SFK

HAZARDOUS INCIDENTS COMMISSION

under the
Federal Ministry for the Environment,
Nature Conservation and Nuclear Safety (BMU)

Guideline

Combating Interference by Unauthorised Persons

by the ad hoc Working Group
“Interference by Unauthorised Persons”

SFK-GS-38

Hazardous Incidents Commission (SFK)

Guideline

Combating Interference by Unauthorised Persons

approved at the 41st meeting of the SFK on 23 October 2002

The Hazardous Incidents Commission (Störfall-Kommission – SFK) is a commission set up pursuant to Section 51a of the Federal Immission Control Act under the Federal Ministry for the Environment, Nature Conservation and Nuclear Safety.

Its office is located at GFI Umwelt – Gesellschaft für Infrastruktur und Umwelt mbH.

Contents: Page:

1. Assignment

In view of the terrorist attacks in the USA on 11 September 2001, the Federal Ministry for the Environment, Nature Conservation and Nuclear Safety (BMU) requested the Hazardous Incidents Commission (SFK) to investigate the consequences arising from the new threat situation in the field of installation safety. At it's meeting on 25/26 September 2001 the SFK thereupon decided to set up an ad hoc working group. The results of its deliberations are set out in this Guideline, which the SFK approved at its meeting on 23 October 2002.

The Ministry indicated that the SFK was to examine the following issues in particular:

- Examination of the paper produced by the VCI [German Chemical Industry Association] (see below) with a view to suitable specification of the aspects mentioned there.

- Proposals regarding the extent to which the safety report and the emergency plans should cater for preventing attacks and minimising the consequences of attacks.

- Proposals on the extent to which the General Administrative Provision on the Major Accidents Ordinance, prepared by the Ministry, should take account of interference by unauthorised persons in its requirements regarding safety precautions and scenario descriptions.

- Proposals on achieving a balance between the legitimate public interest in information on the safety of industrial establishments and the potential security risks arising from such information.

The ad hoc group looked into all these aspects. To this end it studied the VCI policy paper of 2 October 2001 on "Safety Precautions by Chemical Industry Companies against Terrorist Attacks", which describes the preventive measures against terrorist attacks that operators currently need to take as part of their duty to combat interference by unauthorised persons, and recommends the member companies to use these measures. Also on the table were statements by various members of the ad hoc group, the "Site Security Guidelines for the U.S. Chemical Industry" (2001), a brochure by BP entitled "Getting Security Right – The Basics for Security Management" (Issue September 2000), and German Federal Environmental Agency Research Report 104 09 210 on "Technical and organisational measures for protecting installations governed by the Major Accidents Ordinance against interference by unauthorised persons" (1988).

Important results, which are also taken as a basis for this Guideline, were summarised in an interim report in December 2001, which was approved by the SFK on 16 January 2002 and published by the Ministry on 12 February 2002.

2. Scope of application

In line with the terms of reference of the Hazardous Incidents Commission, the present study is confined entirely to examining installations and establishments in accordance with the Major Accidents Ordinance. The starting point is the operator's duty to secure them from interference by unauthorised persons in accordance with Art. 3 Para. 2 no. 3 of the Major Accidents Ordinance. This must be done in such a way that hazardous substances present in the installations are protected from intentional disturbances such that a serious danger within the meaning of the Major Accidents Ordinance can reasonably be excluded.

The Guideline primarily addresses upper tier establishments and installations. However, lower tier establishments and installations pursuant to Art. 1 Para. 3 and 4 of the Major Accidents Ordinance may also be concerned if examination of the individual case reveals a possibility that an object meriting special protection may be affected.

In line with the existing provisions of the Major Accidents Ordinance, a number of the measures or examination steps suggested below are necessary in any case. This is indicated in the text by using ***italics***.

This Guideline focuses on dangers to people. Although terrorist attacks aimed at the environment ("eco-terrorism") may indeed represent a serious threat, in the interests of a pragmatic, step-by-step approach this Guideline does not deal specifically with purely environmental impacts. It is however possible to use the same approach with appropriate modifications.

External transportation of dangerous goods is not subject of this guideline. In principle, however, the security approach required for transportation of dangerous goods is basically similar to the approach adopted here for stationary installations. Entry and exit paths and especially their security must be examined in the individual case for interfaces with the transport sector and dealt with accordingly. Special consideration must also be given to theft or deliberate misuse of chemicals.

Attacks via companies' electronic networks ("cyber attacks") are regarded as a less serious hazard. As a rule, external access to the computers that directly control installations (and it is only these that are relevant for installation safety) is extremely difficult (no link or no permanent link with externally accessible data networks, different operating systems, process systems that revert to safety setting if the computer fails). If these conditions are not satisfied in individual cases, the operators should take suitable measures to prevent interference by unauthorised persons. The ad hoc group was however unable to make a closer scrutiny of these aspects.

Neither does the study examine other forms of criminal attack on companies, such as industrial espionage.

3. Definitions (for the purpose of this Guideline)

Facilities requiring special protection are establishments that are regularly intended for the presence of large numbers of people (schools, meeting places, hospitals, stations etc.). This includes densely populated residential areas and transport routes with high traffic densities. In this connection the study considers only those facilities requiring special protection where there is a direct or indirect threat to the lives of large numbers of people or their health is seriously impaired.

Security-relevant installations are installations in an establishment pursuant to Art. 3 Para. 5a of the Federal Immission Control Act in conjunction with Art. 1 Para. 1 and 2 of the Major Accidents Ordinance, and installations pursuant to Art. 1 Para. 3 and 4 of the Major Accidents Ordinance which are, in the event of interference by unauthorised persons, capable of giving rise to a serious danger within the meaning of the Major Accidents Ordinance to facilities requiring special protection.

An **unauthorised person** within the meaning of Art. 3 Para. 2 no. 3 of the Major Accidents Ordinance is in this case any person who deliberately commits acts with the aim of directly or indirectly causing damage. For this purpose it is irrelevant whether the person is an employee of the operator, an agent of the operator, or a third party.

Security means all activities designed to prevent dangers, which may arise from interference by unauthorised persons, and to achieve preventive minimization of the consequences of any major accidents nevertheless caused by unauthorised persons. Operators, authorities or other third parties may contribute to security. It is important to distinguish here between “security” [“Sicherung” in the German text] and “safety” [“Sicherheit” in the German text].

A **security analysis** is the identification and assessment, by systematic means, of potential interference by unauthorised persons and of the dangers that may result from such interference. In particular, such an analysis calls for knowledge of the possible motivation and capability for acts of unauthorised persons. The security analysis brings together the identification and assessment of the specific threat situation (**threat analysis**) with the results of identifying hazards in the context of the **hazard analysis** that is in any case required under the Major Accidents Ordinance. The security analysis may be a prerequisite for drawing up **security objectives** and the necessary **security measures** as part of preparing a **security concept**. Documentation and regular reviewing and updating of the security analysis are advisable in the event of both significant changes and special circumstances.

4. Concept for identifying and protecting security-relevant installations (security concept)

Proofing that adequate precautions have been taken by the operator in particular against interference by unauthorised persons should be part of a security analysis. A suitable method is outlined here and an example is described in Appendix 1. For this purpose the operators must in particular:

a) undertake, in agreement with the authorities responsible for public security, a systematic examination of establishments and installations pursuant to the Major Accidents Ordinance to determine whether they may represent a special target (threat analysis, see Appendix 1, Chapter 3) and
b) investigate, in consultation with the authorities responsible for external emergency management, whether interference by unauthorised persons with destructive intent is capable of giving rise to a serious hazard (hazard analysis).

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 threat 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. The approach taken in the following text, i.e. performing the hazard analysis first, makes use of information that is usually available in any case to narrow down in a first step the group of installations to be examined (and hence the scope of application of this Guideline). The approach adopted in Appendix 1 of first analysing the threat due to interference by unauthorised persons and only then the possible consequences, has the advantage that it also identifies security problems that are below the level of a serious hazard.

4.1 Hazard analysis

For the purpose of this Guideline, special consideration must be given to parts of the establishment (e.g. installations) where a “major accident despite precautions” [“Dennoch-Störfall” in the German text], which occurs in the vicinity of facilities requiring special protection, threatens people’s lives or gives cause to fear serious impairment of people’s health.

Here the impacts of possible interference by unauthorised persons should be taken into account by:

- Describing the “major accidents despite precautions” (release, explosion or fire of the largest single quantity of substance) in accordance with Art. 3 Para. 3 of the Major Accidents Ordinance in conjunction with Guideline SFK-GS 26. “Domino effects” must be taken into account, especially on industrial estates (chemical parks). *Among other things, this information is a prerequisite for notification of the emergency management authorities pursuant to Art. 10 Para. 1 no. 2 of the Major Accidents Ordinance (see below) and, as recommended by the Hazardous Incidents Commission, should also form part of the safety reports.*
- Identification of facilities requiring special protection within the meaning of the above definition (see also Appendix 1, Chapter 4). Such facilities will usually be in the area surrounding the establishment. In “open” industrial estates, however, they may also be within the industrial estate itself. *This information is part of the safety reports.*

- Assessment of the impacts of “major accidents despite precautions” on the facilities requiring special protection. *This information is in any case necessary as part of the information to be supplied to the emergency management authorities in accordance with Art. 10 Para. 1 no. 2 of the Major Accidents Ordinance.*

It is advisable to review the studies of “major accidents despite precautions” that already exist to check that they take account of the hazards that could, according to the threat analysis, arise from interference by unauthorised persons even if it was reasonable to exclude the likelihood of their occurring as disturbances of normal operation (e.g. destruction of passive safety equipment, see also Appendix 1, Chapter 5).

4.2 Threat analysis

If the hazard analysis in 4.1 reveals that a serious hazard within the meaning of the Major Accidents Ordinance may be caused to facilities requiring special protection, 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. In some cases the operator must obtain the necessary information from the authorities responsible for public security, and it is advisable to involve them in this step in any case.

- Assessment of the threat 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),
- Location of establishment and installations (vulnerability from outside and inside, distance from factory fence, visibility from outside, roads on and off site, case 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, relevance of the company from an economic strategy point of view etc.).

4.3 Protecting security-relevant installations

Where installations are identified by steps 4.1 and 4.2 to be security-relevant, the operators in conjunction with the authorities responsible for public security 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 (e.g. damaging site fence, attacking security staff) or fraudulent misrepresentation (e.g. forging site IDs) and that ingress by force is detected within a reasonable time (e.g. by means of alarm systems, video monitoring, patrols etc.).
- Non-site personnel should be identifiable, e.g. by openly wearing distinguishable site ID badges. Visitors and staff of external companies must be monitored appropriately.
- The installations themselves are to be protected such 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, e.g. by means of team training, seminars, training courses etc. (see also Chapter 7).

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).

It is advisable to make the choice of suitable measures by means of the security analysis described here. Examples of security measures are described in **Appendix 1, Chapter 7**, and examples of preventive measures against attacks in Appendix 2**.**

Most of these measures are already in use or can be introduced relatively quickly. Operators should review the effectiveness of existing measures, if they have not done so already, and take any measures that may be necessary. A particularly important role is played by the qualitative and quantitative human and technical resources assigned to staff involved in security aspects (e.g. site security). The authorities for their part should examine the measures taken as part of their supervisory duties pursuant to Art. 16 of the Major Accidents Ordinance.

Safety reports are to be supplemented and/or updated in accordance with Art. 9 Para. 5 no. 3 of the Major Accidents Ordinance by including the analyses of the potential consequences and threats and also the resulting measures and information for drawing up external emergency plans. Where only lower tier installations and establishments are concerned, it is recommended that the relevant information also be documented in writing.

In addition to possible improvements in security technology and organisation, good and close cooperation between operators and the public security and emergency authorities is particularly important. Where external support, e.g. by the police, is necessary to ensure protection from interference by unauthorised persons, the operator should make contact with the competent authorities without delay.

4.4 Measures to minimise the consequences of major accidents

In the event of a "major accident despite precautions", the operators shall take measures to minimise its consequences (Art. 3 Para. 3 of the Major Accidents Ordinance). Widely used and tested measures for minimising the consequences of "major accidents despite precautions" are listed, for example, in Appendix 6 to SFK Report SFK-GS-04.

In order to be able to control the consequences of possible interference by unauthorised persons with security-relevant installations, this information about "major accidents despite precautions" must be in the possession of the emergency authorities. They in turn must transpose the scenarios into appropriate emergency plans.

The legal situation here is that operators of upper tier establishments or installations must provide the emergency management authorities with such information without being asked (Art. 10 Para. 1 of the Major Accidents Ordinance). Operators of lower tier establishments or installations must compile the information necessary for compiling external emergency plans and must supply it to the emergency management authorities on request (Art. 6 Para. 4 of the Major Accidents Ordinance). In individual cases the authorities may impose on them obligations under Articles 9 to 12 of the Major Accidents Ordinance, e.g. to compile a safety report containing information on protection against interference by unauthorised persons, or to compile an internal emergency plan.

The following **recommendations** are made with regard to consequence minimisation measures:

- Even Operators of lower tier establishments and installations which have proved to be security-relevant should, in their own interests, contact the emergency management authorities without delay to provide them with the information necessary for compiling external emergency plans. The environmental protection and emergency management authorities should liaise with a view to identifying such potentially relevant installations.

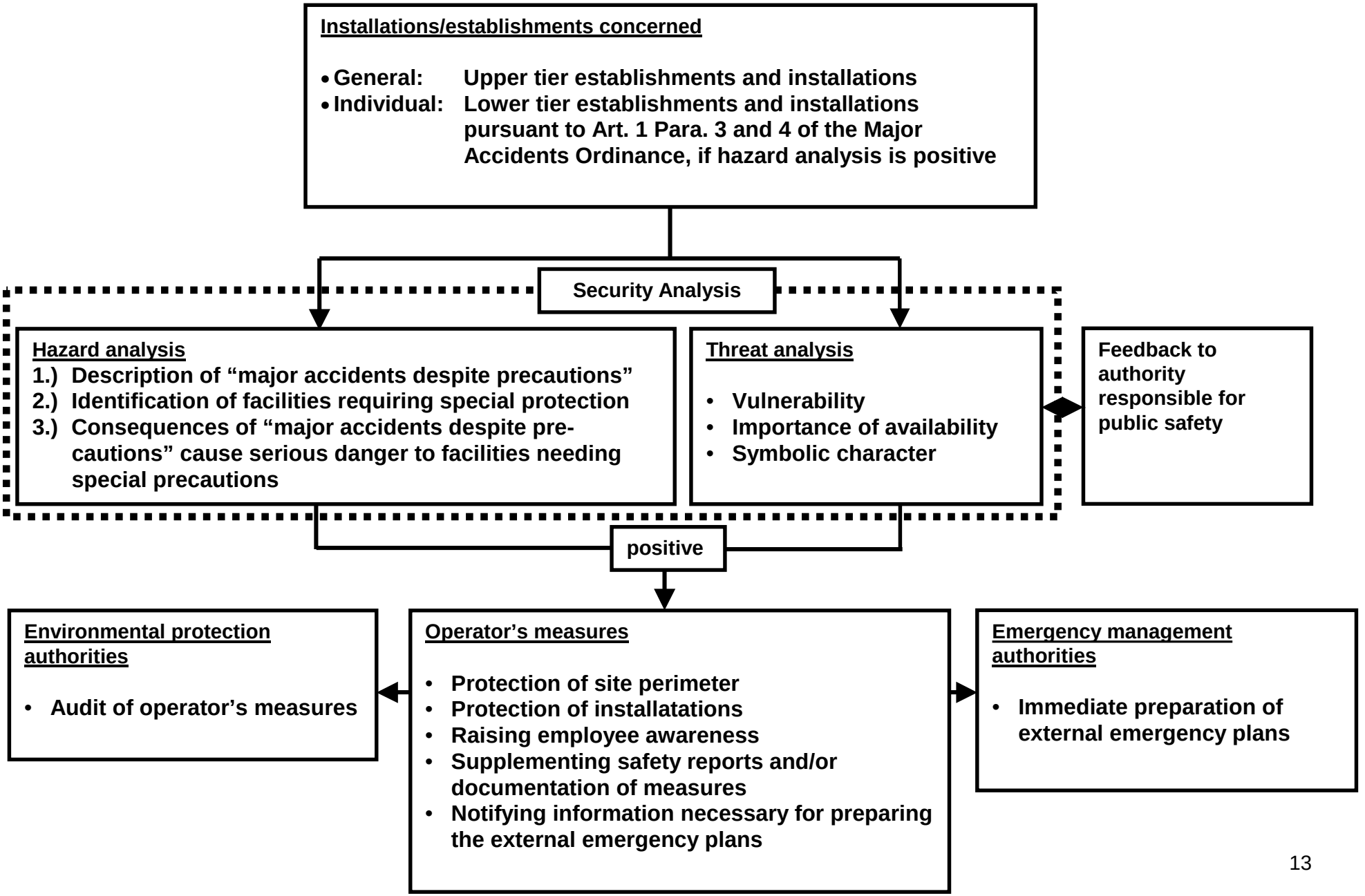
- The competent emergency management authorities should draw up the necessary external emergency plans without delay on the basis of the available information from the operators in order to protect the public from interference by unauthorised persons.

- Regarding the preparation of the necessary documentation by the operator for the emergency management authorities, see Report SFK-GS-26.

4.5 Graphic outline of concept for identifying and protecting security-relevant installations

The following diagram gives an overview of the concept suggested in Chapter 4:

Protecting establishments/installations from interference by unauthorised persons



5. “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. Information on establishing and maintaining a security management system can be found in **Appendix 3**.

Operators are recommended to grade the measures in terms of the current threat situation (from “no threat” to “establishment invaded by unauthorised persons”). It should also be borne in mind that the threat situation may change very quickly as a result of internal and external developments, and should therefore be kept under constant observation.

6. Disclosure of security documentation

With regard to reservations about the publication of sensitive data in licensing procedures or in the safety report, it must first be noted that the existing legal basis is already sufficient to permit restrictions if necessary. 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. As well as weighing up the legal assets, therefore, it is necessary to develop criteria for weighing up the possible loss of safety against a possible gain in security.

Art. 11 Para. 3 of the Major Accidents Ordinance lays down that the operator must keep the safety report available for inspection by the public. The operator may however demand from the competent authority that certain parts of the safety report, inter alia *for reasons of public safety, do not have to be disclosed. This requires the consent of the competent authority. In that case a modified safety report must be made available to the public. This report must be sufficiently detailed to enable third parties in particular to judge whether and to what extent they could be affected by the consequences of a major accident in the establishment (on the lines of Art. 10 Para. 2 of the Federal Immission Control Act).*

It is recommended that a restriction of disclosure of information for reasons of public safety should only be permitted for establishments/installations, which are to be regarded as security-relevant on the basis of the hazard analysis (Chapter 4.1) and the threat analysis (Chapter 4.2). Only then is a restriction of disclosure permissible, with modification or omission of the specific security-relevant information in the form of a revised version (“qualified presentation of content”), but this must remain an intrinsically comprehensible and coherent presentation (on the lines of Art. 4 b Para. 3 of the Ninth Federal Immission Control Ordinance).

An example of a decision as to which items of information should be treated in confidence and which should be made available to the public is given in Appendix 4.

7. 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.

8. Summary

The situation can be summarised as follows:

1. It is basically possible for attacks on an establishment to be mounted by external or internal offenders. Both the state as the guarantor of public security and the operator have duties with regard to preventive measures. This calls for additional input by both parties.

2. For many years it has been the duty of operators under the Major Accidents Ordinance to protect their establishments and installations against interference by unauthorised persons. For this purpose the concept in Chapter 4 is recommended. Under the new threat situation it is necessary to impede and if necessary detect ingress by unauthorised persons into the relevant establishment, for example by means of effective fences kept under surveillance, organisation of gate controls and patrols etc. It may be necessary to take additional measures to protect installations or parts thereof that are especially hazardous and endangered by terrorist attacks from interference by unauthorised persons.

3. 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. Examples of this are given in Appendix 2. The necessary resources for this purpose must be made available even in times of limited budgets.

4. The measures taken by the state and by the operator should be in keeping with the nature and extent of the risk.

5. 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.

6. Much of the information necessary for assessment of the threat situation by the operators and the authorities is already available under the provisions on the safety report (Art. 9 of the Major Accidents Ordinance) and on the emergency plans (Art. 10 of the Major Accidents Ordinance, and legislation on fire and disaster control of the *Länder*) or was to be compiled not later than 3 February 2002.

7. An important legal basis for the necessary measures already exists, in particular in Articles 3 to 6, 9 and 10 of the Major Accidents Ordinance and the legislation on fire and disaster control of the Länder. Further details of these requirements on the lines of this Guideline are to be given in the new General Administrative Provision on Major Accidents planned by the Federal Ministry for the Environment, Nature Conservation and Nuclear Safety (BMU).

8. 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 analysis (Chapter 4.1) and the threat analysis (Chapter 4.2). Only then is a restriction of disclosure permissible, with modification or omission of the specific security-relevant information in the form of a revised version ("qualified presentation of content"), but this must remain an intrinsically comprehensible and coherent presentation (on the lines of Art. 4 b Para. 3 of the Ninth Federal Immission Control Ordinance).

9. Generally speaking, it must be said that a threat to establishments/installations from terrorist attacks must be looked at in a differentiated light as regards both its probability and its potential consequences. Security measures of the kind regularly adopted in the past continue to provide a considerable degree of protection. They should therefore be used rigorously and having regard to the recommendations made in this Guideline, insofar as this is necessary following 11 September 2001 and has not yet been done. If this is done, it is largely possible to deal with any threat to establishments/installations from terrorist attacks.

Appendices

The Appendices are intended to provide examples illustrating the content of this Guideline. They are taken from a variety of sources. They are to be updated in the future. In cases of doubt, reference should be made to the information in the foregoing text.

Appendix 1

Model of a Security Concept[1]

Contents

[1] 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 Safety 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 Guideline 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 threat situation
2. Identifying the specific security-relevant parts of the establishment
3. Assessment of hazards in relation to protection objectives
4. Selecting security measures, preparing the integrated security concept.

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 threat situation

When determining the threat 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
- Installation-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 threat, 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 security-relevant parts.

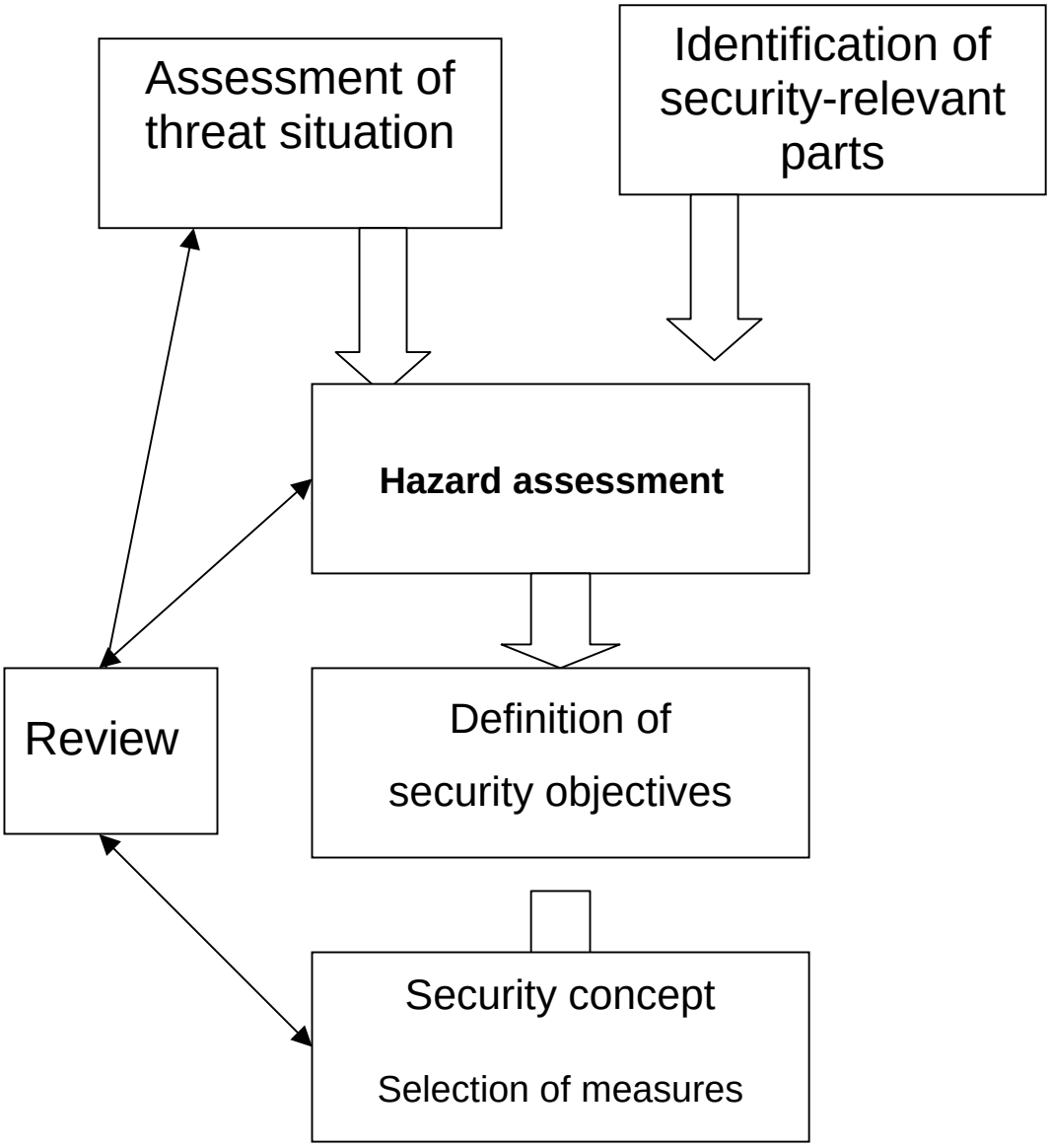


Fig. 1: Security analysis procedure

The question of the potential perpetrators that can be expected and their mode of action are 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 *(Threat 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 threat category table can be found in Appendix 1, *Chapter 3 "Threat situation"*.

2.2 Identifying the specific security-relevant parts of the establishment

Reliable determination of the security-relevant parts within an establishment is an easier task. A picture of the hazards 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 security-relevant parts)*.

A special indication of potential hazards is provided by the safety report pursuant to Art. 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 security-relevant parts of the establishment are explained in Appendix 1, *Chapter 4, "Security-relevant parts"*.

2.3 Assessment of hazards in relation to protection objectives

A comparison of the results of the threat situation analysis (determination of kinds of threats) with the individual security-relevant parts reveals the individual threat to the establishment. It is now possible to estimate what impacts can reasonably be expected to occur at what parts of the establishment. 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 Art. 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 concept

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 concept, which* shows how they are interrelated. An example of a possible structure for such a concept is explained in Appendix 1, *Chapter 7, "Description of the security measures/security concept"*.

3 Threat situation

3.1 Overview

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

3.2 General security situation

The general security situation describes threats 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 security situation with regard 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 Holding by 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 threat situation for the company as a whole. This applies primarily to politically motivated crimes.
Experience shows that the threat 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 security situation.

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

3.5 Security management

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

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 division is 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 Work Safety Specialists. They should devote increased attention to preventing deliberate faulty acts and minimising any consequences of such acts. Larger establishments also have works fire brigades and environmental protection departments that are involved in particular in the damage minimisation 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 "Security-relevant parts"*).
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 threat 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 Work force

The first aspect to consider in relation to the work force 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 security 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 associations or parties, 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 Threat categories

On the basis of the analysis of the company's general threat situation, it is possible to allocate certain threat 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 threats must reasonably be considered.

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

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

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

The matching assumptions within a threat 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 threat 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 threat category applies. In almost all cases, several threat categories will be possible.

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

Threat 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 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 service, - Interference with production processes, - Non-notification of critical installation status, - Arson, vandalism after unsuccessful break-in, - Arson for other motives.

Threat 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	:	Reconnaissance of safety-relevant establishment parts and weaknesses. Exploiting surveillance loopholes. Obtaining complicated instruments if necessary. Putting safety equipment out of service.
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.

Threat 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, religion related motives.
c)	Preparatory activities	:	Logistical preparations, reconnaissance, putting safety equipment out of service.
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 especially sensitive areas.

4 Security-relevant parts

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

4.1 Division into sectors

The threat categories established after discussing the threat 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 sections of installations, there are usually certain parts 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 Art. 9 of the Major Accidents Ordinance, it is also necessary in the case of facility security to examine not only the actual hazard 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 hazards.

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 installation.

The installation complex in question is classified as security-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 related to objects endangered by major accidents, and the analysis should not be unnecessarily extended to wide-ranging overall systems.
Examples of useful groupings of security-relevant parts or areas might be:

- Tanks, containers, storage facilities
- Filling stations
- Control centres, switch panels, computer systems
- Pipe ducts
- 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 security concept.

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 security-relevant parts

If one lists a number of conceivable forms of interference and compares them with the identified security-relevant parts, this produces a table providing a clear picture of the parts 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	Security-relevant part 1 "Tank storage"	Security-relevant part 2 "Process technology building"	Security-relevant part 3 "Pipeline bridge"	Security-relevant part 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-hazards sector)	Yes (in explosion-hazards 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 in-stallation 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 security-relevant parts

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 signals,
- Preparatory prevention of starting of emergency equipment,
- Switching off safety 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 on every site (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 (05)

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 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 homemade, 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 installation 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 hazard potential in the surrounding facilities (domino effect as in Art. 15 of the Major Accidents Ordinance).

Potential impacts 01 to 10 assume events that may relate more or less to all establishments. 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 threat 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 threat categories are equally applicable, as is the case with the majority of installations, the table of security-relevant parts can be reduced accordingly. For example, if the possibility of massive terrorism (threat 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 threats *(see Fig. 3).*

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

Fig. 3: Reduced table of security-relevant parts

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 security-relevant part of the establishment identified; instead it will usually be possible to group together several security-relevant parts.
For example, if a building includes several rooms with important components that are identified as security-relevant parts, 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 area with security-relevant parts 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 concept

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 with security-relevant parts
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 of the establishment 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 case 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,
- Security-relevant areas and parts 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 metal lattice 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 security systems. These may relate to the following functions, for example:

- Receiving safety/security alarms of all kinds (fire, water, abnormal operation, break-in),
- Alerting internal or external assistance providers in emergency 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 work force, 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 reports (frequently only after the end of normal working hours), it must not be possible to prevent forwarding of such reports 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 concept 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 security-relevant items requiring protection. The information should include:

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

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

7.4 Protecting security-relevant areas

Protecting the individual security-relevant areas 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 hazard 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 security-relevant parts 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 security-relevant part, 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 “Security-relevant parts”*. It goes without saying that this information in particular must be treated especially confidentially.

The following information should be provided for the individual security-relevant parts:

- Position on the site (site plan), position within buildings or areas (building plan),
- Pedestrian and vehicle access points, escape routes,
- Constructional/mechanical measures to separate areas (walls, lattice 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 security-relevant areas, workplaces within security-relevant areas,
- 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, contamination of 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

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. Basic information on this point is contained in Chapter 6 of this Guideline and in Appendix 4.

Preventive measures to combat interference

1. General

When considering defensive measures, one first has to look at attacks by external parties, i.e. attacks originating from outside the site perimeter. But it is also necessary to consider attacks undertaken by perpetrators from within the site (internal offenders). These may be company employees or external individuals who have gained access to the company.

Measures, which the operator is required to take, must conform to the principle of proportionality. This applies in particular to intervention measures such as altering the position of the hazardous installation with the aim of making it difficult or impossible to attack from outside the site. If this possibility does not exist or is unreasonable, the operator must inform the authorities.

If measures by the security authorities are necessary, the operator should establish direct contact with the latter.

2. Aircraft attacks

It is impossible for the company to take preventive defensive measures against attacks by aircraft. Here there is a need for state measures that make it difficult or impossible to fly aircraft deliberately at an industrial installation. Conceivable measures are restrictions on overflying rights, targeted observation of the air space in question, and measures relating to aircraft use or deployment.

3. Rockets and anti-tank arms

On the basis that attacks with long-range weapons such as rockets or anti-tank arms always originate from outside the site, public security measures are called for here too. One could for instance consider surveillance or large-scale patrols of the site of endangered installations by personnel provided by or hired from the public security forces. Special attention must be paid to high ground in the vicinity of installations.

4. Bombs in vehicles

If installations are situated close to the site perimeter, so that an attack using a bomb in a car (or boat) located outside the site holds prospects of success, then the area (water) outside the site perimeter must be subject to surveillance from within the site. Alternatively one could consider inspections outside the perimeter fence. Greater security can also be achieved by defining vehicle routes and car parks/parking bans next to endangered areas.

If it has to be assumed that external offenders will seek to bring a car bomb onto the site, this can be countered by making suitable checks on fences and/or access at the gates. Fence controls must involve constant checks on the barrier function. This may be done by means of regular inspection or video cameras. In the case of access controls it is important to make a precise check on the identity of the incoming person. Another important criterion is the justification for entry by the person requesting access: has he or she a legitimate interest in or right to such access? As a basic principle, external individuals should not be allowed to move on the site unaccompanied.

Bombs could also be brought into the site by internal offenders, i.e. company employees. It is likewise possible that external offenders could attach bombs to employees' vehicles without their knowing it. To exclude this possibility, incoming vehicles – even those belonging to company employees – should constantly be checked, or at least examined in frequent spot checks.

The precise details of how access controls and vehicle controls are to be carried out (including for internal employees) must be guaranteed by the security management system.

5. Small explosive or incendiary devices

In the case of small incendiary or explosive devices that can be transported in briefcases, handbags, envelopes or small packages it is also necessary to consider both external and internal offenders.

As in the case of car bombs, access control is of paramount importance. It is essential to prevent unauthorised persons from gaining access to the site. Even in the case of authorised persons who are granted access, the contents of bags etc. should at least be subjected to spot checks.

The precise details of how access controls and vehicle controls (including for internal employees) are to be carried out must be guaranteed by the security management system.

These measures are equally effective against external and internal offenders.

6. Truck carrying dangerous goods

An attack using a truck carrying dangerous goods (with or without an additional ignition device) is usually an external attack. Defensive measures are possible by means of state measures, i.e. surveillance of the site surroundings. To assist the police, the company itself should identify possible points where a truck could break through the site fence.

One preventive measure, which the installation operator can take, is to insist on extremely exact identification of drivers carrying dangerous goods into or out of the site. This can do a great deal to prevent unauthorised persons from driving a truck carrying dangerous goods.

The operator can also take measures to ensure that roads providing a straight approach to the site are interrupted by obstacles within the site (embankments, ditches etc.).

7. Manipulation

To disturb an installation by manipulating the instrumentation and control systems, the perpetrator must first gain access to the site. An effective defensive measure here is intensive access and fence controls. In especially endangered areas it may be useful to have patrols conducted within the site as well by security personnel.

Additional measures should be taken to protect particularly security-relevant installation parts, since in that case unauthorised personnel need to use technical resources (for parts of installations that are not electrically controlled) that make them easier to identify. Moreover, highly sensitive parts of installations can be given additional protection by means of classic surveillance measures (camera, sign-in access). Where security facilities are provided on a redundant basis, physical separation should be considered for security reasons.

If the manipulation is performed by an internal offender, there is scarcely any possibility of defence. From the point of view of the systems the internal offender is not an unauthorised person (for the present purpose we do not consider here the legal question of whether such interference does in fact constitute interference by unauthorised persons). More precise identification or access controls are no help in dealing with such offenders, as the systems will never succeed in keeping the offender away because they identify him as a person who is authorised to have access. Such an offender also has the necessary detailed knowledge to cause a serious disturbance by means of targeted manipulation. Protection from such attacks may be afforded by a functioning corporate culture, a good working climate and functioning teams.

If a relevant risk remains after all other security measures have been taken, it is advisable to consult the authorities responsible for public security. As a “last resort” one cannot rule out the possibility of security screening of employees in highly sensitive areas.

Security management

The Security Management System (SeMS) described below extends the Safety Management System (SMS) pursuant to Annex III to the Major Accidents Ordinance to cover the protection of establishments against interference by unauthorised persons. The individual measures are to be suitably incorporated in the predetermined systematic structure of Annex III to ensure that **a single** management system is maintained within the meaning of Annex III. The procedure is to be described accordingly in the safety report. The authority includes examination of the SeMS modules in its monitoring pursuant to Art. 16 of the Major Accidents Ordinance.

Security management
In the past, management systems have proved their value as an instrument for systematic handling and review of corporate workflows. Especially in connection with company security, constant systematic improvement in the efficiency and transparency of processes is of the utmost importance. The approach and the additional elements of a management system for corporate security are outlined briefly below. Companies should introduce such systems as a binding requirement so that they can at all times prove that they have taken the necessary steps to ensure protection from interference by unauthorised persons.

Corporate policy
In a voluntary declaration (security policy) the company makes clear its attitude to safety and security. The company declares that it will, together with its employees and its contractors, seek to ensure that a safe working environment is always guaranteed in which its assets and operations are protected against the risk of injury, loss and destruction by criminal, hostile or treacherous attacks and any consequences for the neighbourhood are mitigated. The company also declares its commitment to keeping the relevant security measures in line with best practice techniques and to review the SeMS regularly. It promises that its measures must not violate basic ethical principles and must not run counter to the interests of the general public.

Documentation
To make it possible to verify and monitor a management system, it is necessary to be able to compare the results with the objectives. This represents a challenge for a security management system, because on the one hand there should be a description of the target situation, while on the other this must not result in a situation where the real objective – namely preventing interference by unauthorised persons – is cast into doubt by an over-detailed description of all organisational and technical security measures.

For this reason details of the specific and technical measures should be protected from access by all persons who have no direct need to know, and should be kept in a form that is not accessible to the public. When the security management system is examined by the competent authorities, the relevant documents must be checked and the result of the examination must be documented.

Moreover, documents should also be present which make it clear to all employees and also to third parties (neighbours, external companies etc.) that the operator has instituted and is maintaining the necessary measures to protect the establishment and installations against interference by unauthorised persons. This could be done by giving a general description of the resources and measures employed.

Basic statements on disclosure of safety and security documents can be found in Chapter 6 of this Guideline.

Organisation and responsibility
Responsibility for the security of an establishment is assigned to the management of the business branch. As part of this responsibility, the managers must develop approaches, which ensure that the security risks are identified (see Chapters 4.1 and 4.2) and are reduced in accordance with company policy (see Chapter 4.3). The managers ensure an effective process that ensures implementation on the basis of the security expectations. The security expectations are accordingly integrated in planning and decision processes of the business sector. A process is introduced which ensures that any security incidents are reported to top management immediately.

Communication and training
Information about security incidents and experience of security technology is shared with others to ensure that the companies own measures are always in line with the latest best available techniques. Constant training must be provided to ensure that only competent specialist personnel are employed and that personnel are fully aware of current security risks. This is achieved by constant instruction to train awareness of security risks and a special training programme for personnel with security functions.

Defining security processes
All company processes in which security plays a role must be defined, documented and planned. The following processes in particular must be taken into account:

- Supervision of contractors
  All contractors who have business relations with the company must adhere fully to the company's security rules and procedures and submit to an audit complying with these rules.

- Risk assessment
  The business branch must conduct annual reviews of the security risk. Such reviews are to be performed more frequently if the risk situation so demands (procedures see Appendix 1, Chapters 3 to 5).

- Planning and construction of installations
  When planning and constructing installations, compliance with the security requirements (see Appendix 1, Chapter 6) is a major element. Compliance with the security objectives must be documented accordingly.

- Management of change
  The security impacts of temporary and permanent changes must be carefully investigated, managed and documented and their consequences taken into account if necessary. In order to permit an immediate response to any changes in the security situation, lists of measures are to be kept available for the various levels of threat situations.

- Product responsibility
  Security risks associated with the company's products must be examined and investigated to ensure safe handling, carriage and delivery and safety for the customers.

- Emergency management
  Equipment, installations and personnel for dealing with security emergencies must be identified and kept available at all times. For dealing with emergencies, a crisis response organisation must be maintained, including a constantly available crisis re-

sponse team. The “core” of the team should be defined in advance. The composition of the complete crisis response team may however vary depending on the situation. Examples of possible members of a crisis response team are company management, representatives of legal department, representatives of internal audit, representatives of safety and security department, representatives of occupational medicine service, representatives of the works council ....

- Cooperation with public authorities
  Open dialogue and open discussion with authorities and interest groups ensure that any security problems caused by the installations can be identified and the risks minimised. The fears and concerns of external parties must always be taken seriously. If regulatory measures are possible, public authorities should be involved in monitoring of the measures.

Operation and maintenance of security facilities

Security facilities must be operated and maintained such that they are always in line with the latest best available techniques, always operational and always in a good state of repair. A list of security operating requirements must be drawn up and the security equipment must be carefully selected so that these requirements are satisfied. A quality assurance programme exists to guarantee that the equipment is always kept operational. The possibility of replacing the existing equipment with more effective and possibly cheaper or more cost-effective systems must be reviewed at regular intervals.

Monitoring measures

In accordance with company policy the situation must be investigated and documented in regular reviews of the security management system. Annual and ad hoc audits must be conducted by experts. These audits check the specific expectations defined in the company’s security policy against the security measures in place. The following might be elements of such security audits:

- Existence of the security analysis, a security plan and an audit plan
- Responsibility rules for security
- Condition of perimeter enclosure security (access, condition of fence, lighting, video surveillance, inspections)
- Security control room facilities
- Qualifications of security personnel
- Identification of points of special threats
- Security screening of company personnel
- Information, instruction, training
- Other security processes such as key management, alarms on attempts to gain access, action in the event of bomb alerts, mail checks etc.

Correction and precautionary measures

Security incidents must be documented, reported and investigated. This applies in particular to serious incidents and incidents with the potential to develop into serious incidents. Investigation should concentrate on the causes, especially on root, background causes of the incident. The investigation of the incident must be documented and the necessary preventive measures recorded. The implementation of additional preventive measures is also to be documented.

Appendix 4

Example of criteria for “qualified description of content”

Installation for producing toluylene diisocyanate (TDI) using phosgene

The following are possible items of confidential information:

- Organisational, technical and constructional security measures for the installation
- Hold-up of phosgene in individual components of the installation
- Exact location of individual components of the installation
- Materials and wall thicknesses of individual components of the installation, e.g. the containment

The non-confidential information, which must be made available to the public, must normally include the following:

- Objectives of the security measures (e.g. ingress by unauthorised persons into the site without technical aids is not possible because of the constructional and technical security measures. Approaches to the installation by unauthorised persons are detected by security staff as a result of suitable security measures. Access to the installation is only possible after separate identification of the person and checking of all objects carried.)

Public access must be provided to all other details required by the Major Accidents Ordinance with the exception of those mentioned above, especially:

- Hold-up of the entire installation
- At least approximate location of the installation within the site
- Possible consequences in the event of a major accident
- Possible consequences in the event of a “major accident despite precautions”
- Warning and informing the public in the event of accidents
- Necessary behaviour by the public in the event of accidents.

GFI Umwelt - Gesellschaft für Infrastruktur und Umwelt mbH

Office
Hazardous Incidents Commission and
Technical Committee on Installation Safety

Königswinterer Str. 827
D -53227 Bonn

Tel. 49-(0)228-90 87 34-0
Fax 49-(0)228-90 87 34-9
e-mail sfk-taa@gfi-umwelt.de