U-21

'Bhopal and its Effects on Process Safety'

International Conference on the 20th Anniversary of the Bhopal Gas Tragedy,

December 1 - 3, 2004 at I.I.T., Kanpur, India

Combating Interference by Unauthorised Persons

-German Approach-

Dr. Hans-Joachim Uth (<mailto:jochen.uth@uba.de>)

Federal Environmental Agency
FG III 1.2 Process Safety, Major Accident Control
P.O. 330022
14191 Berlin
Federal Republic of Germany
fon: +49 (030) 8903 3457/2360/2919
fax: +49 (030) 8903 3099
www.umweltbundesamt.de/zema/
www.umweltbundesamt.de/anlagen/

Keywords: interference by unauthorised persons; security analysis; emergency planning;

Abstract

Under the new threat situation it is necessary to impede and if necessary detect ingress by unauthorised persons into the relevant establishment. It may be necessary to take additional measures to protect installations or parts thereof that are especially hazardous or at risk from terrorist attacks from interference by unauthorised persons.

It is the duty of the state to take precautionary and preventive measures to impede or prevent external terrorist attacks or entry by force into establishments. The necessary resources for this purpose must be made available even in times of limited budgets.

Since total protection can never be guaranteed, external emergency measures have a particularly important role to play. The competent authorities in this sector must receive the necessary information from the operators and must take the measures within their sphere of responsibility without delay.

Much of the information necessary for assessment of the risk situation by the operators and the authorities is already available under the provisions on the safety report and the alarm and emergency plans according to German Hazardous Incident Ordinance

It is recommended that a restriction of disclosure of information on the grounds of public safety should only be permitted for establishments/installations which are to be regarded as security-relevant on the basis of the hazard and the risk analysis.

The systematic approach of a security analysis is described in detail separately (Annex 1).

Combating Interference by Unauthorised Persons[1]

Introduction

In view of the terrorist attacks in the USA on 11 September 2001, the German Federal Ministry for the Environment, Nature Conservation and Nuclear Safety requested the Major Incidents Commission (SFK) to investigate the consequences arising from the new threat situation in the field of major accident control. In particular was to examine weather the safety reports and the alarm and emergency plans according to the German Hazardous Incident Ordinance are sufficient for preventing attacks and minimising the consequences of attacks and develop proposals for the current discussion on a Administrative Guideline on the German Hazardous Incident Ordinance.

Strategy for identifying and protecting security-relevant installations

The SFK proposed a unique strategy for identifying and protecting security-relevant installations. In a 4 step procedure the hazards and risks of the establishments are identified, the vulnerability for interference by unauthorised persons are assessed and the framework for appropriate measures is given. A graphical overview see *Fig. 1*. The systematic approach is done in the framework of a **Security Analysis** (*Example see Appendix 1*) in which it is also shown that adequate precautions have been taken in particular against interference by unauthorised persons.

For this purpose the operator must in particular:

a) undertake, in agreement with the authorities responsible for domestic security, a systematic examination of his establishment and installations pursuant to the Hazardous Incident Ordinance to determine whether they may represent a special target (risk analysis, *see Appendix 1, Chapter 3)* and
b) investigate, in consultation with the authorities responsible for external hazard prevention, whether interference by unauthorised persons with destructive intent is capable of giving rise to a serious hazard (hazard analysis).

Note: The operator is at liberty to select methods other than that described in *Appendix 1*. Such methods should however guarantee the same level of protection.

Hazard analysis and risk analysis are of equal status as elements of the security analysis. The decision on which of these steps to begin with should be taken in the individual case.

Hazard analysis

[1] The approach is developed on the Report of the German Hazardous Incident Commission SFK-GS-38,

Special consideration must be given to parts of the establishment (e.g. installations) where a major accident threatens people's lives or gives cause to fear serious impairment of people's health.

- Describing the establishments with potential of major accidents
- Identification of neighbouring facilities requiring special protection (*see Appendix 1, Chapter 4*).
- Assessment of the impacts of major accidents despite precautions on the facilities requiring special protection.

Note: This information is usually part of the safety reports according to German Hazardous Incident Ordinance .

Risk analysis

If the hazard analysis reveals that a serious hazard may exist, it is necessary to investigate whether the installations appear to be particularly "attractive" for terrorist attacks. To this end a systematic analysis must be performed taking account of the following aspects in particular.

- Assessment of the risk situation (general security situation, size and composition of work force, quality of security organisation, social position of members of company management, nature of sales connections and foreign activities, crime situation to date etc.; *see also Appendix 1, Chapter 3*),
- Local position of establishment and installations (vulnerability from outside and inside, distance from factory fence, visibility from outside, roads on and off site, situation of industrial estate; *see also Appendix 1, Chapter 3.4*),
- The importance of availability of the installations for downstream production processes and services,
- The symbolic character of the company or the installation (ownership situation, type of production and storage of substances, product range, significance of the company from an economic strategy point of view etc.).

Protecting security-relevant installations

So identified security-relevant installations must take special measures to secure them against interference by unauthorised persons. Security objectives must be defined for this purpose (*see Appendix 1, Chapter 6*). To achieve such security objectives the following measures in particular may be considered:

- The perimeters of establishments – or if appropriate the common perimeter in the case of industrial estates – (site fence, gates etc.) must be secured by technical and organisational means to ensure that unauthorised persons cannot gain access without using force.
- Non-site personnel should be kept identifiable. Visitors and external companies must be monitored appropriately.
- Installations are to be protected in such a way that unauthorised persons cannot cause a major accident without internal knowledge and/or technical aids.

- Employees must be made aware of the need to secure the establishment, and must be involved. (*see also Appendix 1 Chapter 7*).

Note: Industrial estates (especially chemical parks) place special demands on security measures because of the large number of legally independent operators. As a rule the vulnerability of hazardous installations can only by minimised by means of a single security system (common site fence and security personnel).

"Good Security" Practice / Security Management

To implement the security objectives and security measures, it is recommended that a security management system be used, which may form part of the safety management system.

Disclosure of security documentation

In decisions on this issue it is important to weigh up carefully the legal assets concerned in the individual case: It must also be noted that informing parties concerned about risks relating to them is not only a right of freedom, but also an element of precaution against major accidents. Therefore it is necessary to develop criteria for weighing up the possible loss of safety against a possible gain in security.

Measures against internal offenders

So-called "internal offenders" in particular may represent a risk. These are employees of the operator's own company or of external companies who are authorised to be on the premises of security-relevant installations and who commit unauthorised interference. They may possess a good knowledge of the relevant installations and may seek to use it with criminal intent.

Even if this group of offenders is a special problem, it is still possible for operators to take preventive measures in addition to the general measures taken by the security authorities. They belong in particular to the field of personnel management and supervision (creating identification with the company, motivation, sensitive handling of stressful personnel measures, training of superiors etc.). In addition, steps should be taken to raise the general awareness of all employees about this problem group (*cf. also Appendix 1, Chapter 3.9*). Counselling by specially qualified psychologists may be useful in certain circumstances.

If a relevant risk remains after all these security measures and those described above have been taken, it is advisable to consult the authorities responsible for public security. As a "last resort" it may even be necessary to undertake security screening of employees in highly sensitive areas, provided this is legally permissible, especially from a data protection point of view.

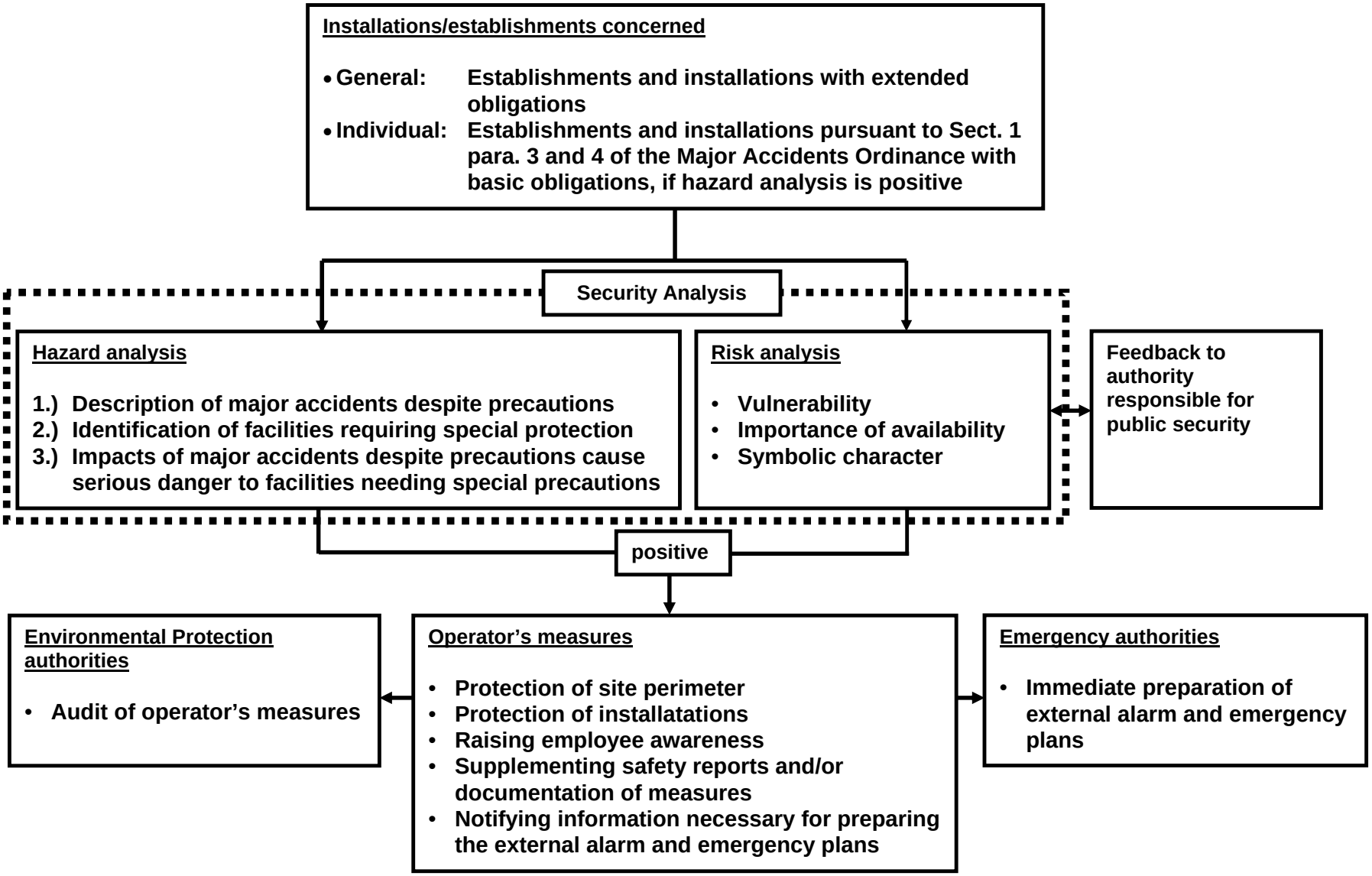
Installations/establishments concerned
• General: Establishments and installations with extended obligations
• Individual: Establishments and installations pursuant to Sect. 1 para. 3 and 4 of the Major Accidents Ordinance with basic obligations, if hazard analysis is positive
Security Analysis
Hazard analysis
1.) Description of major accidents despite precautions
2.) Identification of facilities requiring special protection
3.) Impacts of major accidents despite precautions cause serious danger to facilities needing special precautions
Risk analysis
• Vulnerability
• Importance of availability
• Symbolic character
Feedback to authority responsible for public security
positive
Environmental Protection authorities
• Audit of operator's measures
Operator's measures
• Protection of site perimeter
• Protection of installatations
• Raising employee awareness
• Supplementing safety reports and/or documentation of measures
• Notifying information necessary for preparing the external alarm and emergency plans
Emergency authorities
• Immediate preparation of external alarm and emergency plans

Figure 1

Annex 1

Combating Interference by Unauthorised Persons

- Security Analysis[2]-

by Hans-Joachim Uth (<mailto:jochen.uth@uba.de>)

Contents

[2] This example of a security analysis is based on German Federal Environmental Agency R&D project 104 09 210 “Technical and organisational measures for protecting installations subject to the Major Accidents Ordinance from interference by unauthorised persons”, Verband für Sicherheit in der Wirtschaft Baden-Württemberg e.V. (Baden-Württemberg Industrial Security Association), (1988).

1 Preliminary remarks

The procedure presented here is an example that satisfies the requirements for a security analysis set out in Chapter 4 of this Guide and provides appropriate explanations. The operator is at liberty to choose different procedures. Such methods should however guarantee the same level of protection.

2 Procedure for performing a security analysis

As a rule, adequate protection of establishments against interference by unauthorised persons is only possible on the basis of a systematic analysis. A step-by-step procedure is adopted:

1. Determining and assessing the risk situation
2. Identifying the specific points at risk in the establishment
3. Assessment of hazards in relation to protection objectives
4. Selecting security measures, preparing the integrated security strategy.

An overview is provided in *Fig. 1*. The assessments are to be reviewed regularly and in the light of new information.

2.1 Determining and assessing the risk situation

When determining the risk situation it is necessary to take account of a number of different factors for each establishment, e.g.:

- Type of production
- Storage of hazardous substances
- Local situation of establishment
- Surroundings of establishment
- Nature and extent of buildings
- Human resources
- Plant-specific special features

The extent of the threat depends on

- the potential perpetrators and their potential types of behaviour or modes of action, referred to hereinafter as type of risk, and
- the number, type and nature of individual points in the establishment at which a major accident could be caused by more or less substantial effort, referred to hereinafter as points at risk.

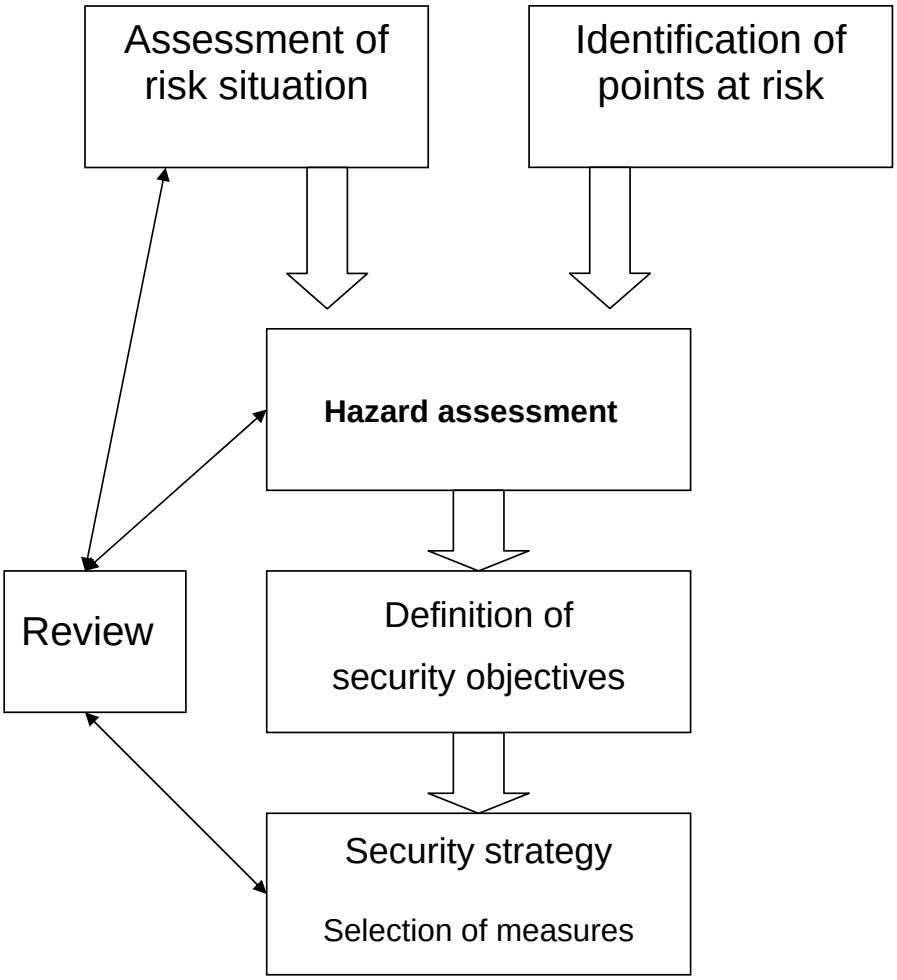

Fig. 1: Security analysis procedure

The question of the potential perpetrators that can be expected and their mode of action is naturally impossible to answer with certainty. However, on the basis of plant security experience it is nevertheless possible to make a rough classification of author or offender categories, their typical motives and possible types of behaviour in a table graduated on the basis of degrees of danger *(Risk category table)*.

This presupposes a detailed scrutiny of the overall situation in the establishment. Information on how to perform this scrutiny and a proposal for compiling a risk category table can be found in Appendix 1, *Chapter 3 "Risk situation"*.

2.2 Identifying the specific points at risk in the establishment

Reliable determination of the points at risk within an establishment is an easier task. A picture of the risk situation can be gained from asking how and where a major accident might be caused or where there is a major risk of this occurring.

Here too a table can be useful for presenting a clear overall picture *(Table of points at risk)*.

A special indication of potential risks is provided by the safety report pursuant to Sect. 9 of the Major Accidents Ordinance, which must be regarded as an important source of information for investigating negligent or intentional impacts in the context of the proposed security analysis. The investigations necessary for determining and assessing the points at risk within the establishment are explained in Appendix 1, *Chapter 4, "Points at risk"*.

2.3 Assessment of hazards in relation to protection objectives

A comparison of the results of the risk situation analysis (determination of risk categories) with the individual points at risk reveals the individual threat to the installation. It is now possible to estimate what impacts can reasonably be expected to occur at what points. This process is described in Appendix 1, *Chapter 5, "Hazard assessment"*.
On the basis of the hazard assessment performed in this way, it is possible to arrive at basic protection objectives (see also provision in Sect. 3 of the Major Accidents Ordinance) and the individual measures necessary to prevent the occurrence of major accidents caused by persons *(Appendix 1, Chapter 6 "Security objectives")*.

2.4 Selecting security measures, preparing the integrated security strategy

Security for an establishment always forms an overall system in which the components of an organisational, human resources and constructional/technical nature must all act in concert. It is therefore useful to describe the individual *security measures* in the context of a comprehensive *security strategy* which shows how they are interrelated. A example of a possible structure for such a strategy is explained in Appendix 1, *Chapter 7, "Description of the security measures/security strategy"*.

3 Risk situation

3.1 Overview

The risk situation in an establishment depends on a number of different factors. This chapter therefore discusses the parameters necessary for assessing the situation. The main factors include

- the general safety situation,
- the establishment's membership of other companies,
- the local situation of the establishment,
- the type of production and storage of substances,
- the importance of the establishment for downstream production and services,
- the size and composition of the work force,
- the quality of security organisation,
- the social position of members of company management,
- the nature of sales contacts and international activities,
- crime to date.

The relative importance of individual factors for the risk situation will vary greatly with the individual establishment. By discussing the factors it should however be possible to classify them in certain risk categories providing an indication of possible perpetrators, their motives, modes of action, instruments used etc. Three risk categories are described.

3.2 General safety situation

The general safety situation describes risks of the kind that apply generally to establishments, with regional differences where appropriate. Reliable yardsticks with regard to "classic" crime are police crime statistics and publications by insurance companies. The safety situation with regarded to politically motivated crimes is determined by ongoing information obtained by public authorities in the course of their criminal investigation and anti-subversion activities. This may permit greater attention to regional aspects.

3.3 Membership of other companies

If the establishment belongs to a large company or group (division, subsidiary, majority interest etc.), it is also necessary to take account of the risk situation for the enterprise as a whole. This applies primarily to politically motivated crimes.
Experience shows that the risk generally increases with the size and (global) importance of the company as a whole.

3.4 Local situation of establishment

To some extent the degree of the threat also depends on the local situation of the establishment. For example, long established establishments in rural areas can usually rely on the loyalty and commitment of their employees, a factor that may contribute to a stable safety situation.

Neighbouring establishments or other facilities may play a role if they are a source of special hazards (domino effect), e.g. fire/explosion.

Other factors relate to the immediate surroundings of the establishment site. Examples of relevant questions include whether persons can approach the site perimeter unnoticed (e.g.

because of the vegetation) or conversely whether the presence of local residences increases the possibility of persons being discovered when trying to climb over the fence. Other aspects to be considered are the average time the police take to reach the site and their possible access routes. For example, if there is only one access road to the site, this increases the risk of its being blocked by winter conditions or deliberate obstruction.

To sum up, the following information should be available:

- Information on the general surroundings of the site
- Characteristics of the surroundings, and if appropriate information about special hazards arising from the surroundings
- Information about the immediate periphery of all sides of the site
- Information about the access roads from the nearest town, and if appropriate about possible obstructions
- Average arrival time of external assistance forces, especially the police
- Site plan with all details of importance for site security (requirements for a site plan are described in Appendix 1, *Chapter 7.8*).

Security management

Formatiert: Nummerierung und Aufzählungszeichen

Information on the structure and documentation of a security management system can be found in Appendix 3 to this Guide.

3.6 Security organisation

The size and training of the security organisation (personnel with security tasks), especially the site security personnel, for an establishment play a special role in averting hazards that may arise from deliberate actions by individuals.

The site security staff are of great importance here, as their mission includes in particular the prevention of deliberate or criminal acts.

Responsibility for the necessary preventive measures for avoiding damage due to incorrect operation or negligence rests with the operators, assisted by their Major Accident Officers and their occupational Safety Specialists. They should devote increased attention to preventing deliberate faulty acts and minimising any consequences of such acts. Larger establishments also have company owned fire brigades and environmental protection departments that are involved in particular in the damage limitation measures.
.
An extremely important aspect is cooperation between all the organisations, and experience shows that this is particularly likely to function where they are under common management.

3.7 Nature of production and storage

This chapter is intended to provide an overview of the production and storage of hazardous substances and the risks that can in principle arise from them (a detailed discussion can be found in Appendix 1, *Chapter 4 "Points at risk"*).
It is also necessary to consider neighbouring parts of the establishment that are not subject to the Major Accidents Ordinance. Risks may arise here if, for example, fires started here can spread to the "major accidents sector" or if the production/storage in the neighbouring installation provides a special incentive to crime.

Finally, one aspect of great importance for risk classification is the extent to which the product produced and stored or the production process is the subject of considerable political or social controversy.

3.8 Importance of establishment for downstream production and services

Certain installations may have a key role for downstream production or services. These include installations that are unique within an economic area or where capacity is fully utilised and cannot be reconstructed in a short time. The economic damage caused by their elimination and the resulting political consequences may be the goal of politically motivated offenders in particular.

3.9 Employees

The first aspect to consider in relation to the employees is its size. The more employees there are, the more difficult it is to assess the threat from this group and hence the larger one can expect the number of persons to be who are willing and able to harm the establishment (internal offenders).

In this connection the working climate in the establishment plays an important role. An unsatisfactory working climate results in demotivation of employees, and this may also be reflected in lax application of safety regulations. A poor working climate – which may be confined to individual sectors/departments – usually results in lack of interest, especially with regard to safety facilities and rules; this reduces the threshold for negligent or intentional acts.

Foreign employees do not basically constitute a greater safety risk than German employees. A risk may however arise if safety or security rules are misunderstood or disregarded as a result of language barriers or differences in mentality.

External personnel similarly do not present a greater risk than employees, provided they are familiar with the site conditions and safety/security measures and have a firm relationship with the establishment.

Finally, working hours and allocation to shifts should be taken into account. Of special interest here are times when people are not working and when there are only a few employees on site or none at all. The risk of criminal acts by external individuals is greatest during non-working hours – e.g. at weekends.

To sum up, the following information should be available:

- Total numbers of work force with break down by gender and age groups
- Numbers of foreign workers, with breakdown by nationalities
- Number of hired staff or external company personnel permanently on site and information about their ties with the establishment (especially how long they have been working together)
- Average number of visitors
- Working hours and shift allocation in the installations that are the reason why the establishment is subject to the Major Accidents Ordinance
- If appropriate, information about relations between the work force and company management, which may be reflected in personnel turnover and the public image of the establishment
- Information about activities by radical political groups in the establishment or its surroundings.

3.10 Company management

The focus here is on whether members of company management are in the public eye as a result of social controversies, for example through their activities or their position in parties or associations, and whether action against the establishment cannot be ruled out for this reason.

3.11 Sales connections

In this connect it is worth considering whether certain sales connections give rise to greater risks. This might be the case, for instance, with business connections with politically unstable countries. Since export-oriented establishments usually ship all over the world, there is above all an increased risk where links with such countries are particularly strong.

3.12 Crime to date

The number, seriousness and nature of offences recorded in an establishment to date may also give an indication of the degree of risk. A period of about 5 years can be considered for this purpose. All in all, the following information should be available:

- Overall information about minor offences recorded, such as simple theft (high, medium, low)
- Number of cases of breaking and entering or major theft
- Information about organised crime in the establishment
- Number of acts of sabotage to date, including unsolved cases where there is a significant suspicion of sabotage
- Number of bomb threats or other threats to date
- Number of cases of arson or use of explosives, including suspected cases.

3.13 Risk categories

On the basis of the analysis of the company's general risk situation, it is possible to allocate certain risk categories. The individual stages provide an overview of the perpetrators that are potentially to be expected, their possible or typical modes of operation, their objectives and motives, and their criminal energy. These stages make it possible to show clearly what risks must reasonably be considered.

The extent to which the assumed perpetrators are actually capable of causing serious damage, the points where this is possible and likely, must form the subject of further investigations (*see Appendix 1, Chapter 4 "Points at risk"*).

The three risk categories shown contain a number of assumptions that are intended to permit classification of the risk situation determined. These assumptions essentially concern the:

- possible circumstances surrounding the action,
- possible motives and typical modes of action.
- instruments likely to be used and
- expected criminal energy.

The matching assumptions within a risk category are based on criminal investigation experience, but need not necessarily be an exact match in every case.

This being so, they should not be interpreted too narrowly when allocating them to an installation. It is useful to assess the probability of the existence of a risk category on the following four-point scale:

1: must be assumed
2: likely
3: hardly likely
4: can be ruled out

If the result is "level 1 or 2" it is assumed that the relevant risk category applies. In almost all cases, several risk categories will be possible.

The individual risk categories are described below. This security strategy does not take any account of negligent actions. For more detailed information on the instruments used, see Appendix 1, Chapter 4.3.

Risk category 1

a)	Attendant circumstances	:	Contingent intent: The perpetrator (criminal) aims to cause what from his standpoint is limited damage. He accepts or is unaware of the possibility that a much greater hazard situation may occur (major accident).
b)	Motives	:	Revenge, frustration, “prove” existence of deficits, achieve social-political effects
c)	Preparatory activities	:	Spying out the situation, obtaining tools and other instruments
d)	Instruments	:	Simple or major tools, possibly simple incendiary equipment
e)	Criminal energy	:	Dependent on motive, average
f)	Group of persons	:	Criminals from inside or outside company, acting for themselves or others. Dismissed employees, former employees, employees, staff of outside companies, visitors.
g)	Remarks / Examples	:	- Putting safety equipment out of action, - Interference with production flows, - Non-notification of critical plant status, - Arson, vandalism after unsuccessful break-in, - Arson for other motives.

Risk category 2

a)	Attendant circumstances	:	Direct intent: The perpetrator (criminal) aims to bring about major damage and the resulting risk situation up to and including a major accident, possibly as a diversion.
b)	Motives	:	Political radicalism, revenge, gaining financial/competitive advantages
c)	Preparatory activities	:	Reconnoitre safety-relevant installation parts and weaknesses. Exploiting surveillance loopholes. Obtaining complicated instruments if necessary. Putting safety equipment out of action.
d)	Instruments	:	Simple and specialised tools, incendiary equipment, simple explosives (home-made).
e)	Criminal energy	:	Above average

f)	Group of persons	:	Individuals, groups, including as part of “organised crime”, radical political groups.
g)	Remarks / Examples	:	- Arson/bomb attack, - Destruction of important operating facilities, - Interference with control systems, - Deliberate incorrect programming of control processors.

Risk category 3

a)	Attendant circumstances	:	<u>Massive terrorist attacks:</u> Brutal action dangerous to the public, often without regard to people’s lives (own or others). Armed action.
b)	Motives	:	“Lighting a beacon”, anarchy, using violence to bring about social change, “punishing” companies, religious motives.
c)	Preparatory activities	:	Logistical preparations, reconnaissance, putting security equipment out of action.
d)	Instruments	:	Simple and heavy tools, weapons, incendiary devices, explosives.
e)	Criminal energy	:	Extremely great.
f)	Group of persons	:	Extremist and terrorist individuals and groups.
g)	Remarks / Examples	:	- Armed ambush, - Blowing up tanks/containers, - Firing on facilities, - Setting fire to major installations, - Attacks on security personnel, - Targeted bomb attacks on specially sensitive areas.

4 Points at risk

The risk categories described in the previous section must always be seen in connection with specific points at risk. It is important to take a differentiated view of the points or areas where the damage (major accident) can be caused. For example, there is a considerable difference if at one point the damage could be caused simply by turning a hand wheel or the same damage could only be caused at another point by using explosives.

4.1 Division into sectors

The risk categories established after discussing the risk situation, with their pointers to the threats that are basically conceivable, initially relate to the company as a whole. However, every establishment is made up of areas, units or installation parts which vary in their hazard potential, constructions, use, technical design and – above all – their sensitivity to disturbance factors.

Even within parts of installations, there are usually certain points that are particularly sensitive (example: tanks, safety valves, emergency cooling systems etc.). It may be appropriate to identify these in a separate investigation.

As in the safety report pursuant to Sect. 9 of the Major Accidents Ordinance, it is also necessary in the case of facility security to examine not only the actual risk potentials (types and quantities of substances), but also the substance transport systems and the facilities for supplying and controlling the installations.

As a rule, therefore, it makes sense to divide the establishment into a number of subsectors of different types and risks.

An exhaustive investigation of all potential weaknesses combined with the many and various conceivable actions usually results in a bewildering number of variants. For this reason it makes sense to attempt a broader grouping of installation areas or parts.

It may for example be practical to regard a coherent complex as a single entity, in other words without investigating in great detail what individual components and parts are sensitive and what precise effects any attack might have on individual components of the plant.

The installation complex in question is classified as safety-relevant and protected as a whole so that all individual components are covered by the whole. For example, if access by unauthorised persons to a battery of valves is prevented, it is immaterial which valves could be manipulated and how.

In the cases of supply systems used throughout the entire establishment, one should as far as possible form subsectors relating to items at risk from major accidents, and the analysis should not be unnecessarily extended to wide-ranging overall systems.
Examples of useful groupings of risk areas might be:

- Tanks, containers, storage facilities
- Filling stations
- Control centres, switch panels, computer systems
- Pipe channels
- Cable routes
- Pump buildings
- Valve batteries
- Production buildings, sections
- Cooling units

- Emergency systems of all kinds
- High-voltage lines and in-feed points
- Electrical supply facilities
- Energy supply systems of all kinds etc.

4.2 Consulting safety report

When discussing the possible ways in which damage can arise, the information in the safety report must be consulted. The factors which have to be covered here, such as process description, sequence of events, information about storage quantities and above all the description of individual sources of danger, are of fundamental importance for the safety strategy.

When considering deliberate acts by persons, however, the question has to be examined in a broader context, because the deliberate action permits additional possibilities for damage taking place. Thus from a safety point of view it may be regarded as sufficient to provide a double emergency supply, but this is not the case if where criminal acts are assumed, if – for example – both emergency systems can easily be switched off by interfering with the control system. In safety reports the simultaneous occurrence of different disturbance factors (e.g. substance contamination resulting in thermal reactions, plus failure of the cooling system) is frequently regarded as improbable. In the context of security analysis it is essential to examine the extent to which the two disturbance factors could be deliberately provoked at the same time.

4.3 Table of points at risk

If one lists a number of conceivable forms of interference and compares them with the identified points at risk, this produces a table providing a clear picture of the points or areas in the establishment where a serious disturbance could be caused and the various methods and means used to do so. The following *Fig. 2* gives an example of this approach. In practice it may also be possible to summarise the various possible actions, e.g. “interference using simple or heavy tools” etc..

No.	Possible act	Point at risk 1 “Tank storage”	Point at risk 2 “Process technology building”	Point at risk 3 “Pipeline bridge”	Point at risk 4 “Control centre”
01	Deliberate misoperation	Yes	Yes (by employees during production)	No	No
02	Manipulation	No	No	No	Yes
03	Vehicle traffic	Yes	No	No	No
04	Interference using simple tools	No	Yes	No	No
05	Interference using heavy tools	Yes	Yes	Yes	No
06	Arson using simple means	Yes (in explosion-risk sector)	Yes (in explosion-risk sector)	No	No
07	Arson using incendiary devices	Yes	Yes	No	No
08	Use of explo-sives	Yes	Yes	Yes	No
09	Shooting	Yes	No	Yes	No
10	Incidents out-side the plant itself	Yes (fire in build-ing ‘X’)	No	No	No
11	Theft of haz-ardous sub-stances	No	No	No	No

Fig. 2: Example of a table of points at risk

The following **acts of interference / instruments** are assumed to be basically conceivable:

Deliberate misoperation (01)
This is taken to mean all deliberate acts by means of which a major accident could be caused by simple operations and without the use of instruments.
Such acts could include:

- Switching equipment on/off,
- Opening/closing pipeline valves,
- Turning hand wheels, actuating levers in the course of the process etc.

Such deliberate misoperation might be caused by employees or external individuals.

Manipulation (02)
Manipulation is taken to mean deliberate alteration or adjustment of system parts with the aim of causing a critical installation state. Examples of this might be:

- Deliberate incorrect programming of control systems,
- Deliberate incorrect adjustment of measuring equipment,
- Suppression of process, fault or alarm reports,
- Preparatory prevention of starting of emergency units,
- Switching off protective systems etc.

Only “insiders” with a detailed knowledge of the installation are possible perpetrators.

Vehicle accident (03)
Vehicle accidents affecting road or rail traffic in the establishment could release hazardous substances or damage or destroy important parts of the installations. Examples include:

- Leakage from drum due to accident with fork lift truck.
- Derailment of tank cars,
- Destruction of installations due to truck impact etc.

Possible perpetrators are employees and external individuals.

Interference using simple aids (04)
These are cases of deliberate, usually spontaneous, interference with important parts of installations using tools and aids that are present in every plant (hammer, chisel, pliers, hand axe, blowtorch, lock-cylinder puller). Examples of this might be:

- Cutting wires,
- Breaking glass parts of installation (e.g. level gauges),
- Jamming moving parts of an installation,
- Admixture of non-permitted substances to a process etc.

The most likely offenders are employees.

Interference using major aids (04)
Such acts presume the prepared destruction of installation parts by force.
The tools used might be crowbars, power drills, cutting torches, bolt cutters, sledgehammers, unblocking tools for cylinder locks, powder cutting torch, diamond-bit drill, oxygen lance.
Examples of this are:

- Breaking open doors and subsequently destroying equipment,
- Demolishing instrumentation and control equipment,
- Breaking open tanks and pipelines, resulting in major leakages etc.

Instead of a targeted attack, vandalism may occur, e.g. in a blind destructive frenzy following an unsuccessful break-in.

Arson using simple means (06)
Simple means is taken to mean igniting with matches, lighters or cigarette ends. As a result, this kind of interference is only possible in the presence of adequate quantities of combustible and easily flammable materials.
Examples of this might be:

- Igniting flammable liquids from the process sequence,
- Setting fire to storage facilities, resulting in release of hazardous substances,
- Setting fire to peripheral rooms or equipment having an impact on important parts of installations.

Arson using incendiary devices (07)
This is a mater of incendiary attacks performed with the aid of substances that burn quickly and fiercely. Examples of such attacks might be:

- Pouring out and lighting flammable liquids (e.g. petrol),
- Throwing “Molotov cocktails” (e.g. through windows),
- Attaching professional incendiary devices with timed or remote controlled ignition.

Such attacks presuppose a high level of criminal energy.

Use of explosives (08)
Such attacks may use home-made, commercial or military explosives. Possible modes of attack include:

- Placing a home-made “fire extinguisher bomb” inside sensitive installation parts or, more probably, at the edge of buildings,
- Blowing up tanks and pipelines,
- Blowing up load-bearing structures, resulting in the collapse of tanks,
- Destroying parts of installations etc.

As a rule this kind of attack involves external interference with a radical political background.

Shooting (09)
This may range from the simplest case of air rifles or catapults (steel balls) right up to use of heavy weapons by terrorists. The forms of interference could include

- Causing leakages in free-standing tanks or pipelines,
- Eliminating instrumentation or control equipment from a distance,
- Causing failure of supply systems at a distance.

Shooting is above all possible from outside the external enclosure of an establishment or industrial estate; installation parts located close to the fence are at greater risk.

Incidents outside the plant itself (10)

The entire installation or security-relevant parts of the installation may also be affected by accidents caused deliberately in neighbouring establishments or transport systems. Possible impacts might be:

- Spreading of fire from neighbouring facilities,
- Flying debris following an explosion in neighbouring facilities,
- Failure of supply systems as a result of disasters outside the installation etc.

Such impacts presuppose special risk potential in the surrounding facilities (domino effect as in Sect. 15 of the Major Accidents Ordinance).

Potential impacts 01 to 10 assume events that may relate more or less to all establishment. It is also possible to conceive of establishment-specific hazards that are dependent on the production process. Such cases may open up additional opportunities for acts by unauthorised persons.

For each cell in the table it is necessary to discuss the extent to which such interference can cause a major accident at this place. As a rule it is necessary to assess the risk of a major accident, e.g. on the basis of the assumptions:

1. Major accident not possible,
2. Major accident unlikely,
3. Major accident can only occur together with other impacts,
4. Major accident is possible,
5. Major accident is unavoidable.

For assumptions 1 and 2 the relevant cell is labelled “No”, for 4 and 5 it is labelled “Yes”. If only a combination of two or more possible impacts can bring about a major accident (assumption 3), an appropriate entry should be made.
Examples of combinations are:

- Leakage and arson
- Failure of cooling system and emergency cooling system etc.

In most cases it is not necessary to assume excessively complicated interference by unauthorised persons with simultaneous action or complex preparations in several places.

5 Hazard assessment

A hazard assessment taking account of the risk categories yields, for each of the possible forms of interference, an indication of whether there are reasonable grounds for expecting the possibility assumed.

If not all the risk categories are equally applicable, as is the case with the majority of installations, the table of points at risk can be reduced accordingly. For example, if the possibility of massive terrorism (risk category 3) is ruled out entirely, this usually results in the elimination of interference using explosives (08) or firearms (09), and the result is a picture of the effective risk *(see Fig. 3).*

No.	Possible interference	Point at risk 1 "Tank storage"	Point at risk 2 "Process engineering building"	Point at risk 4 "Control centre"
01	Deliberate misoperation	Yes	Yes	_____
02	Manipulation	_____	_____	Yes
04	Interference using simple aids	_____	_____	_____
06	Arson using simple means	Yes (in explosion-risk sector)	Yes	_____
07	Arson using incendiary devices	Yes	_____	_____
10	Incidents outside the plant itself	Yes Yes (fire in building 'X')	_____	_____

Fig. 3: Reduced table of points at risk

Further reductions can be achieved if possible forms of interference are considered at different times. For example, the possibilities "deliberate misoperation" and "vehicle traffic" can be disregarded after working hours. During working hours, for example, the risk of interference using major aids is considerably smaller than outside working hours.

6 Security objectives

Meaningful planning of security measures is only possible if clearly defined objectives exist as to what they are intended to achieve.

The table drawn up at the hazard assessment stage *(cf. Appendix 1, Chapter 5)* indicates where a major accident could be caused by what means. Conversely, one can use it to derive security objectives, namely the prevention of major accident occurrence at the points in question.

On the basis of the security objectives it is expedient to set out the basic direction for the design of security measures, so that detailed design does not get bogged down in discussing an excessive diversity of alternative solutions, many of which are completely out of the question. As a rule it will not be necessary here to lay down a special security measure for each individual weak point identified; instead it will usually be possible to group together several points at risk.
For example, if a building includes several rooms with important components that are identified as points at risk, the security measure could be: "Steps must be taken to prevent external personnel entering building XY."

It is clear from this example that the security measures must be considered very carefully by specialists to ensure that they can be implemented and that the measures to be taken can be effected with a reasonable input of resources.

For example, if closer investigation reveals that access to the building for external personnel cannot be prevented for reasons relating to essential workflows (e.g. external maintenance company), the security measure could be modified as follows: “Steps must be taken to prevent external personnel entering rooms A, B and C in building XY” or, if this cannot be enforced: “External personnel must not be allowed to enter the building except when accompanied by members of the relevant department”.
Other typical security requirements might be:

- The control equipment including the software must only be accessed by specially authorised personnel.
- Security-relevant switching systems must be monitored by the hazard warning system. In the event of incorrect operation an alarm sounds in the control room.
- The danger area is to be separated from the rest of the building by constructional/ mechanical means.
- Ingress into the storage building after working hours is to be impeded by mechanical barriers and reported by electronic surveillance measures etc.

7 Description of security measures / security strategy

As already explained, proper functional interaction of all security measures of a personnel, organisational, constructional and technical nature is a precondition for effective site security. In order to make these relationships clear, the individual measures should be described within the context of an overall strategy. For this purpose the use of a **structure** tried and tested in practice is recommended. The main items of this might be as follows:

1 Location and position
2 External enclosure
3 Site access controls (pedestrians and vehicles)
4 Protecting areas at risk
5 Organisational measures
6 Security organisation
7 Alarm, surveillance and communication systems

A comprehensive description of the security measures necessarily includes information requiring special confidential treatment, cf. Appendix 1, Chapter 8.

7.1 Location and position

The location and position are already described in the safety report. Additional information is useful at this point if any security measures are dictated merely by the location and position of the site. For example, this is the cases with installations lying within a large site complex that is itself already protected by security measures.

A site plan is necessary to provide a clear picture of the local geography. Many of the items of information required below can be shown in the site plan. It should contain the following details:

- Position of legal boundary of the establishment,
- Position of perimeter enclosure with details of type and nature,
- Position of gates and access points including gatehouses,
- Details of immediate surroundings of the establishment (terrain, buildings)
- Transport routes to the establishment,
- Transport routes within the establishment,
- Car parks inside and outside the establishment, local lighting arrangements,

- Buildings and facilities on the site with details of the functions,
- Areas and points at risk in the establishment with identification of access points, special enclosures etc., and
- Routing of security-relevant cables and pipes.

7.2 External enclosure

The external perimeter enclosure of an establishment or industrial estate is intended to keep unauthorised persons off the site and to direct pedestrian and vehicle traffic via controlled access points. This presupposes not only suitable general quality of the perimeter enclosure, but also its complete continuity without any gaps.
The description of the perimeter enclosure should include the following details:

- Description of perimeter enclosure, preferably with the aid of a site plan giving details of the nature of the surrounding terrain.
- Details of the type and construction of the enclosure, such as wire mesh fence, masonry wall etc. – where appropriate with identification of different sections on site plan.
- Details of the quality of the perimeter enclosure, including
  - mechanical structure,
  - height,
  - protection against climbing over,
  - protection against crawling/digging under.
- Details of pedestrian and vehicle access points, including:
  - construction (escape door, traffic gate, turnstile),
  - lock,
  - remote control,
  - electronic surveillance,
  - surveillance with video camera.
- Details of lighting arrangements around perimeter.

7.3 Site access controls

7.3.1 Control measures

The reliable functioning of a perimeter enclosure presupposes control of pedestrian and vehicle access to the site or industrial estate. This section should describe the arrangements for

- Pedestrian traffic entering and leaving the site, with access points and routes (site plan), control procedures for employees, control procedures for visitors, control procedures for third-party employees, where appropriate (e.g. random) checks on material taken into/out of site, and

- Vehicle traffic entering and leaving, with access points (site plan), control procedures for persons and materials in company and third-party vehicles.

7.3.2 Gatehouses

Gatehouses or porters' lodges are important security facilities with the principal function of controlling pedestrian and vehicle access to the site.

Except in large establishments or industrial estates with their own alarm centre, the security buildings at the gate usually contain central technical safety systems. These may relate to the following functions, for example:

- Receiving safety/security alerts of all kinds (fire, water, abnormal operation, break-in),

- Alerting internal or external emergencyresponsers by telephone, public address system, paging system, receivers for radio warnings etc.,
- Remote surveillance and remote control of access points, e.g. using video systems,
- Switching on lighting,
- Informing emploees, e.g. by public address system,
- Communication with own security staff, e.g. by walkie-talkie,
- Taking calls received by branch exchange after working hours etc.

Thus the gatehouses have a considerable security significance above and beyond the task of controlling pedestrian and vehicle access. This raises the question of the security of the gatehouses themselves. For example, if the main gatehouse is the only place for receiving alarm and abnormal operation alerts (frequently only after the end of normal working hours), it must not be possible to prevent forwarding of such alerts to assistance providers by taking control of the telecommunications equipment or threatening the security staff in the gatehouse. This must be ensured by appropriate technical protective measures in particular. Uninterrupted manning of the gatehouse is also of central importance.

In this case the security strategy must pay particular attention to the main gates. The details should include the following:

- Position of gatehouses on the site (site plan),
- Constructional/mechanical design,
- Steering of vehicle traffic with traffic direction at gatehouse, position of barriers and gates, seat/position of controlling member of security staff, position of visitor car park,
- Direction of flow of people with traffic routes, clearance points (for employees and visitors),
- Lighting of gatehouse area,
- Description of constructional design, especially barrier effect of doors and windows,
- Plan view with room layout and details of functions,
- Gatehouse manning details (numbers, shift times),
- List of alarm, surveillance, control and communication systems and operating equipment in gatehouse.

7.3.3 Site

Information about the site serves to provide an overview of position of items at risk and requiring protection. The information should include:

- Transport routes,
- Buildings with details of use/function,
- Where appropriate, identification of individual important areas,
- Routing of safety-relevant cable and pipe connections, underground pipes/channels etc.,
- Points of special danger.

Important details of the information about the site may be shown on the site plan.

7.4 Protecting areas at risk

Protecting the individual areas at risk is usually the most important defence measure, since the “external” measures relating to the site as a whole can rarely achieve completely adequate protection. For example, a risk of deliberate action by employees is not affected by “external” measures.
Moreover, control of access to the establishment (e.g. at the start of a shift) can scarcely be ensured without any gaps at all. By contrast, there are certainly means of performing much more effective checks at individual points in the establishment.
In most cases, therefore, the measures to protect the site as a whole have a basic protection function; they form a first threshold for keeping out unauthorised persons.
Individual protection for all existing points at risk must be provided in addition as the most effective form of defence. Here the “classic” measures aimed at plant security play a significant role. This applies in particular to redundant provision of especially critical safety facilities; security considerations may make it necessary to locate these in separate places.

Defence measures against terrorist attacks in particular are described in Appendix 2.

The security report should therefore describe separately the security measures for each individual point at risk, though it makes sense to group them in terms of areas, buildings, sections or functional units on the lines shown in Appendix 1, *Chapter 4 “Points at risk”*. It goes without saying that this information in particular must be treated especially confidentially.

The following information should be provided for the individual points at risk:

- Position on the site (site plan), position within buildings or areas (building plan),
- Pedestrian and vehicle access points, escape routes,
- Constructional/mechanical measures to separates areas (walls, fences),
- Constructional design of buildings and security-relevant rooms (materials, reinforcement, wall thicknesses),
- Mechanical protection of doors, windows and openings,
- Electronic surveillance measures for doors, windows, rooms etc.,
- Handling of access controls to the points in question during and after working hours for employees and external persons,
- Protection of individual operating elements against incorrect operation or sabotage, e.g. by means of mechanical locks or electronic monitoring,
- Attaching cautionary and warning notices,
- Special security measures,
- Working and shift hours for the relevant department; if necessary, differentiated security measures,
- Patrols of objects by security staff (patrol routes, times).

7.5 Organisational measures

Organisational measures form an important framework in which to incorporate a variety of individual measures to ensure the reliable functioning of the security system as a whole. Aspects that should be dealt with in this connection include:

- Site ID badges with issuing/return of badges, badge coding (nature and handling), storage of badges (access protection), competencies,
- Appointment and monitoring procedures for employees with security functions, permission to enter points at risk, workplaces within areas at risk,
- Training and instruction of individuals, e.g. to avoid incorrect operation,
- Rules for supervision and regular controls relating to work in security-relevant areas,
- Individual key arrangements with lock system (type, extent, age), issuing, return and registration of keys, keeping of keys and cylinders,
- Cleaning of security-relevant areas with company or external personnel, cleaning

times, supervision during cleaning, check on personnel (for external personnel).
- List of instruction sheets for all measures connected with security,
- Alarm plans for fire/explosion, leakages, threats to wastewater, installation-specific incidents etc.

A comprehensive description of security management can be found in Appendix 3.

7.6 Security organisation

This chapter is intended to provide an overview of the human resources organisation necessary for the security of the establishment. This includes site security, fire protection, work safety and environmental protection, and the departments responsible for the repair and maintenance of the installations. The overall organisation should be shown in an organisation chart that gives a clear picture of the hierarchical relationships.

A central role in installation security is played by the site security department, about which detailed information is necessary such as:

- Hierarchical relationships (organisation chart), total numbers,
- Shifts and numbers,
- Use of company and/or external personnel,
- Supervision/spot checks (for external personnel),
- Functions and assignments,
- Education and equipment,
- Training, and
- Instruction sheets, alarm plans.

7.7 Alarm, surveillance and communication systems

The following items should be described for the individual systems employed with security functions:

- Function and use in the establishment,
- Local arrangement in establishment,
- Location and security of central facilities,
- Arrangement and security of operating station,
- Routing and security of cables.

For large systems it is useful to have an overview circuit diagram.

8 Documentation

Formatiert: Nummerierung und Aufzählungszeichen

The analysis and the measures based on it should be documented. This documentation, however, is especially confidential and should only be accessible to a limited group of employees within the company. It should however be clear from documents available to all employees and the public that the operator has taken the necessary measures to protect the establishment and installations from interference by unauthorised persons.