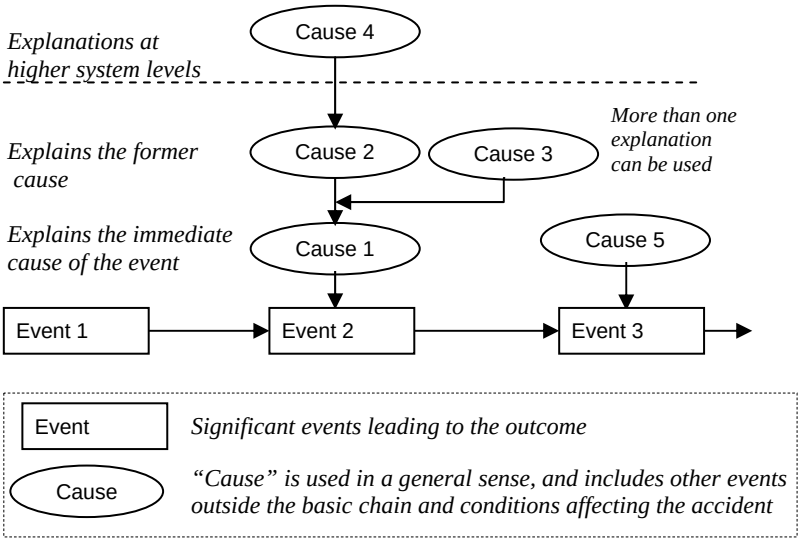


Figure 13.5 The basic MTO event investigation chart

Both causes with a direct impact on the basic chain of events, and the underlying causes must be searched for. A horizontal line can be used to highlight causes that are related to the management system. These are sometimes called *root causes* or *basic causes*. Figure 13.5 shows an investigation chart after Step 2, with a basic chain of events, causes, and a dividing line.

3) Identify barriers

At this step, the question of what could have prevented the accident is addressed. The definition of barriers varies between different applications, and has also varied over time (Rollenhagen, 2011). Barriers can be classified as:

- Technical and physical
- Human
- Administrative

Barriers are also divided into:

1. *Failing barriers*, which were in place but did not function satisfactorily
2. *Functioning barriers*, which stopped the event
3. *Missing barriers*, which were not in place

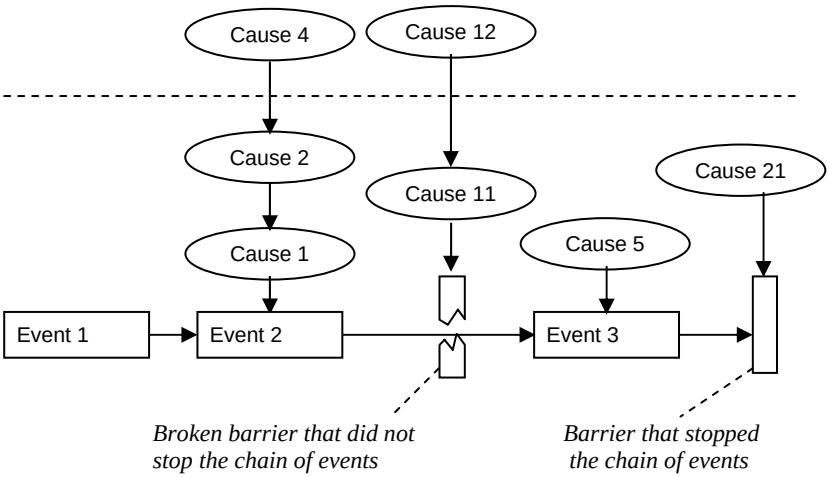


Figure 13.6 Introduction of barriers into an MTO event investigation chart

A missing barrier is defined as an element that, in retrospect, was found to be essential to ensuring safety in the system. It might be difficult to distinguish between a missing barrier and a failing barrier.

The barriers are inserted into the diagram, and failures of barriers are investigated further by looking for conditions and causes. Examples of the introduction of barriers are shown in Figure 13.6.

4) Analyse consequences
This step is optional, but can sometimes be of interest. It deals with what might have happened, e.g., a worst case scenario. It can be useful in setting priorities and in discussing improvements.

5) Develop recommendations
Based on the analysis, recommendations for improving safety should be developed. The method does not have a specified procedure for this step.

Comments
The MTO Analysis method has developed over a long period through practical use. This has taken place in various organisations, which has led to alternative definitions and practices. The developments have been discussed by Rollenhagen (2011). He points out that an event investigation is a result of a "construction process" and will therefore reflect the knowledge, culture, values, etc. of the people engaged in the investigation.

MTO Analysis has become popular in many organisations, and is widely used in Norway and Sweden. One advantage of the method is that it gives a graphical overview of the course of an accident and the influencing factors.

13.7 AcciMap
Background
An accident occurs in a physical and social context, such as place, victims and the physical objects directly involved. There are also other actors involved in a more or less direct way, who might be individuals, companies, other organisations, or authorities. The interaction between these actors can be complex and difficult to grasp, but are important from a systems perspective.

Originally, *AcciMap* was a format for the analysis and graphical representation of an accident or critical event (Rasmussen, 1997; Rasmussen & Svedung, 1997). It has many similarities to a *mind map*, which gives a structure and framework for describing an event. AcciMap actually means accident map.

The approach has been further developed, and is described in detail by Jens Rasmussen and Inge Svedung (2000); there is also a shorter version (Svedung & Rasmussen, 2002). The account here is based on these

descriptions, and also on a guide to the method by Strömgren (2009). The fairly free format for modelling has been retained in the analytic method. Alternative methodologies have also been put in practice, which are discussed below.

The structure

A basic idea is a division into different system levels, which is illustrated in the model in Figure 2.2 in Section 2.3. This principle characterizes the structure of the AcciMap. It is illustrated in Figure 13.7, the left part of which shows a division into seven system levels, which can be used for analysis. It differs somewhat from the original model, and the highest level (7) is based on a suggestion by Strömgren (2009). The three basic levels (1–3) are always relevant in an accident, but the arrangement of the higher levels can vary according to the circumstances at a specific accident.

An analysis starts from a *critical event*, which might be an accident, a near-accident, or another critical event. This is symbolised by a framed box, whereas other events are marked as simple boxes. On the bottom row (2), the events are shown (in greater or lesser detail) in time order. Events leading to the critical event, and also consequences, can be shown here.

The elements that influence the events and the outcome at the bottom are entered vertically (see Figure 13.7). Boxes can also be used to denote the consequences of decisions, and also other circumstances. How to use the symbols is not strictly specified in the manuals, which means that they might vary according to the analyst. The map is composed of rectangles and arrows.

- A rectangle with a frame symbolises the *Critical event*, the starting point of the analysis.
- A normal rectangle is used rather freely and it can represent different things, such as an event, a consequence, or a condition.
- A rectangle with round corners shows a precondition for the accident that is not analysed further.
- An influence arrow does not have to represent a strict cause-consequence relationship.
- A number in a square is a reference to an annotation explaining events, conditions and influences more thoroughly. In the map, there is no space for any detailed information.

Actors are usually not shown explicitly in an AcciMap diagram, but they often relate to a specific system level and event. One option is to develop an ActorMap, which is part of the original concept, but will not be shown here.

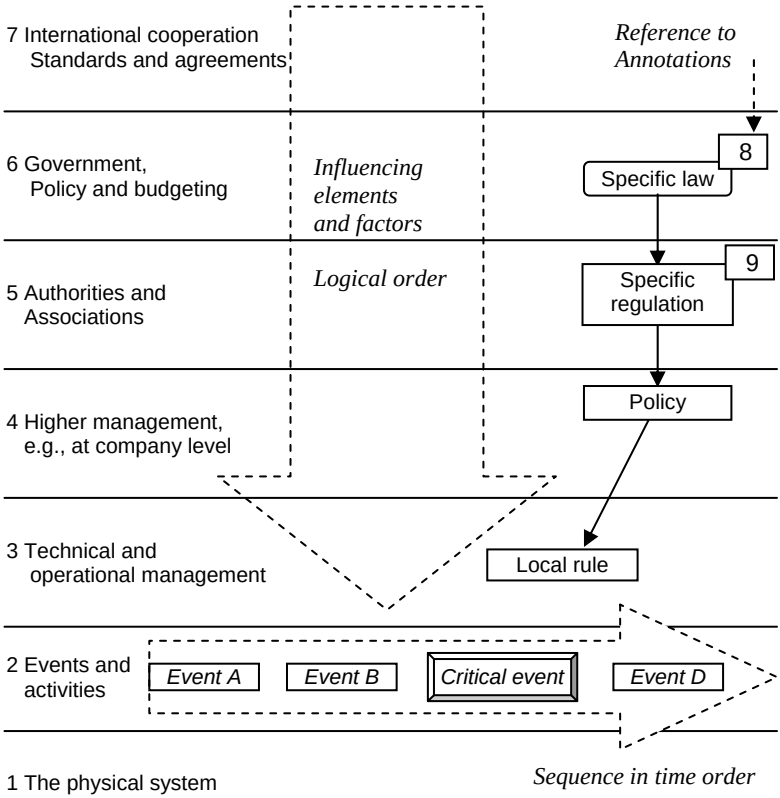


Figure 13.7 The basic dimensions of an AcciMap

Analytic procedure

The original publications (e.g., Svedung & Rasmussen, 2002) did not really discuss the analytic procedure, but a more concrete manual was developed later (Strömgren, 2009). This account is a simplified variant on this. The procedure is divided into a few stages:

1) Preparation
2) Data collection
3) Summing up the data
4) Arranging the sequence
5) Construction of the map
6) Verification and improvement
7) Summing-up and reporting

1) Preparation

Usually, an investigation has been made using a simpler method (e.g., STEP). The AcciMap will then represent a deeper analysis of the socio-technical system related to the system. The preparation stage includes a definition of the goal and more precise demarcation of the analysis. A team with experience from various fields related to the accident is almost obligatory.

In teamwork, it is practical to use a white-board and stickers, on which you write down different events and conditions. The space on the white-board should then also be divided up by using horizontal lines to mark the system levels. This makes it easier to successively improve the map by moving the stickers when the relations get clearer. Then, it is useful to have a camera for documentation, both of the gradual development and of the final results.

2) Data collection

Information about the accident and some conditions related to it are probably available at the outset. Before the analysis starts, some further data can be useful, such as a chart of the accident site, and instructions for the job that was involved. Much of the data collection, however, is done during the analysis, which generates questions and further searches for information.

3) Summing up the data

Making a list of the data obtained is a practical start; the concrete events directly related to the critical event are put first, followed by other items. The list can be generous, and also have items that will not necessarily be included in the final result.

4) Analysing the sequence

The analysis starts with a summary of what happened. The results are placed at *Level 2 Events and activities*. The first thing is to select the critical event that is to be studied. The preceding events are placed to the left and the consequences to the right, thereby positioning the events in time order.

The technical and physical conditions that have affected the sequence are placed at the lowest level, *Level 1: The physical system*. The events and the conditions are connected by arrows, which indicate some kind of influence.

5) Construction of the map

The events (or conditions) shown at the two lowest system levels are then investigated. For each event, an identification of conditions or situations that have contributed to the event is made. The essential ones are inserted in the diagram, and placed at a suitable system level.

The text for the items (events, conditions, actors, and influences) on the map must be short, and it is practical to make separate annotations when needed. Each annotation can have a unique number, which is then attached to the specific item.

Identification can follow a single path or a combination of paths:

- Start with events at the bottom. Each item is followed upwards through the system levels until it is no longer meaningful to go further.
- Analyse one system level at the time, going from the lowest to the highest.
- Choose one or more actors (or categories of actors), which are to be investigated further.

A crucial step is to arrange the different items and connect them with influence arrows. The influences are not always obvious, and annotations can also be useful here. During construction of the map, you should be aware that an AcciMap can look very different according to the analyst. The design is a trial-and-error process that works towards a more logical and consistent diagram.

6) Verification and improvement

After a preliminary diagram is obtained, it needs to be thoroughly controlled. The first thing is to check the diagram, which includes looking for errors in time order, logical faults, and interpretation problems. Changes and more annotations might be needed.

One aspect is to decide how far up in the system the map should reach, which depends on the general aim of the analysis. If an investigation is to be published, it is appropriate to go high, since publication might also concern more general problems. However, the analysis should not be based on speculation; if the data are not sufficient, you should not go further. A hypothesis may be acceptable, but it should be clearly marked as such.

7) Summing-up and reporting

Basic information from the analysis is the AcciMap itself, but this can be quite complicated and require explanation. In addition, a list of annotations is essential for explaining the results. Other valuable documentation that might have been produced is:

- A list of actors
- A list of problems and safety defects
- A list of suggested improvements

During the analysis, a number of problems and safety defects might have been identified. They can be seen as a part of the results. Development of safety improvements is not part of the original method. However, nothing restrains you from suggesting improvements.

Example

There are several published examples of AcciMaps. Figure 13.8 gives an outline of an analysis, of an industrial fire with loss of life. The chosen critical event is the start of the fire: *Fire starts*.

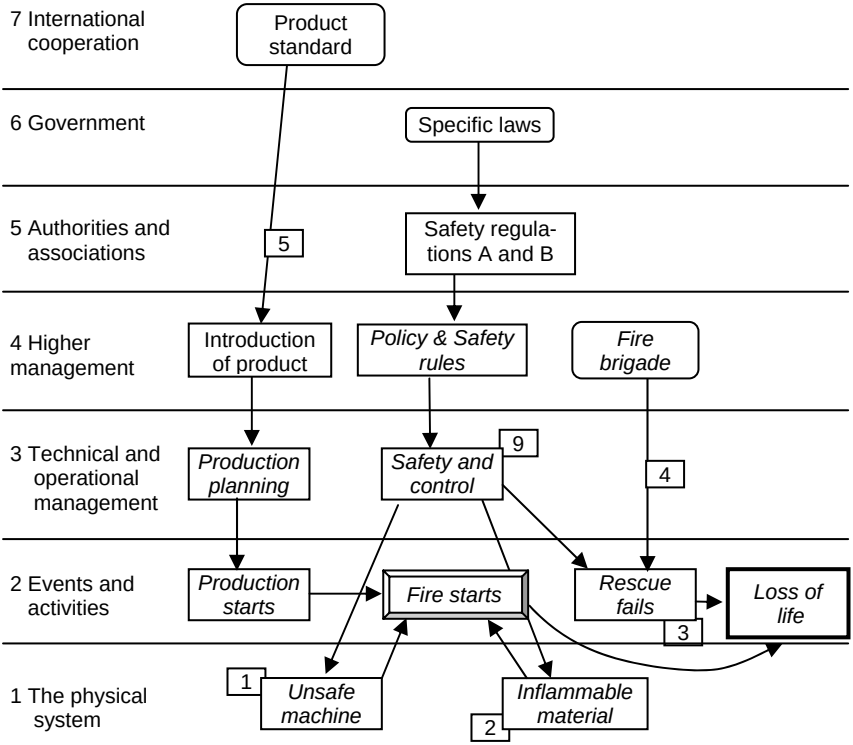


Figure 13.8 An industrial fire, as summarized in an AcciMap diagram

On the bottom row, an unsafe machine and lots of inflammable material define the dangers in the physical system. Row 2, with events and activities, shows the major events that led to the accident. The sequence is only faintly outlined, but all the details do not have to be shown in the diagram if the course of event is summarised elsewhere. A fire can break out, since there is an unsafe machine, inflammable material, and a potential triggering event when production starts.

Row 3 shows company management for production planning. It also includes a safety and control function, which has influenced the presence of an unsafe machine and inflammable material in the workplace. This is shown by arrows, which also show an influence on the failed emergency operation.

Row 4 is related to higher levels, where new products are initiated and the company safety policy and rules are formulated. Community rescue services belong to another organisation, but fit best at this level.

The two rows at the top illustrate that national laws and international standards have had an influence on the case.

The text in the diagram is brief, and it is essential to have a comprehensive list of numbered annotations to link to the numbers on the map. This simple example contains 14 boxes and 13 influence arrows. A real case is more complex, and a study could easily generate more than 50 boxes and many more arrows. An example of a traffic accident (Svedung & Rasmussen, 2002) has around 60 boxes.

Comments

The AcciMap can be seen as a general concept, and a number of variants have been developed from it. In the original version, the arrows are used in a flexible manner, and they designate some kind of influence. A rectangle can represent events, consequences, or conditions.

As well as the first version, other forms of AcciMap have also been published. An overview of different approaches has been summarised by Branford (2007), who also discussed the possibilities of obtaining stricter and more easily reproducible results from such an analysis.

An alternative manual for AcciMap has been developed (Branford, 2007; Branford et al., 2009). The aim was to get more stringent and reproducible maps. This manual recommends that there should be strict causal relationships between rectangles connected with arrows. The rectangles usually denote a cause and/or an outcome. There are also fewer system levels, namely:

a) External
b) Organisational

c) Physical/ actor events, processes and conditions
d) Outcomes

The opportunity to use different variants of the method is positive, and the variants have different pros and cons. In a practical case, it is essential clearly to define how the analysis was done, and on which manual it was based. For example, clearly state whether the arrows indicate strict causal relations or more general influences.

Often accident investigations are near-sighted, and may miss more general aspects. In many applications, it is advantageous to use AcciMap to obtain a fairly free and broad overview. When it is considered relevant, stricter relationships can be developed and investigated further.

13.8 Change Analysis

Changes to a system can create new hazards or lead to deteriorations in the control of hazards that are already being handled. Changes can be planned, predictable and desired, or they can be unintentional and unwanted. The method *Change Analysis* is designed to identify the causes of increased risk arising from system changes. It has been employed since the 1960s, and is well-documented (Bullock, 1976; Johnson, 1980; Ferry, 1988; DOE, 1999). The method was originally designed for application to organisational systems (Kepner & Tregoe, 1965).

A Change Analysis is based on a procedure in six main steps (DOE, 1999):

1) Describe the accident situation
2) Describe a comparable accident-free situation
3) Compare the accident and non-accident situations
4) Identify differences, summarising changes and also the results of those changes
5) Analyse differences for effects on accident
6) Combine the results with findings from other methods

For describing the accident-free situation, a *baseline situation* is needed. It could be:

- The same or similar situation before the accident (e.g., previous shift, last week, or last month)
- A model or ideal situation (i.e., as designed or engineered)

The DOE (1999) points out that, at the early stages of an investigation, there is often insufficient information to determine whether a change is important or not. As the investigation proceeds, it will become clear that some of the changes noted are insignificant.

A special record sheet can be used for Change Analysis. It shows the factors that may be subject to change. For each factor, there should be descriptions of current and previous situations, differences, and changes that may have an effect. Twenty-five factors are divided into eight main groups:

1. What
2. Where
3. When
4. Who
5. Tasks
6. Work Conditions
7. Trigger Event
8. Managerial Controls

Both planned and unforeseen changes are included, and the method has similarities to Deviation Investigation. However, in Change Analysis it is assumed, more or less clearly, that the old system has an adequate level of safety. In using the method, it is important to be aware of this, since such an assumption might be over-optimistic.

13.9 Deviation Analysis of events

The method *Deviation Analysis* can be used both for the analysis of a system and for the investigation of an event. In the later case, it can also be called *Deviation Investigation*. The method is described in detail in Chapter 8, and the text here just gives complementary advice on how it can be applied in the analysis of events. In the study of events, the focus is on actual deviations that have happened or still exist. The forecasting application is to look for deviations that may occur, which is more theoretical and hypothetical. In Chapter 16, there are three examples of accident investigations based on this method (see sections 16.2, 16.3, and 16.4).

Analytic procedure

The analytic procedure (Figure 13.9) is similar but not identical to the other application (Figure 8.1 in Section 8.3). The preparation stage includes clarifying aim, scope and other general aspects (also Section 3.5). Here, it also includes initial data collection, such as interviews, documentation and other information.

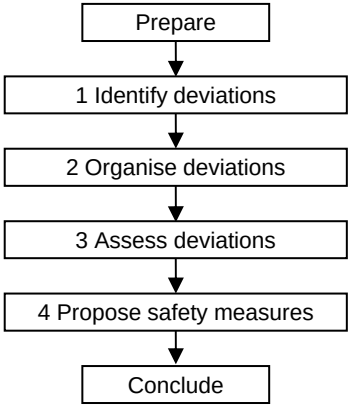


Figure 13.9 Procedure for Deviation Analysis of events

1) Identify deviations

The aim of this stage of the analysis is to find deviations related to the event. The search is rather wide, and a deviation does not need to have a direct cause-consequence relation to the event. The deviation might cause an increased likelihood of other deviations, or make the system more vulnerable to damage, or something else.

The result of this stage is a list of deviations. A practical way is to use a table for the recording events. One column is of course for deviations, and in order to make the data collection traceable, a further column can be added, where the source of information is entered.

Identification can embrace some of the techniques below:

A) Trace the events backwards
B) Text analysis
C) Analysis of interviews
D) Supplementary identification

A) Trace the events backwards

The chain of events is followed backwards in time (like rewinding a film in slow motion). The deviations that are discovered are included in the list.

B) Text analysis

A text analysis is based on written information, which can be of any kind. The text is read through, while you try to identify words or phrases that directly or indirectly point to a deviation. A practical way of proceeding is to highlight the relevant words with a marker pen. The deviations are entered in the table.

C) Analysis of interviews
Using this technique you listen carefully to what is said, and when something can be interpreted as a deviation, you note it down on the list. This can be done directly during the interview, or it can be done on the basis of a recording or written summary. It is similar to a text analysis, and is based on existing material, not on active questioning.

D) Supplementary identification
During supplementary identification, the analyst is searching actively in various ways. It can be done in discussion with a working group, or during interviews. This can be achieved rather freely by being curious and asking questions, where there are indications of some kind of deviation.

One option is to employ the checklist of deviations in Table 8.2 in Section 8.2. It can be used both during interviews and in group discussions. In order to be meaningful, the checklist needs to be reformulated. For example, ask:

- Was the machine working normally? (T1)
- Was there anything unusual about the materials being used? (T3)
- Was the safety equipment working OK? (T5)

Deviations related to human errors can be expressed more concretely.

- Were all the parts of the job performed in the regular manner? (H2)
- Who planned the job? (H4)
- Were there any misunderstandings involved? (H6)

Organisational functions are important, and an investigation that does not consider them is incomplete. The checklist may make it easier to pose questions in such a way that they are not perceived as being loaded against any individual. Questions based on the checklist might be:

- Was planning adequate? (O1)
- Were planning procedures followed? (O1, H3 and H4)
- Was the training of the operator appropriate? (O2 and O3)

When problems with technical equipment have been observed:

- Why had the fault not been discovered before? (O5)
- Was the component covered by the maintenance programme? (O4)

2) Organise deviations
Identification will generate a list of deviations, usually in a rather arbitrary order. There might also be duplicates, e.g., when a specific deviation has been mentioned by several sources.

The aim of the organising stage is to arrange the data in a logical way and to reduce duplicates, before the analysis continues. There is no unique solution to how this should be done. One approach is to base the sorting on time, such as a categorisation into:

a) Before the acute situation
b) During the acute situation
c) After the acute situation
d) Permanent situation

Another principle for sorting can be based on the actors, e.g., the companies or the departments involved. A third approach is to base the grouping on types of deviations:

T Technical deviations
H Human deviations
O Organisational deviations

This organising is best done as an iterative process, and you can start simply with the time dimension. In practice, this can be achieved by adding a new column, where each deviation gets a code a) to d). The deviations can then be sorted on the basis of that column. If that type of categorisation is unsuitable, you can try an alternative.

One alternative or complementary procedure is to base structuring on a categorisation of actors. If that is not sufficient, types of deviations can also be used. At this organisation stage, duplicates will be detected rather easily.

3) Assess deviations

The result of the two previous stages is a list of deviations in a structured order. The aim at this stage is judge their importance, and establish whether safety improvements are needed. The principles for this are discussed in Chapter 5. In the evaluation of things that already have happened, a discussion of probabilities can be rather complicated. For that reason, the Direct Evaluation approach is preferable, and the risk evaluation scale shown in Table 5.2 in Section 5.2 is suitable.

4) Propose safety measures

The proposal of safety measure and concluding the analysis is the same as in the general method Deviation Analysis.

Comments

Deviation Analysis is a general method that can be used to analyse most types of events in various situations. The number of deviations on the original list can be high, and up to one hundred is not unusual in a large

investigation. At the organising and assessment stages, selection and sorting of deviations are performed. This is an essential aspect of the method since data are reduced in a controlled manner.

Data can be collected without any particular hypothesis about what may be the cause of the accident, or how deviations are related. This procedure also reduces the problem of jumping to conclusions too early before all facts are compiled.

13.10 Safety Function Analysis of events

Safety Function Analysis (SFA) can be used both for the analysis of a system and for the investigation of an event. *Safety function (SF)* is a broad concept (see Section 11.3), and is something that contributes to reducing risks in a system. It comprises technical and organisational functions, and also human actions. An application of this method is described in Section 16.2, which concerns an incident in a hospital.

In the study of events, the focus is on SFs that were involved in one way or another in the course of events. During the analysis of a specific event, the aims are usually:

- To identify SFs related to the event
- To evaluate how well the SFs worked
- To suggest improvements

This means that only a subset of all possible SFs will be identified. It is essential that the boundaries of the investigation are set wide, which means that the investigation can go from the specific workplace upwards in the organisation. Experience has shown that interplay between different levels is essential to understanding how an accident occurred (Harms-Ringdahl, 2009).

Analytic procedure

The SFA procedure for events is similar but not identical to the systems-oriented application. The method is described in detail in Section 11.4, but the text here gives supplementary advice on how it can be applied to the analysis of events.

1) Data collection

This stage will focus on the specific event, and data can be collected from available documentation. A preliminary accident investigation might be available. Interviews give valuable information, in particular about informal SFs which are not seen in official documents.

2) Identify SFs

The aim of this stage of the analysis is to find safety functions (SFs) related to the event, and the result is a list of these. As in Deviation Investigation (Section 13.9), the search is wide and relatively free. An SF does not need to have a direct cause-consequence relation to the event.

Identification can involve some of the techniques below (very similar to Deviation Investigation in Section 13.9):

A) Trace the events backwards
B) Text analysis
C) Analysis of interviews
D) Supplementary identification

A) Trace the events backwards

The chain of events is followed backwards in time (like rewinding a film in slow motion). The SFs that could have stopped or actually did stop the sequence are included in the list.

B) Text analysis

A text analysis is based on written information, which can be of any kind. The text is read through, while you try to identify words or phrases that directly or indirectly point to an SF. A practical way is to highlight the relevant words with a marker pen. The SFs are entered onto the list. In order to make the data collection traceable, a further column can be added where the information source is entered.

C) Analysis of interviews

One technique is to pose open questions, and then listen carefully for SFs. The first question addresses the sequence, and the two following take directly up SFs:

- Describe the event and the circumstances under which it occurred.
- How do you think a recurrence can be prevented?
- Do you think something could have prevented the event?

You listen carefully to what is said, and when something can be interpreted as a SF arises, you note it down on a list. This can be done directly at the interview, or it can be based on a recording or written summary. This is similar to text analysis, and, is based on existing material, not on active questioning.

D) Supplementary identification

During supplementary identification, the analyst does active searches in various ways. They can be done in discussion with a working group, or

during interviews. This can be achieved rather freely by being curious and asking questions, when there are indications of some kind of SF.

3) Organise the SFs

Identification generates a list of SFs, which will tend to appear in a rather arbitrary order. The list will contain duplicates, when a specific SF has been mentioned by several sources, sometimes differently phrased. The number of SFs might be rather high, and structuring is important. How to proceed with structuring is described in Section 11.4.

4) Evaluation of SFs

Different approaches to the evaluation of SFs have been thoroughly described in Section 11.5. The most interesting characteristic is how the individual SFs functioned at the event: *Did it work or not?*

In event investigations, the *performance* parameter is important. It describes whether the SF worked adequately during the studied incident. This is closely related to efficiency, but here it describes how the SF worked in reality on a specific occasion, e.g., during the accident.

Table 13.2 Classification of safety function performance

Code	Description
a	Yes – the SF was in place and performed satisfactorily
b	Partly – the SF worked to some extent but not completely
c	No – the SF did not perform as expected
d	Suggested – the SF did not exist and is a suggestion
e	The SF was not related to the incident
f	Counter-effect – the SF increased risk in some way
u	Unclear – performance was uncertain

A classification can be made, as shown in Table 13.2. In a simple study, the first three (a–c) could be enough, but the others may be useful. It is possible to include suggested improvements in the list of SFs, but then the classification should show that (Code d).

Some identified SFs might not have been related to the incident at all, and accordingly are not estimated (Code e). It might be that an SF has a negative effect (f), meaning that it increases the probability of an incident or its consequences. That can be due to poor design, or to lulling someone into a sense of false confidence. Finally, if an assessment is uncertain, it can be better to classify the SF as unclear (u) rather than to make a guess.

Another basic evaluation is whether improvements are needed or not, where the principle of *Direct Evaluation* is most practical (Table 5.2 in Section 5.2). In addition, other techniques for evaluation might be applied in more sophisticated applications (Section 11.5).

5) Propose improvements
The advice in Section 11.6 can also be directly applied in event investigations.

Comment
Safety Function Analysis is a generic method that can be used to analyse barriers related to events in various systems. Usually, a great number of safety functions are identified, which are compiled at the organising and assessment stages. This part of the analysis is important, since the data are compressed in a controlled manner.

Data can be collected without any particular hypothesis about what may be the cause to the accident. This procedure also reduces the problem of jumping to conclusions too early before all facts are compiled.

13.11 Tree analysis of events
In an accident investigation, many findings are logically connected with one another. There are several techniques for how the logical connections can be analysed and illustrated. Some examples are discussed below.

Event Tree
Event Trees are presented in Section 12.3 as a tool for system analysis. It is used to study alternative paths after a defined event and the event's various consequences. The method considers barriers and the course of events in a logical framework. In a near-accident study, it can be used to judge the seriousness of the event. In an accident investigation, it can be applied backwards to trace the barriers that might have prevented the accident.

Fault Tree
A *Fault Tree* is a diagram showing logical combinations of causes of an accident or an undesired event – the *top event*. The method is extensively described in Chapter 10. It can be attractive to design a fault tree to show how the accident occurred.

A first consideration is whether the tree is to be strictly concerned only with well-defined events and with clear cause–consequence relations. The alternative is to work with an informal fault tree, as described in Section 10.5. In either case, you should be aware of the differences and the degree

of formality you want to apply. Both types are useful, and the choice depends on the situation. I suggest that you start by trying to be strict, and when needed go informal.

In principle, the analysis is performed in the same way as usual (see Section 10.3). A fault tree describing an accident will usually only contain AND gates. OR gates will only appear when there are alternative ways in which the accident might have occurred.

In an accident investigation, there may be a lot of events and states that need to be put in place. This implies that several simplifications need to be made; otherwise, the tree will be quite complicated.

Arbre des Causes

One variant of fault tree is the French methodology, *Arbre des Causes*, which can be translated as causality-tree analysis. It is described by Leplat (1978), and there are short accounts in Wikipedia, and by Eude and Lesbats (2011). A tree is built of events or situations that are rather freely defined. The logical connections are based on AND gates, but they are only shown as points in the tree.

Safety Barrier Diagrams

There is a group of methods that combine the features of Fault Tree and Event Tree (Section 12.4). One example is the *Cause-Consequence Diagram*, sometimes also called the Bow-Tie diagram. In the analysis of a specific event, one of these techniques can be useful.

MORT

Management Oversight and Risk Tree (MORT) is a method for the analysis of a safety organisation and for the investigation of accidents (Section 12.7). The method is based on a logical tree that is supported by a large number of questions. These questions can help the investigator systematically to go through the circumstances related to the accident.

14 Planning and implementation

14.1 Decisions before the analysis

Over the years, I have seen many safety analysis reports – good as well as bad. Surprisingly often, they have omitted basic information, such as the aim and conclusions of the analysis. Other rather common problems are that it is unclear how the hazards and problems were found, and how the evaluations of risks were performed. Often, the impression is that nobody made clear decisions about how the analysis should have been conducted.

In planning, there are a lot of decisions to make, both before and during the analysis. Most people would agree that it is best to do things right from the beginning; otherwise, you might end up with a useless analysis that nobody needs. The aim of this chapter is to help in planning an analysis in order to get reasonable quality. Note that the chapter treats both analyses of systems and accident investigations in the same framework.

The approach in the book has been to regard safety analysis as a rational procedure. Planning and things to consider in planning have been discussed quite a lot, especially in Chapter 3. The themes have been analytic procedure (Section 3.2), the context of the analysis (Section 3.3), and accident investigation (Section 3.5).

Looking at the analytic procedure, you can easily see that there are a number of choices to be made. Figure 14.1 summarises these in a diagram that shows 12 important decisions during the analysis of a system or accident. The decisions are divided into four major blocks:

1) Main decision on whether an analysis should be performed
2) Specification of the analysis
3) Doing the analysis
4) Using the analysis

The blocks often involve actors and decision-makers with different roles in the company. In Block 3, a consultant or specialist might be the responsible partner. The diagram (Figure 14.1) can be an aid to seeing the general picture before details take over the scene.

The initial decision concerns whether and when an analysis is to be performed. A well-organised company might be prepared for this and have a readiness for analysis (see Section 3.3). Otherwise, the decision will be made more ad-hoc, and might be triggered by a severe accident or a demand from an authority, e.g., the Labour Inspectorate.

Specifying the analysis

In many cases, there is a customer who wants an analysis performed by someone else, here called the consultant. In order to get the job done properly, a specification of the analysis is needed. It defines what is to be analysed, the types of results needed, quality demands, and so on.

Developing a proper specification can be tricky sometimes. The customer might not know much about safety analysis, and therefore only provides an outline. On the other hand, the consultant has lots of ideas about what he wants to do. A dialogue between customer and consultant can lead to the final specification. My view is that the consultant has a clear responsibility to help the customer understand his needs.

Defining the aim of the analysis might at first seem trivial. However, in practice, it is not so easy. I have seen many analysis reports where the aim has been unclear, unsuitable, or not formulated at all. In the worst case, the final result might be something the customer does not need.

A common situation is that the customer only has vague knowledge of safety analysis. A fair and straightforward dialogue with the consultant is then needed. It is helpful to start by answering two important questions. When they are answered, there is a basis for formulation of the analytic aim and specification. The questions are:

1. Why is an analysis required?
2. How shall the results from the analysis be used?

Table 14.1 gives examples of how results can be used. It is important to note that the same analysis can have several different applications, which makes it more useful. The first group represents a formal perspective; quite simply, an analysis is something that must be done. Accident investigations, in particular, is often seen just as a formality.

The rest of the list concerns support in decision-making or in finding possible improvements. The effects of a successful analysis can be immediate if the results are employed directly. Also, there are often indirect effects, such as increased understanding and changed attitudes among participants in the analysis, which can be reinforced by positive interest from top management.

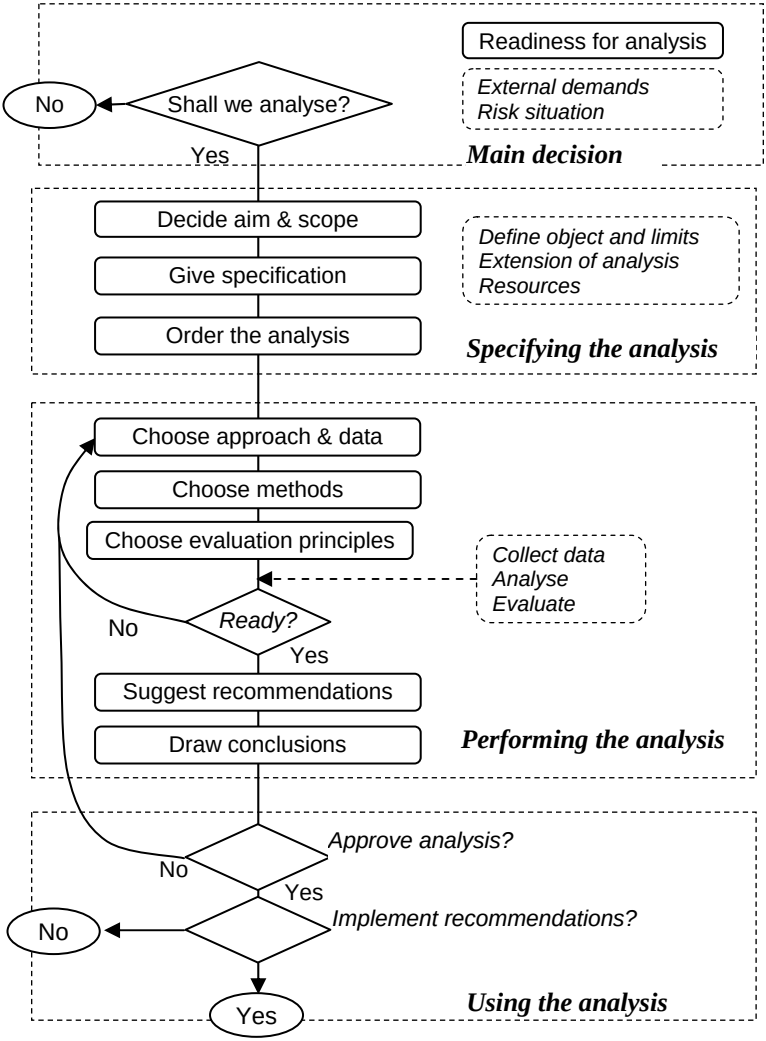


Figure 14.1 Important decisions to be made in the analysis of systems and events

Table 14.1 Examples of how results from a safety analysis can be used

***Control and check** – a formal target*
Send documentation to the authority concerned
Circulate documentation within the company for checking
Support in project management
Choose between different alternative solutions
Approve proposal to accomplish a project
Support project work:
- during design for new equipment
- during development of new management system
Develop suggestions for improvements:
- of existing equipment
- of existing procedures and management
Support in development work
Basis for discussions with partners and clients
Support to improve the company's own safety work

Scope

It is essential also carefully to consider the scope of the analysis. Otherwise, disagreements between customer, consultant and other stakeholders can arise due to misinterpretations of the scope of an analysis.

One aspect is to define how large a part of the system should be considered in the analysis: the whole system, or certain subparts. Relevant boundaries concern interfaces with other parts of the system and with the surrounding world.

Another aspect is to decide which elements the analysis should consider, such as:

- Technical equipment, hardware and/or software
- The humans in the system, including man-machine interfaces and other ergonomic aspects
- Organisation, local (in the workplace) or also general management
- Interactions between different elements, seen from a systems perspective

Aim and specification

Examples of basic aims are given in Table 14.2, which can be used as a first approximation. The further development of aims and specifications can be based on the aspects: *Why*, *How to use*, and *Scope*. It is important to formulate these clearly, since there will be a number of actors involved.

The analysis has to be performed by someone, and the tasks, the responsibilities and the roles need to be clarified. The analyst can be someone in the company, or an external consultant. In both cases, it is good for the commissioner of the analysis (the customer) to have a good basis for ordering the analysis.

There are difficulties involved, and it can be hard to know how extensive and complex the results will be. This also means that there are uncertainties to estimates of the time required.

Table 14.2 Examples of the basic aims of safety analysis

System analysis	**Event analysis**
Identify hazards	Find out what happened
Estimate the risk level	Investigate the sequence
Evaluate the risk level	Identify influencing factors

Safety analysis in general
Meet the requirements of the authorities
Evaluate needs for improvement
Suggest improvements
Identify barriers and safety features
Evaluate their efficiency
Learn how to utilise safety analysis at company level

14.2 Performing the analysis

After the initial decisions and planning, the analysis can start. Performing the analysis is the third block in the decision flow (Figure 14.1). In this block, new actors may take over the process, and we can assume that an analyst is in charge. Some of the elements might already have been decided upon earlier in the planning, or in the actual specification. However, when the real analysis starts, it is wise, as a second thought, to check on the earlier choices that have been made.

Choose approach

At the beginning of an analysis, there are a number of alternatives to consider. One concerns the analysis itself:

- Start with a coarse analysis of the whole system (or accident), and decide later about how to expand and look into details.
- Start directly at a detailed level, based on aim and scope.

Sometimes, the choice can be between an analysis of an accident, and an analysis of the system. It might look self-evident, but giving a second thought to the matter might be worthwhile.

Data collection

A general data collection is performed early in the analysis, followed by more specific information that is related to the methods that have been chosen. Information to consider is:

- Written documentation, such as on routines, descriptions of procedures, etc.
- Electronic information from computers, logs from control systems.
- Accident and incident reports.
- Drawings.
- Photos.
- Interviews with individuals; different actors might have various impressions of the system and its risks.
- Group discussions, especially in a working group. When there is limited time for the analysis, and/or a coarse analysis is performed, group discussions might be the most efficient way of collecting data.

Working group

Especially when an external consultant is in charge of the analysis, a working group should be compulsory. An alternative term is reference group, and the expression might indicate how active the group should be. The group should represent different roles and categories in the company, organisation or project in order to get differing perspectives on the issues involved. Such a group could be used to:

- Support data collection
- Check and verify data
- Take part in the evaluation stage
- Help in developing improvements
- Contribute to distribution and acceptance of the results, since a written report cannot be too long, and will not present all findings

Choose method

Choosing a method should not be the first thing. It is quite common to suggest a method too early, before needs have been established. For a good result, it is essential carefully to consider the methods that should be employed.

The aim and scope in the analysis specifications can guide the selection of method. One or more suitable methods for the analysis should be selected. An overview of methods and their characteristics is given in Chapter 15, which can be of assistance in making the choice.

In an ideal situation, there might be a clear rational choice, but it is seldom the case. Different methods give different perspectives; one approach is to apply two methods separately to the case and combine the results.

In most analyses, there is a stage for evaluation of the identified hazards. A routine solution is to adopt the Risk Matrix approach, but this has some difficulties and drawbacks. There are other ways of doing the evaluations, which are sometimes more favourable. Chapters 5 and 15 expand further on this issue.

Stop the analysis

One issue is how thorough the analysis should be. Sometimes, the analysis specification provides some kind of stop rule. In practice, there is often a time or cost limit. The decision on when to stop has to be made at some point during the performance stage.

In many situations, it is fine to complete an analysis quickly, instead of performing a lengthy analysis that aims to be perfect. This could be achieved by omitting complicated issues, while clearly stating what was missing and the problems that were not solved. The report could then give recommendations for complementary analyses. Problems might concern:

- Uncertainties in the data
- Some parts or aspects of the system that could not be analysed
- Difficulties in evaluating the hazards
- Complex functions or relations, which were hard to analyse within the time limits

14.3 Improvements and conclusions

Suggestions for improvements and conclusions are important elements in safety analysis. Both should be handled as systematically as the other parts of the analysis. In my experience, there are too many analyses with inadequate conclusions and unsatisfactory suggestions.

However, how this should be done is not treated much in the literature, and it is not always self-evident how you should proceed.

Develop improvements

We assume that the purpose is to develop a set of reasonable suggestions, and that the company management will make the final decisions. In developing improvements, a working group is highly valuable, both for creating ideas and for judging the final suggestions. This can be done in a few consecutive stages.

1) Preliminary suggestions

At first, you can search rather freely for ideas. This can be done in the form of a brain-storming session in the workgroup, in order to let different aspects encounter one another. This can be combined with a systematic approach. Some analytic methods provide support for finding suggestions for improvements (see tables 15.3 and 15.6).

The best way to proceed is to start with the largest and most important hazards, which are distinguished by the values obtained at the evaluation stage. In cases where the information is uncertain, or where the working group disagrees, a good solution is to suggest a further investigation before any final decision is taken.

2) Organise and refine

The suggestions might come in a rather arbitrary order, especially in event investigations. They can be arranged in themes or *packages* in a suitable way. Similar suggestions can be combined, such as routines, competence issues, communication, and need for further investigations. A structure can be based on different principles. One way is to combine:

- Technical changes
- Management actions, such as new routines, agreements between partners, and the training of staff
- Further studies and investigation, due to lack of information or time
- Responsible actors, such as companies or other organisational entities

3) Assess and refine

An evaluation of the suggestions is essential before they are presented as a complete proposal. This means that the suggestions are refined, or sometimes even removed. Issues in assessment can be:

- Usefulness, and whether the original problem will be solved
- Efficiency of the suggestions, both as a whole and in their more detailed parts
- Local or general effects

- Time perspective, i.e., how quickly things can be done, and how long the effects will last
- Practicality and the balance between benefit and cost

Efficiency of the solutions can involve:

A) How large a part of the problem (the hazard) is addressed. For example, what proportion of all machines with a certain defect could be identified and corrected.
B) The probability of wanted effects (success rate).
C) Sustainability over time. A technical change will usually last for a long time, while information usually has short-term effects.

Conclusions

A complete analysis should include conclusions and summarising remarks. Parts of this can be done in a fairly straight-forward and simple manner. Below are a number of aspects to consider:

- *The object of the analysis.* Simple or complex; stable over time; importance of interfaces with other systems.
- *Identification*. The number of hazards and problems; types of hazards; the completeness of the identification.
- *Evaluation of risks.* The number of serious risks; difficulties in the evaluation; agreement or disagreement in the working group that made the evaluation.
- *Proposed improvements.* The number of suggestions and the most essential ones; potential for progress; estimated usefulness and effects.
- *The analysis as a whole.* Whether or not the aim was reached (and if it was suitable); how complete the analysis has been; possible issues for further analysis.

If the aim encompassed specific issues to examine, related questions should be answered in the report. Examples of concluding phrases are given below; they can be stated negatively, or they can be reformulated if the problems are minor.

a) The suggested design of the system does not meet the requirements of safe operations.
b) There are several hazards and problems that should be taken care of before operations can start.
c) A large number of needed safety improvements have been identified and should be included in the company's action plan.

14.4 Reporting and decisions

The safety analysis is completed with a report, which is sometimes accompanied by a discussion with the decision-makers. Depending on planned usage, the report can be either brief or extensive. When a report is short, understanding within the working group supplements the written report. This is essential to later decision-making and implementation.

Topics in the report

The contents of a report will vary quite a lot, depending on its aim. In writing the report there are a number of topics that should be considered:

- *Basic information*, such as aim, scope, who did the analysis, and when.
- *Methodology*, concerning data collection, analytic methods, and how the evaluation was performed. Justifying the choices made adds value.
- *Results*, such as tables, diagrams, logic trees, and suggested improvements. If they are lengthy, they could be inserted as appendices, with just an overview being provided in the main report.
- *Discussion* of the results, which might concern uncertainties and confidence in the results, and also notable observations.
- *Conclusions* of the analysis.

Check and approval

In the decision chain (Figure 14.1) we have assumed two role-players – the customer and the consultant. When the results are handed over, a check on and approval of the analysis by the customer are essential. My experience is that this step is often omitted, and perhaps seen as unnecessary. A careful check is needed for quality reasons, and it is advisable for the consultant to provide a preliminary report asking for comments. Such a check could be based on the list of issues presented above. See also Section 14.5, which deals with quality aspects.

Final decisions

After an approval, the main decision to be made by the customer is whether or not the suggestions in the report should be implemented. If people have been engaged in a working group for the analysis, their experience is useful, both for decision-making and for planning implementation.

Update the analysis

After the implementation phase, the whole analysis can be seen as having been concluded, and is put in an archive somewhere. An alternative is to update it, and use the results in different ways. It might be employed for checking the effects of implementation, and for training purposes. It might also be useful when the system is changed next time, and some checks need to be made.

In the nuclear industry, *Living PSA* is a common concept, where PSA stands for *Probabilistic Safety Analysis*. There is a "PSA of the plant, which is updated as necessary to reflect the current design and operational features" (IAEA, 2001). The Living PSA can be used by designers and others for a variety of purposes, such as design verification, assessment of potential changes to plant design or operation, and design of training programmes. Also, in other industries, updated versions of a safety analysis can be valuable.

14.5 Quality aspects

The quality of safety analysis is an interesting subject, but one that is hard to tackle. In the literature, most attention has been devoted to analysis of chemical major hazard installations and the nuclear power industry. Here, criticism has concerned uncertainties in probabilistic estimates, or lack of completeness in hazard identification.

In other areas, quality aspects have been far less considered. They are discussed a bit further here, but much more needs to be done. This section can be used as a basis for examining a completed safety analysis. It may also provide a basis for anticipating and preventing problems when such analyses are planned.

The concept of quality

The meaning of *quality* in a safety analysis is not self-evident. In general, it can be described as its *fitness for purpose*. This represents the degree to which the safety analysis is appropriate for its specified aim. Quality is an abstract and fairly subjective attribute of the analysis. Different actors, such as company management, employees at risk, or authorities, may see the results differently.

Related terms are *reliability* and *validity*. Here, reliability refers to how well different analysts will get the same or equivalent results for the same object. Validity refers to how well the results are related to reality. In a safety analysis, it can concern how accurately hazards are identified and evaluated.

The concepts of reliability and validity can be hard to apply in some situations. This is especially so if:

- The system is complex, which results in a high number of failure combinations
- The system is dynamic and its characteristics change over time.
- The aim is to identify possibilities for improvements.

Rouhiainen (1992) has suggested four major questions to address in any discussion of quality:

- How well have the hazards been identified by the analysis?
- How accurately are the risks of an activity estimated?
- How effectively has the analysis introduced remedial measures?
- How effectively are resources used in comparison with the results achieved?

The questions are essential, but hard to answer with any high degree of precision. Since there are a large number of different applications, it is not possible to find any universal measures of quality.

Benchmark studies

Problems of uncertainty in the risk assessment of chemical process plants have been recognised for a long time. In the late 1980s, a benchmark study was organised in Europe (Contini et al., 1991; Amendola et al., 1992). Eleven different teams analysed the same ammonia plant, and the aims were to identify sources of risk and estimate the probabilities of injury. The largest difference in the results was of a factor of around 10 000 for a certain estimated value. A follow-up showed many contributory explanations for the extreme discrepancy in results. Important differences were in:

- Approaches to the accomplishment of the analysis
- Data on component failures
- Estimates of success in the actions of operators
- Assumptions about how ammonia release happens

A follow-up study was conducted ten years later, which showed reduced variation in results. But it still showed variation in a factor of about 100 between the teams (Lauridsen et al., 2002). Although the teams were aware of the problem, the uncertainties were considerable.

Problems

The quality of safety analysis is a key field, but also a problematic one. It is worthy of greater attention than it is given today in most application areas. These two benchmark studies were interesting and important, but the results were depressing in terms of low reliability and validity.

My own experiences of quality issues are based on examination of a number of analysis reports, and on my work as a teacher of safety analysis. Some examples of problems are:

- Complacency. The analyst is usually satisfied both with the result and choice of method. That he or she has difficulties in checking their own results is quite natural, and the examination of an independent person would be helpful.
- Competence. The skill of the analyst is essential, but sometimes difficult for the customer to judge.
- It is common to deviate from the prescribed analytic procedure.
- Assumptions and delimitations are often implicit rather than explicit, and not clearly stated.

On the other hand, my impression is that customers are usually satisfied with the results. They have received an analysis that looks nice, and they cannot judge its quality. In general, there appears to be a need for greater awareness of quality issues, especially among buyers of analyses and examiners of results.

Quality assurance

One basis for obtaining a favourable result consists in adopting a good safety analysis procedure, one that it is well-planned and implemented. This is in line with the general standards for quality assurance (ISO 9000), which are based on the idea that a suitable procedure is followed and documented. There are also Norwegian and Danish standards for risk analyses (Norsk standard, 1991; Dansk standard, 1993), both of which support quality aspects. They are primarily based on a procedural approach.

As the readers have seen, one of the major themes of this book is to highlight the importance of a well defined analytic procedure.

15 Choice and summary of methods

15.1 Basic considerations

In Chapter 14, we discussed the planning and accomplishment of a safety analysis. However, the important issue of choice of methods has not yet been addressed.

The aim of this chapter is to sum up and compare methods from earlier parts of the book. It concludes with a general discussion of choice of methods, and also discusses the aspects that should be considered in the choice of methods. Choices have been placed in three major groups:

A) Methods for the analysis of systems (Section 15.2)
B) Methods for the analysis of events and accidents (Section 15.3)
C) Evaluation of risks (Section 15.4)

A number of tables of methods have been presented above. The point here is to focus on characteristics that can be of help in choosing one or more methods suited to the needs of the analyst. All methods cannot be included, and three criteria have been applied for the selection. They are not very precise, but they have acted as a guide:

1. A systematic analytic procedure, which guides the user through the method and supports reliable results
2. A publicly available method description (which excludes proprietary methods)
3. A method that is fairly easy to apply

Table 15.1 Numbers of the methods presented in this book

Type of method	In table	Number
Selected for system analysis	15.2	10
Other for system analysis*	12.1	12
For event investigation	13.1	16
For evaluation	15.7	5
Total		43

* The number is reduced for methods already referred to in Table 15.2

Table 15.1 sums up the numbers in the other tables, and 43 methods for the analysis of systems and events have been referred to. There are key differences between the methods, and choice of method affects what type of results you will obtain. Methods of evaluation have been presented

separately, since they can often be chosen to match the needs of both system analyses and event investigations.

One method may be good for technical issues, and another more suited to organisational factors. This applies to the analysis of both systems and events. How the separate methods cover different areas is illustrated as a Venn diagram in Figure 4.2 in Section 4.4.

In the literature, choice of methods has not been paid much attention. In any case, I have had difficulties in finding such studies. For the analysis of systems (Group A above), the benchmark studies mentioned in Section 14.5 are interesting, but they do not address the properties of the methods used. Methods for investigation of accidents have been more thoroughly investigated, as is discussed in Section 15.3.

15.2 Methods of system analysis

One group of methods is used to examine a system and anticipate which accidents and problems might occur in the future. Here, this application is called *system analysis*. In this book, 22 such methods are more or less thouroughly presented (see the two first rows in Table 15.1). The methods have different features, and all have supporters with confidence in them.

Ten methods have been selected to be compared in a detailed manner (Table 15.2). They meet the criteria above (in Section 15.1), and they also represent different approaches. This does not mean that other methods are unsuitable. If the method you look for is not on the list, the comparison scheme in this chapter can in principle be applied to any method.

Comparing characteristics

Five characteristics have been used to compare the methods shown in Table 15.3. Similar grounds for comparing methods are used for both system analysis and event analysis (in Section 15.3).

Application area

Originally, all ten methods were developed for technical industrial installations. However, many can be useful in a wider set of applications. The second column (Table 15.3) summarises this, and shows that six of the methods can be used for all types of systems. *Job Safety Analysis* is supposed to be applied in workplaces, but it could embrace all the types of systems in the generalised method *Direct Hazard Analysis* (see Chapter 7).

Table 15.2 Ten methods of system analysis

Method	Characteristics	Ref.
Deviation Analysis	Identifies hazardous deviations in equipment and activities. Structures the system in functional blocks.	8
Energy Analysis	Identifies hazardous forms of energy. Structures the system into physical volumes.	6
Event Tree Analysis	Logical tree of alternative consequences of an initiating event. Binary – a barrier works or fails.	12.3
FMEA – Failure Mode and Effects Analysis	Identifies failures in component or subsystems. Structures a technical system into functional blocks.	12.2
Fault Tree Analysis	Logical tree of the causes of an accident (top event). Binary - a failure exists or does not.	10
Hazop – Hazard and Operability Studies.	Identifies hazardous deviations in chemical process installations. Structures a chemical system into units.	9
Human Error Identification	Identification of operator's errors in a well-defined procedure in, e.g., process industry (the Action Error Method).	12.5
Job Safety Analysis	Identifies hazards in work tasks. Structures the work procedure of a worker or a team into different tasks.	7.2
Preliminary Hazard Analysis	Free search for hazards, often brainstorming (example of a coarse analysis method).	12.8
Safety Function Analysis	Analysis of the safety characteristics of a system. Safety functions and barriers are identified, structured and evaluated.	11

Ref. = Refers to a chapter or section where the method is thoroughly described.

Manuals

The description of how an analysis shall be performed is an important feature, since it guides how the method will be applied. Instruction manuals for the methods can be more or less detailed, and they are divided here into three major groups:

A. Step-by-step description with clear advice how to perform an analysis.
B. The manual gives some advice, but the method contains creative and iterative parts that are not fully rule-based.
C. The manual gives little or no advice on practical application.

Difficulty

Some methods are simple to use, but others are quite difficult. The degree of difficulty has been categorised according to needs for training. The scale is:

1. No training needed, only a short introduction and a simple instruction
2. Practical training for a few hours
3. Education and training for one or two days
4. Comprehension and skills corresponding to some weeks of training and practice
5. Expert knowledge, prolonged experience

The scores should only be seen as relative. The estimates are quite uncertain, and are based on my experience as a teacher. They depend on students' background knowledge, and what skill is required. *Preliminary Hazard Analysis* and *Job Safety Analysis* are considered to be easiest.

Table 15.3 Characteristics of ten selected methods for system analysis

Method	Application area	Manual	Difficulty	Improvement	Perspective
Deviation Analysis	All types of systems	A	2	3	T H O
Energy Analysis	All types of systems	A	2	3	T
Event Tree Analysis	All types of (technical) systems	B	3	0	T (H)
FMEA	Mechanical and electrotechnical systems	A	3	2	T
Fault Tree Analysis	All types of (technical) systems	B	4 (5)	1	T
Hazop	Chemical installations	A	3	1	T
Human Error Identification	Well-defined procedure in, e.g., process industry	A	3	2	H
Job Safety Analysis	Workplaces	A	1 (2)	2	T H
Preliminary Hazard Analysis	All types of systems	C	1	1	T
Safety Function Analysis	All types of systems	A	3	3	T H O

Improvements to safety
The development of safety improvements is supported in some methods. The scale is:

0. Not mentioned or regarded
1. Mentioned and generally discussed
2. Described and contains instructions and/or categorisations
3. A distinct activity in the method that is clearly described

Perspectives
The methods have different perspectives on the system under study, and how accidents occur. In a rather simplified manner, we can consider three categories:

T Technical
H Human action
O Organisation

Five methods have an apparently technical perspective, at least in their initial versions, but sometimes they are used from a wider perspective. *Deviation Analysis* and *Safety Function Analysis* have explicit integrated organisational features even in their original versions.

Model of the system

How the object of analysis is treated in the different methods is another key characteristic. Six of the methods have a specific stage where the system is divided into parts, and each of these is studied. The principles for modelling are closely related to the THO perspective (see above), and differ between the methods:

- *Deviation Analysis* – activities, e.g., the production flow or job procedure
- *Energy Analysis* – volumes, which jointly cover the entire object
- *FMEA* – technical components or modules, sometimes also procedures
- *Hazop* – physical components, e.g., pipes or tanks
- *Human Error Identification* – detailed description of the operator's phases of work
- *Job Safety Analysis* – elements in an individual's job task

Advantages and disadvantages

Table 15.4 gives a summary of the advantages and disadvantages of these methods. It is a simplification of a rather complicated situation, and should therefore be treated with caution. It does not contain definitive judgements. For practical reasons, the summary is short, and may be somewhat cryptic.

Table 15.4 Ten system analysis methods – positive and negative arguments

Method	Positive arguments	Negative arguments
Deviation Analysis	Structuring of the system gives overview. General method – can be applied on any system. Checklist of deviations. Support for improvements.	Sensitive to structuring, requires attention. Deviations at different system levels can sometimes be difficult to handle.
Energy Analysis	Simple principle, quick, gives an overview of potential hazards. Checklists of energies and for finding improvements.	Only technical perspective, with limited analysis of causes.
Event Tree Analysis	Lucid diagram shows barriers and different outcomes. Can be used for probabilistic calculations.	Limited application; not for identifying hazards and problems. Binary approach is a simplification.
FMEA	Supports detailed analysis of technical system and can be very thorough. Application area can be extended.	Time-consuming since many possible failures can occur. This might weaken a comprehensive view.
Fault Tree Analysis	Lucid diagram shows causes, and their relations. Can be used for probabilistic calculations. Application area can be extended in soft trees.	Difficult to design and check; can easily go wrong. The impressive diagram can be seductive and misleading. Binary approach is a simplification.
Hazop	Supports detailed analysis of a chemical system. Guide words make for efficient identification of deviations.	Time-consuming since many possible deviations can occur.
Human Error Identification	Straightforward to use, rather simple.	Focuses on normal processes. Might overlook failures in instructions. Many possible failures take time.
Job Safety Analysis	Simple to learn and apply, similar to traditional safety thinking. Applications can be extended in Direct Hazard Analysis	Not suitable for automatic systems. Too traditional, latent hazards easily overlooked.
Preliminary Hazard Analysis	Quick and can give an overview. With an expert team leader, results can be good.	Uncertain results. Large variation in how methods are applied.
Safety Function Analysis	Gives an overview of safety features in a system, including technical and organisational aspects. Support for improvements, especially related to management.	A safety system is often extensive, and can be difficult to present and analyse.

15.3 Methods of event analysis

In order to make an accident investigation credible, it is essential to describe how it has been conducted. An important stage in an event analysis is consciously to select a methodology. The aim of this section is to summarise and compare methods to help the reader to make wise choices.

A large number of methods for accident investigations have been published. A few comparative studies have been performed, most of which are based on studies of the literature and theoretical aspects. Examples of comparisons come from the Energy Institute (2008), which has chosen methods for analysing human and organisational factors. Sklet (2004) focuses on methods considered suitable for the analysis of major accidents. A benchmark study (Salmon et al., 2012) has compared three methods (AcciMap, HFACS, STAMP) applied to the same outdoor accident. The studies are interesting, and are based on different approaches. However, it is hard to draw general conclusions from them with regard to *common* accidents.

One study (Strömgren et al., 2013) reports on an evaluation of nine accident investigation methods, which is based on general use of the methods. The evaluation in this chapter has many similarities to the evaluation this study, and some of the parameters and evaluations have been used directly.

Chapter 13 has presented a set of methods for event investigation. Eleven of these are summarised in Table 15.5. They meet the criteria listed above in Section 15.1, and they also represent different approaches. Four of the methods can also be used in a system analysis, but the uses differ, and the characteristics and arguments have therefore been reconsidered for this application.

If you should miss a method in the list, remember that the comparison scheme in this section can, in principle, be applied to any method.

Table 15.5 Eleven selected methods of event analysis

Method	Characteristics	Ref.
AcciMap	Sequence of events at different organisational levels, and the flow of decision and information between actors.	13.7
AEB – Accident Evolution and Barrier Function	Sequence of events with technical and human errors, including barriers that might stop the sequence.	13.4
Change Analysis	Analysis of differences between the accident and a normal situation.	13.8
Deviation Analysis*	Identifies and evaluates deviations related to the event.	13.9
ECFA – Events and Causal Factors Analysis	Sequence of events with affecting conditions. Identifies root causes and contributing causes.	13.5
Event Tree Analysis*	Logical tree gives alternative consequences of the investigated event. Binary – a barrier works or fails.	13.11
Fault Tree Analysis*	Logical tree shows how failures have combined to produce an accident. Binary – a failure exists or does not.	13.11
MTO Analysis (Man–Technology–Organisation)	Sequence of events, with direct and underlying causes and safety barriers.	13.6
Safety Function Analysis*	Safety functions and barriers related to the event are identified, structured and evaluated.	13.10
STEP – Sequentially Timed Events Plotting	Event and actors are plotted in a time diagram following strict rules.	13.2
Simple Event Mapping	Event and actors are plotted in a time diagram in a rather free manner.	13.3

Ref. = Refers to chapter or section where the method is thoroughly described.

* = The method is also included in the tables for system analysis

Comparing characteristics

Seven characteristics have been used to compare the methods, and the results are summarised in Table 15.6. Most of the parameters are the same as for the comparison of methods for system analysis (Table 15.3). They are also in line with another study of accident investigation methods (Strömgren et al., 2013). To make the account easier to read, the parameters are repeated in a condensed version here.

Application area
All these methods can, in principle, be applied to any type of system. Even, if they from the beginning were intended for industrial installations. For example, there are organisational factors involved in even the simplest accident, if you consider design of equipment, information of hazards, and so on.

Manuals (Instruction manuals)
A. Step-by-step description
B. Some advice
C. Little or no advice

Difficulty
1. No training needs, only a short introduction and simple instruction
2. Practical training for a few hours
3. Education and training for one or two days
4. Some weeks of training and practice
5. Expert knowledge, prolonged experience

Improvements to safety
0. Not mentioned or regarded
1. Mentioned and generally discussed
2. Described and contains instructions and/or categorisations
3. A distinct activity in the method that is clearly described

Perspective
T Technical, H Human action, O Organisation

Evaluation
Most methods for system analysis include evaluation in one form or another. This is not self-evident in accident investigation, where lots of information is gathered. Some methods include an evaluation of what is important, and/or a verification of the consistency of the material. A scale for classification is:
1. Evaluation and/or verification not mentioned or regarded
2. Mentioned and generally discussed
3. Described and contains instructions and/or categorisations
4. A distinct activity in the method that is clearly described

Two of the methods have scored 3 on evaluation. Fault Tree Analysis has a score of 1, under the assumption that the rules of thumb are applied, especially the last three.

Table 15.6 Parameters characterising methods for event analysis

Method	Manual	Difficulty	Improve-ment	Perspec-tive	Evalu-ation¤	*Seq/ Bar
AcciMap	C	4	0	O	0	1 / 0
AEB – Accident Evolution and Barrier Function	A	2	2 (3)	T H	1	2 / 2
Change Analysis	A	3	0	T H O	0	0 / 0
Deviation Analysis	A	2	3	T H O	3	0 / 1
ECFA – Events and Causal Factors Analysis	A	3	0	T H O	1	2 / 1
Event Tree Analysis	B	2	0	T	0	1 / 2
Fault Tree Analysis	B	4	0	T	1	0 / 2
MTO Analysis (Man–Technology–Organisation)	B	3 (2)	1	T H O	0 (1)	2 / 2
Safety Function Analysis	A	2	3	T H O	3	0 / 2
STEP – Sequentially Timed Events Plotting	A	2	2	T H	1	2 / 0
Simple Event Mapping	A	2	0	T H	1	2 / 0

* Seq/Bar stands for Sequence and Barrier (see below)

Sequence and Barrier
The results of an investigation can describe how an accident chain advances, and which barriers might stop it. Two parameters are used – Sequence and Barrier – which are measured on the same scale:

0. Not essential or not shown
1. Somewhat
2. Important

The estimates for the methods are summarised in Table 15.6. It can be noted that six methods include an organisational perspective. This can be compared with the set of methods for system analysis, which only have two (Table 15.3).

Advantages and disadvantages

Table 15.7 gives a summary of the advantages and disadvantages of the methods. It is a simplification, and different people might arrive at different judgments depending on their preferences. For practical reasons, the summary is short, and may be somewhat cryptic.

Table 15.7 Event analysis methods – positive and negative arguments

Method	Positive arguments	Negative arguments
AcciMap	The map supports an overview of the general situation, showing actors and their relations.	Rather difficult method. The result will vary much between different analysts.
AEB – Accident Evolution and Barrier Function	Lucid diagram gives a visual presentation of results. Support for finding and proposing barriers.	Based on a single sequence, difficulties in handling parallel chains. Only events with errors are shown.
Change Analysis	Simple principle, based on questions. Support for collection of data.	Assumes that the *normal* system is safe enough – this might be wrong
Deviation Analysis*	Simple principle, easy to collect data. Support for evaluation and improvements.	Deviations at different system levels can be difficult sometimes.
ECFA – Events and Causal Factors Analysis	Lucid diagram gives a visual presentation of results. Handles multiple causes	The *root cause* concept can be misleading. Stereotyped at high levels.
Event Tree Analysis*	Lucid diagram shows barriers and different outcomes.	Limited application; not for identifying hazards and problems. Binary approach is a simplification.
Fault Tree Analysis*	Lucid diagram shows causes, and their relations. Application area can be extended in soft trees.	Difficult to design and check. The impressing diagram can be seductive and misleading. Binary approach is a simplification.
MTO Analysis (Man–Technology–Organisation)	Lucid diagram shows causes and barriers at different levels.	The *root cause* concept can be misleading. Stereotyped at high levels. Difficulties in handling parallel events.
Safety Function Analysis*	Gives an overview of safety features in a system, both technical and organisational. Support for improvements.	A safety system is often extensive, and can be difficult to present and analyse.
STEP – Sequentially Timed Events Plotting	Lucid diagram. Handles parallel sequences. Support for collection of data, for improvements, and for tests of results.	Limited to strict causal relations, and excludes influencing conditions and organisation. Can be over-ambitious for simple accidents. Only short time range.
Simple Event Mapping	Lucid diagram. Handles parallel sequences with varying time perspectives. Support for collection and checks of data.	Only relates events to each other. Not suitable for a complete investigation; a supplementary method is needed.

* The method is also included in the tables for system analysis.

Two of the methods (ECFA and MTO) are based on the concept of a *root cause* – which can sometimes be misleading. This can sometimes lead to the presentation of stereotyped causes at high levels, such as referring to *inadequate safety work* rather than drawing any more precise conclusions.

15.4 Methods of evaluation

Chapter 5 presented five different approaches to the evaluation of risks. They are primarily designed to be used in system analysis, but can sometimes also be used in event analysis. A summary of their general characteristics is given in Table 15.8.

Table 15.8 Five approaches to the evaluation of risks

Method	**Characteristics**	Ref.
Probabilistic	Values of C&p and of expected loss are calculated and compared with predefined limits.	5.3
Risk Matrix	Classification of C&p based on estimates. Acceptability based on predefined combinations of C&p.	5.4
Direct Evaluation	Judges directly whether safety measures are needed. Several factors, including regulation, are considered.	5.2
Relevance Judgement	Applied in planning situations. The evaluation concerns whether the risk shall be considered in future development.	5.5
Comparison of systems	Compares the level of risk in a planned system with that in a reference system.	5.5

Ref. = Refers to section where the method is described

C&p = Consequence and probability (or frequency)

The general aim of a risk evaluation is to support decisions on whether the analysed system is acceptable, or whether changes are needed. The *object* to be evaluated varies between situations; it might be a specific energy or the risk of a potential accident. In many cases, it can be a set of deviations or failures, which can emanate from Deviation Analysis, FMEA or Hazop. At the evaluation stage, the deviations are judged one by one.

Handling of scenarios

In a system analysis, there are often a number of different accident scenarios to consider in evaluation. For example, a deviation can have several different effects, leading to different scenarios. In such cases, it is necessary to take a number of decisions and make assumptions. The assumptions have a considerable impact on the probabilities. If the ambition is to have high quality, the decision rules and assumptions need to be well-documented. These might concern:

- Whether one single scenario should be considered, or several scenarios.
- Existing barriers and safety functions. One scenario is that all of them work, and another that one or more fail.
- Latent failures – how they are considered and combined with other failures.
- Whether failures are correctly detected and handled

The five methods handle the scenarios differently:

- *The probabilistic approach:* Several sequences can be modelled in detail and used in calculations, e.g., by applying *Safety Barrier Diagrams* (Section 12.4).
- *The Risk Matrix:* The common practice is to choose one consequence, and then estimate its frequency. As far as I know, there are no general rules for making this choice, which means that the result may well vary between users.
- *Direct Evaluation:* The deviation is at first judged as a phenomenon in itself, and whether its occurrence is okay. Secondly, the consequences of the failure need to be considered. Usually, this means that fewer general assumptions have to be made.
- *Relevance Judgement:* Evaluations are only made of general types of failures. The assessment is aimed to judge whether they can cause damage, and accordingly need to be kept under control in the planning process. Only cursory assumptions need to be made.
- *Comparison between systems*: Similar scenarios are compared, which means that this type of evaluation is less sensitive to choices of scenarios.

When the handling of different scenarios is important, supplementary methods can be employed. *Event Tree Analysis* (Section 12.3) is suitable for the analysis of the effects of a triggering event. In addition, *Safety Barrier Diagrams* (Section 12.4), sometimes also called *Bow Tie Models*, have a similar application.

Advantages and disadvantages

In Section 5.6, we discussed a number of critical issues in the evaluation of risks, which must also be considered when comparing the methods. The Risk Matrix has received particular attention, since it is the most common method. Table 15.9 provides a brief summary of the advantages and disadvantages of the methods.

Table 15.9 Evaluation methods – positive and negative arguments

Method	Positive arguments	Negative arguments
Probabilistic	Advanced Scientific basis and technique Several scenarios can be added	Scope limited to severity Difficult and resource-demanding Data are often uncertain
Risk Matrix	Popular Recommended by authorities Numerical output gives quick overview Looks scientific	Scope limited to severity Over-confidence in numbers Poor transparency, comments necessary Depends a lot on the assumptions Sensitive to choice of scenarios
Direct Evaluation	Simple and with guidelines Handles uncertainty Handles disagreement Considers regulations and standards Functions in accident investigations	Poor transparency, comments necessary Can be regarded as subjective
Relevance Judgement	Easy format Supports risk management Designed to handle uncertainty in future conditions	Does not fit common thinking in risk analysis Deals only with general types of hazards and problems
Comparison between systems	Easy format Supports risk management of changes Focuses on changes	No clear guidelines for application Assumes that the reference system is safe enough

15.5 Choosing method

A rational decision?

Section 14.1 has presented an overview of the decisions that need to be taken before a safety analysis is launched. Choice of method is an important decision that will strongly influence the results. Any specific method will highlight certain aspects, and others might be neglected.

The earlier sections in this chapter have summarised the characteristics of a number of methods, with their advantages and disadvantages. In combination with demands in the actual situation, it should be easy in principle to make a rational decision.

One complication is that what is rational for one person might be alien to another. One person thinks it is excellent always to use the same method for accident investigation. He or she knows the type of results that will be obtained, and he can compare accidents over the years. On the other hand, a colleague observes that similar accidents tend to reoccur, and that the company does not seem to learn. Then, the conclusion to be drawn is that the company should try another way of doing investigations.

There are difficulties in principle in objectively comparing and judging different methods on a general basis. One reason is the large variation in applications, which also includes different analysts with their own preferences and work styles.

Common choices

Risk analysis was originally an industrial concern, and its methods have been technically founded. If you look at the academic and practically oriented literature, there are five predominant methods:

1) Fault Tree Analysis
2) FMEA – Failure Mode and Effects Analysis
3) Event Tree Analysis
4) Hazop
5) Job Safety Analysis

To the big five, we can add methods for coarse analysis. In the chemical industry *What-If* is preferred, and in other areas *Preliminary Hazard Analysis* (PHA) is common. Moreover, when it comes to evaluation, the *Risk Matrix* predominates, albeit in a number of variants.

In the safety analysis of systems, it is self-evident that one or more methods should be employed. However in accident investigations, the methods do not have their same natural roles. There are indications (e.g., Roed-Larsen et al., 2004) that authorities and companies seldom make use

of established accident-investigation methods. And, if they are used, the choice is made rather ad-hoc.

A goal-oriented choice

Making a goal-oriented choice means starting with the aim and scope of the safety analysis (or accident investigation), as shown in Figure 14.1. In combination with the actual situation and other facts, this leads to a choice of approach and methods. The aim of chapters 14 and 15 is to support you in that choice.

The most common methods have shortcomings in their analysis of organisational aspects and human behaviours (see Table 15.3). This means that other methods should also be considered, which might give better results.

Sometimes, a single method can be enough, but it may be beneficial to use two or more methods that give complementary perspectives. This does not need to take much more effort, since, in combination, each method can be applied more quickly.

Situations

We can assume some examples of situations and scenarios (cf. Section 2.4), which call for suitable methods. When an analysis is planned, the situation for the company (organisation) can be characterised by a number of parameters, such as:

1. The *size of the accident consequences*, which can range from small to very large.
2. *Level of organisational control*, which can vary between a well-organised company with a clearly defined formal and hierarchical organisation and a situation in which there are free and unorganised activities.
3. The *time parameter* can concern the life cycle and state of the system. This can be at the general planning stage, during detailed design, in normal operation, or one in which changes to technique or organisation are planned.

Scenarios

Figure 15.1 maps examples of different kinds of situations, which are arranged according to the first two parameters, namely *control* and *consequences*. Some scenarios have been constructed, which are based on the three parameters above. The aim is to show a way of reasoning in making a choice of methods; it does not give a comprehensive summary of all potential cases. More about choice of methods can be found in the examples given in Chapter 16.

Scenario 1
A small workplace in mechanical industry has been in operation for some years, and a new type of job has come up. The aim is to establish whether there are new hazards, and whether changes are needed.

Job Safety Analysis may be suitable here. It is simple and all the persons concerned with the new job could easily participate. The analysis may be extended also to detect problematic tasks. The evaluation method can be *Direct Evaluation,* which covers both hazards and production risks.

Chapter 16, which follows, gives examples of similar situations that have been analysed, and also shows the other methods that might be employed (see sections 16.5, 16.6 and 16.7).

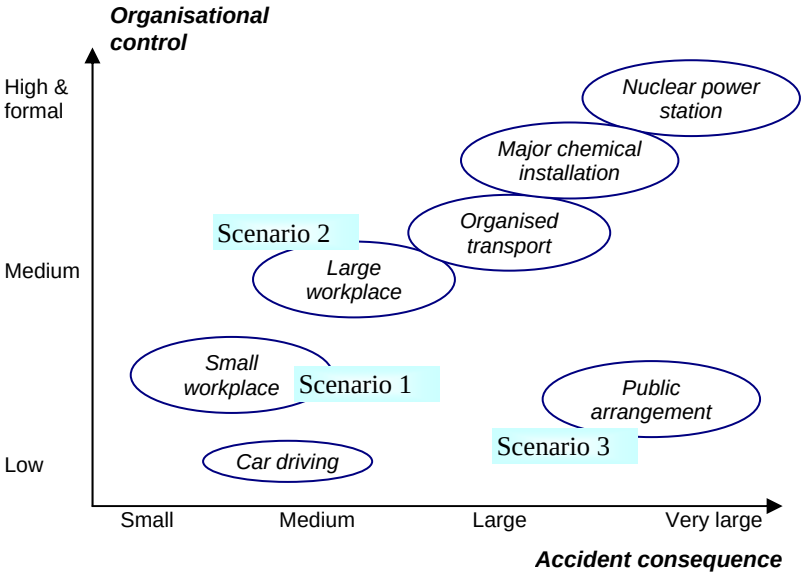


Figure 15.1 Examples of situations related to organisational control and consequences

Scenario 2
A large workplace in manufacturing industry is planning a major change in work organisation, which involves the employment of several subcontractors. A detailed suggestion for the new organisation has been made, but doubts have been raised over whether it will work well enough. The aims of the analysis are to check whether old safety routines will continue to be efficient, and to identify potential improvements.

A method that can handle organisational issues and evaluate the effectiveness of safety routines is required. Table 15.3 shows that a suitable method is *Safety Function Analysis.* It can also be used for developing improvements. An alternative method is *Change Analysis* – usually used for accident investigations. An *audit approach* (Section 12.7) could be considered, but it has disadvantages in that it only deals with formal routines.

Scenario 3

A public event with several thousand potential participants is at the early stage of planning. The aims are to identify hazards that might cause serious injury, and to clarify what might go wrong during planning.

Energy Analysis can be used to obtain a fairly complete summary of potential hazards. For a check on the planning, *Coarse Deviation Analysis* can be applied to obtain a simplified block diagram of the whole arrangement. If detailed information on the accomplishment of the arrangement is missing, the principle of *Relevance Evaluation* (Table 5.10) can be suitably applied. An alternative method is *Preliminary Hazard Analysis*, but the *Risk Matrix*, which is often associated with this method, is less suitable, since information to estimate probabilities is lacking. Or, *Direct Risk Evaluation* may be more appropriate. Section 16.8 gives an example of a safety analysis that is concerned with Scenario 3.

16 Examples of safety analysis

16.1 Introduction

This chapter provides a number of examples of safety analyses. The intention is to give a demonstration of how the methods can be used. The idea is to illustrate choices of methods and types of results. The aim is not to give a full solution to any particular problem, or to show a perfect and comprehensive analysis.

The examples have been selected to illustrate choice of method, analytic design, time spent on the analysis, and the results that can be obtained. Most of the examples come from my own applications of safety analysis. Earlier in the book, every method has been described separately. In these examples, two or more methods have been used in nearly all cases.

Over the last ten years, I have learned that a thorough accident investigation can be as useful as system analysis. Therefore, the set of examples starts with three event investigations, followed by other types of analysis. Another consideration has been to take cases from different kinds of systems and situations. The examples are summarised in Table 16.1.

Table 16.1 Summary of examples of safety analysis

Type	**Section**
Analyses of events	
Incidents with medicines in hospital care	16.2
Household gas fire	16.3
Accident at a mechanical workshop	16.4
Safety analyses of systems	
Mechanical workshop with power press	16.5
School kitchen	16.6
Medical care centre	16.7
Outdoor convention	16.8
Pharmacy production unit	16.9

In all the cases described here, there has been a working group involved. My role has been to act as analysis leader, where detailed knowledge of the studied system has been obtained by the working group. The groups have participated in the evaluations, and they have also been actively been involved in proposing safety improvements.

16.2 Analysis of incidents in hospital care

Background

Patient safety in medical services is attracting increasing interest, and one reason is the large number of medical errors during hospital treatment (see Section 1.2). Among other things, this highlights the need to learn from accidents and incidents (e.g., WHO, 2005), both at local level and generally. One essential question is how incidents should be analysed in order to learn as much as possible.

The first example is taken from a case study (Harms-Ringdahl et al., 2006), which was made in collaboration with a hospital in order to explore the possibilities of improved learning. The scope was pharmaceutical incidents in hospital care, since they represent an important problem area.

For the study, three incidents were selected. One criterion was that no injury to the patient should have occurred. The reason for this was to avoid a situation associated with blame or penalties, which is often regarded as a large problem in this sector. Another condition was that the incident was to be as simple as possible.

Figure 16.1 A patient in hospital care

We will take one of the incidents as an example. A doctor at an emergency ward wrote the number ***two*** instead of the number ***one***, when he transferred an earlier prescribed medication to the patient. This would have meant a double dose, which could have had drastic consequences. Through an

oversight, the patient did not get the double dose; consequently, there were two errors that balanced each other out. The following day, the errors were discovered and corrected by another doctor. The explanation was that a signature in the documentation looked like the number "2".

Aims

The overall aim of the study was to identify the type and amount of information that can be obtained through the use of system-oriented methods for the analysis of accidents and incidents. The goals of the actual investigation were to survey what had happened, to find explanations for how it could have happened, and finally to suggest safety improvements.

Approach and methods

In this case, data were collected from available medical documentation and four interviews. The interviews were limited to about an hour, and they consisted basically of a few open questions such as:

- Describe the event and circumstances when it happened.
- Do you think something could have prevented the event?

The data were analysed, and then a small team from the hospital was engaged for two meetings, each of about two hours. At the first meeting, the findings were checked, and evaluations were performed concerning whether changes were needed. As before, *Direct Evaluation* (Section 5.2) was chosen. At the second meeting, improvements were suggested.

- Three methods with different perspectives were chosen.
- The sequence was investigated using *Simple Event Mapping* (Section 13.3), since STEP (13.2) was regarded as too time-consuming.
- *Deviation Analysis* (13.9) was used to identify the problems, and especially the organisational issues, that were potentially interesting.
- *Safety Function Analysis* (13.10) was employed to give an overview of various organisational and technical barriers in the hospital.

Results

The sequence

The first thing was to reconstruct the sequence of events, which is summarised in Figure 16.2. The diagram is somewhat simplified through removal of parts of the time information, but it was accurate enough for discussions and presentations. The figure shows that seven organisational entities were involved. It also shows a rather complex need for the transfer of information and transport of the patient. In the diagram, the transfers are represented by 9 arrows.

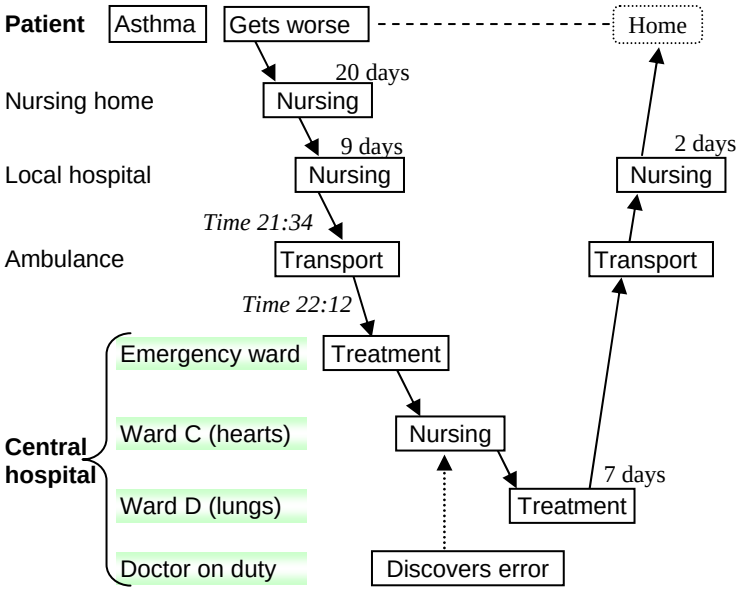


Figure 16.2 Simple Event Mapping of an incident in hospital care

Deviation Analysis

Several deviations had been observed during the interviews and documentation. Examples were:

- A doctor wrote down the wrong number – a **two** instead of a **one**.
- An initialized signature on the list of drugs could be mistaken for the number ***2***.
- The local and the central hospital had different layouts for their lists of drugs.
- It was difficult to distinguish between different kinds of information when the prescribing of a medication had been changed. The consequence was an increased probability of mistakes.

The deviations were recorded on a form (similar to the one shown in Table 16.6 in Section 16.4), and sorted under a few headings. The material was checked, and duplicate information from different sources was removed. Table 16.2 summarises the number of deviations and their evaluation. Fifty-three deviations were found, 70% of which were judged to require some kind of improvement.

Table 16.2 Summary of recorded deviations and evaluation of improvements

Part	Number	Improve*
The patient	4	3
Local hospital	7	5
Emergency ward	5	1
Ward C (heart)	10	5
Ward D (lungs)	1	0
The system for recording medications	13	12
The system for reporting incidents	13	11
Total	53	37

Improve* = Evaluated as needing improvement

Safety Function Analysis

From the interviews and in the documentation, safety functions (SFs) were identified and written down on the record sheet. The material had come in a rather arbitrary order, and it was sorted under a few headings, which made it easier to remove duplicate information from different sources.

Table 16.3 gives a summary of the SFs, with a division under 7 headings. The total number was 52, of which 17 had been proposed during the interviews. At the incident, 20 SFs had worked, of which 8 only partly worked. This indicates a clear need for improvement, especially at higher organisational levels.

Suggestions

At the second meeting of the work group, the results were presented and improvements were suggested. The largest potential for improvement was related to the system for recording medications. In this area, 26 suggestions were made and addressed to the County Council, which was the responsible actor. Another important area was the system for the reporting of incidents. In total, 60 suggestions were made on the basis of this analysis.

Comment

We had chosen a case that we thought was uncomplicated. It was simple in a way, but it occurred in a complex system with several weak points. We were astonished by the results. The study encompassed two more incident investigations, so it was interesting to see whether the results would be similar. The numbers of SFs and suggestions were slightly higher in both of them. (See further in Harms-Ringdahl, 2009.)

A lesson was that incident investigations can be powerful in identifying potential improvements. Maybe they are even better than a systems-oriented safety analysis, since it is easier to discuss things that have happened rather than abstract events that might happen in the future.

Table 16.3 Summary of safety functions at a hospital incident

Category SF	Example	n	OK
A The patient	The patient's knowledge of his medications Support from relatives at the hospital	4	2
B Nursing staff	Nurse asked patient about unfamiliar drug Attentive doctor on duty detected the error	9	7
C Level of ward (several wards)	Way of working at the wards Own instructions at the ward Cooperation between wards	9	4
D Level of department	The system for the reporting of incidents The form for reporting Learning from reported incidents	6	2
E Level of hospital	Instructions for using the medications case-book System for distribution of patients to wards	3	1
F Level of County Council	System for the documentation of patients' drugs Design of medications case-book	18	3
G National level	National regulations for documentation of medications	3	1
Total		52	20

n = Total number of SFs, including suggestions at interviews
OK = Number of SFs that worked well enough

16.3 Household gas fire

Background

Household gas had been involved in serious explosions and fires in a city on several occasions. The city's emergency services had observed that incidents with gas were quite common. Moreover, the frequency was not going down despite the efforts made. In order to prevent a larger accident, it was decided to obtain deeper knowledge of why they had occurred.

A gas fire was selected as a case to study more thoroughly than usual. In order to avoid questions of guilt and blame and to get an open discussion, a fire with minor injury and damage was chosen. A detailed report is available in Swedish (Harms-Ringdahl et al., 2008).

A brief description of the event

Figure 16.3 Gas fire in a kitchen

The owner of an apartment had help from a plumber to remove gas pipes in his apartment. During the work, gas leaked out and started to blaze. Emergency services were quickly alarmed. During the waiting, the plumber let the gas burn to avoid accumulation and a potential explosion. His efforts were directed at preventing the fire from spreading further in the kitchen. After some difficulties, the gas could be shut off by emergency services. The plumber sustained light burn injuries, and the apartment was slightly damaged.

It was regarded as a simple incident. The first explanation for the event was basically that the plumber had been negligent, since he had not turned off the gas before the job was started.

Aim

The aim of the actual investigation was to analyse what had happened and to understand how it could have occurred. A sub-aim was to suggest improvements to how hazards with household gas should be handled in the future.

Approach and methods

Basic initial data consisted in a short report from the emergency services that had extinguished the fire. Data collection was done in parallel with the analysis, since new information gradually came to light. Six interviews were conducted.

After the preliminary analysis had been performed, some of the organisations were invited to a meeting, which lasted a few hours. One purpose of the meeting was that the participants should contribute to the evaluations, and they should also suggest possible improvements. Also, the meeting was an important source of additional information and for checking the data.

As in the previous example, three methods with different perspectives were chosen.

- The sequence was investigated using *Simple Event Mapping* (Section 13.3).
- *Deviation Analysis* (Section 13.9) was used to identify problems, and especially the organisational issues that were potentially interesting.
- *Safety Function Analysis* (Section 13.10) was employed to give an overview of various organisational and technical barriers in the handling of household gas.

Results

The sequence

An early step was to map what had happened in a diagram (not shown here). The preliminary map was presented at the interviews, and it was successively expanded. Seven actors were found to be involved in the acute situation.

The Deviation Analysis

Deviations found in interviews and documents were recorded on a list. Both confirmed deviations and hypothetical ones were included. In this case, there were several divergences between the actors' statements and also between the documents. In addition, such differences were recorded as deviations.

One example is that the exact course of events could not be established. The main reason for this was that a police investigation was pursued in parallel, which meant that the company involved was very cautious about giving out information. Three alternative hypotheses were conceivable. Instead of selecting just one of them, all three were considered. Moreover, improvements were suggested for all three scenarios. They were:

Hypothesis 1: The plumber thought that there was no pressure in the gas pipe.

Hypothesis 2: The plumber knew that there was pressure in the gas pipe.

Hypothesis 3: The plumber was not aware of any hazards in the job.

Examples of deviations:

- The pipe was cut with the gas pressure on. At first this was regarded as an error, but it later emerged as a common work method.
- The plumber used an electric saw to cut the pipe, which then became the source of ignition.
- This was a common practice, although it is forbidden in regulations.
- The gas pipes and valves in the building were not labelled.
- There were several problems involved in closing the gas valve in the cellar of the building.
- It was common for gas valves in the building to be difficult to operate.

The deviations had come in a rather arbitrary order. Accordingly, there was a need for sorting and the removal of duplicates. In total, there were 39 deviations, which were arranged in time order in four categories:

1. Permanent (14 deviations)
2. Before the acute phase (11)
3. Acute phase, from when the gas was released to when the fire was extinguished (8)
4. After (6)

Safety Function Analysis

Safety functions (SF) had been identified in the interviews and documentation, and noted on the record sheet. The material had come in a rather arbitrary order, and the number of SFs was quite high – around 100. The categorisation was therefore based on two dimensions. The first was the time order (as above), and the second was based on actors involved:

a) The authorities
b) The trade association
c) Emergency services
d) The gas company (the provider of household gas in the region)

e) The plumbing firm
f) Individuals

Table 16.4 Extract from a Safety Function Analysis record for a gas fire

Safety function	F*	Ev	Proposed measures	Comment
Law about explosive materials (SFS 1988:868)	Y	1	Improved cooperation between authorities is recommended	Covers comprehensive issues
Supervision of activities based on law	N	1-3	Systems oriented supervision by emergency services	Is not done
Placement of responsibilities – for different activities	N	3	Examine, clarify and communicate	Many statements from actors, but not clear or authorized
Cut-off valve outside building	N	3	Develop strategy for gas accidents – cooperation with emergency services and gas company	Valve did not work, which is a common problem. Important at large gas releases
Gas company operator (GCO) on duty tries to close the valve	N	3	See above	Did not succeed; see above
Cut-off valve in building	P	3	Communicate information to all property owners with gas	Difficult to operate due to defective design and maintenance
GCO closes cut-off valve in building	Y	2	As above Information to emergency services about cut-off valves	The GCO had the tools and knowledge required
Labelling of cut-off valve	N	3	As above	Difficult for emergency services to find the valve
Method for working with pipes with gas pressure	N	2	Inform all service companies about the method	Was not used; method is simple and commonly used by GCOs

F* = Estimation of the SF
Y = Yes SF performed satisfactorily
P = Partly SF worked partly
N = No SF did not perform as expected

Ev = Evaluation of need for safety measure (SM)
0 = No need; 1 = SM can be considered
2 = SM is recommended;
3 = SM imperative

Table 16.4 shows an extract from the record sheet with examples of the SFs. The SFs were judged according to the principal of whether they had worked or not (see Table 13.2 in Section 13.10), and the result is shown in the column F*. The summary gave a total of 91 SFs, which to some extent overlap each other. Of these, 41 had functioned, either fully or partly.

Evaluation
The need for improvements was discussed at a meeting with the actors. The *Direct Evaluation* method (Section 5.2) was applied to both the deviations and the SFs. The result is summarised in Table 16.5, which shows that 87% of the deviations called for improvement, while the corresponding value was 57% for the SFs.

In two cases, there were different opinions in the evaluation. One is shown in Table 16.4, and concerns *Supervision of activities based on the law*. Here, one actor took the stance that supervision of gas installations by the concerned authority was not needed, whereas others thought it was very important. The protocol shows the disparities, which the decision-makers were assumed to handle.

Table 16.5 Result of risk evaluation of deviations and SFs

Code	Description	Dev	SF
0	No need for improvement	0	0
1	Safety measure* can be considered	5	39
2	Safety measure recommended	8	18
3	Safety measure is imperative	26	34
	Total	39	91

Dev = Number of deviations
SF = Number of SFs

Suggested improvements
Discussion of improvements was based on the items with the highest scores, and lasted around two hours. Ideas were directly noted on the record sheets. After the meeting, the suggestions were somewhat reformulated, and then compiled on a new list. In total, there were 73 suggestions for improvements.

Comments
At the beginning, we were told that there were clear rules for working with gas installations in apartments. If the plumbers just followed them, no accidents would occur. The explanation we received was that the fire was caused by a careless individual; he should have turned off the gas before starting the job.

The investigation showed that working with pressurised gas is a common work procedure. In the analysis, many unclear issues appeared, but the plumber, in general, had followed common practise. There were many contributory explanations for the accident, which gave rise to the 73 suggestions.

At the end, this appeared to be an accident with clear organisational roots. The feeling was that Safety Function Analysis had been most useful in analysing the organisational aspects. It concerned the identification and structuring of hazards, and judgements on reliability.

16.4 Accident investigation at a workshop

Background

This metal workshop had several power presses installed, which were used for punching and bending metal pieces. Although the safety technique for pressing is well-known, the company was aware that some safety problems had not yet been resolved. A few minor accidents had occurred, but not a serious one for several years.

The study was performed in two stages; the first was an accident investigation, which was followed by a more exhaustive system safety analysis (described in Section 16.5).

Aim

The general aim of the study was to identify hazards related to presses at the company to check whether safety issues were adequately handled. In addition, when needed, improvements should be suggested. A goal of the accident investigation was to prepare the company's working group for a more exhaustive system-oriented safety analysis.

Approach and methods

As an initial activity, a minor accident was analysed. *Deviation Analysis* (Section 13.9) was preferred for this. One reason was that organisational issues seemed to be important, which the method could handle fairly simple. Another reason was that the study should continue with a systems-oriented safety analysis, meaning that the same method could be used again.

The accident investigation was performed at a meeting of around three hours. Data for the analysis came from an investigation that had been performed earlier, and what the work group remembered of it. No additional external data collection was conducted due to lack of time. With the help of a checklist (Table 8.2 in Section 8.2), a number of deviations were found and listed.

Table 16.6 Extract from a Deviation Analysis record sheet for an accident

Deviation	Consequence	Ev	Proposed measures	Comments
Person A got hand squeezed in press	Minor injury, no absence from work	-		The accident
Tool unsatisfactorily protected	Possibility of a squeeze injury	2	Improve check of tool set-up (see below)	The tool was believed to be safe
Unusual work method	Work could be done in risk zone	3	Investigate whether work process is acceptable Investigate whether there is a problem in other places	Combination of automatic operation and manual feeding
The injured person wore gloves	Increases the risk of being caught in tool	1-2	Clarify and give information on company rules about gloves	Gloves are dangerous in some tasks, but necessary in other
Failure in set-up of tool	Increases risk of squeezing, e.g., if movement is too large.	3	Ensure that all tools are set-up by persons with proper competence Improve setting-up instructions Develop checklist for control	The failure is not certain but possible, and presumed to have existed
Data for set-up are sometimes inaccurate	Can contribute to failure in set-up	3	Routine to ensure that set-up data are always accurate	Can be coupled to production planning
Person A was hired temporarily from another company	Person A does not have full information about tasks and risks	0	-	Common way of handling production needs – but needs consideration
The safety rules of the company had overlooked temporary workers	Increased risk; the temps fall outside training programs and lack adequate information	3	Include temporary workers in safety routines (it was already planned)	The problem did not exist when the original rules were written
The introduction of new workers vary a lot, and there is poor follow up	New workers have unsatisfactory knowledge of safety issues.	3	Check status of the introduction program Ensure that it works well	Breach of formal directives and company policy

Ev = Direct Evaluation 0–4 (Table 5.2) 1 = Safety measure (SM) can be considered 2 = SM recommended 3= SM is imperative

The next step was to determine whether improvements were needed. *Direct Evaluation* (Section 5.2) was chosen. The *Risk Matrix* (Section 5.4) approach would have created difficulties, since it is tricky to define the probabilities of things that permanently exist. The final stage was to suggest improvements for the deviations that obtained a score of 2 or higher.

Figure 16.4 Work at the power press

Results

During the analysis, 12 deviations were identified, of which 10 were scored 2 or 3, meaning that they needed improvement. The three-hour meeting produced 17 suggestions for improvements. Table 16.6 shows a part of the record sheet from the analysis.

Comments

At the beginning, the group remembered just a few deviations, and the investigation proceeded slowly. The following morning, a foreman in the group took me aside, and told me that he had seen three obvious deviations during his first hour of work that day. I interpreted this as that his mental picture of how accidents could occur had changed. This meant that he and the others had become aware of deviations in production, and that the subsequent analysis went quickly and smoothly (see Section 16.5).

16.5 Safety analysis at a workshop

Background

Power presses are known to be dangerous if they are not properly operated. The official regulation of power presses is extensive in most countries. Thus, it might be expected that working with presses is safe, but that is not always the case.

This example comes from the same mechanical workshop as in the first case (Section 16.4), in which a work accident was investigated. The company had several eccentric presses, and was aware of some safety problems. A study had been initiated to see what could be done further to improve safety, and the company had formed a working group for this.

Figure 16.5 Work at the studied power press

Aim

In this specific analysis, the aim was to study one eccentric-press thoroughly to identify most hazards and to find possible improvements. The results from this individual press could later also be used for studying the work at other presses in the workplace. The analysis was to include the

press and the work around it. A detailed technical risk analysis of the electrical control systems for the press was ruled out, since it was presumed already to have been done.

Approach and methods

A clear limitation was that only two working days had been set aside for the analysis. It was performed as group work in just a few sessions, and little time was available for detailed observations.

In working with presses, the obvious hazard is to be pinched by the moving tool. A general idea underlying the analysis was to adopt a wider perspective, and to work more broadly. In order to get an overview of all the physical hazards, *Energy Analysis* (Chapter 6) was chosen. It is a quick method, and a few hours were spent on it.

As a complementary method, *Deviation Analysis* (Section 8.3) was selected. The method was used to study the production flow and the stages in working with the press. One argument was that the method would be suitable for incorporating managerial aspects and company routines. Suggestions for improvements were developed independently for each method, since the two methods have different approaches to the creation of ideas.

Results

The Energy Analysis

In this method, the object is divided into blocks (volumes). The press was divided into three parts, as shown in Figure 16.6. They are not volumes in an orthodox sense, but they are easily understandable as such. Energies were identified, and some examples are shown in Table 16.7. The second row shows that there was disagreement over whether or not something should be done. This was solved by putting both scores (1 and 2) in the protocol, so that the issue could be resolved later at the final round of decision-making.

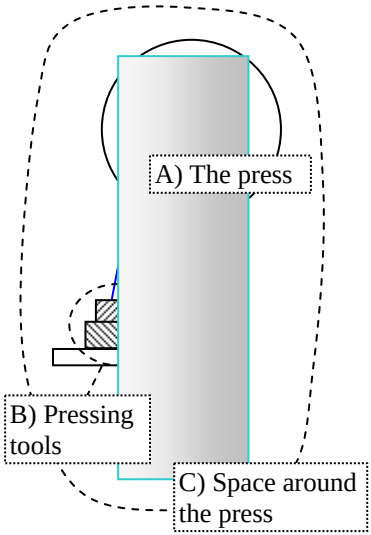


Figure 16.6 Model for Energy Analysis

In the analysis, 22 energies with the potential to cause injury were identified. In the evaluation, two energies scored *3*, and eight scored *2*, meaning that 10 energies had to be handled in some way. Twelve measures were proposed, of which five were of the type *Investigate further*.

In the table, two non-traditional energies are included – *Static load* and *Material on floor*. These represent hazards that were detected during discussion of the analysis, and they could easily be included by adopting a wider perspective on energy.

Table 16.7 Examples from Energy Analysis of a power press

Volume / Part	**Energy**	**Hazard /** *Comments*	**Eva**	**Proposed measures**
A Press / Flywheel	Rotation	Crush / *Cover on the rear is not complete*	1-2	Check on formal demands
/ Lubrication system	Oil under pressure	Slippery / *Oil leakage*	2	Check oil system Improve cleaning routines
/ General	Static load	Poor ergonomics / *Insufficient space*	2	Investigate possible improvements
B Tools	Pressure	Pinch / *Some movements are open*	2	Control of guards to be included on the checklist
C Space around	Material on floor	Trip or slip	3	Improve cleaning routines
/ Input of material	Weight (50–100 kg)	Overload, fall on to feet	3	Lifting equipment always available
/ Output of material	See Input	See Input	3	See Input

Eva = Direct Evaluation 0 - 4 (Table 5.2)

Deviation Analysis

In Deviation Analysis, attention is directed at the production flow and other activities. The first stage of the analysis is to construct a block diagram of activities, as shown in Figure 16.7. The central part shows the production, which is divided into four main blocks. During the discussions, each block was found to be more complex than expected, even for persons in the company. The figure shows how the second block, *Assembling press tools*, was divided further into subparts. This can also be done for the other blocks.

The diagram has two additional blocks. *Planning of production* includes activities that control how the job is performed. The *General* block contains activities that go beyond the individual blocks. At the beginning, it was not clear what it should include, but a number of points were entered one by one:

- Maintenance
- Recruitment of personal
- Design of routines and writing instructions
- Handling of disturbances and changes to routines or techniques
- Safety management
- Annual safety inspections

However, the blocks *General* and *Planning of production* were not included in the analysis, since the time available was not enough. They are likely to be of key importance, and the recommendation to the company was to investigate them further.

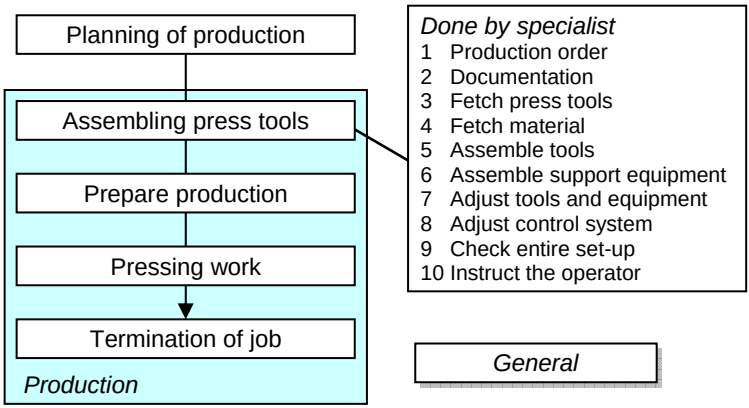


Figure 16.7 Block diagram for production at a power press

In the analysis, 45 deviations were identified and listed. Table 16.8 shows examples from the analysis. The deviations were evaluated, of which 27 required some kind of action (score *2* or *3*).

The evaluation considered both safety and production aspects (see Table 5.1 in Section 5.1). In Table 16.8, we have, for example, *S2*, which means that an improvement is recommended from a safety perspective. Production problems were related to 20% of the deviations, which enhanced motivation for making improvements. The analysis was concluded by looking for safety measures, and 31 suggestions were made.

Comments

Supplementary methods were used to obtain different perspectives on the risks in the workplace. We started with an accident investigation (Section 16.4) at one press, and applied two analytic methods at another press. The working group adapted quickly to new ways of thinking, and this made for a more comprehensive analysis.

In total, 16 items (deviations or energy) were scored *3*, and 31 scored *2*. This meant that 47 items had to be taken care of in one way or another. Together, 59 measures were proposed in the different sessions. There was overlap between them, and the number can be reduced to about 50.

It is important to note that the identification of hazards, the evaluation, and the proposals were produced by the working group. The visiting analyst knew only a little about power presses, and his role was merely to lead the sessions.

The case study was of traditional production at a company that had ambitions for a good working environment. By the end, both the working group and I were surprised to find such a large number of hazards and such great potential for improvements.

Table 16.8 Examples from the Deviation Analysis of a power press

Block / Part	**Deviation**	**Consequence** / *Comments*	**Eva**	**Proposed measures**
Assembling press tools				
/ 2 Documentation	Press differences not considered & Not updated	Press stroke too long Production error / *Easily detected*	S2 P1	Improve routine for update of documentation
/ 3 Fetch tools	Takes wrong tool	Takes longer	P0	
/ 4 Fetch material	Manual lifting (e.g., 100 kg)	Overload on back, falling on feet	S2	Ensure that everyone is aware of lifting rules
	Instable box-stand	Box overturns / *Later during operations*	S3	Install better box-stands
/ 5 Assemble tools	Insufficient competence	Increased risk of failure	S3 P3	Check whether routines are adequate Develop checklist for assembling tools
	Over-long press stroke	Damaged tool Higher squeeze risk	P2 S2	Include on checklist (above)

Eva = Direct Evaluation 0–4 (Table 5.2) S = Safety & P = Production (Table 5.1)

16.6 Safety analysis of a school kitchen

Background

Jobs in kitchens can be dangerous and have a rather high accident rate, and many persons are employed in them. Methods of safety analysis are usually thought to be applied in the industry, and it was interesting to test how well they worked also at such workplaces.

The analysis was performed in collaboration with a school, which was interested in improving its safety work. The kitchen had recently been reorganised in order to prepare considerably more food than before.

Aim

The concrete goal was to identify hazards and find improvements to the school kitchen. The scope of the analysis was restricted to persons directly employed in kitchen work. This choice excluded the risks to other individuals, such as cleaners, repairmen and delivery people. The restriction was applied for reasons of time, but this is not something to be recommended. In addition, hazards for the children who were being served were to be checked at a later stage.

Figure 16.8a A school kitchen

Approach and methods

Job Safety Analysis (JSA) (Section 7.2) was chosen since it is suitable for manual jobs, e.g., in a kitchen. For the judgement of risks, *Direct Evaluation* (Section 5.2) was applied, but an alternative was the *Risk Matrix* (Section 5.4). Information about the job and hazards was obtained from observations at the site, and a few short interviews.

Figure 16.8b A hazardous task is the lifting of plates of hot food, which can easily spill over

Early in the analysis, several essential observations were made, but they did not fit into the record sheet for a JSA. After a while, such findings were treated instead as deviations and recorded on a separate protocol. However, it was not a full Deviation Analysis (Section 8.3). A small work group was organised with all the employees in the kitchen, and a manager from the school. The group participated in the evaluation, and in the development of suggestions.

Results

The job tasks

An early part of the analysis was to list the varied tasks performed in the kitchen (Table 16.9). This was done according to the principle underlying Job Safety Analysis. If the list had been made for Deviation Analysis, a number of items would have been added, such as general cleaning (by other people), repair and maintenance, management and planning, and also child activities.

Table 16.9 Summary of tasks in the kitchen

Tasks	**Subtasks; comments**	**J***	**D***
1 Take in goods	Take in from loading bay, unload, sort, place in storeroom	4	5
2 Prepare	Concerns cooking and serving	2	0
3 Cook food	Chop and cut, boil potatoes, work with cauldrons, other cooking,	3	0
4 Store prepared food	Transport of food, put food plates in heating cabinet or take them out	4	5
5 Serve food	Includes injuries to children	5	3
6 Wash-up	Prepare, main wash-up, clean larger items	6	1
7 Finishing off	Includes general cleaning	2	2
8 Handle garbage		0	1
9 Common	Subtasks that are common to several main tasks	2	0
- Other	Outside the JSA list (1–9)	0	8
	Total	28	25

J* = Hazards requiring improvement
D* = Deviations requiring improvement

Identification and evaluation of hazards

The hazards identified through the JSA were noted on a special record sheet (Table 16.10), and deviations on another. After identification, the hazards and deviations were evaluated by the work group.

The two columns to the right in Table 16.9 summarise how the problems were spread across different tasks. It shows the number of items needing improvement (scored *2* or *3*), which are distributed according to JSA hazards and deviations. It can be seen that improvements were needed for 28 hazards and for 25 deviations.

Table 16.10 Extract from a Job Safety Analysis record sheet for a school kitchen

Job task / Subtask	**Hazard / Injury**	**Eva**	**Proposed measures**	**Comments**
1 Take in goods	Lifting heavy things. Overstrain, lumbago	2	Investigate *Input flow* in general Especially milk flow & storage Remove doorstep More storage shelves	Heavy loads, e.g., milk packages 20 kg Doorstep of 4 cm makes carrying difficult
	Falling from the loading bay	1		Especially when carrying
	Slipping, especially in winter	1		Cleaning procedure is adequate
/ Unloading	Hit by falling object	2	Consider in *Input flow* investigation	Especially in storeroom
	Overstrain	3	Consider in *Input flow* investigation, especially vegetables storeroom	Sometimes, limited space makes transport and lifting difficult
2 Prepare cooking and serving	Hit by falling object	3	Consider in *Input flow* investigation	Similar to above, but here the selected things are harder to get
	Hand gets caught in deep freezer	2	Easily available protection gloves Include on *Checklist for safety*	Worse if hands are wet
3 Cook food / Boil potatoes, pasta, etc.	Eye injuries, burns on hand, forearm and feet	2	Explore alternative cooking equipment Include on *Checklist for safety*	Splashes of hot water or steam Overflow of water is common
	Slipping on floor	2	Consider for new cooking equipment Slip protection carpet Include on *Checklist for safety*	Oil in the boiling water makes the floor slippery
/ Transport of food, especially hot food	Burns in contact with hot liquids, hot surfaces and oven	2	Investigate *Handling of hot material* Better protective equipment Include on *Checklist for safety*	Large food plates with liquid are often wobbly

Eva = Evaluation: 0 = No need for improvement 1 = Safety measure (SM) can be considered 2 = SM recommended 3= SM is imperative

Suggested improvements
Possible improvements were discussed for about an hour in the work group. Suggestions were noted on the record sheet, and sometimes simple changes could be proposed. However, the majority concerned development and working routines, which demand greater consideration before they are accomplished. After the meeting, the proposals were sorted into a handful of themes:

- Overview of overall flow and procedures
- Deliveries and input flow (part of overall flow, but solutions could be accomplished at once)
- Manual handling (lots of lifting and repetitive work)
- Handling of hot materials (food, liquids, etc.)
- Washing-up
- Development of documented routines, including checklists for safety and working procedures, where one important target group comprises persons in temporary employment.

Reporting
The analysis was documented in a four-page summary, supplemented by the record sheets of the two methods employed, in total 13 pages. There was also a brief meeting to present the results. After the analysis, the school held a number of meetings in order to develop the ideas into practical solutions.

Comments

Tasks in the kitchen are largely manual, and the initial idea was that a Job Safety Analysis (JSA) would be enough. However, most jobs are actually quite complex, and organisational issues become important. To resolve these matters in a practical way, the additional issues that came up were handled as deviations, which provided much additional information for the analysis.

An alternative choice of method would have been directly to employ two complementary methods, among which Deviation Analysis was an obvious candidate. In such case, managerial issues would have been considered from the outset, and included in the block diagram.

When I revisited the school two years later, there had been a partial shift in personnel. The safety analysis had been used as part of introduction to work for the new persons. Many of the ideas had been implemented, and the school was therefore eager to update the analysis to check the risk situation again.

16.7 Safety analysis at a medical care centre

Background

The challenge of obtaining good patient safety has received much attention, especially at hospitals (see Section 1.2). However, smaller units may also be important. The occurrence of avoidable medical adverse events is much less well-known compared with what goes on in hospitals. In any case, it is interesting to study potential problems and test the usefulness of analytic methods.

This analysis was conducted in collaboration with a medical care centre. It concerns a small unit with a staff of around fifteen people, with patients from the local neighbourhood. A few simple surgical operations are performed every day.

The question was whether operations were performed well enough, or whether something had to be done to improve the situation. A newly employed doctor was asked to perform a safety analysis to assess the situation.

Figure 16.9 The surgery room

Aim

The objective was to analyse surgical operations to see whether there were any important problems, and whether the routines had to be improved. The result might also be usable for patient safety reports, which Swedish medical services are supposed to provide each year.

Approach and methods

It was decided to examine the whole process by following a patient through the treatment. *Deviation Analysis* (Section 8.3) was seen as suitable, and a straight-forward block diagram was developed. An alternative could have been to use *Hierarchical Task Analysis* (Section 12.6) for the modelling, but, in this case, much of the work is guided by individual doctors, not by a formal system.

The identified deviations were assessed using *Direct Evaluation* (Section 5.2), followed by a round for developing suggestions. A short report would be enough, and the result should be communicated at a meeting with all the unit's staff.

The intention was to form a small working group, which was to participate in the structuring, the identification of hazards, and the development of improvements. However, after a while, it became clear that it was hard to find interested participants with time available. This meant that the analyst mostly had to work without that help.

Results

Structuring the surgery process

The scope of the analysis was based on the patient's perspective. The process description started with the patient's first contact with the doctor and ended with follow-up after surgery. The process is shown in Figure 16.10.

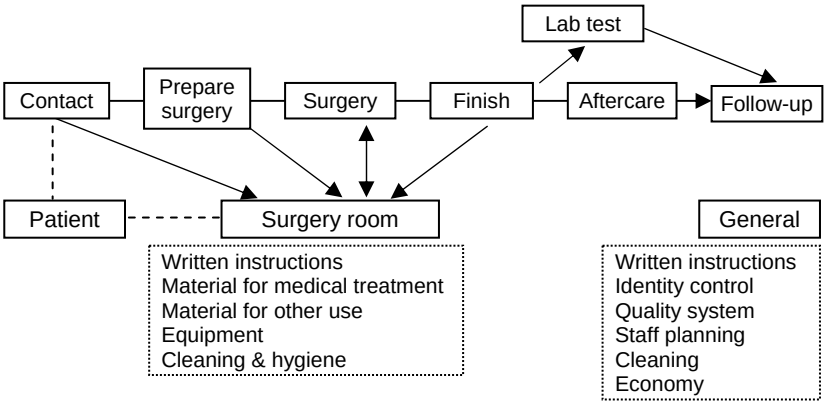


Figure 16.10 Block diagram of the surgical process

The process was divided into 10 main blocks. In the analysis, each block was then divided into further activities. Examples are shown for the *Surgery room* and for *General*. Special attention was paid to the *Surgery room* and activities related to it. It is the main area of activities, and a number of actors are involved.

Identification of deviations

Identification was based on consideration of each block at a time. Two nurses had been asked about deviations they knew about, and they had produced a list that was valuable for finding problems.

Examples of deviations are given in Table 16.12. As usual with protocols, the text is short and sometimes difficult to understand without further information. We take *Patient is infectious, incl. MRSA.* The acronym stands for *Methicillin-Resistant Staphylococcus Aureus*, which is a bacterium that gives rise to infections that are difficult to treat. Infectious patients can cause serious problems, if proper action is not taken.

Evaluation

No working group was available, and the evaluation had to be performed by the doctor alone. She did not have full knowledge of routines and daily work. Instead of marking an unreliable estimate, a special score (u) was introduced, which indicated that information was unclear or insufficient, and that the manager of the care centre must take responsibility for it. If the doctor knew that something was not working well enough, she could give a score of *2* or *3*.

Table 16.11 Summary of evaluation of deviations found in the surgical procedure

Code	Comment	n
0	No need for improvement	3
1	Safety measure (SM) can be considered	4
2	SM is recommended	10
3	SM is imperative	11
u	Unclear or insufficient information; evaluation is postponed	29
	Total	57

A summary of the results is given in Table 16.11. In total, 57 deviations were found. Half of them were evaluated, 21 of which were judged to require improvement or further study.

Table 16.12 Excerpt from the protocol of a Deviation Analysis of surgery

Block / *Sub*	**Deviation**	**Consequences**	**Eva**	**Improvements**
Contact	Reservation of surgery room fails	Room is not prepared Assistance not available	2	-
Patient	Patient is infectious, incl. MRSA	Risk of infection for staff and patients Serious contamination	u	-
Prepare surgery	Incomplete preparations	Operation is more difficult. Takes time to look for material	2	Check system for booking and related routines
Surgery room */ General*	Objects on the floor, e.g., electric cords	Injuries; tripping; obstruct movement of equipment; complicated cleaning	3	Investigate how improvements can be made
	Unclear system for storage of material	Stress; delayed operations; improper material is used	3	-
	Gap in responsibilities for cleaning	Deficiencies in cleaning; increased risk of infection	3	Identify responsibilities and routines for cleaning
/ Equipment	Surgical lamp unstable	Rollover risk, poor lighting	2	Investigate technical improvement;
Surgery	Staff do not disinfect their hands	Risk of infection	3	–
Finish	Patient is not informed about future actions	Complications	3	Develop information leaflet for patients; include individual info
Lab. test	Erroneous identification of patient and sample	Lab results do not reach the proper patient	u	–
General	Different views on the need for order and control	Compliance with hygiene variable; increased risk of infection	3	–

Eva = Evaluation codes: See Table 16.11

Suggested improvements
In this case, no working group was available, which made it difficult systematically to develop improvements. However, a number of ideas arose at the evaluation stage and were noted. The result was 19 suggestions, of which a majority were organisational.

Comments
Although the evaluation was not complete, the conclusion was that improvements were needed, which included checking several routines and items. In my view, the most serious problem was the low priority given to safety work; no one had time to participate in evaluations and discuss improvements.

However, you cannot draw the conclusion that the situation at the care centre really is dangerous. There may be informal and individual-based ways of working that give a satisfactory safety level.

The routines are not documented and clearly communicated, and if new staff are employed the risk level might rapidly rise. Hopefully, the results of the analysis would raise interest in safety, and that might be its greatest benefit.

16.8 Safety analysis of an outdoor convention
Background
A large outdoor convention was being planned. Such a convention had taken place a number of times before, and several thousand visitors were expected. The convention was to last for a few days, which meant that many different activities and overnight facilities had to be arranged. With so many people gathered together, there is potential for severe accidents, and the safety and security arrangements were therefore carefully considered (Mattias Strömgren, personal communication, 2012).

Aim
The safety manager of the convention wanted to check that all important hazards were considered, and that earlier routines were adequate. He was new in the position. A further aim was to establish a more systematic approach to the handling of safety.


Figure 16.11 Outside and inside one of the smaller tents

Approach and methods

A working group of persons with safety responsibilities was formed. The group met a few times, in good time before the convention. Bases for planning were earlier experiences and advice from "The event safety guide" (HSE, 1999).

A coarse application of *Deviation Analysis* (sections 8.3 and 12.8) was chosen as method. This meant that the division into functions (the structuring) was done rather crudely. There was a rather broad perspective at the identification stage, which considered injury to people, and damage to property and the environment (similar to Table 5.1 in Section 5.1). This was directly done at a session with the work group, based on the participants' experiences. *Direct Evaluation* (Section 5.2) was applied, and an assessment was made of whether previous safety arrangements were good enough.

Results

Structuring for the analysis

The convention would be too complex to model directly; instead, a division was made, primarily on the basis of the zones where activities took place. The convention was structured into the following zones or functions:

- Camping grounds (a handful of places)
- Tents for meetings and performances
- Food and food distribution
- Traffic (public roads and private roads inside the convention area)
- Leisure areas (places for bathing and barbecues)
- Dormitory arrangements

Table 16.13 Extract from Deviation Analysis of an outdoor convention

Zone/ Function	**Deviation**	**Consequence**	**Eva**	**Improvements**
Camping	Spread of fire (grill or camping stove)	Large fire	1	Arrange safe places for grilling Distribute fire extinguishers
Tent	Storm	Tents unstable, squeeze injuries, and falls	2	Better mast fixtures Readiness for evacuation
	Persons loosen equipment	Heavy objects can fall	2	Installation routines Improved fixing equipment
	Disturbance to audience movements	Crowding, panic causing injury	3	Improved time planning Emergency plan & instructions
	Quick evacuation (fire or threats)	As above	2	As above
	High sound volume	Impaired hearing, discomfort	1	Limit sound level Distance to loudspeakers
	Failures to electric equipment	Electric shock	2	Routine for checking Install earth-fault breakers
Traffic on road	Excessive speed	Collisions, especially involving children and elderly	3	Speed limit (30 km/h) Surveillance by police Change to road design

Eva = Evaluation codes:
0 = No need for improvement 1 = Safety measure (SM) can be considered
2 = SM recommended 3 = SM is imperative

Identification and evaluation of hazards

The identified deviations were noted on the record sheet, and some simplified examples are shown in Table 16.13. The analysis found 21 deviations, of which 14 were given a score of *2* or *3*.

Suggested improvements

Improvements were discussed at a meeting of the work group, and possible improvements were also noted even when the score was 1. The total number of suggestions was 37, a majority of which were accomplished at the following convention.

Comments

The structuring was concrete and practical. If the ambition had been to perform a more complete Deviation Analysis, additional organisational functions in the structuring would have been interesting. Additions might have been:

- Site management
- Stage performance (planning and accomplishment)
- General

The function *General* concerns things that are either common to or go beyond other specific functions. What it includes might not be clear from the outset, but it is quite likely that interesting issues will come up.

16.9 Analysis at a pharmaceutical company

Background

A part of the production line at a pharmaceutical company was investigated. It is the same unit as described in the example of Safety Function Analysis (Section 11.7). It is fairly simple batch production. However, the system uses technical equipment, computer control, manual operations guided by formal procedures, and batch protocols. The workplace was new, and partly based on a novel design concept. Production had only recently started. The design of a similar production system was in progress.

This system was analysed using a number of different methods, and a brief account of experiences is presented here. A more detailed description of the case study has been published (Harms-Ringdahl, 2003A).

Aim

One aim of the Safety Analysis was to find the hazards that were inadequately handled. A further objective was to study the workplace in order to find design improvements for the next planned production site. The intention of presenting this example is to illustrate the different types of results that can be obtained using different methods.

Approach and methods

In the first part of the study, the three methods, *Energy Analysis*, *Deviation Analysis*, and *Safety Function Analysis* (chapters 6, 8 and 11) were applied to the object. The analyses were intended to be as independent as possible.

The separate assessments of the items were all based on *Direct Evaluation* (Section 5.2), and concerned whether or not conditions were acceptable. The case study included a total of 144 identified items, which were evaluated. Around half-an-hour of meeting time was devoted to evaluation in each analysis. In total, this meant 1.5 hours, which gives a mean value of less than one minute per evaluated item.

At nearly all the evaluations of items, it was possible to reach a consensus. However, this was not essential, since it was possible simply to note a dissenting opinion on the analysis sheet. If sufficient information was not available, some kind of further investigation was usually proposed.

In a second part of the study, the results of applying the methods were compared. Since the methods focus on different aspects, it is not obvious how such a comparison could be made. One way was to study *items*, which here would mean energies, deviations, and safety functions. An additional comparative approach was to focus on the number of proposals generated by the different methods.

Results

Some general information about the analyses is given in Table 16.14. The first row of the table concerns the efforts required by the safety analyses themselves. Each analysis took two or three meetings, and each meeting took between two and three hours. The Safety Function Analysis was performed as part of a research project, which meant that extra time could be devoted to it.

Table 16.14 Summary of a comparative analysis of three methods

Description	**Method of Analysis**			
	Energy	Deviation	Safety Function	All analyses
1. Number of meetings	2	2	3	7
2. Number of identified items	34	56	54	144
3. Items, not acceptable	21	34	37	92
4. Items, not acceptable due to production aspects	8	24	3	35
5. Proposals for actions, total	23	48	47	118
6. Proposals for further investigation	13	21	15	49

A large number of the hazards were connected with lye and hot water, which could cause serious burn injuries. Under certain conditions, these fluids could be put under high pressure. Explosions could not be ruled out, since the tanks were not designed to withstand high pressure. Other hazards were related to falls from a height, poor ergonomics, errors in follow-up procedures, and so on. Thirteen health-related and ergonomic problems were identified, but nothing was found in relation to the environment.

Comparing items

One measure of results was the number of identified *items*, which varies according to method. The second row of Table 16.14 shows that a total of 144 items were identified.

Row 3 shows the items that were evaluated as not acceptable (scored *2* or *3* in Table 5.2 in Section 5.2), which therefore called for some kind of system change. The evaluation also considered production aspects, e.g., potential disturbances. These are shown in Row 4; 35 items fall into this category, some in combination with safety. It can be noted that 70% of not-accepted deviations were related to production problems.

Analysis of proposals

Another comparison concerns proposed improvements. They are more similar than the items above, and they have therefore been analysed a bit further.

The two bottom rows summarise proposed actions. A total of 118 actions were proposed, of which a majority (59%) concerned improvements to the production system. A large portion (41%) referred to a need for some kind of further investigation. A common reason for such investigation was that there was insufficient knowledge about the system, e.g., with regard to computer control. The proposals have been grouped into four main categories:

- Mechanical
- Control system
- Management
- General or other

Table 16.15 provides an overview of the proposals generated in all three rounds of analysis. Clear differences between the methods can be observed. Deviation Analysis generated many proposals for the computer control system. Safety Function Analysis addressed management issues, leading to three times as many suggestions as the two other methods put together.

Table 16.15 Number of proposals in categories of improvements

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

Coverage of the methods

In the choice of analytic methods, central issues are which types of measures they address, and also how results from the methods overlap. This was examined in this case study, and the principle is illustrated in Figure 16.12. Proposals are easier to compare, and the comparison has focused on these.

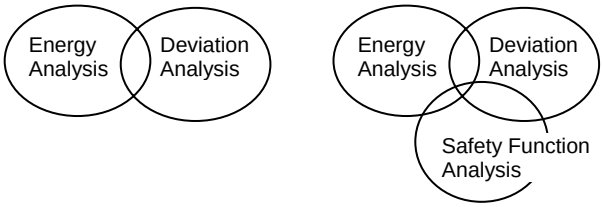


Figure 16.12 Overlap of coverage between methods of safety analysis

Comparing two methods

Energy Analysis and Deviation Analysis were the methods originally selected for the overall safety analysis. Table 16.16 compares the number of proposals from these two methods in various categories. In total, there were 47 proposals, but only 5 were generated independently by both methods.

Table 16.16 Numbers of proposed measures from two methods

Method/Combination	**Category of proposed measures**				
	Mecha-nical	Control system	Mana-gement	General	Total
Energy Analysis only	8	0	0	4	12
Deviation Analysis only	8	12	6	4	30
Both methods	3	1	0	1	5
Total	19	13	6	9	47

Comparing three methods

The set of combinations for all three methods is more complicated. The results are shown in Table 16.17. Eliminating 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. These were connected with emergency equipment, overpressure in the tank, and the blocking of machine movements.

Table 16.17 Number of proposed measures from three methods

Method/combination	**Category of proposed measures**				
	Mecha-nical	Control system	Mana-gement	General	Total
Energy Analysis only	8	0	0	4	12
Deviation Analysis only	8	12	6	4	30
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

Further methods

In addition, other analyses of the system had been performed at the design stage. The first was conducted by the contractor for the tank, who had attached a "*CE label*" to indicate compliance with the Machine Directive of

the European Union (2006). Information about that risk assessment was not available, but obviously this label was not enough to guarantee that the equipment was safe.

At the end of the study, we found that an analysis based on the *What-If* method (Section 12.8) was performed during the design phase by another team. It focused on dust explosions, but also addressed wider issues. This analysis did not result in any proposals for improvement. This meant that a fourth method could be added to the comparison.

Comments

The results can be summarised as follows:

- A large number of improvements (almost 100) were suggested.
- The methods gave clearly different types of results, and the overlap between them was small.
- The What-If analysis did not suggest any improvements.
- Several production improvements were suggested, especially from the application of Deviation Analysis.
- Many needs for improvement of management and organisation were identified; Safety Function Analysis was particularly efficient in identifying such needs.

The findings strongly support the recommendation to use two methods or more to obtain supplementary perspectives in a safety analysis. By comparing the three methods, we can see that:

- Energy Analysis and Deviation Analysis are about equal in finding mechanical improvements.
- Deviation Analysis was best in relation to the control system.
- Safety Function Analysis was best in relation to management issues

These experiences can be useful in choosing method, but it is hard to say how generally valid they are. They are much in line with my practical experiences, but I was surprised by the low overlap. This study is the one that has been most thorough.

17 Concluding remarks

The focus of this book has been on tools for safety analysis, and how they can be used in many different areas, not just in the workplace. The number of methods is large, and more than one hundred have been referred to here. They have to do with investigation of accidents, with analysis of systems, and with evaluation of hazards.

The area might be regarded as intimidating given that there are so many methods. But, in practice, it does not have to be particularly difficult. In many cases, it is enough to be familiar with just a few methods, and planning can be quite easy. When you try out safety analysis for the first time, start with a simple case and do not be overambitious.

Try to start in a rational manner, as has been discussed more thoroughly in chapters 14 and 15:

- Clarify why a safety analysis (or accident investigation) is needed; after that, the aim of the analysis can be defined.
- Consider whether a technical perspective is enough, or whether there is a need also to include human and organisational factors.
- Choose one or two methods that will support you in achieving your goal.
- Choose a methodology for evaluating hazards or setting priorities, when there is a need.

In performing an analysis, it might be useful to work from a variety of perspectives. The examples in Chapter 16 have demonstrated that two or more methods can be combined in order to give a more complete analysis.

I would like to stress one final time that analyses are best conducted in a team. It is advantageous to apply an integrated approach, which means that safety and environmental and production effects are considered in one and the same analysis. This also means that financial arguments can be employed to back up safety proposals.

It is probably only when you have conducted a safety analysis yourself that you recognise the benefits of this way of working. You detect hazards that would otherwise have remained undiscovered. This can be a rewarding and stimulating experience.

18 References

Comment

Web means that the reference is freely available on the Internet. In the electronic version of this book, there are direct links to such reports. The web is dynamic, and the links represent the situation in May 2013. If the link does not work, you can try a web search instead.

A

Amendola, A., Contini,S. and I. Ziomas, I., 1992. Uncertainties in chemical risk assessment: Results of a benchmark exercise. *Journal of Hazardous materials*, Vol. 29, (347-363).

Annet, J. and Stanton, N.A. (eds), 2000. *Task analysis.* Taylor & Francis, London.

Annet, J., Duncan, K.D., Stammers, R.B. and Gray, M.J., 1971. *Task Analysis.* Her Majesty's Stationery Office, London.

Albrechtsen, E. & P. Hokstad, P., 2003. An analysis of barriers in train traffic using risk influencing factors. In Bedford & van Gelder (eds.), *Proceedings ESREL 2003, Safety and Reliability* (25-31).

ARA (Applied Research Associates, Inc.), International Safety Research, Inc., Mac McCall Airport and Aviation Consultants, 2009. *Guidebook for Airport Safety Management Systems* (ACRP 4-05). Web

Aven, T., 2003. *Foundations of Risk Analysis: A Knowledge and Decision-oriented Perspective.* John Wiley and Sons, Ltd.

Aven, T., 2008A *Risk Analysis: Assessing Uncertainties Beyond Expected Values and Probabilities.* John Wiley & Sons, Ltd.

Aven, T., 2008B. *Evaluation of accident risks - Status and trends in risk analysis and evaluation.* Swedish Rescue Services Agency, Karlstad, Sweden. Web

B

Bell, J.B. and Swain, A.D., 1983. *A procedure for conducting a human reliability analysis for nuclear power plants.* U.S. Nuclear Regulatory Commission, Washington.

Bento, J-P., 1999. MTO-analys av händelsesrapporter (in Swedish). OD-00-2 Norwegian Petroleum Directorate, Stavanger, Norway.

Bird, F. & Germain, G., 1985. *Practical Loss Control Leadership.* International Loss Control Institute, Georgia, USA.

Both, R.T., Boyle, A.J., Glendon, A.I., Hale, A.R. and Waring, A.E., 1987. Chase II: The Complete Health and Safety Evaluation Manual for Smaller Organisations. Health and Safety Technology and Management, Birmingham.

Branford, K., 2007. An investigation into the validity and reliability of the AcciMap approach. Unpublished doctoral dissertation, Australian National University, Canberra, Australia.

Branford, K., Naikar, N. and Hopkins, A., 2009. Guidelines for AcciMap analysis. In A. Hopkins (Ed.) *Learning from high reliability organisations*, CCH Australia, (193-212). Sydney, Australia.

British Safety Council, 1988. Five Star Health and Safety Management Audit System. British Safety Council, London.

Brown, D.M. and Ball, P.W., 1980. A simple method for the approximate evaluation of fault trees. *3rd International Symposium on Loss Prevention and Safety Promotion in the process industries.* European Federation of Chemical Engineering.

BSI, 2004. Occupational health and safety management systems – Guide. (British standard BS8800: 2004). British Standards Institution, London.

Bullock, M.G., 1976. *Change control and analysis.* EG&G Idaho Inc, Idaho.

C

Carson W.G. 1979. White collar crime and the enforcement of factory legislation. *British Journal of Criminology*, Vol. 10, (383-398).

Carvalho, F. and Melo, R., 2013. Reliability in Risk Assessment: Evaluation of the Stability and Reproducibility in the use of semi-quantitative assessment methods. *International Symposium on Occupational Safety and Hygiene - SHO 2013*, Guimarães, Portugal, (80-81).

CCPS, 1985. *Guidelines for Hazard Evaluation Procedures.* Center for Chemical Process Safety; American Institute of Chemical Engineers, New York.

CCPS,1993. *Guidelines for Safe Automation of Chemical Industries*. Center for Chemical Process Safety; American Institute of Chemical Engineers, New York.

CCPS, 2011. *Guidelines for Auditing Process Safety Management Systems* (2nd Edition). Center for Chemical Process Safety (CCPS), Wiley, USA (900 p).

Celik, M., Lavasani, S.M., Wang, J. 2010. A risk-based modelling approach to enhance shipping accident investigation. *Safety Science*, Vol. 48, (18-27).

CENELEC, 1999. EN 50126 Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS). European Committee for Electrotechnical Standardization, Brussels.

Chaplin, R. and Hale, A., 1998. An evaluation of the use of the international safety rating system (ISRS) as intervention to improve the organisation of safety. In Hale, A. and Baram, M. (eds): *Safety management - The challenge of change.* Elsevier Science, Oxford.

CISHC, 1977. *A Guide to Hazard and Operability Studies*. Chemical Industry and Safety Council; Chemical Industries Association, London.

Contini, S., Amendola, A. and Ziomas, I., 1991. Benchmark Exercise on Major Hazard Analysis. Commission of the European Communities, Joint Research Centre, ISPRA, Italy.

Cox, L.A., 2008. What's Wrong with Risk Matrices? *Risk Analysis*, Vol. 28, (497 - 511).

D

Dansk standard. 1993. Risk analysis: requirements and terminology. (in Danish) Dansk standard, Copenhagen, Denmark

Dekker, S., 2006. *The field guide to understanding human error.* Ashgate Publishing Co.

DNBIJ, 2006. Guide to Recognition of Accidents. Danish National Board of Industrial Injuries, Denmark. Web

DoD, 2000. Standard practice for system safety; MIL-STD-882D. Department of Defense, USA. Web

DOE, 1999. Conducting Accident Investigations (version 2). U.S. Department of Energy, USA. Web

Duijm, N. J., 2009. Safety-barrier diagrams as a safety management tool. *Reliability Engineering and System Safety*, Vol. 94, (332– 341).

E

Eisner, J. and Leger, J.P., 1988. The international safety rating system in South African mining. *Journal of Occupational Accidents*, Vol. 10**,** (141–160).

European Union, 2006. Directive 2006/42/EC on machinery. Council of the European Communities, Brussels, Belgium. Web

Embrey, D., 1994. *Guidelines for Preventing Human Error in Process Safety*. American Institute of Chemical Engineers, New York.

EN 1050, 1996. European Standard EN 1050:1996 Safety of machinery - Principles for risk assessment. European Committee for Electrotechnical Standardization, Brussels, Belgium.

Energy Institute, 2008. *Guidance on investigating and analysing human and organisational factors aspects of incidents and accidents.* Energy Institute 2008. London. Web

EPA, 2009. Risk management program guidance for offsite consequence analysis. United States Environmental Protection Agency, USA. Web

ESReDA, 2009. *Guidelines for Safety Investigations of Accidents.* ESReDA Working Group on Accident Investigation; European Safety Reliability and Data Association. Web

Eude, M. and M.Lesbats, 2011. Analyser les accidents - Methode de l'arbre des causes. Université Bordeaux, France. Web

EU, 2002. Coding Manual V2000 for Home and Leisure Accidents. European Commision. Web

Eurosafe, 2009 (ed. Bauer R., and Steiner, M.) Injuries in the European Union - Statistics Summary 2005-2007. Eurosafe, Vienna. Web

Evenéus, P., Rollenhagen, C., 2007. In-depth investigation based on a systemic MTO perspective in Vattenfall hydro plants. In: The 4th EADAC Symposium, Chengdu, China, 2007.

F

FAA, 2000. *System Safety Handbook*. Federal Aviation Administration, Washington, DC, USA. Web

Ferry, T.S., 1988. *Modern Accident Investigation and Analysis* (2nd edn). John Wiley & Sons Inc, New York.

Freitag, M., 1999. Structure of event analysis. In Hale, A., Wilpert, B., and Freitag, M. *After the event - From accident to organisational learning.* Pergamon, Oxford, (11-22).

Freud, S., 1914. *Psychopathology of everyday life*. Ernest Benn, London.

G

Gertman, D.I. and Blackman, H.S., 1994. *Human Reliability and Safety Analysis Data Handbook.* John Wiley & Sons, New York.

Gibson, J.J., 1961. Contribution of experimental psychology to the formulation of the problem of safety: a brief for basic research. In *Behaviour Approaches to Accident Research*. Association for the Aid of Crippled Children, New York, (77–89).

Grimaldi, J., 1947. Paper at the ASME standing committee on Safety. Atlantic City, N.J.

Groeneweg, J., 1998. *Controlling the controllable. The management of safety DSWO*. Press, Leiden University, The Netherlands.

Guastello, S.J., 1991. Some further evaluations of the International Safety Rating System. *Safety Science*, Vol.14, **(**253–259).

Guldenmund, F.W., 2000. The nature of safety culture: a review of theory and research. *Safety Science*, Vol. 34 (215-257).

H

Haddon, W. Jr., 1963. A note concerning accident theory and research with special reference to motor vehicle accidents. *Annals of New York Academy of Science*, Vol. 107, (635–646).

Haddon, W. Jr., 1980. The basic strategies for reducing damage from hazards of all kinds. *Hazard Prevention*, Vol. 16, (8–12).

Hale, A., 1999. Introduction: The goals of event analysis. In Hale, A., Wilpert, B., and Freitag, M. *After the event - From accident to organisational learning*. Pergamon, Oxford, (1-10).

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

Hale, A. and Glendon, I., 1987. *Individual behaviour in the control of danger*. Elsevier, Amsterdam.

Hale, A.R., Heming, B.H.J., Carthey, J. and Kirwan, B., 1997. Modelling of safety management systems. *Safety Science*, Vol. 26, (121–140).

Hammer, W., 1972. *Handbook of system and product safety*. Prentice Hall Inc., New Jersey.

Harms-Ringdahl, L., 1982. Riskanalys vid projektering – Försöksverksamhet vid ett pappersbruk. (In Swedish) Royal Institute of Technology, Stockholm.

Harms-Ringdahl, L., 1987. *Säkerhetsanalys i skyddsarbetet – En handledning*. (In Swedish) Folksam, Stockholm. (Original version of this book.)

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*. Balkema, Rotterdam, (1459 -1462). Web

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*. Balkema, Edinburgh, (1373–1378). Web

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

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

Harms-Ringdahl, L., 2003B. Investigation of barriers and safety functions related to accidents. In Bedford, T. and van Gelder, P. (Eds.) *European Safety and Reliability Conference 2003*, Maastricht, The Netherlands. Web

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

Harms-Ringdahl L., 2007. Säkerhetsarbete - innebörd och struktur. (In Swedish) Swedish Rescue Services Agency, Karlstad, Sweden. Web

Harms-Ringdahl, L., 2009. Analysis of safety functions and barriers in accidents. *Safety Science*, Vol. 47, (353–363). Web

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

Harms-Ringdahl, L., Bergqvist, A. and Strömgren, M., 2008. Säkerhetsutredningar av bränder – Fallstudie 1: Stadsgas i lägenhet. (In Swedish) Karlstad university, Karlstad, Sweden. Web

Heinrich, H.W., 1931. *Industrial Accident Prevention*. McGraw-Hill, New York.

Heinrich, H.W., Petersen, D. and Roos, N., 1980. *Industrial Accident Prevention* (5th edn). McGraw-Hill, New York.

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

Henley, J.H. and Kumamoto, H., 1981. *Reliability engineering and risk assessment*. Prentice-Hall Inc., New Jersey.

Hollnagel, E., 1993. *Human Reliability Analysis Context and Control*. Academic Press, London.

Hollnagel, E., 1998. *Cognitive Reliability and Error Analysis Method – CREAM*. Elsevier Science, Oxford, England.

Hollnagel, E., 2000. On understanding risks: Is human reliability a red herring? In Svedung, I. (ed). ESReDa-seminar: *Risk Management and Human Reliability in Social Context*, Karlstad, Sweden.

Hollnagel, E., 2004. *Barriers and Accident Prevention*. Ashgate Publishing, Hampshire, England.

Hollnagel, E., Woods, D. D. and Leveson, N. (eds), 2006. *Resilience engineering: Concepts and precepts*. Ashgate. Aldershot, UK.

HSE, 2008. Five steps to risk assessment. Health and Safety Executive, Great Britain. Web

HSE, 1999. *The event safety guide - A guide to health, safety and welfare at music and similar events*. Health & Safety Executive, HSE BOOKS, Norwich, Great Britain. Web

Hult, P., 2000. MIR Erfarenheter av tillämpning i projektet Botniabanan (in Swedish). Swedish Road Authority (Publication 2000:110), Borlänge, Sweden. Web

Hurst, N.W., Young, S., Donald, I., Gibson, H. and Muyselaar, A., 1996. Measures of safety management performance and attitudes to safety at major hazard sites. *Journal of Loss Prevention in the Process Industries*, Vol. 9, (161-172).

Hult, P. and Harms-Ringdahl, L., 2000. Identifiering och beskrivning av risker - metodik i vägplaneringsprocessen (in Swedish). Swedish Road Authority (Publication 2000:90), Borlänge, Sweden. Web

I

IACS, 2004. A guide to risk assessment in ship operations. International Association of Classification Societies. Web

IAEA, 1994. ASCOT Guidelines: Guidelines for self-assessment of safety culture and for conducting review. International Atom Energy Agency, Vienna, Austria.

IAEA, 2001. Applications of probabilistic safety assessment (PSA) for nuclear power plants. International Atomic Energy Agency,Vienna, Austria. Web

IAEA, 2006. Fundamental safety principles. International Atomic Energy Agency, Vienna, 2006. Web

IAEA, 2007. IAEA Safety Glossary: 2007 Edition. International Atomic Energy Agency, Vienna, Austria. Web

IEC, 1995. Dependability management – Risk analysis of technological systems (IEC 300-3-9). International Electrotechnical Commission, Geneva.

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

ILO, 1988. *Major Hazard Control. A practical manual*. International Labour Office, Geneva.

ILO, 1998. *ILO Encyclopaedia of Occupational health and Safety*. International Labour Organization, Geneva.

ILO, 2001. Guidelines on occupational safety and health management systems. International Labour Office, Geneva. Web

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

ISO, 2001. Risk management –Vocabulary – Guidelines for use in standards (ISO Guide 73:2001). International Organization for Standardization, Geneva, Switzerland. *(Comment: This standard has been replaced by ISO Guide 73:2009; ISO, 2009A).*

ISO, 2009A. Risk management –Vocabulary. (ISO Guide 73:2009). International Organization for Standardization, Geneva, Switzerland.

ISO, 2009B. Risk management – Principles and guidelines (ISO 31000-2009). International Organization for Standardization, Geneva, Switzerland.

ISO, 2009C. Risk management – Risk assessment techniques (ISO/IEC 31010:2009). International Organization for Standardization, Geneva, Switzerland.

J

Jacinto, C., Beatriz, R., Harms-Ringdahl, L., 2013. Safety function analysis in a manufacturing process of paper products. In: Arezes et al (Eds.), *Occupational Safety and Hygiene*, Balkema, Taylor & Francis Group, London, (561-566).

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

K

Kaplan, S., 1997. The Words of Risk Analysis. *Risk Analysis*, Vol. 17, (407 - 417).

Kepner, C.H. and Tregoe, B., 1965. *The rational manager*. McGraw-Hill, New York.

Kohn, L.T., Corrigan, J.M., and Donaldson, M.S.(eds), 2000. *To Err is Human*. Institute of Medicine. National Academy Press, Washington D.C., USA.

Kirwan, B., 1994. *A guide to practical human reliability assessment.* Taylor & Francis Ltd, London.

Kirwan, B. and Ainsworth, L.K. (eds), 1993. *A Guide to Task Analysis*. Taylor & Francis, Washington, D.C., USA.

Kjellén, U., 1984. The deviation concept in occupational accident control – Definition and classification. *Accident Analysis and Prevention*, Vol. 16, (289–306).

Kjellén, U., 2000. *Prevention of accidents through experience feedback*. Taylor & Francis, London.

Kjellén, U. and Hovden, J., 1993. Reducing risks by deviation control – a retrospection into a research strategy. *Safety Science*, Vol.16. (417-438).

Kjellén, U. and Larsson, T.J., 1981. Investigation of accidents and reducing risks – a dynamic approach. *Journal of Occupational Accidents*, Vol. 3, (129-140).

Krug, E. (ed.), 1999. Injury: A Leading Cause of the Global Burden of Disease. World Health Organization, Geneva. Web

Kumamoto, H. and Henley, E.J., 1996. *Probabilistic Risk Assessment and Management for Engineers and Scientists* (2nd edn). IEEE Press, New York.

L

Lauridsen, K., Kozine, I., Markert, F., Amendola, A., Christou, M., and Fiori, M., 2002. Assessment of Uncertainties in Risk Analysis of Chemical Establishments. (Risø-R-1344) Risø National Laboratory, Denmark. Web

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

Leplat, J., 1978. Accident analysis and work analysis. *Journal of Occupational Medicine*, Vol. 1, (331-340).

Leveson, N.G., 2004. A new accident model for engineering safer systems. *Safety Science* 42 (4), (237–270).

M

Markowski,A. & Mannan, S., 2008. Fuzzy risk matrix. *Journal of Hazardous Materials*, Vol. 159, (152-157).

McElroy, F. (ed.), 1974. *Accident Prevention Manual for Industrial Operations* (7th edn). National Safety Council, USA.

N

Nielsen, D.S., 1971. The cause consequence diagram method as a basis for quantitative accident analysis (Report Risö-M-1374). Risö National Laboratory, Denmark.

Nielsen, D.S., 1974. Use of cause-consequence charts in practical systems analysis (Report Risö-M-1743). Risö National Laboratory, Denmark.

Norsk standard, 1991. Requirements for risk analysis. Norges Standardiserings-forbund, Oslo.

NRI, 2009. NRI MORT User's Manual (NRI-1) (Second Edition). Noordwijk Risk Initiative Foundation, Delft, The Netherlands. Web

O

Ozog, 2002. Designing an Effective Risk Matrix. 2002, ioMosaic Corporation, New Hampshire, USA. Web

P

Papazoglou, I.A., and Aneziris, O.N., 2003. Master Logic Diagram: method for hazard and initiating event identification in process plants. *Journal of Hazardous Materials*, Vol. 97, (11–30).

Perrow, C. 1984. *Normal accidents – Living with high-risk technologies.* Basic Books (2nd edn, 1999, Princeton University Press, Princeton, USA).

Pitbaldo, R.M., Williams, J.C. and Slater, D.H., 1990. Quantitative assessment of process safety programs. *Plant Operations Progress*, Vol. 9, (169–175).

R

Rasmussen, J., 1980. What can be learned from human error reports. In Duncan, K.D., Gruneberg, M. and Wallis, D. (eds): *Changes in Working Life*. Wiley & Sons Inc, New York.

Rasmussen, J., 1997. Risk management in a dynamic society: A modelling problem. *Safety Science*, Vol. 27, (183-213).

Rasmussen, J. and Svedung, I., 1997. An Approach to Description of Accident Causation and Identification of Preconditions for Effective Risk Management. Swedish Rescue Services Agency, Karlstad, Sweden.

Rasmussen, J. and Svedung, I., 2000. Proactive risk management in a dynamic society. Swedish Rescue Services Agency, Karlstad, 160 pp. Web

Rausand, M. and Høyland, A. 2004. *System Reliability Theory; Models, Statistical Methods and Applications* (2nd edition). Wiley, New York.

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

Reason, J., 1997. *Managing the Risks of Organisational Accidents*. Ashgate Publishing Ltd, Burlington, VT.

Roed-Larsen, S., Valvisto, T., Harms-Ringdahl, L., and Kirchsteiger, C., 2004. Accident investigation practices in Europe – main responses from a recent study of accidents in industry and transport. *Journal of Hazardous Materials*, Vol. 111, (7-12).

Rollenhagen, C., 2003. *Att utreda olycksfall: teori och praktik.* (In Swedish) Studentlitteratur, Lund, Sweden.

Rollenhagen, C. 2011. Event investigations at nuclear power plants in Sweden: Reflections about a method and some associated practices. *Safety Science*, Vol. 49, (21–26).

Rosness, R. 1998. Risk Influence Analysis. A methodology for identification and assessment of risk reduction strategies. *Reliability Engineering and System Safety*, Vol. 60, (153–164).

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

Rouhiainen, V., 1993. Modelling of accident sequences. In Suokas, J. and Rouhiainen,V. (eds): *Quality Management of Safety and Risk Analysis*. Elsevier, Amsterdam.

Ruuhilehto, K., 1993. The management oversight and risk tree (MORT). In Suokas, J. and Rouhiainen,V. (eds): *Quality Management of Safety and Risk Analysis*. Elsevier, Amsterdam.

S

Salmon, P.M., Cornelissen, M., Trotter, M.J., 2012. Systems-based accident analysis methods: A comparison of Accimap, HFACS, and STAMP. *Safety Science*, Vol. 50, (1158–1170).

Schurman, D.L. and Fleger, A.F., 1994. Human factors in HAZOPS: guide words and parameters. *Professional Safety*, Vol. 39, (32–34).

Schofield, S., 1998. Offshore QRA and the ALARP principle. *Reliability Engineering and System Safety*, Vol. 61, (31–37).

Sklet, S., 2002. *Methods for accident investigation*. Norwegian University of Science and Technology, Trondheim (p 77). Web

Sklet, S., 2004. Comparison of some selected methods for accident investigation. *Journal of Hazardous Materials*, Vol. 111 (29-37).

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

Socialstyrelsen, 2008. Vårdskador inom somatisk slutenvård. Socialstyrelsen, Stockholm, Sweden. Web

Stamatelatos, M., Vesely, W., Dugan, J., Fragola, J. Minarick III, J., Railsback, J., 2002. Fault Tree Handbook with Aerospace Applications. National Aeronautics and Space Administration, Washington, USA. (218 p). Web

Stanton, N. A., Salmon, P. M., Walker, G. H., Baber, C., and Jenkins, D. P., 2005. *Human factors methods: a practical guide for engineering and design*. Ashgate Pub. Co., Aldershot, England.

Strömgren, M., 2009. Manual för AcciMap. Kompendium för kursen Kvalificerad olycksutredningsmetodik (in Swedish). Karlstad University, Karlstad, Sweden.

Strömgren, M., Bergqvist, A., Andersson, R., and Harms–Ringdahl, L., 2013. A process-oriented evaluation of nine accident investigation methods. To be published.

Svedung, I. and Rasmussen, J., 2002. Graphic representation of accident scenarios: mapping system structure and the causation of accidents. *Safety Science*, Vol. 40, (397-417).

Suokas, J. and Rouhiainen, V. (eds), 1993. *Quality Management of Safety and Risk Analysis.* Elsevier, Amsterdam.

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

Svenson, O., 2000. Accident Evolution and Barrier Function (AEB) Method – Manual for Accident Analysis. Swedish Nuclear Power Inspectorate, Stockholm. Web

Swain, A.D. and Guttman, H.E., 1983. *Handbook of human reliability analysis with emphasis on nuclear power plant applications*. U.S. Nuclear Regulatory Commission, Washington DC.

T

Takala, J. 1999. Global estimates of fatal occupational accidents. *Epidemiology.* Vol. 10, (640-646). Web

Taylor, J.R., 1979. A background to risk analysis. Electronics Department, Risö National Laboratory, Denmark.

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

Taylor, J.R., Becher, P., Pedersen, K.E., Kampmann, J., Schepper, L., Kragh, E. and Selig, R., 1989. Quantitative and qualitative Criteria for the Risk Analysis. Danish Environmental Agency, Copenhagen, Denmark.

V

Vesely,W., Goldberg, F., Roberts, N.H., and Haasl, D., 1981. Fault Tree Handbook. (NUREG–0492) Nuclear Regulatory Commission. Washington, USA. (209 p)

W

Wagenaar, W.A., Groeneweg, J., Hudson, P.T.W. and Reason, J. T., 1994. Promoting safety in the oil industry. *Ergonomics*, Vol. 37, (1999–2013).

Wallén Warner, H., Ljung, M., Sandin, J., Johansson, E., & Björklund, G., 2008. Manual for DREAM 3.0, Driving Reliability and Error Analysis Method. Chalmers University of Technology, Gothenburg, Sweden. Web

WHO, 2005. Draft Guidelines for Adverse Event Reporting and Learning Systems. World Health Organization, Geneva, Switzerland . Web

WHO, 2004. Injury surveillance guidelines. World Health Organization. Geneva, Switzerland. Web

WHO, 2012. 10 facts on patient safety. World Health Organization. Geneva, Switzerland. Web

Wilde, G., 1982. The theory of risk homeostasis: implications for safety and health. *Risk Analysis*, Vol.2, (209–225).

19 Index

About the book

This book is about how safety analysis can be practically applied as a tool for accident prevention. The main focus is on qualitative methods, which can be used to analyse systems and to investigate accidents. The book presents more than 40 methods, including techniques for risk evaluation, such as the Risk Matrix. The emphasis is on general methods that can be applied in various contexts, such as industry, production, transport, medicine, and public events.

The planning section discusses the practical aspects of a safety analysis, such as defining its aims and specifying the types of results desired. It also considers arguments for and against specific methods. The examples section presents case studies of accident investigations, and of analyses of systems in different settings.

About the author

Lars Harms-Ringdahl has been engaged in safety as a researcher, consultant and teacher for many years. He works at the Institute for Risk Management and Safety Analysis in Stockholm, and has been professor at the Royal Institute of Technology, Stockholm, and at Karlstad University, Sweden.

Paperback
Available from
shopmybooks.com, or
www.gmlforlag.se

Published by IRS Riskhantering AB
Stockholm, Sweden

www.irisk.se