1

Introduction to Risk Analysis of Fine Chemical Processes

Case History

A multipurpose reactor was protected against overpressure by a rupture disk, which lead directly to the outside through the roof of the plant. During a maintenance operation, it was discovered that this disk was corroded. Although it was decided to replace it, there was no spare part available. Since the next task to be carried out was a sulfonation reaction, it was decided to leave the relief pipe open without the rupture disk in place. In fact, a sulfonation reaction is unlikely to lead to overpressure (sulfuric acid only starts to boil above 300 °C), so such a protection device should not be required. During the first batch a plug of sublimate formed in the relief line. This went unnoticed, and production continued. After heavy rain, water entered the relief tube and accumulated above the sublimate plug. As the next batch began, the plug heated and suddenly ruptured, allowing the accumulated water to enter the reactor. This led to an abrupt exothermal effect, due to the dilution of concentrated sulfuric acid. The increase in temperature triggered sudden decomposition of the reaction mass, causing the reactor to burst, resulting in huge damage.

Lessons Drawn

This type of incident is difficult to predict. Nevertheless, by using a systematic approach to hazard identification, it should become clear that any water entering the reactor could lead to an explosion. Therefore when changing some parts of the equipment, even if they are not directly involved in a given process, especially in multipurpose plants, one should at least consider possible consequences on the safety parameters of the process.

Introduction

Systematic searches for hazard, assessment of risk, and identification of possible remediation are the basic steps of risk analysis methods reviewed in this chapter. After an introduction that considers the place of chemical industry in society, the basic concepts related to risk analysis are presented. Section 1.2 reviews the steps

Thermal Safety of Chemical Processes: Risk Assessment and Process Design,
Second Edition. Francis Stoessel.

of the risk analysis of chemical processes discussed. Safety data are presented in Section 1.3 and the methods of hazard identification in Section 1.4. The chapter closes with a section devoted to the practice of risk analysis.

1.1 Chemical Industry and Safety

The chemical industry, more than any other industry, is perceived as a threat to humans, society, and the environment. Nevertheless, the benefits resulting from this activity cannot be negated: health, crop protection, new material, colors, textiles, and so on. This negative perception is more enhanced after major accidents, such as those at Seveso and Bhopal. Even though such catastrophic incidents are rare, they are spectacular and retain public attention. Thus, a fundamental question is raised: "What risk does society accept regarding the benefits of an activity, of a product?" Such a question assumes that the corresponding risk can be assessed a priori.

In the present chapter, we focus on the methods of risk analysis as they are performed in the chemical industry and especially in fine chemicals and pharmaceutical industries.

1.1.1 Chemical Industry and Society

The aim of the chemical industry is to provide industry and people in general with functional products, which have a precise use in different activities such as pharmaceuticals, mechanics, electricity, electronics, textile, food, and so on.

Thus, on one hand, safety in the chemical industry is concerned with product safety, that is, the risks linked with the use of a product. On the other hand, it is concerned with process safety, that is, the risks linked with manufacturing the product. In this book, the focus is on process safety.

1.1.1.1 Product Safety

Every product between its discovery and its elimination passes through many different steps throughout its history: conception, design, feasibility studies, market studies, manufacturing, distribution, use, and elimination, the ultimate step, where from functional product, it becomes a waste product [1].

During these steps, risks exist linked to handling or using the product. This enters the negative side of the balance between benefits and adverse effects of the product. Even if the public is essentially concerned with the product risks during its use, risks are also present during other stages, that is, manufacture, transportation, and storage. For pharmaceutical products, the major issues are secondary effects. For other products, adverse effects are toxicity for people and/or for the environment, as well as fire and explosion. Whatever its form, once a product is no longer functional, it becomes a waste product and thus represents a potential source of harm.

Therefore, during product design, important decisions have to be made in order to maximize the benefits that are expected from the product and to minimize the

negative effects that it may induce. These decisions are crucial and often taken after a systematic evaluation of the risks. Commercialization is strictly regulated by law, and each new product must be registered with the appropriate authorities. The aim of the registration is to ensure that the manufacturer knows of any properties of its product that may endanger people or the environment and is familiar with the conditions allowing its safe handling and use, and finally safe disposal at the end of the product's life. Thus products are accompanied by a material safety data sheet (MSDS) that summarizes the essential safety information such as product identity, properties (toxicity, ecotoxicity, chemical, and physical properties), information concerning its life cycle (use, technology, exposure), specific risks, protection measures, classification (handling, storage, transportation), and labeling.

1.1.1.2 Process Safety

The chemical industry uses numerous and often complex equipment and processes. In the fine chemical industries (including pharmaceuticals), the plants often have a multipurpose character, that is, a given plant may be used for different products. Inversely a given process may be performed in different plant units, leading to a great number of possible combinations. Moreover, when we consider a chemical process, we must do it in an extensive way, including not only the synthesis itself but also the workup by physical unit operations and finally also storage and transportation. This comprises not only the product but also the raw material.

Risks linked with chemical processes are diverse. As already mentioned, product risks include not only toxicity, flammability, explosion, and corrosion but also additional risks due to chemical reactivity. A process often uses conditions (temperature, pressure) that by themselves may present a risk and may lead to deviations, which can generate critical effects. The plant equipment, including its control equipment, may also fail. Finally, since fine chemical processes are work intensive, they may be subject to human error. Therefore, all of these elements, that is, chemistry, energy, equipment, and operators and their interactions, constitute the object of process safety.

1.1.1.3 Accidents and Risk Perception in Chemical Industry

Despite some incidents, the chemical industry presents good accident statistics. A statistical survey of work accidents shows that chemistry is positioned at the end of the list, classified by order of decreasing lost work days [2] (Table 1.1). Further, only a minor part of these accidents is due to chemical accidents, the greatest part consisting of common accidents such as falls, cuts, and so on that can happen in any other activity.

Another instructive comparison can be made by comparing fatalities in different activities. Here we use the fatal accident rate (FAR) index that gives the number of fatalities for 10^8 h of exposure to the hazard [3, 4]. Some activities are compared in Table 1.2. This shows that even with better statistics in terms of work accidents and fatalities, industrial activities are perceived as presenting higher risks. This may essentially be due to the risk perception. The difference in perception is that for traveling or sporting activities, the person has the choice

Table 1.1 Accidents at work in different activities in Switzerland, from the statistics of the Swiss National Accident Insurance (2016).

Activity	Work accidents for 1000 insured
Construction	155
Agriculture	138
Metallurgy	112
Wood	107
Terrestrial transport	81
Rubber, plastics	78
Restaurants	75
Food	67
Machinery	56
Energy	51
Offices, administration	43
Textile	41
Electrical equipment	34
Chemistry	31

Table 1.2 Some values of the FAR index for different activities.

Industrial activities	FAR	Non industrial activities	FAR
Coal mining	7.3	Alpinism	4000
Construction	5	Canoe	1000
Agriculture	3.7	Motor bike	660
Chemistry	**1.2**	Travel by air	240
Vehicle manufacturing	0.6	Travel by car	57
Clothing manufacturing	0.05	Travel by railway	5

whether to be exposed or not, whereas for industrial activities, exposure to risk may be imposed. Industrial risks may also impinge on people who are not directly concerned with the activity. The pressure wave or toxic release may impact people living in the vicinity of a chemical plant. The lack of information on what goes on in an industrial site or the lack of technical knowledge induces a fear from the unknown and biases the risk perception [5].

1.1.2 Responsibility

In industrial countries, employers are responsible for the safety of their employees. On the other hand, legal texts often force the employees to apply the safety rules prepared by employers. In this sense, the responsibility is shared.

Environment protection is also regulated by law. Authorities publish threshold limits for pollutants and impose penalties in cases these limits are surpassed. In the European Union, the Seveso directive regulates the prevention of major accidents: if dangerous substances are used in amounts above prescribed limits, industries have to perform a risk analysis describing quantitatively the possible emissions and their effect on the neighboring population. They also have to provide emergency plans in order to protect that population.

In what concerns process safety, the responsibility is shared within the company by the management at different levels. The health safety and environment staff plays an essential role in this frame; thus during process design, safety should have priority (see Chapter 18).

1.1.3 Definitions and Concepts

1.1.3.1 Hazard

Hazard is defined by the European Federation of Chemical Engineering (EFCE) [6] as:

> A situation that has the potential to cause harm to human, environment and property.

Thus, hazard is the antonym of safety. For the chemical industry, the hazard results from the simultaneous presence of three elements:

1. A threat stemming from the properties of processed substances, chemical reactions, uncontrolled energy release, or from equipment.
2. A failure that may be of technical origin or stem from human error, either during the operation or during process design. External events, such as weather conditions or natural catastrophe, may also be at the origin of a failure.
3. An undetected failure in a system as non-identified hazards during risk analysis, or if insufficient measures are taken, or if an initially well-designed process gradually deviates from its design due to changes or lack of maintenance.

1.1.3.2 Risk

The EFCE defines risk as a *measure* of loss potential and damage to the environment or persons in terms of probability and severity. An often-used definition is that risk is the product of severity time probability:

$$\text{Risk} = \text{Severity} \times \text{Probability} \tag{1.1}$$

In fact, considering risk as the product is somewhat restrictive: it is more general to consider it as a combination of the terms severity and probability. Thus the risk is linked to a defined incident scenario that must first be identified and described with the required accuracy, in order to be evaluated in terms of severity and probability of occurrence. The severity is measured on the effects, that is, consequences and impact of a potential accident on people, environment, assets, business continuity, and company image. The probability of occurrence is often replaced by the frequency expressed as one incident in a given time.

1.1.3.3 Safety

Safety is a quiet situation resulting from the real absence of any hazard [7].

Absolute safety (or zero risk) does not exist for several reasons: first, it is possible that several protection measures or safety elements can fail simultaneously; second, the human factor is a source of error, and a person can misjudge a situation or have a wrong perception of warning signs, or may even make an error due to a moment's inattention.

1.1.3.4 Security

In common language, security is a synonym of safety. In the context of this book, security is devoted to the field of property protection against theft or incursion.

1.1.3.5 Accepted Risk

The accepted risk is a risk inferior to a level defined in advance either by law, technical, economical, or ethical considerations. The risk analysis, as it will be described in the following Sections 1.2–1.4, has essentially a technical orientation. The minimal requirement is that the process fulfills requirements by the local laws and that the risk analysis is carried out by an experienced team using recognized methods and risk-reducing measures that conform to the state of the art. It is obvious that nontechnical aspects may also be involved in the risk acceptation criteria. These aspects should also cover societal aspects, that is, a risk–benefit analysis should be performed.

1.2 Steps of Risk Analysis

A risk analysis is not an objective by itself, but is one of the elements allowing the design of a technically and economically efficient chemical process [1]. In fact, risk analysis reveals the process inherent weaknesses and provides means to correct them. Thus, risk analysis should not be considered as a "police action," in the sense that, at the last minute, one wants to ensure that the process will work as intended. Risk analysis rather plays an important role during process design. Therefore, it is a key element in process development, especially in the definition of process control strategies to be implemented. A well-driven risk analysis leads not only to a safe process but also to an economic process, since the process will be more reliable and give rise to less productivity loss.

There are many risk analysis methods, but all have three steps in common:

1. Hazard identification.
2. Risk assessment.
3. Definition of risk-reducing measures.

If these three steps are at the heart of the risk analysis, it is also true that performing these steps requires preliminary work and other steps that should not be bypassed [1, 8].

By systematically studying past incidents in the chemical industry, several causes can be identified. These are summarized in Table 1.3.

Table 1.3 Causes of incidents and their remediation.

Causes	Remediation
Lack of knowledge concerning the properties of material and equipment, the reactivity, the thermal data, etc.	Collection and evaluation of process data, physical properties, safety data, thermal data. Definition of safe process conditions and critical limits
Non-identified deviation or failure	Systematic search for deviations from normal operating conditions
Wrong risk assessment (misjudgment)	Interpretation of data, clearly defined assessment criteria, professional experience
No adequate measures provided	Process improvement, technical measures
Measures neglected	Plant management, management of change

Thus, the risk analysis must be well prepared, meaning that the scope of the analysis must be clearly defined; data must be available and evaluated to define the safe process conditions and the critical limits. Then, and only then, the systematic identification of process deviations from the safe conditions can be started. The identified deviations lead to the definition of scenarios, which can be assessed in terms of severity and probability of occurrence. This work can advantageously be summarized in a risk profile, or risk matrix, enhancing the major risks that are beyond the accepted limits. For these risks, reduction measures can then be defined. The residual risk, that is, the risk remaining after implementation of the measures, can be assessed as before and documented in a residual risk profile showing the progress of the analysis and the risk improvement. These steps are reviewed in the next Sections 1.2.1 through 1.2.8.

1.2.1 Scope of Analysis

The scope of the analysis aims to identify the process under consideration in its frame: the plant it will take place in, and the chemicals with which it will be performed. The chemical reactions and unit operations must be clearly characterized, and the technological environment must be defined: utilities, peripheral equipment like waste treatment, personnel and its skills, automation, and also regulatory requirements [9].

In this step, it is also important to check for interface problems with other plant units. As an example, when considering raw material delivery, it can be assumed that the correct raw material of the intended quantity and quality is delivered from a tank farm. Thus, it can be referred to the tank farm risk analysis, or the tank farm is to be included in the scope of the analysis. Similar considerations can be made for utilities, to ensure that the appropriate utility is delivered. Nevertheless, loss of utility must be considered in the analysis, but it will be assumed that if, as an example, nitrogen is required, nitrogen will be delivered. This allows checking for non-analyzed items in a whole plant, completing the analysis.

At this stage, the depth of the analysis, meaning the degree of details must also be defined. The required depth often depends on the stage of the process in its development: for new processes at early development stages, a preliminary hazard analysis is often sufficient: here only global risks as fire, explosion, and exposure to toxic material are considered. Later on, once the process and the plant are defined or in the design stage, a detailed analysis can be performed.

1.2.2 Safety Data Collection

The required data must be collected prior to the risk analysis. This can be done gradually during process development as the knowledge on the process increases. The data can be summarized on data sheets devoted to different aspects of the process. They typically should encompass the following:

- Involved chemical compounds
- Chemical reactions
- Technical equipment
- Utilities
- Operators (shift organization and skills)

The required data are reviewed in detail in Section 1.4. In order to be economic and efficient, the data collection is accompanied by their interpretation in terms of risks. This allows adapting the amount and accuracy of the data to the risk. This procedure is illustrated with the example of thermal data collected following a cooling failure scenario (see Section 3.2.1).

1.2.3 Safe Conditions and Critical Limits

Once the safety data have been collected and documented, they must be evaluated with regard to the process conditions in terms of their significance for process safety. With the interpretation of the safety data, the process conditions that provide safe operation and the limits that should not be surpassed become clear. This defines the critical limits of the process, which are at the root of the search for deviations in the next step of the risk analysis.

This task should be performed by professionals having the required skills. Practice has shown that it is advantageous to perform, or at least to review, the interpretation with the risk analysis team. This ensures that the whole team has the same degree of knowledge and understanding of the process features.

1.2.4 Identification of Deviations

During this step, the process is considered in its future technological environment, that is, the plant equipment, the control systems including the operators, and the delivery of raw material. The utilities are included in the critical examination of deviations from normal operating conditions. Here the following fields may be distinguished:

- Deviations from operating mode, which are a central part in batch processes.

- Technical failures of equipment, such as valves, pumps, control elements, and so on, which represent the central part of the equipment-oriented risk analysis.
- Deviations due to external causes, such as climatic impacts (frost, flooding, storms).
- Failure of utilities, especially electrical power or cooling water.

With continuous processes, different stages must be considered: steady state, start up and shut down, emergency stops, and so on.

The methods for search of hazards can be classified into three categories [8, 10, 11]:

1. Intuitive methods, such as brainstorming.
2. Inductive methods, such as checklists, failure mode and effect analysis (FMEA), event trees, decision tables, and analysis of potential problems (APP). These methods proceed from an initial cause of the deviation and construct a scenario ending with the final event. They are based on questions of the type: "What if?"
3. Deductive methods, such as the fault tree analysis (FTA) that proceeds by starting from the top event and looking for failures that may cause it to happen. These methods are based on questions of the type: "How can it happen?"

Some examples of those methods, commonly used for hazard search in chemical processes, are presented in Section 1.5.

The triggering mechanism to make a real threat out of a potential threat is called the cause. Each potential threat can have several potential causes, which should preferably be handled in different scenarios. The possible consequences of a triggered event are referred to as the effects. This description of hazard causes and effects build an event scenario. Here it is important to clearly structure the scenario: each scenario has an initiating event and may require one or several enabling events to achieve the final consequences. As an example, a leakage must not result in a fire, for this the leak may be the initiating event but requires enabling events as the presence of an ignition source to cause a fire.

It must be ensured that the scenario is developed until its final causes. As an example a loss of containment cannot represent the final consequence: a loss of containment may result in exposure of the personnel to toxic material or may result in a fire or on an explosion that may have the potential for injuries or even fatalities.

The listing of the scenarios in a table with an identifier, a short description of possible causes and the consequences, makes up the hazard catalog. The table may also contain risk assessment, a description of risk-reducing measures, assessment of residual risk, and who is responsible for the action decided on. This is of great help for the follow-up of the project. An example of such a hazard catalog is presented in Figure 1.1.

1.2.5 Risk Assessment

The deviation scenarios found in the previous step of the risk analysis must be assessed in terms of risk, which consists of assigning a level of severity and probability of occurrence to each scenario. Before starting the assessment, the team

Id	Hazard	Trigger	Effects	Risk 1		Measures	Status	Responsible	Risk 2	
				S	P				S	P

Figure 1.1 Example of hazards catalog with deviation causes effects and actions decided by the team as well as their status.

must clearly define at which state the scenario is assessed. In principle there are three possible states:

- The first possibility is the so-called raw risk, which means that the scenario is assessed without any risk-reducing measure. This has the advantage to show the real risk potential of the scenario.
- The second possibility is to assess the scenario taking into account the measures already in place. This type of assessment only reveals the remaining risks if no additional safeguards are applied.
- The third possibility is to assess the scenario with all measures in place, the already implemented and the additional measures required to reduce the risk to the acceptable or at least tolerable level. An assessment performed in this state in fact analyzes the residual risk or the goal to be met after the risk analysis.

It is advisable to report the raw risk in the cells "Risk 1" in Figure 1.1 and residual risk in the cells "Risk 2" in Figure 1.1.

This assessment is qualitative or semiquantitative, but rarely quantitative, since a quantitative assessment requires a statistical database on failure frequency, which is difficult to obtain for the fine chemicals industry with such a huge diversity of processes. The severity is clearly linked to the consequences of the scenario or to the extent of possible damage. It may be assessed using different points of view, such as the impact on humans, the environment, property, the business continuity, or the company's reputation. Table 1.4 gives an example of such a set of criteria. In order to allow for a correct assessment, it is essential to describe the scenarios with all their consequences. This is often a demanding task for the team, which must interpret the available data in order to work out the consequences of a scenario, together with its chain of events.

The probability of occurrence (P) is linked to the causes of the deviations. It is often expressed as frequency (f), referring to an observation period (T) often of 1 year:

$$P = f \cdot T \Rightarrow f = \frac{P}{T} \tag{1.2}$$

Table 1.4 Example of assessment criteria for the severity.

Category	1. Negligible	2. Marginal	3. Critical	4. Catastrophic
Life/health in company	Injury without lost workdays	Injury with lost work days	Injury with irreversible effects	One or more Fatalities
Life/health outside company	Complaints about bad smell	First aid cases	Severe injuries	Fatality
Environment	Only short-term on-site effects	Effect on water treatment plant	Spill outside site, recovery within 1 month	Long-term pollution of water, soil
Property	Cleaning up	Production line to be repaired	Loss of production line	Loss of plant
Business continuity	Short-term repair without production loss	Production stopped over 1 week	Delivery interrupted several weeks	Business interruption more than 6 months
Image	No report outside company	Report in local media	Report in national media	Impinge the company survival

In this case, a probability of 0.01 is equivalent to an occurrence of one incident in 100 years. An example of evaluation criteria for the probability is given in Table 1.5. There are two approaches for the assessment of probability: one is the qualitative approach, based on experience and using analogies to similar situations. The other is the quantitative approach, based on statistical data obtained from equipment failure databases [4]. These data were mainly gathered from the petrochemicals industry and bulk chemical industry, working essentially with dedicated plant units. For the fine chemicals and pharmaceutical industries, where the processes are carried out in multipurpose plants, this approach is more difficult to use. This is because the equipment may work under very different conditions from process to process, which obviously has an impact on its reliability. An efficient strategy is to use a frequency to characterize the initiating event and to multiply by the probability of consecutive events. This strategy is developed in Chapter 17.

The quantitative analysis must be based on a method, to allow for the identification of the interactions between different failures. Such a method, such as the FTA, is presented in Section 1.4.6. To get a better idea of the probability, a semiquantitative approach consists of listing the logical relationships between the different causes. This allows identifying if the simultaneous failure of several elements is required to obtain the deviation and gives access to a semiquantitative assessment.

The criteria mentioned in Tables 1.4 and 1.5 are given as an example of a possible practice, but as a part of the company's risk policy, they must be defined for each company with respect to its actual situation. Severity and frequency of occurrence of an event form the two coordinates of the risk profile.

Table 1.5 Example of qualitative assessment criteria for the frequency.

Category		Qualitative description	Frequency	Definition/examples for initiating events
A	Frequent	Happens frequently, often experienced	>1/10a	Loss of utilities (without backup), control loop with complex sensor, exposure during handling of liquid or solid chemicals, corrosion hole on flexible hose
B	Moderate	Happened or was experienced several times	≤1/10a >1/100a	Failure on demand of control loop with simple sensor, of valve, pump, single mechanical seal, nonreturn valve fails open
C	Occasional	Happened or was experienced once	≤1/100a >1/1000a	Failure of redundant control loop, of double mechanical seal with alarm, check valve internal leak
D	Remote	May happen or be experienced	≤1/1000a >1/10 000a	Leakage at reactor or tank jacket, valve minor leak, pipe leak
E	Unlikely	Cannot be excluded but never happened yet	≤1/10 000a >1/100 000a	Valve: major leak, pipe rupture
F	Almost impossible	It is very unlikely that this will be experienced	≤1/100 000a	Heavy earthquake, aircraft impact

1.2.6 Risk Matrixes

Risk assessment is not an objective by itself, but represents the required step for the risk evaluation. This is the step whereby it is decided if a risk is acceptable, or if it should be reduced by appropriate measures. This is usually done by comparing the risk to acceptance criteria defined in advance. This can be done graphically by using a risk diagram or risk matrix, as the example presented in Figure 1.2. The identifiers characterizing the different scenarios can be placed into the matrix, thus allowing a visual risk evaluation. Such a risk diagram should comprise at least three zones corresponding to the clearly negligible or acceptable risk (white in Figure 1.2), unacceptable risk (dark gray in Figure 1.2), a third zone (light gray in Figure 1.2) is also used [12, 13]. This third zone corresponds to undesirable risk that is tolerable only if risk reduction is impracticable or the costs are grossly disproportionate to the improvement gained. This practice corresponds to the as low as reasonably practicable (ALARP) principle [14–16]. The borderline separating the white zone from the others is called the protection level: this is the limit of accepted risks and represents an important decision for the risk policy of a company.

The risk matrix presented in Figure 1.2 is based on Tables 1.4 and 1.5 and defines a 4×6 matrix. Experience has shown that choosing too narrow a matrix,

Frequent				
Moderate				
Occasional				
Remote				
Unlikely				
Almost impossible				
	Negligible	Marginal	Critical	Catastrophic

Figure 1.2 Example risk diagram with unacceptable risk in dark gray, undesirable risk in light gray, and accepted risk in white.

for example, a 3×3 matrix, with the levels low, medium, and high, has the drawback of being too rough. It is unable to show the improvement of a risk situation especially with high severities, since such a situation often remains with high severity and low probability, even if additional measures are defined. On the other hand, too precise a matrix is not useful for risk evaluation and may lead to tedious discussions during its assessment [17].

The 4×6 matrix presents some advantages:

- Six frequency categories allow for an accurate representation of risk reduction with steps by one order of magnitude between successive categories, each step representing a risk reduction factor of 10.
- The low frequency category $f \leq 1/100\,000$ a corresponds to common tolerance criteria for fatalities. Several fatalities occurring in 10 000 years would not be tolerated.
- The high frequency categories allow for discriminating between events occurring often (every several years) like power failure and typical technical failures occurring every 10 years or less.

1.2.7 Risk-Reducing Measures

If the risk linked to a scenario falls into the unacceptable field, it must be reduced by appropriate risk-reducing measures. These are usually classified following two viewpoints, the action level and the action mode. The action level can be elimination of the hazard, risk prevention, or mitigation of the consequences. For the action mode, different means can be used: technical measures that do not require any human intervention or organizational measures that require human intervention and are accompanied by procedural measures defining the operating mode of the measure. Some examples are given in Table 1.6.

Eliminating measures are the most powerful since they avoid the risk, meaning that the incident can simply not occur or at least they strongly reduce the

Table 1.6 Example of measures classified following their action level and their action mode.

	Elimination	Prevention	Mitigation
Technical	Alternative synthesis route	Alarm system with automatic interlock	Emergency pressure relief system
Organizational	No operator in hazardous field	Control by operators	Emergency services
Procedural	Access control	Instruction for behavior in abnormal situations	Instruction for emergency response

severity of the consequences of an eventual incident. This type of measures was especially promoted by Trevor Kletz in the frame of the development of inherently safer processes [18–20]. For a chemical process, eliminating the risks can mean that the synthesis route must be changed avoiding instable intermediates, strongly exothermal reactions, or highly toxic material. The choice of the solvent may also be important in this frame, the objective being to avoid flammable, toxic, or environmentally critical solvents. Concerning runaway risks, an eliminating measure aims to reduce the energy potential in such a way that no runaway can take place.

Preventive measures provide conditions where the incident is unlikely to happen, but its occurrence cannot be totally excluded. In this category, we find measures such as inventory reduction for critical substances, the choice of continuous rather than batch process leading to smaller reactor volumes, and a semi-batch rather than a full batch process providing additional means of reaction control. Process automation, safety maintenance plans, etc. are also preventative measures. The aim of these measures is to avoid triggering the incident and thus reducing its frequency of occurrence. In the frame of runaway risks, a runaway remains theoretically possible, but due to process control, its severity is limited and the probability of occurrence reduced, such that it can be controlled before it leads to a critical situation.

Mitigation measures have no effect on triggering the incident, but avoid it leading to severe consequences. Examples of such measures are emergency plans, organization of emergency response, and explosion suppression. In what concerns runaway reactions, they may be triggered, but their impact remains limited, for example, by a blow down system that avoids toxic or flammable material escaping to the environment.

Technical measures are designed in such a way that they require no human intervention, nor need to be triggered or executed. They are designed to avoid human error (in their action, but not in their design!). Technical measures are often built as automated control systems, such as interlocks or safety trips. In certain instances, they must be able to work under any circumstances, even in the case of utility failure. Therefore, great care is required in their design, which should be simple and robust. Here the simplification principle of inherent safety, the Keep It Simple and Safe (KISS) principle, should be followed. Depending on

the risk level, they must also present a certified high degree of reliability. This is described in the international standard IEC 61511 [15] that advises on the different safety integrity levels (SILs) with the required reliability as a function of the risk (see Chapter 17).

Organizational measures are based on human action for their performance. In the fine chemicals and pharmaceutical industries, reactor-charging operations are often manual operations, and the product identification relies on the operator. In this context, quality systems act as support to safety, since they require a high degree of traceability and reliability. Examples of such measures are labeling, double visual checks, response to acoustic or optical alarms, in process control, and so on. The efficiency of these measures is entirely based on the discipline and instruction of the operators. Therefore, they must be accompanied by programs of instructions, where the adequate procedures are learned in training.

During the risk analysis, the measures must be accurately described to establish terms of reference, but no detailed engineering must be done during the analysis. It is also advisable to define a responsible person for the design and establishment of these measures.

1.2.8 Residual Risk

This is the last step of risk analysis. After having completed the risk analysis and defined the measures to reduce risks, a further risk assessment must be carried out to ensure risks are reduced to an accepted level. However the risks cannot be completely eliminated: risk zero does not exist; thus a residual risk remains. This is also because only identified risks were reduced by the planned measures. Thus, the residual risk has three components:

1. The consciously accepted risk.
2. The identified, but misjudged risk.
3. The unidentified risk.

Thus, a rigorous and consciously performed risk analysis should reduce both of the last components. This is the responsibility of the risk analysis team. Hence, it becomes obvious that risk analysis is a creative task that must anticipate events, which may occur in the future and has the objective of defining means for their avoidance. This may also be seen in difference to laws that react on events from the past. Therefore, it is a demanding task oriented to the future, which requires excellent engineering skills.

At this stage, a second risk diagram can be constructed, in a similar way to that shown in Section 1.3.6. This allows the identification of the risks that are now strongly reduced, and thus the measures, which require special care in their design, should perhaps be submitted to a reliability analysis, as described in Chapter 17.

1.3 Safety Data

In this section, a safety dataset, resulting from over 30 years of practical experience with risk analysis of chemical processes, is presented. These data build

the base of risk analysis in the fine chemicals and pharmaceutical industries, essentially in multipurpose plants. Therefore, the dataset introduces plant considerations only at its end. This allows exchanging them without any need for recollecting the whole dataset, in cases where the process is transferred from one plant unit to another. Moreover, this dataset may be used in the frame of different risk analysis methods.

There are many different sources for safety data, such as MSDS, databases [21–23], company databases, and reports. Great care is required, when using MSDS, since experience has shown that they are not always reliable.

The safety data used in risk analysis can be grouped into different categories, described in the following Sections 1.3.1 through 1.3.6. The data should be provided for raw material, intermediates, and products, as well as for reaction mixtures or wastes as they are to be handled in the process. Missing data, important in risk analysis, may be marked with a letter "I" in the appropriate field of the table to indicate that this information is missing or as a default by a letter "C" if its value is unknown but judged to be critical.

1.3.1 Physical Properties

Physical properties such as melting point, boiling point, and vapor pressure, as well as densities and solubility in water, are especially important in the case of a release, as well as giving important restrictions to the process conditions. For instance, the melting point may indicate that the contents of a stirred vessel solidify below this temperature. This gives a lower limit to the heating or cooling system temperature, which would forbid using an emergency cooling system. In a similar way, the vapor pressure may define an upper temperature limit if a certain pressure level is not to be surpassed. Densities may also indicate what the upper and lower phase in a mixture is. Solubility in water is important in case of spillage.

1.3.2 Chemical Properties

The chemical properties allow summarizing observations or experiences made during process development or previous production campaigns. The following characteristic chemical properties should be identified during the risk analysis: acidity, autoignition temperature, pyrophoric properties, reaction with water, light sensitivity, air sensitivity, and storage stability. Further, impurities in the product may affect the toxic and ecotoxic properties of substances or mixtures.

1.3.3 Toxicity

The odor limit compared with other limits may indicate an early warning of a leak, but this practice is not recommended since odor perception is individual and consequently varies for different people. Therefore more reliable and reproducible limits are used in the industrial practice.

The maximum allowed workplace concentration (MAC) is the maximum allowed average concentration expressed in $mg\,m^{-3}$ of a gas, vapor, or dust

in air in a workplace, which has no adverse effects on health for an exposure of $8\,h\,d^{-1}$ or $42\,h\,wk^{-1}$ for the majority of a population [24]. Since it is an average, maintaining the concentration below this value does not guarantee no effects, since the sensitivity may differ within a population. On the other hand, a short-term exposure to a concentration above MAC does not imply consequences on health.

A distinction should be made between acute toxicity and chronic toxicity. For acute toxicity, the following indicators may be used:

- Lethal dose LD_{50}: Gives the amount of a toxin that caused 50% of fatalities within five days in an animal population exposed once to the amount. It may be an oral or dermal exposure and is expressed in $mg\,kg^{-1}$ of organism with a specification of the test animal used.
- Lethal concentration LC_{50}: Is the concentration in air that caused 50% of fatalities within five days in a test in an animal population exposed to this concentration. It is through inhalation and is expressed in $mg\,kg^{-1}$ of organism with a specification of the test animal used.

The lethal dose (LD_{50}) and threshold concentration (TC_{50}) for humans would be more directly applicable but, for obvious reasons, only very sparse data are available:

- The toxic dose lowest (TDL_0 oral) is the lowest dose that induced diseases in humans by oral absorption.
- The toxic concentration lowest (TCL_0 oral) is the lowest concentration in the air that induced diseases in humans by inhalation.

More qualitative indicators are also useful: absorption through healthy skin, irritation to skin, eyes, and respiratory system, together with sensitization with the following indicators: carcinogenic, mutagenic, teratogenic, reprotoxic, and so on. These properties can be summarized by indication of a toxicity class.

To judge the effect of short-term exposure, such as during a spillage, the short-term exposure limit (e.g. IDLH, immediately dangerous to life and health) can be used. The different levels given by the Acute Exposure Guideline Levels (AEGLs), issued by the US Environmental Protection Agency, may also be used in this frame. The data are not given as a single value, but as a table with different severity levels and exposure durations. An example is given in Table 1.7. The severity levels are defined as follows [22, 23, 25]:

AEGL 1 is the airborne concentration (expressed as parts per million or milligrams per cubic meter [ppm or $mg\,m^{-3}$]) of a substance above which it is predicted that the general population, including susceptible individuals, could experience notable discomfort, irritation, or certain asymptomatic, nonsensory effects. However, the effects are not disabling and are transient and reversible upon cessation of exposure.

AEGL 2 is the airborne concentration (expressed as ppm or $mg\,m^{-3}$ of a substance) above which it is predicted that the general population, including susceptible individuals, could experience irreversible or other serious, long-lasting adverse health effects or an impaired ability to escape.

Table 1.7 AEGL data for acetone, concentrations in ppm.

Severity level	10 min	30 min	60 min	4 h	8 h
AEGL 1	200	200	200	200	200
AEGL 2	9 300	4 900	3 000	1 400	950
AEGL 3	16 000	8 600	5 700	2 500	1 700

AEGL 3 is the airborne concentration (expressed as ppm or mg m^{-3}) of a substance above which it is predicted that the general population, including susceptible individuals, could experience life-threatening health effects or death.

The use of carcinogenic material should be avoided as far as possible, by replacement with nontoxic or at least less toxic substances. If their use cannot be avoided, appropriate technical and medicinal measures should be applied in order to protect the workers from their effects. Among such measures, the reduction of the exposure in terms of concentration and duration as well as a medical follow-up may be required. The exposure can be limited by using closed systems, avoiding any direct contact with the substance, or personal protection equipment. Moreover, the number of exposed operators should be limited.

1.3.4 Ecotoxicity

In instances of spillage or release, not only humans may be concerned, but also the damage may also affect the environment. In order to assess these risks, the following data are required:

- Biological degradability
- Bacteria toxicity (IC_{50})
- Algae toxicity (EC_{50})
- Daphnia toxicity (EC_{50})
- Fish toxicity (LC_{50})

The $P_{o/w}$, that is, the distribution coefficient between octanol and water, indicates a possible accumulation in fat. Malodorous or odor intense compounds should also be indicated.

The symbol LC_{50} means lethal concentration for 50% of a test population. The symbol EC_{50} means efficiency concentration for mobility suppression of 50% of a test population. The symbol IC_{50} means inhibition concentration for 50% of a population in a test for respiratory suppression.

1.3.5 Fire and Explosion Data

The most common property in the assessment of fire hazards is the flashpoint that is applicable to liquids or melts and is the lowest temperature at which the vapor above the substance may be ignited and continue to burn. The reference pressure for the flashpoint is 1013 mbar.

The combustion index is applicable to solids and gives a qualitative indication about combustibility, ranging from one to six. Index 1 corresponds to no

combustion and Index 6 to a violent combustion with fast propagation. From Index 4, the combustion propagates through to the solid.

Electrostatic discharging may provide an ignition source for the explosion of a gas, vapor, or dust cloud. Electrostatic charging can occur only if a separation process is involved. Since this is a frequent phenomenon as soon as a product is in motion, separation processes are common in chemical processes, during pumping, agitation, pneumatic transport, and so on. Charge accumulation occurs when the conductivity is too low to allow charge relaxation. This may lead to an electrostatic discharge that may ignite an explosive atmosphere if present at the same time. For this to occur, the concentration of combustible must be in a given range, and oxygen must be present. In order to assess such situations, the explosion characteristics are required.

Explosion limits indicate in which concentration range a mixture of combustible substance can be ignited. For the combustible substance, there are two limits, the lower explosion limit (LEL), below which the concentration is too low to produce an explosion, and the upper explosion limit (UEL), above which the oxygen is in default and no explosion occurs. Concerning the oxygen, the limiting oxygen concentration (LOC) is useful for designing an inerting procedure. Further, the explosion is characterized by the maximum explosion pressure and its violence by the maximum pressure increase rate. In order to decide if an explosion can be ignited, the minimum ignition energy (MIE) is required. For dust explosions, temperature limits are defined as the hot surface ignition temperature of a dust layer (LIT, layer ignition temperature) and the minimum ignition temperature (MIT) of a dust cloud.

The self-sustaining decomposition (also called deflagration) is a phenomenon whereby the decomposition is initiated by a hot spot and then propagates through the solid with a velocity of some millimeters to centimeters per second. In difference to combustion, the decomposition does not require oxygen, so it cannot be avoided by using an inert atmosphere (see Section 13.2.7).

The shock and friction sensitivity of a solid is also an important parameter, especially when it is to be submitted to mechanical stress during processing.

1.3.6 Interactions

The reactivity of chemicals used in a process must be assessed, since these chemicals may become in contact in a desired way or accidentally during the process. These interactions are usually analyzed in a triangular matrix where the desired and undesired reactions are marked at the intersection of each row and column. Beside chemicals or mixtures, the different fluids (i.e. heat carrier), waste streams, and construction materials must also be considered. An example of such a matrix, summarizing the safety data and the interactions, is represented in Figure 1.3.

1.4 Systematic Identification of Hazards

In this section, a selection of commonly used hazard identification techniques is presented. These techniques can be used in the fine chemicals and pharmaceutical industries. The methods presented here are designed to

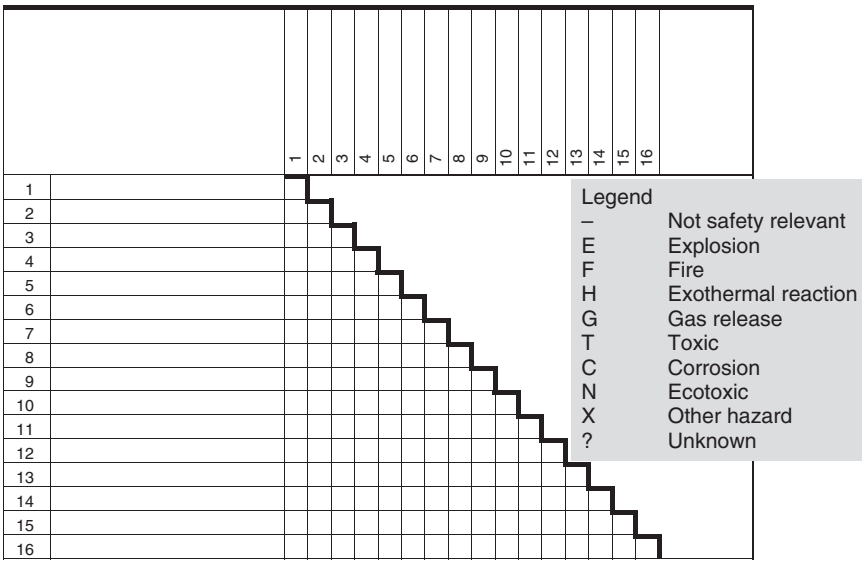

Figure 1.3 Interaction matrix, also called hazard matrix, summarizing the safety data of chemicals involved in a process.

provide a systematic search for hazards with the final objective of providing a comprehensive analysis.

1.4.1 Checklist Method

The checklist method is based on past experience. The process description, the operating mode, is screened using a list of possible failures or deviations from this particular operating mode. Thus, it is obvious that the quality and comprehensiveness of the checklist directly govern its efficiency. Indeed, the experience of the authors confirms that the checklist is essential [26]. This method is well adapted to discontinuous processes as practiced in the fine chemicals and pharmaceutical industries, where processes are often performed in multipurpose plants. The basic document for the hazard identification is the process description, also called operating mode. For an efficient analysis, it is advisable to group several process steps into sequences in order to avoid getting lost in useless detail. As an example, the preparation of a reactor may comprise a sequence grouping steps, such as the check for cleanness, proper connections, valve positions, inerting, heating to a given temperature, and so on. Each sequence is then analyzed with the checklist.

The checklist presented here is constructed as a matrix with a row for each keyword of the checklist and a column for each sequence of process steps. The list itself is in two parts: The first (Figure 1.4) is devoted to the utilities and the corresponding question is: "May the failure of the considered utility lead to a hazard in a given sequence of process steps?" In the second part (Figure 1.5), the operating mode is analyzed using the checklist, by questioning if a deviation from

Deviation	Step sequence:	A	B	C	D	E	F	G	H
1	Electrical power								
2	Water								
3	Steam								
4	Brine								
5	Nitrogen								
6	Compressed air								
7	Vacuum								
8	Ventilation								
9	Absorption								

Figure 1.4 Checklist for utilities. Question: "May the failure of a utility lead to a hazard?"

Deviation	Step sequence:	A	B	C	D	E	F	G	H
10	Cleaning								
11	Equipment check								
12	Emptying								
13	Equipment ventilation								
14	Charging, feeding								
15	Amount, flow rate								
16	Feed rate								
17	Order of charging								
18	Mixup of chemicals								
19	Electrostatic hazards								
20	Temperature								
21	Pressure								
22	pH								
23	Heating/cooling								
24	Agitation								
25	Reaction with heat carrier								
26	Catalyst, inhibitor								
27	Impurities								
28	Separation, settling								
29	Connections								
30	Pumping								
31	Waste elimination								
32	Process interruption								
33	Sampling								

Figure 1.5 Checklist for the operating mode. Question: "May a deviation from these conditions lead to a hazard?"

these conditions may lead to a hazard. This also allows checking the thoroughness of the process description, to see if the process conditions are given with sufficient precision and to avoid any misunderstandings.

The checklist presents some intended redundancies in order to ensure the comprehensiveness of the analysis. For the documentation, if a critical situation is identified, the corresponding box is marked with a cross, and the corresponding hazard identified by the coordinates of the box (e.g. F6: referring to the effect of failure of compressed air in sequence F), as described in the hazard catalog (Figure 1.1) in terms of possible causes, effects, risk assessment, measures, and residual risk.

1.4.2 Failure Mode and Effect Analysis

The FMEA is based on the systematic analysis of failure modes for each element of a system, by defining the failure mode and the consequences of this failure on the integrity of that system. It was first used in the 1960s in the field of aeronautics for the analysis of the safety of aircraft [10]. It is required by regulations in the United States and France for aircraft safety. It allows assessing the effects of each failure mode of a system's components and identifying the failure modes that may have a critical impact on the operability safety and maintenance of the system. It proceeds in four steps:

1. The system is to be defined with the function of each of its components.
2. The failure modes of the components and their causes are established.
3. The effects of the failure are studied.
4. Conclusions and recommendations are derived.

One important point in this type of analysis is to define clearly the different states of the working system, to ensure that it is in normal operation, in a waiting state, in emergency operation, in testing, in maintenance, and so on. The depth of decomposition of the system into its components is crucial for the efficiency of the analysis.

In order to illustrate the method, we can take the example of a pump as a component. It may fail to start or to stop when requested, provide too low a flow rate or too low a pressure, or present an external leak. The internal causes for pump failure may be mechanical blockage, mechanical damage, or vibrations. The external causes may be power failure, human error, cavitation, or too high a head loss. Then the effect on the operation of the system and external systems must be identified. It is also useful to describe the ways for detecting the failure. This allows establishing the corrective actions and the desired frequency of checks and maintenance operations.

As it can be seen from this example, the FMEA may rapidly become very work intensive and tedious. Therefore, a special adaptation has been made for the chemical process industry: the Hazard and Operability Study (HAZOP).

1.4.3 Hazard and Operability Study

The HAZOP was developed in the early 1970s by ICI [27], after the Flixborough incident [28]. It is derived from the FMEA, but specially adapted for the process industry in general, and in the chemical industry in particular. It is essentially oriented toward the identification of risks stemming from the process equipment. It is particularly well suited for the analysis of continuous processes in the steady state but can also be used for batch processes. The first steps of the risk analysis – of scope definition, data collection, and safe conditions definition – are the same as for other methods. Using the process and instruments design (PID) and the process flow diagram (PFD) as basic documents, the plant is divided into nodes and lines. For each of these divisions, a design intention is written that precisely summarizes its function. For example, a feed line could be defined as "the line A129 is designed to feed 100 $kg\,h^{-1}$ of product *A* from Tank B101 to reactor R205."

Table 1.8 HAZOP guidewords with definitions and examples.

Guideword	Definition	Example
No/not	Negation of the design intention. No part of the design intention is realized	No flow, no pressure, no agitation
Less	Quantitative decrease, deviation from the specified value toward lower value. This may refer to state variables as temperature and quantities, as well as to actions such as heating	Flow rate too low, temperature too low, reaction time too short
More	Quantitative increase: deviation from the specified value toward higher value. This may refer to state variables as temperature and quantities, as well as to actions such as heating	Flow rate too high, temperature too high, too much product
Part of	Qualitative decrease: only part of the design intention is realized	Charging only a part of a predefined amount, omission of a compound at charging, reactor partly emptied
As well as	Qualitative increase: the design intention is realized, but at the same time something else happens	Heating and feeding at the same time, raw material contaminated by impurity with catalytic effect
Reverse	The design intention is reversed, logical opposite of design intention	Reversed flow, back flow, heating instead of cooling
Other/else	Total substitution: The design intention is not realized, but something else happens instead	Heating instead of dosing, charging A instead of B, mix-up of chemicals

Then in a kind of guided brainstorming approach, using predefined guidewords applied to different parameters of the design intention, the process is systematically analyzed. These guidewords are listed in Table 1.8, together with examples. In cases where batch processes are to be analyzed by the HAZOP technique, additional guidewords concerning time and sequencing – for example, too early, too late, too often, too few, too long, or too short – may also be added. It is then verified that the deviation generated by applying the guideword to a parameter is meaningful. For example, "reverse flow" may be meaningful, but it would hardly be the case for "reverse temperature." If the generated deviation has no sense, it is skipped and the next deviation is generated with the next guideword. For traceability of the thoroughness of the analysis, it may be marked as not applicable, "n.a."

For the meaningful deviations identified by the procedure described above, the possible causes for triggering the deviation are systematically searched. As an example, possible causes for "no flow" may be an empty feed tank, a closed valve, an inadvertently open valve to another direction, a pump failure, a leak, and so on. In this context, it may be useful to indicate the logical relationship between the causes, such as where simultaneous failure of several elements is required

in order to trigger the deviation. This is of great help for the assessment of the probability of occurrence.

The effects are searched in order to allow the assessment of the severity. These results are documented together with the risk evaluation and, where required, with risk-reducing measures in a hazard catalog, as presented in Figure 1.1.

The analysis is performed on the totality of the nodes and lines defined by the division of the plant. This allows checking the comprehensiveness of the analysis. The HAZOP technique, as its name indicates, is devoted not only to the identification of hazards but also to the identification of operability issues. In this frame, the hazard catalog also provides a list of possible symptoms for the early identification of abnormal situations and remediation. Then it becomes an efficient tool for process design, especially for the design of automation systems and interlocks.

1.4.4 Decision Table

The decision table method consists of logically combining all possible states of each element of a system and outlining the consequences on the entire system. It can be applied to a part of a system or to an operating mode. The combinations are analyzed by Boole's algebra that gives the analysis a strong logical backbone. A part of such a decision table is shown by the example of the collision of a car with a deer (Figure 1.6). It is the most powerful method for analyzing combinations of failures, exhaustive in this respect. Nevertheless, the combinations rapidly become so numerous that it is difficult to retain an overview of the system by this method. Thus, it has a more academic character.

1.4.5 Event Tree Analysis

The event tree analysis (ETA) is an inductive method that starts from an initial event and searches for the different possible effects. It is especially useful for studying the scenario of what may happen after the initial event when developing emergency plans. Starting from the initial event, one searches for consecutive events, until the system reaches a final state. These different generations of events are represented as a tree. An example, again based on the collision of a car with a deer, is represented in Figure 1.7. The vertical lines leading from one event to the next are related in a logical "AND" relationship and the corresponding probabilities must be multiplied. Horizontal lines indicate a logical "OR" relationship and

Deer on the road?	No	Yes	Yes	Yes	Yes	Yes	Yes	...
Driver sees it in time?	No	No	No	No	No	No	No	...
Brakes in time?	No	No	No	No	No	Yes	Yes	...
Brake fails?	No	No	No	Yes	Yes	No	No	...
Deer stays on road?	No	No	Yes	No	Yes	No	Yes	...
Collision?	No	No	Yes	No	Yes	No	No	...

Figure 1.6 Decision table for the collision of a car with a deer. Source: Schmalz 1996 [8].

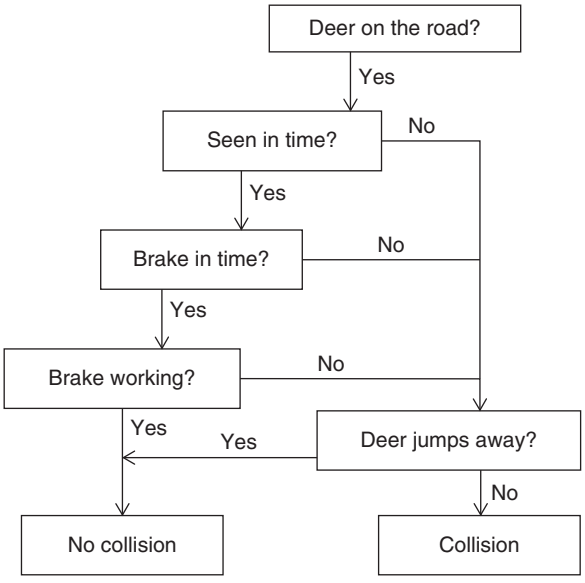

Figure 1.7 Event tree for the collision of a car with a deer.

the corresponding probabilities must be added. Thus, the tree can be quantified for the probability of entering one or the other branch after an event is known. Hence, it allows assessing quantitatively the effects of different possible chains of events and focuses the measures on the avoidance of the most critical chains.

1.4.6 Fault Tree Analysis

The FTA is a deductive method, whereby the top event is given and the analysis focuses on the search of the causes that may trigger it [11]. The principle is to start from the top event and identify the immediate causes or failures. Then each of these failures is again considered as an event and is analyzed to identify the next generation of causes or failures. In this way, a hierarchy of the causes is built up, where each cause stems from parent causes as in a generation tree (Figure 1.8). Such a tree may be developed to infinity; nevertheless, the depth of the analysis can easily be adjusted to function as the objectives of the analysis. In most cases, the depth of the analysis is adjusted to allow the design of risk-reducing measures. For example, in the analysis of a chemical process, when a pump failure is found, it is not useful to find out what caused the pump failure. For the process safety, it may be more appropriate to provide a backup pump or to increase the maintenance frequency of the pump. Thus, in general, the analysis is stopped at the failure of elementary devices such as valves, pumps, control instruments, and so on.

A special feature of the FTA is that different events are linked by logical relationships. One possibility is the logical "AND," meaning that two parent events must be realized simultaneously in order to generate the child event. The other possibility is the logical "OR" meaning, whereby only the realization of one parent event is sufficient to generate the child event. It becomes clear that the realization of an event behind an "AND" gate is less likely to occur than events behind an

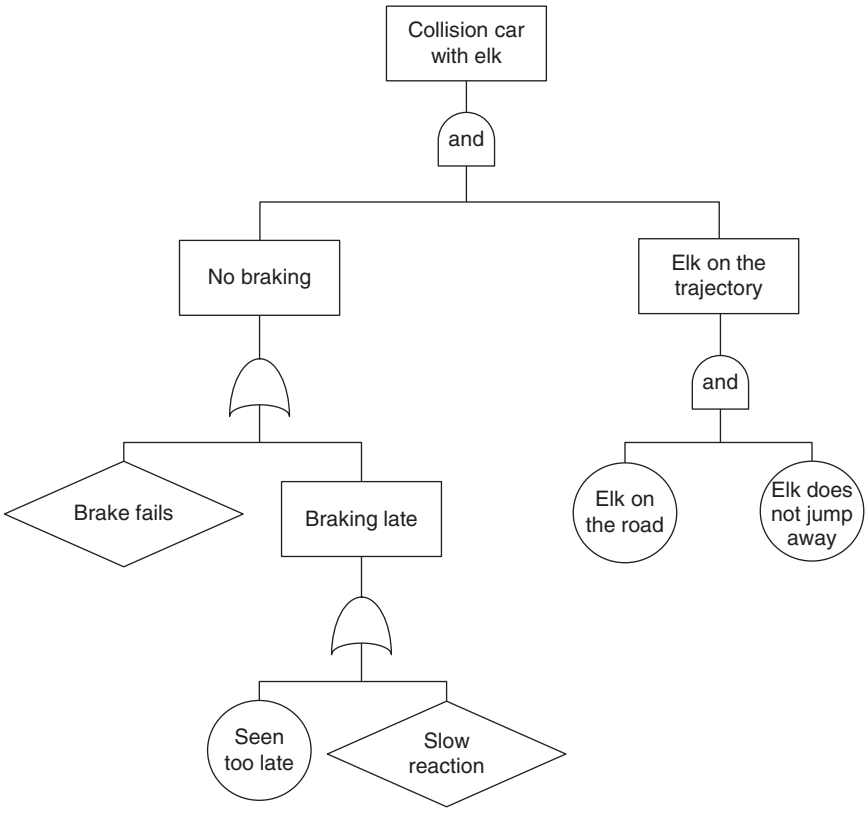

Figure 1.8 Example fault tree analysis for the collision of a car with an elk.

"OR" gate. This allows for a quantification of the fault, and using Boolean algebra, it is often possible to simplify the logic relationships of a complex tree leading to a cut set, which is easier to handle for the quantification.

The probability of occurrence of an event C depending on the simultaneous realization of two events A and B, that is, behind a logical gate "AND," is the conditional probability of A and B:

$$P_C = P_A \cdot P_B \tag{1.3}$$

Since probabilities are comprised between zero and one and should be low figures, the conditional probability usually becomes significantly smaller. In other terms, an "AND" gate strongly reduces the probability of the occurrence of an event, and it is advisable to design a safety system in order to provide such "AND" relationships before the top event.

The probability of occurrence of an event C, where only the realization of one parent event from A or B is required (behind an "OR" gate), is the sum of probabilities of all parent events:

$$P_C = P_A + P_B - P_A \cdot P_B \tag{1.4}$$

In this expression, the subtraction of the product of probabilities takes into account the fact that the simultaneous realization of both events is still taken

into account in the realization of individual events. This correction is usually very small, since individual probabilities are small.

In this way, the fault tree can be quantified, which makes this technique very powerful for the reliability analysis of protection systems. The prerequisite is the availability of statistical reliability data of the different devices and instruments that is often difficult to obtain for multipurpose plants, where devices can be exposed to very different conditions when changing from one process to another. Nevertheless, if the objective is to compare different designs, semiquantitative data are sufficient.

Both methods, the event tree and the fault tree, are often used together as the so-called "bow tie" method. The top event, often a loss of containment, is at the center of the bow tie. At its left, the fault tree analyzes the causes leading of the top event, and at its right, the event tree analyzes the success or failure of the different safeguards, allowing a quantification of the resulting situations.

1.4.7 Brainstorming

Brainstorming is an intuitive method based on the creativity of the participants. It is organized in two steps. In the first step, participants are invited to explain spontaneously what can go wrong in the analyzed process. It is important that in this step, ideas, even "bad ideas," are no criticized. The principle is that the feeling of the participants contains some truth. The team must feel free to explain what they have in mind. The ideas expressed during this step are carefully documented by the secretary. In the second step, the ideas are systematically analyzed and classified as relevant or not.

Since there is no systematics in this method, it is not possible to ensure the comprehensiveness of the analysis. Hence it cannot be used as the only analysis technique in a process risk analysis. Nevertheless it is sometimes useful to allow the participants to spontaneously express their ideas about a process or an equipment and to become familiar with the object of the analysis.

1.5 The Practice of Risk Analysis

The quality of a risk analysis depends essentially on three factors:

1. The systematic and comprehensive hazard identification.
2. The experience of the risk analysis team members.
3. The quality and comprehensiveness of the data used during the analysis.

In Sections 1.5.1–1.5.4, some hints about the key factors of success for the risk analysis are reviewed.

1.5.1 Preparing the Risk Analysis

Performing a risk analysis requires important resources since it is essentially a team work that must be performed as far as possible in an efficient way. This means that an important preparation work must be done prior to the risk analysis sessions in the team. As described in Section 1.3, the very first step of a process

risk analysis is to define its scope, which must be done together with the definition of its purpose and objective. This is essential in order to choose the most appropriate method and the required resources [9]. At this stage, the process data and documentation must be collected and prepared and the risk analysis team must be defined.

1.5.2 The Risk Analysis Team

A risk analysis *must* be performed in a team for several reasons: risk analysis is a creative task that requires knowledge of professionals in different specialties, and one person cannot cover all required knowledge fields. Complex problems are often solved in discussions resulting in original solutions, which require team work. Obviously, the composition of the risk analysis team is of primary importance for the quality of the work. Here the professional experience of the participants plays a key role, since the objective of the analysis is to identify events that have not yet occurred. It is a creative task not only to identify the hazards but also to define risk-reducing measures. Thus, besides the risk owner who is in general a plant manager, different professions must be represented in the team, including chemists, chemical engineers, mechanical engineers, and automation engineers. It is highly advisable that an operator or a shift leader who has a good knowledge of the plant situation is also present. Depending on the nature of the process, safety experts in explosion protection, toxicology, and so on may also take part in some sessions. Each member of the risk analysis team bares the responsibility of his own field of knowledge. When a new process is to be analyzed, the experience gained during process development should be available to the team; hence members of the process development team must be represented in the risk analysis. The plant manager, who is the risk owner, takes a determining part in the analysis.

1.5.3 The Team Leader

The team leader or moderator is responsible for the quality of the analysis, caring for its thoroughness, for discipline in the team, and for the time management. As such he should preferably be independent from the project organization. In the choice of risk-reducing measures, the moderator drives the group toward efficient solutions. The moderator must be a systematic well-organized, and open-minded person. More generally, the group dynamics is important, so the participants should also be creative and open-minded. The moderator ensures that all opinions can be expressed, leading the team toward consensual solutions. It is advantageous that the moderator has a sound industrial experience and, if possible, some experience in dealing with risks or in incident analysis. The team leader must also compensate for the weaknesses inherent to the analysis method [29].

The preparation work mentioned above is an important part of the team leader task. In order to be efficient, the analysis must be organized in advance. As an example, when the HAZOP method is used, the installation can be structured in lines and nodes. With the checklist method, the grouping of process steps into sequences must also be prepared in advance. This greatly facilitates the analysis

and allows an easy check of the systematics and consequently comprehensiveness of the work.

During the analysis sessions, the team leader must ensure that every opinion can be freely discussed and that all members participate in the elaboration of the scenarios and risk assessment. He also avoids tedious discussions and detail engineering but ensures that the safeguards or risk-reducing measures are clearly defined in order to facilitate the task of the engineers who will design and work it out.

1.5.4 Finalizing the Risk Analysis

The hazard identification methods presented in Sections 1.4.1–1.4.7 are all based on strongly systematic procedures. In the checklist method, the systematic is provided by the checklist itself. The comprehensiveness can be verified in the matrix (see Figures 1.4 and 1.5). With the FMEA, the systematic is provided by the division of the system into elements and the failure modes considered. In the HAZOP study, the systematic stems from the division of the plant into nodes and lines and then the systematic application of the keywords. With the decision table method, the systematic is inherent to the table. For the FTA and ETA, the systematic is given by the tree and the logical ports. Nevertheless, the work of the team must be traceable, even by persons who did not participate to the analysis. Thus, it is recommended to also document the hazards that were not considered as critical.

The risk analysis represents an important part of the process know-how, and therefore the hazards catalog (see Figure 1.1) cannot be a static document, but a part of the process documentation at the same level as the operating mode and mass balances. It may be useful to describe the risk-reducing measures together with the status, such as new, accepted, rejected, implemented, and so on. The hazard catalog then becomes a management tool and a living document, which must regularly be updated and accompany the process throughout its life. The list of measures is a significant part of the documentation, since it also describes the function of all safety relevant elements.

1.6 Exercises

1.1 Risk and Hazard

1. What is the definition of risk, and how does it differentiate from hazard?
2. What are the severity categories?
3. Quote four aspects used in the evaluation of the severity

1.2 Risk Reduction

During a risk analysis, two deviations from the operating conditions were identified and the corresponding risks assessed as follows:

(1) High severity and low probability
(2) Low severity and high probability

Question

1. Which of the risks should have the first priority in risk reduction (1, 2, both are equivalent)?

1.3 Risk Reduction Measures

When planning for risk reduction measures, different types of measures may be considered. Classify the following types of measures by decreasing priority (first priority first):

Write the ranking numbers into the boxes:

- ☐ Preventive measures
- ☐ Eliminating measures
- ☐ Emergency measures

Give an example for each category in the frame of a runaway scenario.

1.4 Hazard Identification Techniques

The different risk analysis methods differ in the approaches for searching and identifying process deviations.

Questions

1. Describe three different techniques, one in each category (inductive, deductive, and intuitive).
2. Comment on the advantages and draw backs of each technique.

1.5 Checklist and HAZOPs

Two hazard identification techniques the checklist and the HAZOP were presented in detail in this chapter.

Questions

1. Give the main application fields of these techniques.
2. What is the required basic documentation in each case?

References

1 Hungerbühler, K., Ranke, J., and Mettier, T. (1998). *Chemische Produkte und Prozesse; Grundkonzepte zum umweltorientierten Design*. Berlin: Springer.

2 SUVA (2018). Effectif assuré et risque par branche d'activité 2016. In: *Statistique des accidents 2016* (ed. CSAA). Lucerne: SUVA.

3 Laurent, A. (2003). *Sécurité des procédés chimiques: connaissances de base et méthodes d'analyse de risques*. Paris: Tec&Doc - Lavoisier.

4 Lees, F.P. (1996). *Loss prevention in the process industries hazard identification assessment and control*, 2e, vol. 1–3. Oxford: Butterworth-Heinemann.

5 Stoessel, F. (2002). On risk acceptance in the industrial society. *CHIMIA* 56: 132–136.

6 Jones, D. (1992). *Nomenclature for Hazard and Risk Assessment in the Process Industries*, 2e. Rugby: Institution of Chemical Engineers.

7 Rey, A. (ed.) (1992). *Le Robert dictionnaire d'aujourd'hui*. Paris: Dictionnaires Le Robert.
8 Schmalz, F. (1996). *Lecture script*. Zürich: Sicherheit und Industriehygiene.
9 Baybutt, P. (2014). The importance of defining the purpose, scope, and objectives for process hazard analysis studies. *Process Safety Progress* 34 (1): 84–88.
10 Villemeur, A. (1988). *Sûreté de fonctionnement des systèmes industriels*. Paris: Eyrolles.
11 CCPS (1992). *Guidelines for Hazard Evaluation Procedures*. New York: AIChE.
12 Baybutt, P. (2018). Guidelines for designing risk matrices. *Process Safety Progress* 37 (1): 49–55.
13 Cox, A.L. (2008). What's wrong with risk matrices? *Risk Analysis* 28 (2): 497–512.
14 Baybutt, P. (2014). The ALARP principle in process safety. *Process Safety Progress* 33 (1): 36–40.
15 IEC-61511 (2016). *Functional Safety – Safety Instrumented Systems for the Process Industry Sector*. Geneva: IEC.
16 Schwarz, H.V., Koerts, T., and Hoercher, U. (2019). Semiquantitative risk analysis an EPSC Working group. *Chemical Engineering Transactions* 77: 37–42.
17 Baybutt, P. (2016). Designing risk matrices to avoid risk ranking reversal errors. *Process Safety Progress* 35 (1): 41–46.
18 Kletz, T.A. (1996). Inherently safer design: the growth of an idea. *Process Safety Progress* 15 (1): 5–8.
19 Crowl, D.A. (ed.) (1996). *Inherently Safer Chemical Processes. A Life Cycle Approach*, CCPS Concept book, 154. New York: Center for Chemical Process Safety.
20 Hendershot, D.C. (1997). Inherently safer chemical process design. *Journal of Loss Prevention in the Process Industries* 10 (3): 151–157.
21 Sorbe, S. (2002). *Sicherheitstechnische Kenndaten chemischer Stoffe*. Landsberg: SicherheitsNet.de.
22 Sorbe, S. (2005). *Sicherheitstechnische Kenndaten chemischer Stoffe*. Ecomed Sicherheit: Landsberg.
23 Lewis, R.J. (2005). *Sax's Dangerous Properties of Industrial Materials*, 11e. Reinhold.
24 Koller, M. (2013). Liste des valeurs limites d'exposition (VME/VLE). In: *Valeurs limites d'exposition aux postes de travail en Suisse*. Lucerne: SUVA.
25 EPA (2015). *AEGL Definitions*. Environmental Protection Agency.
26 ESCIS. *Introduction to Risk Analysis of Chemical Processes*, vol. 4. Lucerne: ESCIS.
27 Kletz, T. (1992). *Hazop and Hazan: Identifying and Assessing Process Industry Hazards*, 3e. Rugby: Institution of Chemical Engineers.
28 Kletz, T. (1988). *Learning from Accidents in Industry*. London: Butterworths.
29 Baybutt, P. (2015). A critique of the Hazard and Operability (HAZOP) study. *Journal of Loss Prevention in the Process Industries* 33: 52–58.