



Security Manual
Perimeter



These Manual is binding only if their application has been agreed between VdS and the applicant on an individual basis. Otherwise, an application of this Manual is non-binding; an agreement on the application of this this Manual is purely optional. In individual cases, third parties may also accept other safety precautions or installation or maintenance companies under conditions that are defined at their sole discretion and that do not comply with these technical specifications.



Kompetent. Kostenlos. Neutral.

We wish to thank the Police, in particular the „Kommission Polizeiliche Kriminalprävention der Länder und des Bundes“ (German Police Committee for Crime Prevention) for the good and constructive cooperation in developing these guidelines.

Publisher:

Gesamtverband der Deutschen Versicherungswirtschaft e.V. (GDV)

Publishing house:

VdS Schadenverhütung GmbH

Security

Amsterdamer Straße 174

50735 Köln

Phone: +49(0)221-7766-375

Fax: +49(0)221-7766-377

E-Mail: security@vds.de

Internet: www.vds.de, www.vds-home.de



Copyright by VdS Schadenverhütung GmbH. All rights reserved.

Security Manual

Perimeter

Content

1	Preamble	5
2	General	6
2.1	Scope of application	6
2.2	Application	7
2.3	Validity	7
3	Normative references	8
4	Terms and abbreviations	9
4.1	Terms	9
4.2	Abbreviations	12
5	Hazard and risk analysis	13
5.1	Introduction	13
5.2	Hazard analysis	14
5.3	Risk analysis	14
5.4	Protective measures	15
6	Conception	17
6.1	Sector concept	17
6.2	Consultation by the police	18
6.3	Installation	18
6.4	Planning documents	18
7	Protection provided by structural-physical measures	19
7.1	General	19
7.2	Structural measures	20
8	Detection through electronic surveillance systems	28
8.1	General	28
8.2	Overview of electronic surveillance systems	30
8.3	Audio cable systems	31
8.4	Fibre optic sensor cable	31
8.5	Infrared light barriers	32
8.6	Tilt/acceleration sensor systems	33
8.7	Capacitive proximity detector	34
8.8	High-frequency transmission cable systems	34
8.9	Seismic detectors	35
8.10	Pressure change sensors	36
8.11	Laser scanner	37
8.12	Passive infrared motion detectors	37
8.13	Micro wave sensors	38
8.14	Radar detectors	39
8.15	Video sensor technology	39
8.16	Fence detection systems	41
8.17	Intelligent video analysis	42
9	Activation of the perimeter detection system	43
9.1	General	43
9.2	Activation/deactivation	43
9.3	Partial activation	44

9.4	Ancillary control equipment.....	44
9.5	Signalling of system status	44
9.6	Activation meeting Zwangsläufigkeit.....	45
9.7	Deactivation meeting Zwangsläufigkeit	45
10	Types of alarm messages	45
10.1	General	45
10.2	Perimeter messages	45
10.3	Sabotage messages	46
10.4	Fault messages “monitoring mode of operation“	47
10.5	Fault message “disqualification“	47
11	Alarm coordination	48
11.1	General	48
11.2	Stand-alone solutions	48
11.3	Connection to IAS/HMS	48
12	Addition by organisational measures and personnel resources.....	52
12.1	Basics.....	52
12.2	Intervention measures	52
12.3	Lighting.....	52
12.4	Guards/Patrols	53
13	System documentation and operation	53
13.1	Design documentation	53
13.2	Operator’s documentation.....	54
13.3	Acceptance and acceptance protocol.....	54
13.4	Trial operation	54
13.5	Handover to operator and commissioning	54
13.6	Maintenance.....	55
13.7	Operating manual	56
14	Examples of security concepts	57
14.1	General	57
14.2	Key for the examples	58
14.3	Examples of security concepts	59
Annex A	– Impact loads as safety standards for road blocks (informative).....	66
A.1	General	66
A.2	Requirements in line with DOS, US specification	66
A.3	Requirements in line with PAS 68 and 69, British specification	66
Annex B	– Further references (informative).....	67
Annex C	– Dispensation with projections on metal fences up to < 1.80 m height of wire mesh cover – Recommendations for safe fencing in the sense of personal protection (informative)	69
Annex D	– Protection and security for areas frequented by the public by fencing and gates – Leaflet for practical implementation (informative).....	71

1 Preamble

Many municipal facilities, industrial parks and buildings as well as their outside storage areas such as warehouses, machine depots, scrap yards or logistics centres and car dealers with open areas represent worthwhile targets and not too much of a challenge for potential burglars.

In general, security concepts for commercial and industrial facilities tend to focus on safeguarding the buildings and protecting their contents. The application of physical safeguards, often in combination with intruder alarm systems is well-known and commonly accepted by occupants and property insurances.

Depending on the size and occupancy of such premises, perimeter surveillance and protection of buildings located on the premises may not be sufficient. Market-related aspects, legal provisions and custom regulations, among others, may require comprehensive protection strategies to ensure continuous and safe operation (e.g. in the sense of just-in-time approaches). For products and goods stored on the premises, open production facilities or sensitive infrastructures become liabilities if unauthorised third parties manage to get access to the premises unnoticed. As operating processes are becoming increasingly interdependent, even the slightest disturbance may cause considerable economic loss.

One of the first perimeter safeguards (from Greek *peri* meaning around) certainly were (water) moats around existing physical barriers, in this case palisades or walls. The purpose of these highly effective perimeter safeguards was to prevent potential attackers from getting close to the physical barriers or make intrusion as difficult as possible. At the same time, it was possible to take countermeasures or call for support.

The only difference between medieval moats and today's perimeter safeguards is the design. In addition to modern physical safeguards, electronic detection and video surveillance systems are also available. Combined with effective additional organisational protection measures, perimeter safeguards are able to provide effective protection against e.g. unauthorised access, intrusion and burglary or arson.

This Security Manual are designed to provide users with guidance on how effective perimeter protection may help to reduce exposure and risks in advance. It describes various options for safeguards to protect perimeters as part of a consistent overall security concept. Due to the diversity of objects to be protected and their environment, this Manual do not intend to provide a classification of various security levels but instead describe possible protection objectives and outline possible solutions on the basis of different perimeter safeguards.

In addition, the examples of typical and established practical cases depicted in this Security Manual represent possible concepts for effective perimeter protection.

2 General

2.1 Scope of application

In the context of this Manual, the term perimeter is defined as the environment (in general surrounding a building or technical facility such as, for instance, solar panels), the boundary of this environment as well as focal points in this environment (e.g. particularly exposed outdoor storage areas). On a horizontal level (extension of the surface), the outer demarcation of the perimeter represents the legal boundary of the premises. In individual cases, it may be necessary to take the area beyond the legal boundary into account. A building shell, a facility or something similar located inside the area defined by the legal boundary may constitute an internal boundary that may not necessarily exist. Outer walls of buildings inside the perimeter area may constitute an internal boundary, while parts of a building's interior (e.g. a self-service area in a foyer, cf. chapter 14.3.7) may also be considered as part of the perimeter area. In addition, a perimeter also has vertical legal boundaries.¹ Depending on the exposure, it may be necessary to contemplate perimeter surveillance on a vertical level (top/bottom extension).

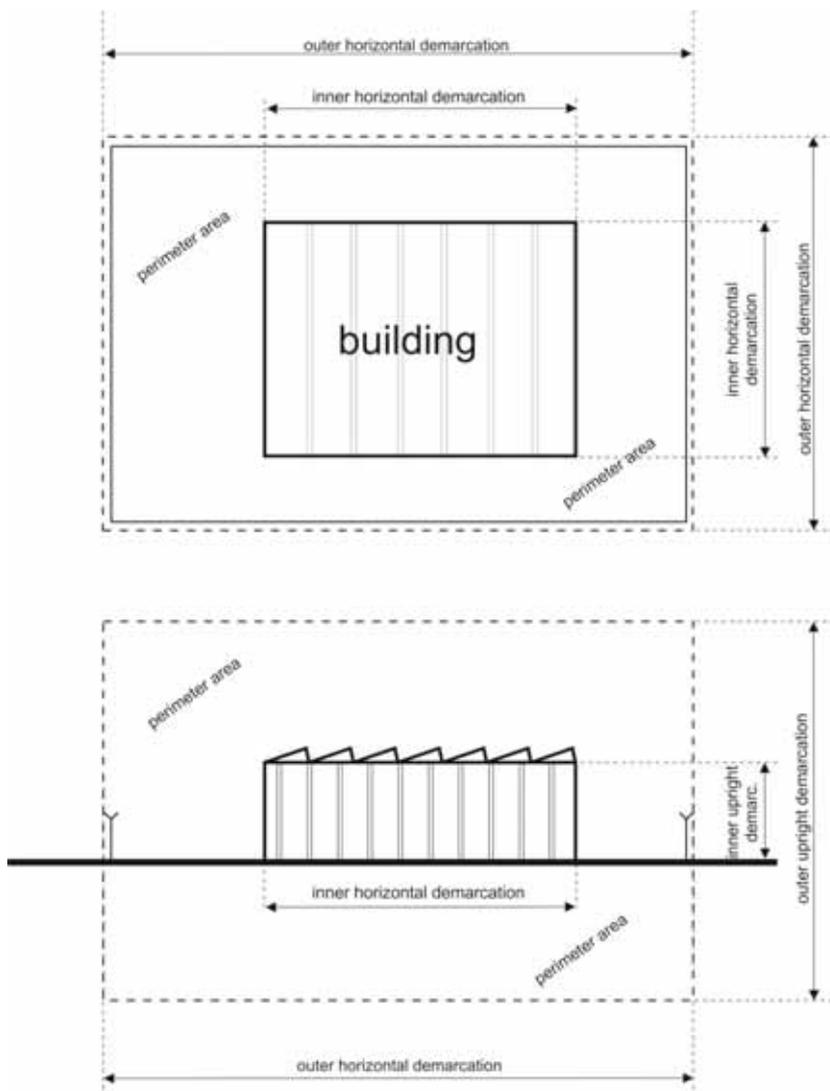


Figure 2-1: Scope of the Manual

¹ Limitations to a property on a vertical level resulting in particular from municipal, regional or Federal laws and regulations.

Note: This example portrays a fence with Y-shaped booms. Consequently, the fence has been included in the perimeter area in such a way that the outer boom does not extend beyond the legal boundary (dashed line).

The perimeter area does not necessarily end at the outer wall of a building. The perimeter area may also include areas in buildings that are accessible to the public. The self-service terminal area of banks (Area "1" pursuant to VdS 2472, chapter 3.2) could be one area of application.

This Manual contain recommendations for the protection and surveillance of perimeter areas against unauthorised access, burglary, intentional and malicious destruction (vandalism), sabotage and arson based on technical concepts. Perimeter safeguards may enhance protection of buildings against burglary. This Manual describe the protection goal and how to include perimeter protection into a consistent overall security concept in a reliable manner meeting the operator's requirements.

Other regulations, in particular Manual for Intruder Alarm Systems – Planning and Installation, VdS 2311, the national specifications for installers of hold-up and intruder alarm systems as well as the Manual for Hold-up and Intruder Alarm Systems connected to the Police and the Security Manual for Shops and Business, VdS 2333, remain unaffected. When perimeter detection systems are connected to intruder and hold-up alarm systems or their alarm transmission systems, it is necessary to ensure that there is no feedback. Provisions on lighting and overvoltage protection must also be considered.

This Security Manual have been designed for:

- experts entrusted with the planning and installation of perimeter safeguards and perimeter detection systems
- manufacturers
- operators interested and
- employees of insurance companies.

This Security Manual are a summary of experience gathered by the police, manufacturers and installers of security systems as well as property insurers and VdS Schadenverhütung. As this experience is subject to continuous changes, this Manual is not binding.

Overviews, tables and classifications systematically address and illustrate the problems and highlight different issues. Consequently, the graduations and demarcations provided refer to the internal system of this Manual and do not represent an absolute assessment.

2.2 Application

This Security Manual describe protective measures against external perpetrators and are designed for industrial and commercial undertakings as well as infrastructures (e.g. municipal, regional or Federal establishments) relative to the risk situation ascertained. In addition, measures are geared towards protection of assets – in particular in the commercial sector. This Manual do not cover individual safeguards for personal protection.

This Manual may serve as a basic document for high-risk objects such as nuclear power plants, military facilities or penitentiaries.

2.3 Validity

These guidelines are valid starting from 01.11.2012.

Note: This is a translation of the German Manual. In case of doubt, the German version shall be binding.

3 Normative references

This Manual contains dated and undated references to other publications. The references are made in the respective chapters, the titles are listed below. Amendments of or additions to dated publications shall only be valid if they have been published by amendment of this Manual. Regarding undated references, the respective most recent version of them shall be deemed relevant.

ASR-A 1.7	Work Place Regulation ASR-A 1.7 Doors and Gates of DGUV
National Specifications	by the police for installers of hold-up/intruder alarm systems
DIN EN 12453	Safety in use of power operated doors – Requirements
DIN EN 13241-1	Industrial, commercial and garage doors and gates – Product standard – Part 1: Products without fire resistance or smoke control characteristics
ISO 31000	Risk Management – Principles and Guidelines
HU/IAS Guidelines	Guidelines for Hold-up and Intruder Alarm Systems Connected to the Police
VdS 2252	Guidelines for Intruder Alarm Systems – Control and Indicating Equipment (CIE) of Classes B and C – Requirements
VdS 2311	Intruder Alarm Systems – Planning and Installation
VdS 2333	Security Guidelines for Shops and Businesses
VdS 2366	Video Surveillance Systems – Planning and Installation
VdS 2465	Transmission Protocol for Alarm Systems
VdS 2465-S3	VdS Guidelines for Alarm System (AS) – Transmission protocol for Alarm Systems, Amendment S3: Protocol extension for connection of video surveillance systems to alarm systems
VdS 2472	Security Guidelines for banks, savings banks and other credit institutions
VdS 2529	Alarm service and intervention certificate
VdS 3146	Systems for monitoring of open areas, planning and installation (at draft stage)
VdS 3456	System Components for Monitoring of Open Areas, Requirements and Test Methods
VdS 3463	System components for monitoring of open areas on base of video surveillance, Requirements and test methods (at draft stage)

4 Terms and abbreviations

4.1 Terms

Alarm: Indicates a certain condition that makes it necessary to take protective measures.

Alarm service and intervention certificate: Document that specifies all intervention measures related to perimeter protection and detection systems. It may be part of a contract and consequently become mandatory.

Alarm transmission equipment (ATE): ATE receive messages from alarm systems, prepare them for transmission via transmission routes and serve as interfaces to these routes. Moreover, they process the commands issued by the alarm receiving device and transmit them to the alarm system connected to it.

Alarm verification: Validation and assessment of an alarm message to ascertain whether it is real or false.

Attack types: Modi operandi aimed at overcoming security measures.

Note: Chapters 7 and 8 provide a detailed description of individual safeguards and to what extent they are suited for defence and/or detection of certain types of attack. In this context, the following applies:

Walking/running: Refers to all systems that are able to identify walking or running as the actual incident which is not predominantly the case with systems fixed to barriers.

Climbing: Refers to systems where climbing of the system itself triggers an alarm which is the case only for systems fixed to barriers.

In the case of systems not fixed to barriers, it is by definition not possible to climb over the zone under surveillance without aids.

Cutting: Similar to climbing, a physical barrier is absolutely necessary to be able to recognise this incident which can be explained analogue to "climbing". The definition of recognition is actually regarded as the incident.

Aid used for climbing over barriers (ladder): Overcoming a physical barrier by way of aids such as ladders, for instance, requires a differentiated consideration:

- using a ladder contacting the barrier (leaning)
- using a ladder without contacting the barrier (A-frame ladder)

Depending on the detection system, this distinction may have significant influence on recognising this incident. For instance, detection systems directly affixed to the physical barrier may initially not recognise contactless ladders and/or aids for climbing over while ladders leaning against the barrier are recognised.

Crawling under: In principle, crawling under can only be recognised by detection systems in the floor as they are the only ones directly connected to the ground.

Driving through: Compare with walking/running through at a higher speed and greater mass. In contrast to walking and running, the higher energy of driving is able to break through a physical barrier.

Zwangsläufigkeit (German term without translation): Measure that prevents an IAS whose parts are not all functional from being set or a set IAS from being activated erroneously by external alarm raised by the operator (e.g. inspection of rooms without prior unsetting).

- **Structural Zwangsläufigkeit:** All structural measures to comply with the Zwangsläufigkeit criterion, e.g. locking bolts, one-sided locks on outer doors.
- **Electrical Zwangsläufigkeit:** All electrical measures to comply with the Zwangsläufigkeit criterion, e.g. monitoring locks on outer doors, electrical operation of locking de-

vices when IAS is set, blocking of the ancillary control equipment designed as a shunt lock in case the IAS is not fully functional.

- **Organisational Zwangsläufigkeit:** All organisational measures to comply with the coerciveness criterion, e.g. access, attendance and exit monitoring of persons.

Danger: A condition caused in the system that makes it necessary to initiate defence measures.

Deceitful alarm: A (→) false alarm raised as intended by a detector due to its physical-technical operating principle whose triggering incident does not require protective measures.

Note: A nuisance alarm may be caused by e.g. a smoke detector erroneously activated by cigarette smoke.

Energy supply: Component that supplies alarm systems or parts thereof with electrical energy.

False alarm: Alarm not based on actual threat. Erroneous signal indicating a condition caused in the system that would make it necessary to initiate protective measures.

In the case of a false alarm, a change of condition not actually caused may erroneously be signalled as an (→) alarm or a prevailing yet irrelevant change of condition may be misinterpreted and raised as an alarm. (→) Fault alarms or (→) nuisance alarms may also be false alarms.

Note: In the strictest sense of the word, the term false alarm describes a so-called (→) non-alarm as a prevailing relevant change of status that would require an alarm but is not indicated (missing alarm).

Fault alarm: A (→) false alarm caused by a technical fault, e.g. a defective component.

Fault message: A message created by a system component or the burglar alarm system or the perimeter detection system about an identified or actual fault.

Intruder alarm: Alarm triggered by function of the (→) intruder alarm system as intended or a (→) false alarm in the (→) intruder alarm system.

Intruder alarm system (IAS): Alarm system to detect and signal presence, intrusion or attempted intrusion of a burglar into a surveillance area and to monitor objects for unauthorised removal.

Intruder alarm system concept (IASC): Entirety of system components synchronised towards functional synergy (e.g. intruder control and indicating equipment, ancillary control equipment, intruder detector).

Intruder control and indicating equipment (I-CIE): System which receives, processes, controls, indicates and initiates transmission of information (e.g. burglar, sabotage and fault messages).

Intruder detector: System component of an intruder alarm system that monitors a suitable physical parameter for detection of an attempted intrusion/burglary in the surveillance area either constantly or at consecutive intervals.

Investigation time: Time following an alarm during which the system verifies whether protective measures need to be taken or whether the alarm was false.

Message: Output of information via a defined interface aimed at this information being received and processed by other elements of the perimeter protection and detection system. A message may, for instance, be based on an alarm or false alarm.

Non-alarm: Situation in which an incident that requires protective measures to be initiated occurs, yet no (→) alarm is raised. The non-alarm rate of a detector is reciprocal to the (→) POD.

Note: Faulty system settings, inadequacy, improper installation or maintenance as well as technical failures may cause a non-alarm (which is also referred to a “negative false alarm”) or default alarm.

Nuisance Alarm: (→) Deceitful alarm

Nuisance Alarm Rate (NAR): Parameter that describes the ratio of (→) nuisance alarms relative to the total of (→) alarms and nuisance alarms. The goal for this parameter is 0 which is a conflicting goal to the (→) POD.

$$NAR = \frac{\sum \text{Nuisance alarms}}{\sum \text{Alarms} + \sum \text{Nuisance alarms}}$$

Note: The original English term Nuisance Alarm Rate is commonly used in other languages as well.

Perimeter: Boundary between inner and outer perimeter area.

Perimeter alarm: Alarm triggered by proper function of the (→) perimeter detection system or a (→) false alarm in the (→) perimeter detection system.

Perimeter area, inner: In the context of this Security Manual, the area enclosed by the (→) perimeter which starts immediately at the perimeter and potentially ends at an object to be protected that is located inside the perimeter area.

Perimeter area, outer: Area located outside the (→) perimeter area yet still inside the legally defined boundaries (sector 0).

Note: See also the regulations contained in chapters 2.1 and 6.1.

Perimeter detection: Detection of defined incidents in the (→) perimeter area.

Note: In individual cases, it is also possible to install perimeter detection measures in sector 0.

Perimeter detection system: System for recognition of defined incidents at the (→) perimeter.

Perimeter protection system: Entirety of all facilities at the (→) perimeter or in the (→) perimeter area (e.g. fences, gates) designed as defence against attempts to overcome the secured boundary.

Perimeter surveillance: see perimeter detection

Probability of Detection (POD): Parameter that describes the ratio of (→) alarms relative to the entirety of states of danger. The goal for this parameter is 1.0 which is a conflicting goal to the (→) NAR.

$$POD = \frac{\sum \text{Alarms}}{\sum \text{Risc - Conditions}}$$

Note: The original English term Nuisance Alarm Rate is commonly used in other languages as well.

Protected premises, enclosed: The enclosed protected premises comprise self-contained objects, locked parts of objects and demarcated rooms to be monitored. Access is permitted to authorised persons only.

Protected premises, open: The open protected premises comprise objects, sections of objects and rooms to be monitored but not to be considered as locked. Unauthorised persons can get access to them as well.

Note: In the context of this Security Manual, the perimeter area including the open space is defined as open protected premises.

Risk management system: A software system that takes over, enters, generates, saves, transmits, processes and indicates messages and data and controls various safety-related components of one or several systems.

Risk bearer: Originally, the owner of the object is the one who bears the risks resulting from this property. He may transfer individual risks either fully or in part to third parties by means of insurances who then becomes the risk bearer in the sense of this Security Manual.

Tamper signal: Signal (message) that surveillance elements have been activated, e.g. by opening or penetrating enclosures.

Sectors: Individual areas for which individual technical solutions can be implemented.

Security object: Individual object located inside the (→) perimeter area which is protected by safeguarding the (→) perimeter and/or the perimeter area (if need be, indirectly).

Technical detector: Detector than can be connected to an alarm system (e.g. detector for hazard and emergency situations) designed for early recognition of discrepancy situations such as e.g. when the temperature exceeds or falls below a set value, discrepancies of set points on machines and the like.

Technical signal: Signal (message) indicating that a (→) technical detector has been activated.

4.2 Abbreviations

ACE	Ancillary control equipment
APR	Accident prevention regulations
ATE	Alarm transmission equipment
ATM	Automatic teller machine
CFPA	Confederation of Fire Protection Association
DGUV	Deutsche Gesetzliche Unfallversicherung (German statutory accident insurance)
HF	High frequency
IAS	Intruder alarm system
IASC	Intruder alarm system concept
IC	Intervention company
I-CIE	Intruder control and indicating equipment
ID	Identification feature
IR	Infrared
NAR	Nuisance Alarm Rate
POD	Probability of Detection
RMS	Risk management system
VdS	VdS Schadenverhütung GmbH

5 Hazard and risk analysis

5.1 Introduction

Consideration of a “holistic security concept“ for an object should start with the building’s and/or property’s perimeter. When developing such a holistic security concept, the scheme illustrated and outlined below will provide guidance to decision-makers in order to adopt a systematic approach based on a logical structure. It is based on ISO 31000² and divided into the steps of “hazard analysis” and “risk analysis” which are essentially brought together into “suitable safeguards”. This ensures that all relevant factors can be identified, goals specified and safeguards defined effectively.

Since the decisions taken in developing the concept are of a fundamental nature and are of paramount importance for subsequent steps and consequently for a company’s security, it is imperative for the company’s management to be involved in the decision-making process. At any rate, this may facilitate subsequent decisions to the extent that they can be derived from the principal decisions initially taken by the company’s management. Moreover, the safeguards are to be prioritized, if necessary, by the management in a rational manner. As part of an integrated risk management, it is also necessary to review performance periodically, among other things.

The approach can be structured as described below:

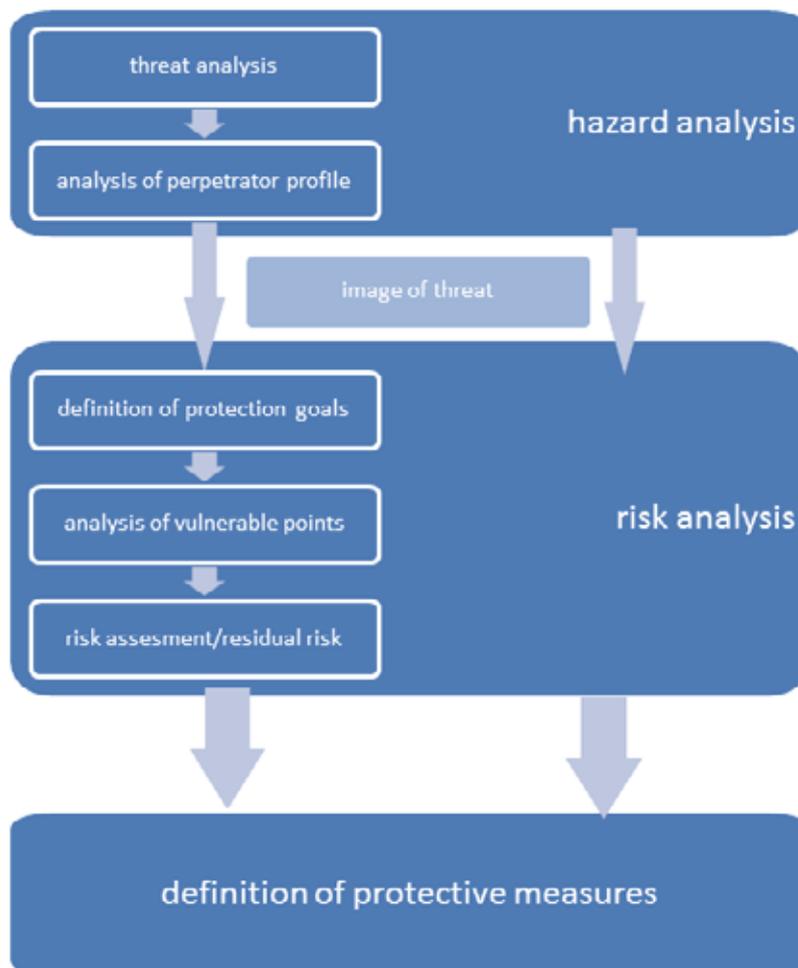


Figure 5-1: Workflow for definition protective measures

² ISO 31000: Risk management – Principles and Manual

5.2 Hazard analysis

5.2.1 Threat analysis

As part of the threat analysis, it is necessary to establish first which types of hazards can be expected for the object to be protected. With a view to perimeter security measures, the following threats are likely, among others:³

- assaults,
- arson,
- burglary,
- intrusion into a building,
- threat to persons,
- sabotage, tampering,
- espionage,
- vandalism

or consequences thereof such as e.g. business interruption.

Once the threats to be expected have been established, the decision-makers need to decide which threats are relevant with a view to perimeter protection measures.

5.2.2 Analysis of perpetrator profiles

A perpetrator makes abstract threats defined in advance much more tangible.

Figuratively speaking: *Image of threat* = Σ (*Threat* · *Perpetrator*)

Therefore, it is necessary to determine which criminal profiles are relevant for the security concept. In this context, various factors can be distinguished:

- Number: single perpetrator – group of perpetrators
- Local knowledge: insider threat⁴ – non-insider threat
- Professionalism: casual perpetrator – organised crime
- Technical knowledge and equipment: amateur – professional
- Openness to risks: cautious perpetrator – willing to take great risks

The analysis of relevant threats and criminal profiles results in an individual risk-specific threat scenario based on which the protection goals are defined below.

5.3 Risk analysis

5.3.1 Definition of protection targets

The primary protection goal is to avoid or minimise loss. In the context of defining the protection goals it is necessary to establish which risks are to be addressed. Where necessary, there may be constellations where certain parts of the threat scenario can be factored out and should be ignored deliberately – either fully or in parts.

The definition of specific protection goals is the basis for the subsequent analysis of vulnerable points.

³ Naturally, it is not possible to provide an exhaustive list.

⁴ Insiders may not only be current and former staff but also e.g. suppliers, customers and similar groups who legally obtained knowledge about the premises and similar specific details (e.g. operating procedures, roles and responsibilities).

5.3.2 Analysis of vulnerable points

Based on the protection goals and threat scenarios defined, the next step is to screen the respective object for any vulnerable points that could have a negative impact on the threat situation. Aside from obvious vulnerabilities, safety-related systems available that are no longer state-of-the-art or whose design is no longer suitable for the current occupancy may also represent vulnerable points.

The results of this analysis provide the basis for the subsequent risk assessment.

5.3.3 Risk assessment and residual risk

It is necessary to determine how much expenditure is required to eliminate the vulnerable points identified. For this purpose, the weak spots of the risk have to be assessed (risk assessment⁵).

The risk assessment forms the basis for decisions on which risks should be countered. As part of this process, the causes of threats, their repercussions and their probability of occurrence need to be determined.

It is necessary to establish which risks are tenable for the company (risks deliberately accepted, either fully or in part), which risks necessarily require mitigation measures and what residual risk is, if need be, acceptable. It is also necessary to clarify whether the risk may be taken on by another risk bearer (e.g. insurance).

5.4 Protective measures

The last step for now defines possible protective measures including selection of one or several risk management options.

The definition of protective measures is based on structural-physical, electronic and organisational measures and is designed to address the risks identified. It involves specification of protective measures and their interaction as part of a holistic security concept.



Figure 5-2: “Triad“ of protective measures

⁵ Cf. in particular ISO 31000, chapter “risk assessment“

In this context, the structural-physical measures should form the basis. They are complemented by surveillance, detection and alarm systems if physical protection alone is considered to be insufficient. And finally, these protective measures should be flanked by intelligent organisation and intervention measures. Organisational measures with a view to burglar protection include e.g. visitor and ID management, police rounds or patrols as well as intervention services. Tailor-made effective protection systems will always make use of all three types of protective measures; the latter may be more or less pronounced depending on the situation at hand.

When coordinating different protective measures it is necessary to ensure that physical safeguards and electronic detection and alarm systems are synchronised in such a way that alarms are activated at an early stage when physical barriers have not yet been fully compromised. This way, intervention can be brought forward which makes it more likely to apprehend the perpetrator (or at least considerably minimise loss).

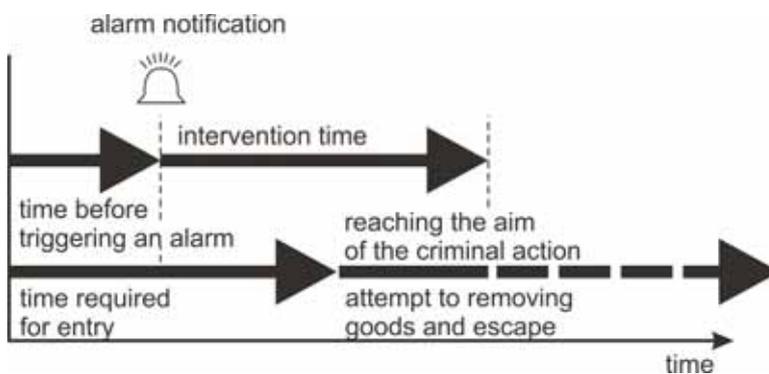


Figure 5-3: Coordination of alarm activation and overcoming of barrier

What this means in practical terms is, for instance, considering whether a change of building occupancy (or even removal/relocation) might represent a more cost-efficient solution compared with rather elaborate physical and electronic security, surveillance, detection and alarm systems. Assuming a warehouse with trapezoidal sheet walls where it may be less costly, for instance, not to store the valuable goods in shelves arranged directly along the outer walls but in an inner zone possibly separated by a door or grating. This way, the perpetrator is forced to enter the building and is not able to empty the shelves from behind through an opening in the wall. This arrangement does not make an intruder alarm system and, if available, an additional perimeter detection system obsolete but it provides two important benefits in addition: Firstly, it may be possible to do without expensive surface surveillance (penetration surveillance) under these circumstances. Secondly, a combination with early detection makes it possible to buy valuable intervention time. At the same time, special attention must be drawn to the overall concept. The various measures must be coordinated and harmonised.

6 Conception

6.1 Sector concept

6.1.1 Overview

A well designed perimeter protection and detection system provides for optimum harmonisation of the various protection measures. In order to meet the different requirements in various perimeter areas, they should be divided into different sectors. Depending on the location of each sector, different protection measures make sense. An individual risk assessment (cf. chapter 5.3) should provide the basis for dividing the area into different sectors depending on the specific location. Based on the protection goal, adequate physical and/or electronic measures should be developed.



Figure 6-1: Layout of different sectors, example

6.1.2 Sector 0

Sector 0 is the surrounding field, i.e. a strip of land demarcated individually and located outside the (inner) perimeter area (so-called outer perimeter area).

Inside sector 0, it is possible to make unauthorised approaches to the perimeter more difficult and/or to detect them.

Surveillance of this sector makes sense only if persons approaching the perimeter should be detected. The physical safeguards in sector 0 should be designed in such a way that they hamper persons approaching the protected area (perimeter area). For this purpose, sector 0 must be located within the legal demarcations of the premises. Security guards should be able to notice potential perpetrators as early as possible.

6.1.3 Sector 1

As a perimeter, sector 1 constitutes the boundary of the perimeter area. It may consist of a closed barrier such as e.g. a fence, moat, gate, barrier.

The protection target is to prevent and/or detect any trespassing in sector 1.

Surveillance of this sector makes sense if the purpose is to detect whether persons obtain unauthorised access to the perimeter area.

6.1.4 Sector 2

Sector 2 is the perimeter area, i.e. the entire area inside the perimeter excluding sector 3.

A possible protection target is to prevent and/or detect persons entering sector 2.

Surveillance of this sector makes sense if the purpose is to detect whether persons are lingering in this sector without authorisation.

6.1.5 Sector 3

Sector 3 refers to e.g. a building's shell as well as facilities and/or objects located in sector 2 which are relevant for security.

A possible surveillance objective is to detect and/or prevent any entry and/or climbing of such buildings or facilities respectively any damage or removal of parts thereof.

Surveillance of this sector makes sense if the purpose is to detect that persons are illegally trying to get access to buildings or parts of facilities. The proper protection of buildings in sector 3 does by no means replace the shell protection of buildings by way of intruder alarm systems pursuant to Guidelines VdS 2311.

6.2 Consultation by the police

All over Germany, the information centres of the police (German term: Kriminalpolizeiliche Beratungsstellen) also provide professional information and recommendations on perimeter protection. The police experts are able to identify weak points on site, if necessary, and give advice on suitable protection measures. The address of the nearest information centre can be obtained from www.polizei-beratung.de.

6.3 Installation

Perimeter protection and detection systems should be installed by a VdS-approved installer for intruder alarm systems with additional qualification in and certification of "Perimeter protection and detection systems (VdS, CFPA)" to ensure a consistent high quality of workmanship.

6.4 Planning documents

Plans for perimeter protection and detection systems which should be neutral in terms of manufacturers show which measures contribute to achieving the protection goals defined in the security concept. If possible, they should include layout plans that make it easy to identify structural and topographical features and highlight the location and functions of all protection measures serving perimeter protection and detection. The sector concept should be used to provide structure to the planning documents. The planning documents must be suitable to derive a project plan from them and make it possible for a third party without knowledge about the conditions on the premises to assess whether the project plan is suitable or not.

As to how vegetation or planting are to be handled later during operation should be defined as early as the planning or project development phase. If required, it might be necessary to trim the planting at shorter intervals in order not to thwart the effectiveness of protection measures. It is also necessary to take into account that parts of the perimeter protection and detection system may only be serviced by horticultural and landscaping companies if vegetation is incorporated into the concept of the security system at all. The planning documents have to include a clear definition of all interfaces (structural, technical and organisational interfaces) and responsibilities required for the operation of the perimeter protection and detection system.

Note: Services by different trades need to be taken into consideration (e.g. power supply, pylons, lighting etc.).

7 Protection provided by structural-physical measures

7.1 General

Aside from demarcating the boundaries of a property, structural-physical safeguards are predominantly designed to hamper or prevent any approach to and/or free movement in the perimeter area.

The basis for selecting suitable safeguards is the desired protection level subject to the perimeter area divided into four different sectors.

In general, physical safeguards are elaborate and costly and difficult to correct once installed. It is therefore imperative for the security concept to specify the protection level. At the same time, it is necessary to take into account that different political risk situations or changing environmental conditions may affect the physical security concept. Protection measures should at any rate be designed in such a way that they are adequate no matter what the environmental conditions are.

The following table show possible physical safeguards and corresponding protection goals in relation to the respective sector and the desired protection level.

physical safeguards	protection level	goal	example
sector 0	basic	---	---
	increased	approach to the perimeter area should be hampered	low shrubs, small ditches
	high	approach to the perimeter area, also with additional aids (e.g. car) should be hampered	larger stones, bushes, ditches, borders, bollards, road barriers, design and road lay-out
sector 1	basic	the relevant demarcation of the property is to be highlighted and spontaneous entering of perimeter area is to be hampered	fence or wall, height in general > 1.2 m (demarcation fence)
	increased	the relevant demarcation of the property is to be highlighted and targeted entering of perimeter area without additional aids is to be prevented	fence or wall with simple anti-climb guard (height > 2 m)
	high	the relevant demarcation of the property is to be highlighted and targeted entering of or breaking out of the perimeter area with additional aids is to be prevented	fence or wall (height \geq 2.4 m) with enhanced anti-climb guard; double fence system, protection against crawling under (depth \geq 0.6 m)

physical safeguards	protection level	goal	example
sector 2	basic	---	---
	increased	movement in certain places of the perimeter area is to be hampered	low shrubs, artificial water bodies (e.g. ponds), bushes
	high	movement in the perimeter area is to be considerably hampered	low shrubs, artificial water bodies (e.g. ponds), bushes, fences, walls
physical safeguards	protection level	goal	Example
sector 3	basic	---	---
	increased	reaching the protected object is to be hampered	fence or wall (height > 2 m)
	high	reaching the protected object is to be prevented	fence or wall (height > 2.4 m) with simple anti-climb guard

Table 7-1: Physical safeguards according to the protection level and sector

7.2 Structural measures

7.2.1 Landscape

Every terrain to be protected has topographic features that constitute unique conditions which should be considered in every protection plan. In many cases, the scenic features such as ditches and walls, prickly shrubs, moats or ponds can be well integrated into perimeter protection as they hamper or even prevent entry into the protected area and removal of objects.

Geographical and meteorological influences also need to be considered. In areas with cold winters, a frozen river may turn into a bridge that can easily be crossed just as great volumes of snow may provide assistance in climbing over barriers.

The analysis of the scenic features should provide a basis for determining the landscaping measures required as a next step.



Figure 7-1: Protection measures using scenic features (here: moat)

7.2.2 Landscaping measures

Landscaping measures are targeted measures to change the scenic features, e.g. by adding more vegetation, blocks of stone (boulders), digging ditches and dumping earth to build borders, designing water features or constructing walls.

Road planning and traffic routing on and particularly towards the premises has to be incorporated into the planning. Courses of roads, for instance, that allow vehicles to accelerate to such a high speed that they are able to crash barriers and give perpetrators access to the premises are unsuitable. Therefore, traffic abatement measures such as e.g. curves or junctions should be used for road design, if possible.

Landscaping measures must on the one hand be geared towards the geographical and consequently also meteorological conditions but on the other hand, they must be aligned to the protection goals defined for a certain object. Boulders, for instance, are able to avert and/or divert or guide vehicles, while they do not block access to the premises for cyclists or pedestrians, whereas e.g. moats or vegetation may also keep pedestrians and cyclists off the premises.

In general, landscaping measures are given priority over physical safeguards – because they are more widely accepted for aesthetic reasons.



Figure 7-2: A serpentine access road prevents an attacking car from reaching a critical speed.

7.2.3 Structural conditions

Structures or buildings located directly on or close to the boundary of the premises have to be assessed with a view to protection measures required, and taken into account in the perimeter protection concept. It is in particular necessary to check and assess their height, features facilitating climbing or growth on parts of the building. If necessary, the physical safeguards have to be aligned with these structural situations. In particular the height, features facilitating climbing or growth on parts of the building should be analysed to determine their relevance for the security concept. If necessary, the physical safeguards have to be aligned with these structural conditions.

7.2.4 Fences and walls

7.2.4.1 General

Fences are suited to demarcate the legal boundaries of a property and are designed to hamper unauthorised access to the perimeter area. They may also enclose additional sensitive objects inside the perimeter area.

The type and design of barriers is determined by the protection goal for the respective sector. A scale of physical barriers

- simple demarcation fence (prevents entry *by mistake*), behind it
- fence/wall (prevents *intentional* entry)

hampers persons trying to enter certain areas effectively.

Depending on the purpose, there is a multitude of types of fences; the next chapter is going to present a few of them.

7.2.4.2 Wire mesh fence

A wire mesh fence consists of wire netting attached to posts with tensioning wires at regular intervals. In general, this interval is 3 m as a maximum. The wire mesh is commonly available in heights of 0.8 to 2 m and mesh widths of 30 x 30 to 60 x 60 mm (in 10 mm increments). The wire thickness generally varies from 2 to 5 mm. Due to their reasonable material price and the little effort required to install them wire mesh fences are suitable for enclosing large areas that require only low protection levels. They prevent an entry by mistake to these areas, though simple tools can easily cut and compromise them.



Figure 7-3: Wire mesh fences

7.2.4.3 Bar grating fences

Bar grating panels which are generally 2.5 m wide and between 0.6 to 2.4 m high in 200 mm increments are fastened to rectangular posts. For a fence higher than 2.4 m, different heights of bar grating panels have to be combined. The gap between bar gratings (mesh width) is generally 50 x 200 mm. Mesh widths of 20 x 200 mm or 25 x 200 mm are used for stricter reach-through protection requirements.

Bar grating panels are available as single or double panels with grates between 5 to 8 mm thickness. Examples (of double bar grating panels): 8/6/8 mm, 6/6/6 mm or 6/5/6 mm.

The posts of the rectangular tubes are anchored in concrete foundations taking into account structural requirements.

The main benefits compared to a wire mesh fence are the little maintenance effort (no tightening required), a higher mechanical stability and greater protection from breaking through.



Figure 7-4: Bar grating fence



Figure 7-5: Bar grating panel
(Double bar grating panel)

The 2.5 m wide bar grating panels (double bar grating panels) are fastened to the middle of the post to join them. There are various means to fasten the panels such as metal clamps, plastic holders or cover strips.

As a variation, “endless fences” that consist of bar grating with horizontal U-shaped or flat steel profiles can be used to install the fence aligned to the terrain. In doing so, the bar grating panels are connected regardless the posts. They are fastened to the post by way of hook bolt or U-bolts. In this case, there is need for a specific spacing between the posts.

The most important requirement for all varieties is the connection (bolted) which must not be on the outside (exposure) but on the opposite side. Unclamping with simple tools must be prevented e.g. by using tamper-resistant bolts.



Figure 7-6: Bar grating fence with horizontal U-shaped profiles as endless fence with variable distances between posts



Figure 7-7: Bar grating fence with horizontal flat steel profile as endless fence with variable distances between posts

7.2.4.4 Front guard fence

Front guard fences are predominantly customised and depending on the requirements consist of welded tubular profiles.

Front guard fences are often more mechanically stable than bar grating fences and generally more appealing due to their customised design. The only way to break through such a fence is by applying considerable force.



Figure 7-8: Front guard fence with post mounted underground



Figure 7-9: Front guard fence with floor plates

7.2.4.5 Other fences

In addition to the types of fences described here, there are other types such as fences of expanded metal, waved grate fences and wooden fences which are not covered in more detail since they are of secondary practical importance from a security point of view.

7.2.4.6 Walls

In addition to fences, walls (stone, concrete walls) also provide privacy protection and enhanced physical resistance. Moreover, walls make it more difficult to climb over or through or crawl under.

In case of a high protection level, a combination of fence and wall might be suitable as these progressive safeguards help to win additional intervention time.

Security may be even more enhanced by anti-climb guards such as barbed or razor wire, extensions etc. on fences or walls. Buildings in the perimeter's course should also be equipped with these guards.

Pursuant to the security concept, it is necessary to assess whether protection from crawling underneath is required for fences. It may consist of bar grating panels partially buried underground, a concrete edge boulder or a strip of foundation.

7.2.5 Anti-climb guard

There are suitable and/or complementary anti-climb guards for all the protection measures outline before. Specifically, these may be the following e.g.:

- barbed wire, galvanised or stainless steel on straight or offset extensions
- barrier razor wire, as flattened wire or coiled with different loop sizes
- expanded metal, simple or folded over
- serrated edges or projecting spires on gates, front guard fences or bar grating panels



Figure 7-10: Flexible plate of expanded metal as anti-climb guard



Figure 7-11: Barrier-B barrier belt (razor wire)



Figure 7-12: Razor wire, coiled with concertina effect (barrier belt)



Figure 7-13: Classical barbed wire as extension of bar grating fence



Figure 7-14: Serrated ledge as anti-climb guard

Anti-climb guards are predominantly used for walls (protecting the top of the wall), wire mesh, bar grating fences and paling fences or gates. However, for reasons of personal protection, they are only used from a height > 1.8 m.

In individual cases, such safeguards may also be used for turnstile systems or adjacent buildings in order to hamper persons climbing over.

For high security requirements in particular, a combination of these safeguards e.g. bar grating panels with extended posts with expanded metal combined with barrier belt might be suitable.



Figure 7-15: Combined anti-climb guard (expanded metal with coiled razor wire)

7.2.6 Openings in barriers

7.2.6.1 General

Closed barriers require access and exit points (for persons or vehicles). These panels in the course of the barrier require separate design and implementation in order to meet the security requirements.

In terms of the security level, openings in barriers must provide the same level of protection as the barrier itself. They require special attention in organisational terms because the safest gate becomes useless if left open “night and day”. Smart implementation of suitable access controls could make sense here. For the interaction of various protection measures, see also chapter 5.4.

For all power-operated gates, the relevant standards and other regulations must be complied with (including redesign and major changes). The following standards apply to gates, among others:

- DIN EN 13241-1 Industrial, commercial and garage doors and gates – Product standard
- DIN EN 12453 Industrial, commercial and garage doors and gates – Safety in use of power operated doors
- ASR-A 1.7 (Work place regulation)

7.2.6.2 Doors, gates, turnstiles/turn barriers

Doors and gates required to block access should provide the same level of protection as the wall or fence surrounding them.

Turnstiles provide controlled access and/or exit for individual persons (separation). In general, turnstiles are integrated into the wall or fence.

7.2.6.3 Gates

Gates are predominantly installed in access and exit areas (vehicles). Their purpose is to separate vehicles as well as to prevent forceful driving through when combined with road blocking.

7.2.6.4 Bollards, car barricades

Car barricades are used to complement gates systems while bollard constructions are predominantly used to provide access to persons and stop vehicles. Both types of struc-

tures are able to withstand high impact loads that may be caused by vehicles of different sizes and weight categories obstructing the vehicles' passage.

Taking into account the respective protection level, requirements may be defined pursuant to established test procedures of American and/or British standards (see Annex A). Different types of bollards can be distinguished such as dynamic bollards respectively road blocks that are retractable depending on the situation and static bollards that are stationary. Adjustable barriers are generally operated by electro-hydraulic mechanisms.



Figure 7-16: Retractable crossing block (BLS, "barrier lift system")



Figure 7-17: Car block ("Wedge barrier")



Figure 7-18: Bollard construction

8 Detection through electronic surveillance systems

8.1 General

For the purpose of securing perimeters, fences, boundaries or roofs with electronic surveillance, systems specific for different applications are suitable which can be classified as follows:

- systems for ground monitoring
- systems for fence protection
- systems for wall surveillance
- systems for door/gate surveillance
- systems for volumetric surveillance
- systems for optical surveillance (video systems)

Aside from installation of individual systems, it may also be necessary to install a combination of systems depending on the requirements in order to be able to

- rule out the possibility of weak points
- implement an AND operation (to reduce the NAR) or
- achieve a redundant protection of a sector.

Selecting a suitable detection system depends on the respective location (sector) and in particular on the protection goal. The operating principle of the sensor technology has to be suited to the environmental conditions such as weather and distance of the operating site to public roads and paths. For instance, an audio cable sensor on a fence directly located on a highly frequented public route is less suited for a fence since pedestrians more than likely touch the fence quite often or cyclists lean their bikes against it causing too many false alarms.

The following table shows possible electronic surveillance measures and the corresponding protection goals depending on the sector and the required security level.

electronic surveillance measures	security level	goal	example
sector 0	basic	---	---
	increased	detection of persons approaching the perimeter area	volumetric surveillance video surveillance (only when sector 0 is not a public area)
	high	detection and localisation of persons and objects approaching the perimeter area	volumetric surveillance ground monitoring Intelligent video analysis

electronic surveillance measures	security level	goal	example
sector 1	basic	detection of persons passing the boundary of the premises without aids	fence protection
	increased	detection of intruders climbing over the barrier without additional aids	ground monitoring fence protection Intelligent video analysis
	high	detection and localisation of intruders climbing over, crawling under or penetrating the barrier with or without additional aids	ground monitoring fence protection video sensor technology intelligent video analysis
sector 2	basic	detection of persons lingering in the sector	volumetric surveillance
	increased	detection of persons lingering in the sector	volumetric surveillance floor monitoring
	high	detection and localisation of persons lingering in the sector	volumetric surveillance ground monitoring video sensor technology intelligent video analysis
sector 3	basic	---	---
	increased	detection and localisation of persons active in sector 3	volumetric surveillance
	high	detection and localisation of persons active in sector 3	fence protection volumetric surveillance ground ground monitoring video sensor technology intelligent video analysis

Table 8-1: Electronic surveillance measures relative to the protection level and sector

Video surveillance is a key component in this context. Verification of alarms of all perimeter detectors by way of video surveillance technology is an important factor which should be considered in every project. This way, guards of a security company are able to use video images as important information to verify what caused the alarm. The number of intervention forces and additional tactical parameters for intervention can be specified well in advance of an intervention. If video images are used to verify false alarms, interventions can be avoided which saves unnecessary expense.

8.2 Overview of electronic surveillance systems

Electronic surveillance systems have different principles of detection designed for specific applications. The following chapters will describe the individual systems in more detail. In this context, the classification of systems based on their suitability for barrier, floor and volumetric surveillance may provide guidance on the suitability of the sensor systems outlined.

The following table highlights the suitability of the electronic surveillance systems described later:

surveillance	chapter	suitable for barrier surveillance	suitable for floor monitoring	suitable for volumetric surveillance
audio cable system	8.3	+++	---	---
fibre optic sensor cable	8.4	+++	+++	---
infrared light barriers	8.5	+++	---	---
tilt/acceleration sensor systems	8.6	+++	---	---
capacitive proximity detectors	8.7	+++	---	---
high frequency transmission cable systems	8.8	---	+++	---
seismic detectors	8.9	---	+++	---
pressure change sensors	8.10	---	+++	---
laser scanner	8.11	o	---	+++
infrared motion detectors	8.12	o	---	+++
micro wave sensors	8.13	---	---	+++
radar detectors	8.14	---	---	+++
video sensor technology	8.15	o	---	+++
Detection systems for fences	8.16	+++	---	---
intelligent video analysis	8.17	+++	---	+++
+++ well suited		o partly suited	--- not suited	

Table 8-2: Suitability of surveillance systems for barrier, ground and volumetric surveillance

8.3 Audio cable systems

8.3.1 Detection principle and specification

Audio cables are able to sense the slightest noise (structure-borne noise) on a barrier, e.g. a fence. The sensors cables are simply fastened (e.g. with cable straps) to the fence; no additional gear on the fence is required. It is also possible to mount these systems to fences afterwards.

The cable registers any vibrations caused by e.g. cutting or climbing over the fence and transform them into electrical signals which are transmitted to a processing unit that evaluates the signals and generates an alarm message.

Different systems can be distinguished such as analogue and digital systems. While analogue systems evaluate vibrations on the basis of their intensity only, digital systems evaluate the intensity of the vibration as well as the transit time of impulses. Since the transit time is proportional to the distance, these detectors are able to accurately determine where the alarm has been triggered.

8.3.2 Application

Audio cable systems are suitable for surveillance of fences. The more rigid the fence the more sensitive should the system's parameters be since noise caused by an attack is muffled and becomes more and more difficult to notice.

Aside from protecting fences, special audio cable systems can also be applied to monitor walls or ceilings for penetration.

8.3.3 Type of attack

Audio cable systems are suitable for detection of persons who **climb over** or **cut through** a fence in order to **climb through** it. Any persons climbing over the protected barrier using tools can only be detected if they touch the barrier creating noise at the barrier. Massive impacts such as e.g. **driving through** a fence with a vehicle can also be detected.

8.3.4 Pros and cons

The systems are fairly easy to install and are also suitable for retrofitting existing fences.

The sensitivity of digital systems can be adapted specifically to suit the respective installation site.

Since the routing of audio cables is visible, the sensor cables are an easy target for sabotage, which causes an alarm.

Extraneous noise at the fence caused by environmental impacts such as storm or heavy rain may be filtered out to varying degrees depending on the system installed. In some cases, considerable vibration caused by environmental impacts may cause false alarms.

8.3.5 Surveillance range/detection

Depending on the system installed, the sensor cables might be several hundred metres long. The surveillance field of a cable is approx. one to two metres circumference around the cable routing. Digital systems are able to localise alarms along the cable routing with an accuracy of several metres.

8.4 Fibre optic sensor cable

8.4.1 Detection principle and specification

Fibre optic sensor cables are able to register noise (structure-borne noise) at a barrier (e.g. fence) or in the ground. The sensors cables are simply fastened (e.g. with cable straps) to the fence; no additional gear on the fence is required. It is also possible to mount these systems to fences or install them underground afterwards.

Vibrations caused by e.g. cutting or climbing over the fence or by digging in areas under surveillance transmitted by the fence influence the optical behaviour of the detector. The vibrations change the reflexion behaviour of the detector. This change is evaluated and leads to an alarm message.

Different systems can be distinguished such as analogue and digital systems. While analogue systems evaluate vibrations on the basis of the intensity of light, comparing between light emitted and light received, digital systems also evaluate the transit time of impulses. Since the transit time is proportional to the distance, these detectors are able to accurately determine where the alarm has been triggered.

8.4.2 Application

Fibre optic cable systems are suitable for surveillance of very long fences. The more rigid the fence the less suitable these systems are since noise caused by an attack is muffled and becomes more and more difficult to notice.

These systems are also suitable for surveillance of objects such as cable trays or underground pipelines.

8.4.3 Type of attack

Fibre optic cable systems are suitable for detection of persons who **climb over** or **cut through** a fence in order to **climb through** it. Any persons climbing over the protected barrier using tools can only be detected if they touch the barrier creating noise at the barrier. Massive impacts such as e.g. **driving through** a fence with a vehicle can also be detected.

Moreover, these systems are suitable for detection of noise caused by **digging** in areas under surveillance.

8.4.4 Pros and cons

Fibre optic cable systems are fairly easy to install and are also suitable for retrofitting existing fences or for surveillance of transmission lines such as pipelines.

Since the routing of fibre optic cables is visible, the sensor cables are an easy target for sabotage, which causes an alarm.

Depending on the system, the fibre optic sensor cable can also be used for transmission of communication data (e.g. video image data).

Extraneous noise at the fence caused by environmental impacts such as storm or heavy rain may be filtered out to varying degrees depending on the system installed. In some cases, considerable vibration caused by environmental impacts may cause false alarms.

8.4.5 Surveillance range/detection

Depending on the product, analogue systems have a range of several kilometres, while digital systems are suitable for distances as long as up to 80 kilometres.

The surveillance field of a cable is approx. one to two metres circumference around the cable routing. Digital systems are able to localise alarms along the cable routing with an accuracy of several metres.

8.5 Infrared light barriers

8.5.1 Detection principle and specification

Infrared light barriers (IR light barriers) are used for linear surveillance by IR light rays. The systems consist of transmitters and receivers and require one or several IR transmitter-receiver kits for a stretch.

Depending on the system, detection is done by interruption, redirection or manipulation of the system by extraneous light.

8.5.2 Application

Light barriers are suitable for application as security curtain in front of objects to be protected.

They can be applied for surveillance of barriers such as walls, fences or gates. They are installed far enough behind the barrier to hamper any climbing over the light barrier from the barrier proper. It is possible to install them on roofs, fences or walls to protect the crest. They may also be used in form of trap protection for monitoring open spaces.

8.5.3 Type of attack

Persons or objects interrupting the light ray between transmitter and receiver are consistently detected.

When installed at fences or windows, these systems detect persons **climbing through**. When installed on fences or walls, these systems detect persons **climbing over**. In general, they detect objects that cut off the light ray.

8.5.4 Pros and cons

The applications for light barriers are manifold. They can easily be retrofitted in existing surveillance systems.

The surveillance range may be restricted by e. g. heavy fog. In this case, the system may generate a disqualification message (cf. Chapter 10.5).

Hills and depressions require special consideration as they may constitute surveillance loopholes.

8.5.5 Surveillance range/detection

Different systems with varying ranges are available.

The individual transmitters and receivers are, in general, installed in posts. The number of stretches (transmitter-receiver pair) may differ.

The height of light barrier systems ranges from a few centimetres to several metres. Since several transmitter/receivers are generally installed in the posts, several alarm areas can be realised.

8.6 Tilt/acceleration sensor systems

8.6.1 Detection principle and specification

Piezo-electric or capacitive sensors register structure-borne noise created at their installation site within a range of a few Hertz up to several Kilohertz. They convert the vibrations into electrical signals. If the installation position of the sensor should also be monitored, special capacitive sensors are the choice.

8.6.2 Application

Tilt/acceleration sensors are suitable for monitoring fences. The more rigid the fence the more sensitive should the system's parameters be since noise caused by an attack is muffled and becomes more and more difficult to notice.

The sensors can be mounted either on a fence panel or a post.

There are also systems available that can be used to monitor walls or ceilings for penetration.

8.6.3 Type of attack

Tilt/acceleration sensors are suitable to detect persons **climbing over** or **cutting through** a fence. Any persons climbing over the protected barrier using tools can only be

detected if they touch the barrier creating noise at the barrier. Massive impacts such as e.g. **driving through** a fence with a vehicle can also be detected.

Moreover, these systems are suitable for detection of noise caused by **digging** in areas under surveillance.

8.6.4 Pros and cons

The systems are fairly easy to install and are also suitable for retrofitting existing fences.

The sensitivity of these systems can be adapted specifically to suit the respective installation site.

Since the installation of these systems is visible, the sensors become an easy target for sabotage, which generally causes an alarm. However, installation in the post may hamper sabotage effectively. Extraneous noise at the fence caused by environmental impacts such as storm or heavy rain may be filtered out to varying degrees depending on the system installed. In some cases, considerable vibration caused by environmental impacts may cause false alarms.

8.6.5 Surveillance range/detection

The individual sensors have a detection range of several metres and, depending on the product, can be connected to systems of different sizes.

8.7 Capacitive proximity detector

8.7.1 Detection principle and specification

Proximity detectors consist of a set of parallel wires (sensor fence) that are electrified. A **capacitive field is created between these wires. If an object approaches, the properties of this field change.** Every object causes a characteristic change of the field, which is evaluated.

8.7.2 Application

Proximity detectors suitable for monitoring fences and walls.

They are commonly installed on or behind a fence or wall.

8.7.3 Type of attack

Persons climbing over or cutting through the proximity detectors or crawl under the electrical field are detected. Persons climbing over with aids are also detected. Massive impacts such as e.g. driving through a fence with a vehicle can also be detected.

8.7.4 Pros and cons

These systems boast a very good detection reliability and protection against circumvention.

As a result of their rather elaborate installation, these systems are primarily used for applications with highest security requirements.

8.7.5 Surveillance range/detection

The systems available can be used to set up alarm sectors of up to 150 m length. The height of the sensor fence may be up to 4 m. Localisation of alarms in different sectors along the fence is possible.

8.8 High-frequency transmission cable systems

8.8.1 Detection principle and specification

Two coaxial sensor cables routed underground create an invisible electro-magnetic HF detection field. The system detects any change to the field that may be caused by persons,

animals or objects. Also, there are systems available that have one cable (mono cable) instead of two parallel ones.

8.8.2 Application

Depending on the product, the cable systems can be used for surveillance of paved, gravelled or asphalt surfaces as well as paths or grassland etc.

8.8.3 Type of attack

HF transmission cable systems are well suited to detect persons or vehicles that **walk, run, crawl** or **drive** over a surface. **Digging** underneath is also detected.

8.8.4 Pros and cons

One of the system's benefits aside from its covered installation is its suitability for uneven terrain since the surveillance field can be aligned to the landscape.

The buried installation does not make it possible to see the detection field from outside.

Slowly changing environmental conditions such as freezing or snow do not have any negative impact on detection accuracy since the systems is able to automatically adjust to slow changes.

The high installation effort required (earthworks) needs to be taken into account for the planning process.

It is necessary to ensure sufficient distance to fences, developments and trees and/or large vegetation in order not to cause any interference in the HF field.

8.8.5 Surveillance range/detection

Depending on the product, the sensor cable might be several hundred metres long. The surveillance field may be approx. one to two metres high and approx. two to three metres wide. Alarms can be accurately localised within a range of several meters along the surveillance field.

8.9 Seismic detectors

8.9.1 Detection principle and specification

Microphones and/or geophones are often built into the masonry or ground. Their electro-dynamic function converts mechanical vibrations into electrical signals.

8.9.2 Application

Depending on the product, the detectors can be used for surveillance of paved, gravelled or asphalt surfaces as well as paths or grassland etc. In addition, there are certain makes suitable for application in masonry.

8.9.3 Type of attack

Seismic detection systems are well suited to detect persons or vehicles that **walk, run, crawl** or **drive** over a surface. Attacks on masonry can also be detected as well as **digging**.

8.9.4 Pros and cons

One of the system's benefits aside from its hidden installation is its suitability for uneven terrain since the surveillance field can be aligned to the landscape.

The advantage of point-by-point seismic systems is their extremely flexible layout.

The high installation effort required (earthworks) needs to be taken into account for the planning process.

Slowly changing environmental conditions such as freezing or snow do not have any negative impact on detection accuracy since the system is able to automatically adjust to slow changes. Vibrations caused by machines and the like may interfere with the system and trigger false alarms.

8.9.5 Surveillance range/detection

Current microphone and/or geophone systems have a detection range of several metres per sensor. Several sensors may be cascaded to larger systems.

8.10 Pressure change sensors

8.10.1 Detection principle and specification

These sensors are installed underground and are designed to detect pressure changes in the soil.

Systems that cover a linear area and those that monitor points have to be distinguished. Linear systems consist of long pipes filled with a special liquid. They are able to register any changes of pressure along the sector under surveillance and transmit them to membranes where these changes in pressure are converted to electrical signals.

Point-type pressure sensors, however, consist of an arrangement of single sensors (without pipes) that register any changes in pressure and convert them to electrical signals.

8.10.2 Application

Depending on the product, the sensors can be used for surveillance of paved, gravelled or asphalt surfaces as well as paths or grassland etc.

Point-type pressure change sensors may also be built into concrete surfaces or false floors (under support elements).

8.10.3 Type of attack

Pressure change sensors are well suited to detect persons or vehicles that **walk, run, crawl** or **drive** over a surface.

8.10.4 Pros and cons

One of the system's benefits aside from its invisible installation is its suitability for uneven terrain since the course of the landscape does not need to be considered especially. These systems can also be applied close to existing developments.

The high installation effort required (earthworks) needs to be taken into account for the planning process.

Slowly changing environmental conditions such as freezing or snow do not have any negative impact on detection as the system only evaluates short-term phenomena.

The invisible installation does not make it possible to localise the detection field from outside.

Another benefit of point-type detector systems is their flexible application; routing does not require compliance with any special bending radius.

8.10.5 Surveillance range/detection

The pipes for the pressure system may be up to approx. 100 m long. Typically, two pipes are installed in parallel. Linear systems have a detection range that is several metres wide. Alarms can be accurately localised within a range of several meters along the surveillance field.

The detection radius of point-type detectors is approx. 1 to 2 m. The sensors may be cascaded to larger systems.

8.11 Laser scanner

8.11.1 Detection principle and specification

Laser scanner sweep their environment with two-dimensional laser beams. They detect objects in the surveillance area by measuring the travel time of light reflected. They are able to determine the size of objects, their distance to the detector and their speed.

8.11.2 Application

Laser scanners are suitable for application as detector with certain characteristic in front of objects to be protected.

They can be applied for surveillance of barriers such as walls, fences or gates. It is possible to install them on roofs, fences or walls to protect the crest. They may also be used as traps for monitoring open spaces.

8.11.3 Type of attack

Persons or objects that influence the reflection of the laser beam are accurately detected.

When installed for surveillance of fences or windows, these systems detect persons **climbing through**. When installed on fences or walls, these systems detect the **climbing over**.

They can also be used for surface surveillance.

8.11.4 Pros and cons

It is possible to specify the surveillance range of individual sensors with geometric accuracy. Laser scanners may be operated horizontally and vertically. However, structural elements located in the surveillance area (e.g. chimneys on roofs) may cause shadows, which make detection in this area impossible.

Analyses of the size of the object make it possible to realise different alarm scenarios assuming different interference factors.

The surveillance range may be restricted by weather conditions such as e.g. heavy fog or snow. If detection fails as a result of weather conditions, the system generates a disqualification message.

As laser beams are invisible to the human eye, the surveillance area cannot be seen which makes it more difficult to outsmart a sensor.

8.11.5 Surveillance range/detection

Depending on the product, surveillance areas with a radius of several hundred metres are feasible. The surveillance area may be divided into several zones.

8.12 Passive infrared motion detectors

8.12.1 Detection principle and specification

Passive infrared motion detectors (PIR motion detectors) register heat reflected from objects in its detection range. Mirror or Fresnel lenses pool the rays of heat and transfer it onto a sensor. For an alarm to be activated, the sensor has to detect a certain temperature difference over a specified period of time which is caused by the object being colder or warmer than its environment. Gradual changes in temperature do not activate any alarm.

8.12.2 Application

Depending on the optics installed, PIR motion detectors are suitable for surveillance of open spaces as well as certain surveillance.

Depending on the system, the area behind a barrier may be subject to either linear or wide-angle surveillance.

No sudden temperature changes should be expected in the surveillance area as they may trigger false alarms.

8.12.3 Type of attack

Persons or objects in the sensor's detection range whose temperature differs sufficiently from their environment are detected.

PIR motion detectors are suitable for surveillance of open spaces in order to detect persons who cross the surface **walking** or **running** by means of detection traps. Also, vehicles **driving through** the surveillance area are detected.

8.12.4 Pros and cons

The detectors are easy to assemble.

The detector's sensitivity can be individually adjusted. Depending on the type, the surveillance areas may be divided into several alarm sectors.

Structural elements located in the surveillance area (e.g. chimneys) may cause shadows, which make detection in this area impossible. Moreover, these structural elements may be a source of false alarms. Due to the nature of its operating principle, the sensor is sensitive to weather. If ambient temperatures are in the range of body temperature, detection is not possible. Sudden temperature changes such as air turbulences or exhaust air from chimneys etc. may activate false alarms.

8.12.5 Surveillance range/detection

Depending on the type, the range may be approx. 100 m. The width of the surveillance area can be adjusted by suitable lenses or partial masking of the optical system (from $< 5^\circ$ to $> 120^\circ$).

8.13 Micro wave sensors

8.13.1 Detection principle and specification

Micro wave sensors consist of physically separated transmission and reception units that create a volumetric electro-magnetic field between themselves. Changes of this field caused by objects, animals or persons are detected and lead to activation of alarms.

8.13.2 Application

Micro wave sensors are applied for surveillance of long stretches in open spaces or on top of roofs.

8.13.3 Type of attack

Persons or objects lingering in the detection range of the sensor are detected reliably.

Micro wave sensors are well suited for surveillance of open spaces to detect persons **walking**, **running** or **crawling**. Also, vehicles **driving through** the area are easily detected.

8.13.4 Pros and cons

Detection is extremely reliable and not sensitive to the weather.

As micro waves are invisible to the human eye, the surveillance area cannot be seen which makes it more difficult to outsmart a sensor.

The sensor is not suited for tight surveillance areas. Hills and depressions require special consideration as they may constitute surveillance loopholes.

8.13.5 Surveillance range/detection

The radius of the elliptically extended surveillance area may be up to 15 m in the middle. It may be up to several hundred metres long.

8.14 Radar detectors

8.14.1 Detection principle and specification

Radar detectors use electro-magnetic radiation in the range of micro waves and consist of combined transmission and receiver units. The transmitter emits electro-magnetic waves, and the receiver receives signals (echo) reflected by objects in the detection range.

The Doppler's principle is able to detect objects and persons with speed, position and direction. This type of detector shows its best detection properties when the object to be detected moves predominantly away from or towards the detector.

There are static systems available that monitor a specified area as well as rotating systems for surveillance of the area all around.

8.14.2 Application

Radar detectors are used for surveillance of straight stretches or surfaces in open spaces or roof tops.

8.14.3 Type of attack

Persons or objects lingering in the detection range of the detector are detected reliably.

These detectors are well suited for surveillance of open spaces to detect persons **walking, running or crawling**. Also, vehicles **driving through** the area are easily detected.

8.14.4 Pros and cons

Detection is extremely reliable and not sensitive to the weather. The surveillance area of the radar detector can be defined exactly. It is possible to divide the surveillance area into several sectors.

However, structural elements located in the surveillance area (e.g. chimneys on roofs) may cause shadows, which make detection in this area impossible.

The sensor is not suited for tight surveillance areas (width < 2 m).

8.14.5 Surveillance range/detection

Depending on the product, areas with a radius of several hundred metres can be monitored.

8.15 Video sensor technology

8.15.1 Detection principle and specification

In general, **video motion detectors** operate on the basis of image analysis. They are able to detect changes in a recorded scene and use these changes to generate an alarm.

In contrast, **video sensor technology** is use complex algorithms to recognise and/or track objects in a scene. In general, video sensor technology is only used for outdoor applications since even slightest changes in images (e.g. caused by fluctuation of brightness) may trigger undesired messages.

8.15.2 Application

Video sensor systems are suitable for open space and volumetric surveillance.

8.15.3 Type of attack

Given a proper installation and **suitable environmental conditions**, typical motion patterns generated by objects or persons create an alarm signal.

Video sensor systems are well suited for surveillance of open spaces to detect persons **walking, running or crawling**. Also, vehicles **driving through** the area are easily detected provided that environmental conditions are suitable.

8.15.4 Pros and cons

The applications for video sensor technology are manifold. The most important prerequisites are environmental conditions suitable for the application of image-processing technology.

Alarms can easily be verified using images recorded.

Video sensor technology are extremely sensitive to weather. A clear field of vision is required for optimum functioning.

Alternatively, in order to better ensure the function at night IR-compliant cameras should be used in combination with IR spotlights in order to illuminate the surveillance area. IR light is generally invisible to the human eye.

Thermographic cameras which do not require any IR spotlights can be used as an alternative to conventional cameras. However, they do not necessarily allow an identification of persons.

However, structural elements located in the surveillance area (e.g. chimneys on roofs) may cause shadows, which hamper detection in this area. In blind sectors a detection is not possible.

8.15.5 Surveillance range/detection

Depending on the product, the surveillance range of video sensor technology may be approx. 50 m; high-performance thermographic cameras have a range of several kilometres.

Depending on the level of detail of the image targeted, maximum distances to the object need to be considered for alarm verification. The requirements for the choice and position of cameras differ depending on whether the aim is to detect an object in a picture detail, recognise, for instance, that it is a person up to identifying the person. It is necessary to specify in advance to which of the three classes in line with VdS Guidelines for Video Surveillance Systems, Planning and Installation, VdS 2366, the image to be generated is attributed.

The performance features of classes 1 to 3 are based on the resolution in the depiction of the target object and the discernibility of details. Three different image sizes can be distinguished (cf. figure 8-1):

Class 1 – Perception: One pixel depicts a maximum of 20 mm in real life.

Class 2 – Recognition: One pixel depicts a maximum of 5 mm in real life.

Class 3 – Identification: One pixel depicts a maximum of 1 mm in real life.

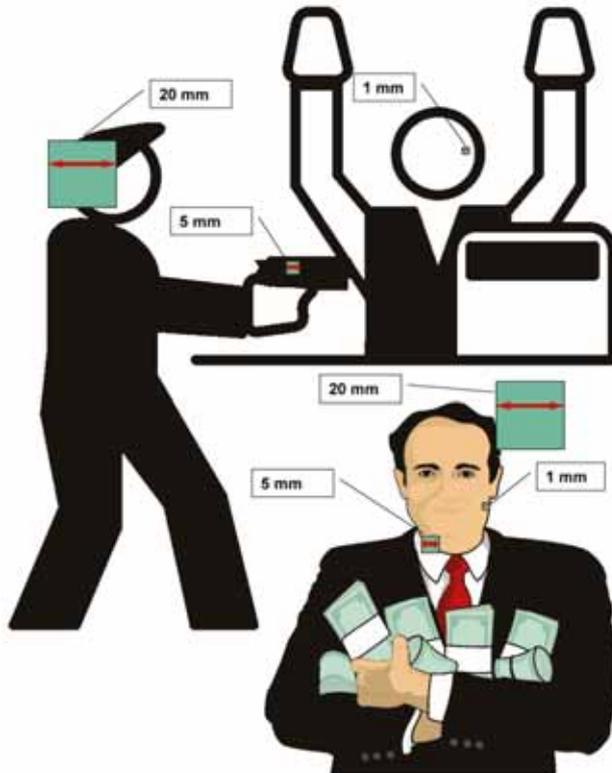


Figure 8-1: Comparison of different image sizes in line with VdS Guidelines VdS 2366

8.16 Fence detection systems

8.16.1 Detection principle and specification

Fence detection systems are based on monitoring the fence by closed-circuit principle. Either the fence proper is used as electric conductor or an alarm wire is inserted into hollow profiles of a fence.

Cutting or breaking parts of the fence interrupts the alarm wire, which triggers an alarm.



Figure 8-2: Detection fence with alarm wire inserted

8.16.2 Application

Fence detection systems are suitable for protection of perimeter boundaries of different lengths or for security.

In combination with a shear-off feature for detection, systems based on closed-circuit principle are also applied as anti-climb guards.

8.16.3 Type of attack

The detection system for fences is well suited to recognise an intruder **cutting** the fence or a vehicle **driving through** it. It also recognises a person climbing over the fence if the zero signal current system is combined with a shear-off feature for detection.

8.16.4 Pros and cons

These systems have a very low false alarm rate, if any. However, they cannot be retrofitted to standard fences. When new fences are installed or old ones replaced completely, these detection systems are a viable option.

8.16.5 Surveillance range/detection

Depending on the product selected, the fence may be up to several hundred metres long.

If the entire fence serves as an “alarm wire”, attacks at any point can be reliably detected (**cutting, severing**). In case the fence is protected by a single inserted alarm wire, the panels of the fence not monitored can be cut or severed without triggering an alarm.

It is not possible to localise where the alarm was triggered.

8.17 Intelligent video analysis

8.17.1 Detection principle

Intelligent video analysis processes information from optical and thermal images taken with colour picture respectively thermal cameras and distinguishes between moving objects and static background. On the basis of pixel-precise image analysis and perspective models, objects in the surveillance area can be detected (localised), traced (tracking), identified (classification) and their properties be determined (speed, colour, etc.).

Calibrated systems are able to accurately localise the position of an object on the property. Depending on the manufacturer, intelligent video analysis is able to detect movement patterns (behaviour analysis) and provides for division into different zones (sectors) which enables greater detection accuracy in various applications.

8.17.2 Application

Intelligent video analysis is suitable for open spaces and volumetric surveillance of objects regardless of their occupancy. It can be applied for surveillance of open spaces, fences, walls and gates as well as for protection of façade of buildings. Under certain conditions, it can even be mounted on roof tops.

8.17.3 Type of attack

Moving objects (persons, vehicles) in the camera’s field of vision are reliably detected provided technical requirements are met. When applied for surveillance of open spaces, intelligent video analysis is able to recognise persons crawling, walking or running over a surface as well as vehicles. When applied for perimeter surveillance, the systems are able to reliably detect objects approaching (outside), suspicious persons (loitering), persons climbing over or through. As part of a façade protection and roof monitoring system, intelligent video analysis is able to reliably recognise persons moving (e.g. abseiling in prisons).

8.17.4 Pros and cons

The surveillance area can be accurately and individually divided into several areas with different functions each. Zoning concepts ensure simple adaptation to different security sectors. Moreover, these specifications make it possible to integrate public areas (surrounding field) in the detection scheme and the overall security concept. Depending on the manufacturer, this allows for straightforward identification friend or foe. The position and extension of the surveillance area is not discernible for the intruder which obstructs overcoming the surveillance area. Alarm verification is quite simple since relevant objects are marked on the video image. Intelligent video analysis is able to self-monitor its functioning by recognising sabotage attempts such as turning of camera, masking, blinding, defocussing as well as signal failure.

To comply with relevant data protection regulations, it is possible to pixelate areas within the camera's field of vision or moving objects, thus obliterating them. If need be, pixilation can be unset by authorised persons.

A free field of vision (no dead angles) is required for optimum operation. Structural elements located in the surveillance area (e.g. chimneys on roofs) may cause optical masking, which makes detection in this area impossible. When using colour and/or day/night vision cameras at night, additional lighting is required (regular or infrared lights). Thermal cameras may be used without lighting.

Due to the nature of their operating principle, opto-electronic detection systems are sensitive to weather. Compliance with maximum permissible range (manufacturer's specifications) reduces weather sensitivity to a large extent.

8.17.5 Surveillance range/detection

Depending on the product, colour cameras have a surveillance range for perimeter surveillance of up to 50 m. Thermal cameras have a surveillance range of 120 to 150 m to achieve optimum detection results. The maximum surveillance range can be multiplied if restrictions caused by weather sensitivity are ignored.

9 Activation of the perimeter detection system

9.1 General

Classical intruder alarm systems meeting the Guidelines VdS 2311 are set or unset by being "activated" respectively "deactivated" with appropriate approved ancillary control systems.

By contrast, perimeter detection systems are activated or deactivated differently. Detectors have to be deactivated if they monitor areas which are frequented during normal business operation, which would otherwise trigger alarms. In any case, perimeter detection systems must be activated/deactivated by authorised persons only.

9.2 Activation/deactivation

Activation of the perimeter detection system turns on the indication of alarm messages by optical/acoustic warning devices and the transfer to a permanently manned station.

Combining information from a perimeter detection system and a video surveillance system makes it possible to verify and, if necessary, document alarms.

In general, perimeter detection systems are directly incorporated into the hazard management system of an external or internal permanently manned station which also activates/deactivates them. If the perimeter detection system should not be activated by the permanently manned station, it is also possible to fit the system with an ancillary control equipment on-site (cf. chapter 9.4) for activation/deactivation. Moreover, it is under certain conditions also possible to activate/deactivate perimeter detection systems by time control.

It must be possible to operate ancillary control equipment outside the surveillance area or activated partial areas. Its design must be sabotage-proof and adapted to the respective environmental conditions.

If the perimeter detection system is activated/deactivated by a control room, prior approval by an authorised person is required.

9.3 Partial activation

Partial activation of a perimeter detection system makes it possible to monitor only parts of an object. Only those detectors of the system are activated which could not trigger an alarm by attendant persons, pets and the like (e.g. detection fence). A large part of the system is always activated.

9.4 Ancillary control equipment

Special ancillary control equipment is used to activate/deactivate perimeter detection systems on site. Systems characterised by a high fail-safety are particularly suitable.

Ancillary control equipment may have different features to authenticate an authorised user (identification features; the term IM is used as abbreviation for the German term "Identifikationsmerkmal") including the following:

- physical identification features, e.g. key, transponder,
- mnemonic identification features, e.g. personal identification code,
- biological identification features, e.g. finger print.

These might be components that require a material or biological identification feature, e.g. a conventional key, transponder or biometric feature. A combination with mnemonic identification features and/or time control is possible. In order to enhance a system's fail-safety, it is possible to have a combined evaluation of several of the above identification features. Activation/deactivation by time control should only be considered in exceptional cases; it is generally not recommended.

protection level	application of at least one IF			combination of at least two IF		
	only physical IM	only mnemonic IM	only biometric IM	physical and mnemonic IM	physical and biometric IM	biometric and mnemonic IM
basic	X	X	X	X	X	X
increased	X	---	X	X	X	X
high	---	---	---	X	X	X

X: admissible

---: not admissible

Table 9-1: Recommended options for activation

When activating ancillary control equipment that works with mnemonic authentication the user has to make sure that other persons are not able to see the code (which also has to be considered for designing video surveillance systems!).

9.5 Signalling of system status

There should be a signal close to the ancillary control equipment indicating that the system is activated. This can be done by an optical or acoustic signal for a specified period of time. Third persons must not be able to notice the current status of activation of the perimeter detection system.

9.6 Activation meeting Zwangsläufigkeit

Activation of the perimeter detection system must be prevented if the system is not functional in all its parts.

Any failed attempt at activation has to generate a “negative acknowledgement“. Preferably it should be indicated by a signal that clearly differs from the activation message.

If necessary, partial activation can be effected if individual parts of the system are operating as stand-alone. Compensation measures should be considered for the inactive part. For instance, if a panel of a protected fence is destroyed (for instance, by windthrow of wood), the remaining part that is still intact could be activated. To compensate for the defective electronic surveillance in the area of the destroyed part e.g. security guards have to be envisaged.

9.7 Deactivation meeting Zwangsläufigkeit

Ideally, access to the monitored perimeter area should be prevented until perimeter surveillance for this part is deactivated.

This can be realised by e.g. installing electro-mechanical locking devices, half cylinders which cannot be operated from outside or by setting electrical motors to idle.

10 Types of alarm messages

10.1 General

All types of alarm messages described below have to be separately evaluated by the perimeter protection and detection system. VdS-approved devices for surveillance of open areas (cf. VdS Guidelines VdS 3456) have up to four defined output interfaces:

1. Perimeter alarm message
2. Sabotage/tamper alarm message
3. Fault message “monitoring mode of operation“
4. Fault message “disqualification“⁶

Alarm messages of the same type may only be transmitted pooled if the alarm receiving unit is able to match the messages unmistakably (in sufficient degree of detail) in order to ensure that intervention is adequate to the risk.

In general, all devices for recording, processing and transmitting alarms must be installed in the locked part of the security area to avoid any disturbing or adverse influences and ensure enhanced protection against access. Only those components that have to be in the open part of the security area due to their technical function (e.g. video cameras, sensors) can be installed there. However, they should be hidden and not installed on the exposed side (attack side).

10.2 Perimeter messages

Perimeter messages need to be connected to an alarm or a hazard management system and respective alarms have to be transmitted to a control room that is manned 24/7. VdS-approved devices for surveillance of open spaces have an interface for perimeter messages which is designed as a low-impedance contact in normal condition that becomes high-impedance in case of a functional defect. Alternatively, there are also interfaces specified by the manufacturer (proprietary solutions).

A perimeter message has to be checked as early as possible to verify whether it is a matter of alarm or false alarm (verification). In case of an alarm, coordinated intervention

⁶ This kind of message is not available for all detection types.

measures must be initiated. In case of a false alarm, processing of the message must be acknowledged and any measures already initiated must be aborted.

Depending on the arrangement with the risk carrier, the alarm can be verified manually or automatically.

If alarm messages are verified **manually** before intervention is initiated, message transfer to the intervention services will be on hold for the time being while verification is done. This "hold period" must be adequate to the risk, may vary depending on the sector and must not exceed a specified period of time e.g. three minutes.

For instance, a message generated by a detection fence is transmitted to a control room manned 24/7 where the guard responsible first verifies and acknowledges the alarm on the basis of an additional video image and then releases the alarm and transmits it to the intervention forces. If there is unscheduled no verification during the "hold period", alarm transfer will be released automatically.

Moreover, alarm verification can be **automated**, for instance through intelligent linking of various sensors of one or more sectors (e.g. barrier-based detection linked with volumetric surveillance in sector 2). As to how alarms shall be automatically verified needs to be agreed with the risk carrier on a case-by-case basis in order to ensure reliable automatic verification to avoid non-alarms to a large extent. In case of doubt, manual verification should be given preference.

Depending on the type of object and technology applied, it is possible to do without verification **prior to** intervention. In this case, verification is done as part of the intervention.

The arrangements made and measures agreed have to be recorded in the system's documentation (cf. chapter 13.1). In order to ensure standardised, reliable and flawless documentation, alarm service and intervention certificates in line with VdS 2529 shall be used.

On the subject of how to deal with alarm messages, see chapter 11.1.

10.3 Sabotage messages

Sabotage messages must be connected to an alarm or a hazard management system and respective alarms have to be transmitted to a control room that is manned 24/7. Sabotage messages must be transmitted separately from other messages and must be identifiable. When activated, sabotage messages have to be assessed like perimeter alarms and handled accordingly.

Availability of sabotage surveillance measures must not be regarded as a substitute for regular security inspections which are nevertheless indispensable since sabotage surveillance measures are able to detect manipulation to a limited extent only. To the extent that other measures by the manufacturer do not effectively prevent tampering attempts, VdS-approved systems for open area surveillance (cf. VdS Guidelines VdS 3456) will cover sabotage surveillance; their interface is designed as a low-impedance contact during normal status that becomes high-impedance in case of a sabotage. Alternatively, there are also interfaces specified by the manufacturer (proprietary solutions).

In order to ensure proper operation of the perimeter detection system, the sabotage message shall only be cleared by the maintenance technician.

The arrangements made and measures agreed have to be recorded in the system's documentation (cf. chapter 13.1). In order to ensure standardised, reliable and flawless documentation, alarm service and intervention certificates in line with VdS 2529 shall be used.

10.4 Fault messages “monitoring mode of operation“

Functional faults of perimeter protection and detection systems may result from e.g.:

- grid failure,
- battery defect,
- faults in central processing nodes,
- defects in processing units.

Failure or defects of programme-controlled processing units (e.g. microprocessors) has to be recognised automatically unless there are other measures to ensure that any failure does not limit functional reliability. VdS-approved devices for surveillance of open areas (cf. VdS Guidelines VdS 3456) have such an automatic monitoring function; their interface is designed as a low-impedance contact in normal condition that becomes high-impedance in case of a functional defect. Alternatively, there are also solutions specified by the manufacturer (proprietary solutions).

Messages of the monitoring function need to be connected to an alarm or a hazard management system and respective alarms have to be transmitted to a control room that is manned 24/7. In case the monitoring function activates an alarm, the maintenance technician should be consulted immediately to restore the smooth operation of the perimeter protection and detection system as soon as possible.

In case a fault message “monitoring mode of operation function“ is generated it must not be transferred or treated as a sabotage or perimeter alarm at any time.

The arrangements made and measures agreed have to be recorded in the system’s documentation (cf. chapter 13.1). In order to ensure standardised, reliable and flawless documentation, alarm service and intervention certificates in line with VdS 2529 shall be used.

10.5 Fault message “disqualification“

Bedewing, fog and the like may cause

- sensor readings to be outside their operating range or
- environmental conditions to be outside their tolerance.

In case the conditions for detection systems deteriorate to such a degree that reliable detection can no longer be expected, some (in general, only activated) perimeter detection systems generate a disqualification message. Such a message is also generated if, for instance, the heating/cooling of a heated/cooled sensor has been deactivated by a grid failure and as a result, the temperature is no longer within a specified tolerance.

Fault messages need to be connected to an alarm or a hazard management system and respective alarms have to be transmitted to a control room that is manned 24/7. In case the fault message “disqualification“ comes on, all parties involved should have agreed in advance whether and what kind of compensation measures (e.g. deploying security guards) should be taken.

The disqualification message is automatically reset once conditions are favourable again. The reset status must be noticeable in order to complete any possible compensation measures initiated.

In case a fault message “disqualification“ is generated, it must not be transferred or treated as a sabotage or perimeter alarm at any time.

The arrangements made and measures agreed have to be recorded in the system’s documentation (cf. chapter 13.1). In order to ensure standardised, reliable and flawless documentation, alarm service and intervention certificates in line with VdS 2529 shall be used.

11 Alarm coordination

11.1 General

Every hazard/burglar alarm message must be taken seriously. This rule must be highlighted to all players, in particular on the operator's part. As soon as alarm messages are no longer taken seriously, any investment in perimeter protection and detection systems is forfeited and the goals of the security concept can no longer be achieved. To ensure compliance with the security concept is the top management's primary responsibility. Responsibilities delegated internally do not cover external third parties. All players involved should realise (and mutually show one another) what is at stake and that a perimeter protection and detection system contributes to achieving protection goals only if it is part of the overall security concepts and embedded in a set of security measures.

A perimeter detection system can meet its intended purpose only if messages generated are processed adequately. This may imply actuation of a local alarm system as well as transfer of the alarm message to a control room manned 24/7. In general, a set of measures is agreed for every type of message and/or every group of detectors (cf. alarm service and intervention certificate in line with VdS 2529) which is implemented in case of an alarm. It may be sufficient under certain conditions to simply save individual alarm messages which could mean, for instance, recording the event activation/deactivation and documenting access rights (who and when). Typically, timeframes may be specified in order for additional measures to be initiated only if the event occurs outside this timeframe (e.g. deactivation outside normal business hours).

Depending on the conditions on site, different alarm constellations are conceivable. In case of perimeter surveillance for premises with a building equipped with a hazard management system, a suitable option is to connect the perimeter detection system to the hazard management system in order to process and document messages centrally and in a standardised format. Display and operation do not necessarily have to be executed on the premises. A hazard management system may be located elsewhere. In case an open space is monitored that does not have an infrastructure as described above with no hazard management system available on site, the latter can be centralised. Often, such a system is used for monitoring several open spaces. A hazard management system consists of systems of the same company (group of companies) or of a special building/premises. Often, different trades are combined. As opposed to that, there are alarm receiving and service centres to which several companies may be connected. The boundaries tend to be blurred.

11.2 Stand-alone solutions

When the messages from the perimeter detection system are transmitted to local optical and acoustic warning device only, this is called a stand-alone solution. Its primary purpose is to deter intruders and psychologically disturb them in their intrusion by acoustic alarm signals. Acoustic alarms are also designed to alert the anonymous public though this is increasingly becoming less promising.

In general, stand-alone designs are not recommended since possible false alarms may easily jeopardise acceptance of such a system.

11.3 Connection to IAS/HMS

11.3.1 General

In general, intruder alarm systems have local display and operating panels as well as transmission lines to a control room manned 24/7. In addition, most IAS also feature a multitude of different parameter types for groups of detectors (burglar, sabotage, fault etc.). These facilities generally lend themselves to process messages from the perimeter detection system as well. However, certain overall conditions need to be considered in

order not to jeopardise the protection goals of the intruder alarm system or the hazard management system.

The combination of different systems generates added value that exceeds the sum of individual system performances. True, information on a fence being compromised (perimeter alarm) or a motion detector in a building being activated (intruder alarm) are useful seen individually, though one-dimensional. Above all, it is not possible to draw any conclusions on their plausibility. If alarms of both systems are combined and the logical link between them taken into account, knowledge about the intruder alarm following soon after the perimeter alarm leads to the conclusion that the perimeter alarm (respectively both alarms) are more than likely “genuine” alarms. A perimeter alarm on its own, by contrast, is often associated with some uncertainty. The added value becomes even more obvious when a camera delivers the relevant video images at the same time that the perimeter alarm is activated (including pre and post alarm frames). This way, multi-dimensional alarm processing ensures almost real-time alarm verification.

However, it should be stressed that a subsequent alarm of an intruder alarm system may serve as a plausibility check for a perimeter alarm – in no case must a singular intruder alarm be left unprocessed because it was not preceded by a perimeter alarm. “Negative alarm verification” of an intruder alarm system by a perimeter detection system is inadmissible.

11.3.2 Provisions of VdS Guidelines VdS 2311

Except for the external warning devices and parts of the ancillary control equipment as well as the alarm transmission system, all parts of an intruder alarm system must generally be installed inside the security area. The aim of minimising the false alarm rate can be achieved by strict compliance with VdS Guidelines VdS 2311 and strict implementation of Zwangsläufigkeit. The products installed have to meet the strictest requirements in terms of zero false alarm rates. Perimeter detection systems which are, by nature, open-air systems cannot meet all of these requirements to the extent desirable and nowadays achievable by intruder alarm systems.

In principle, a perimeter detection system connected to an IAS bears the risk of negative influences on the intruder alarm system – for whatever reasons. Such feedback must be prevented under any circumstances.

Adapting the open-air detectors as intruder detectors is therefore not an option. VdS Guidelines on Intruder Alarm Systems – Planning and Installation, VdS 2311 do not allow adaptation of these detectors for intruder detection. It is therefore necessary to look for alternative solutions.

11.3.2.1 Adaptation as technical detectors

For the reasons described above, the detectors are commonly adapted as so-called technical detectors connected to groups of technical detectors. This type of detector does not trigger intruder or hold-up alarms nor is it incorporated into the intruder alarm system's Zwangsläufigkeit.

When detectors are adapted, the requirements of VdS Guidelines for Intruder Alarm Systems – Planning and Installation, VdS 2311 must be complied with, in particular chapter 12.3.

Excerpt from VdS Guidelines VdS 2311⁷ (*note: VdS 2311 currently available in German only*):

12.3 Detectors for dangerous and emergency situations as well as technical detectors

12.3.1 General

In addition to intruder, hold-up and status detectors of the IAS, other detectors such as e.g. for dangerous and emergency situations as well as technical detec-

⁷ Details of sections and references relate to VdS Guidelines VdS 2311:2010-11 (04)

tors may be installed in VdS-approved IAS provided certain conditions are fulfilled and the following requirements are met.

12.3.2 VdS approval

Detectors for dangerous and emergency situations and technical detectors must be VdS-approved unless these detectors are connected to the IAS by a standard interface as follows and are not powered by the IAS' source of energy.

12.3.2.1 Output or messages

The interface has to meet the following requirements:

- Potential-free output, loading capacity of at least 50 mA at 30 V DC, resistance serially connected < 47 Ω
- Closed in quiescent condition (low-impedance), opens in case of an alarm (high-impedance)
- Response time at least 1 s, maximum corresponding to annunciation of message.

12.3.2.2 Other interfaces

The corresponding specifications must be defined by the manufacturer.

12.3.3 Project development and setting

Manufacturer's specifications and, if required, relevant laws, standards and guidelines need to be considered for project development (e.g. regarding the number and layout of detectors, e.g. smoke detectors, water detectors) and setting.

12.3.4 Connection and function

Detectors for dangerous and emergency situations and technical detectors must be connected only to those inputs of the intruder alarm system which are for these types of detectors specifically or according to manufacturer's specifications for bus-structured IAS.

Detectors for dangerous and emergency situations must generally not interfere with the IAS' Zwangsläufigkeit.

At any rate, the activation of these detectors must not cause intruder and/or hold-up alarms.

12.3.5 Detectors outside the security area

Detectors for dangerous and emergency situations and technical detectors can only be set outside the IAS' security area if attacks on these detectors and their transmission routes do not influence the IAS functions as intended. Moreover, these detectors need to be connected to an independent power supply. The inputs of the control and indicating equipment (group of technical detectors) need to be isolated by a defined, VdS-approved interface (e.g. opto-coupler, isolator). There is no need for this interface if the control and indicating equipment already has such (isolated) inputs.

12.3.6 Power supply

The IAS' power supply may cover only VdS-approved detectors for dangerous and emergency situations as well as VdS-approved technical detectors. They are connected to specially protected outputs of the energy supply in order to prevent a short circuit, for instance, from having adverse effects on the IAS' function. The energy consumption has to be included when determining the bridging time of the IAS' emergency power supply (see chapter 6.9.5).

12.3.7 Installer company responsible

Detectors for dangerous and emergency situations and technical detectors must be set, parameterised and serviced by an installer who is VdS-approved for the respective IAS.

12.3.8 Documentation

Detectors for dangerous and emergency situations and technical detectors must be covered by the maintenance documents and in the installation test as specified in chapters 13.9 and 13.10. The certificate for the IAS, VdS 2170, must include these detectors, e.g. in an annex to the certificate.

In case the detectors are supplied by the IAS' power supply in line with chapter 12.3.7, their consumption must be included in the consumption parameters for clause C.3 of the certificate.

11.3.2.2 Adaptation as perimeter detector

Intruder control and indicating equipment tested and approved pursuant to the latest version of VdS Guidelines VdS 2252 (currently in preparation) may have input interfaces for facilities for open area surveillance in line with VdS Guidelines VdS 3456 ("option with requirements"). If such interfaces are available, they should be used by preference. These interfaces have been optimised with a view to their application and they provide for a simple way of incorporating perimeter detection systems into VdS-approved intruder alarm systems.

11.3.3 Power supply

Perimeter protection systems have to be dedicated to separate electric circuits to which no other consumers should be connected to achieve high availability. The power lines should be installed in a way that hampers any access by unauthorised persons. Separate overcurrent protective devices must be dedicated to individual sectors. If the system features residual current devices (RCDs), separate protective devices must be envisaged for the perimeter detection system's circuits.

In order to ensure there is no reaction on the intruder alarm system, one or several separate power supply unit(s) should generally be envisaged for the perimeter detection systems. The aim should be to ensure continuous power supply of the perimeter detection system for a period to be agreed, e.g. 12 hours by way of rechargeable power points even when the mains power supply fails. Interruptions in power supply must not activate any perimeter alarms, though they should be indicated and transferred as fault messages. In case emergency power supply can only be realised at excessive expense, it may be possible in individual cases and following consultation with the risk carrier to do without emergency power supply for parts of the perimeter detection system. If need be, additional measures may be required to maintain the protection level. These include, for instance, increasing the number of security guards or shorter intervals for the security patrols.

Depending on the system installed and the geographical location, perimeter detection systems and the associated peripheries may be exposed to particular risks posed by overvoltage phenomena (strike of lightning). Therefore, overvoltage protection is of paramount importance. If perimeter detection systems are connected to intruder alarm systems, suitable overcurrent protective devices need to be installed for the interfaces at any rate. Using conjugate interfaces of the intruder alarm system is not sufficient.

Depending on the ambient temperature, some perimeter detection systems require heating for smooth operation. Such heating consumes significant energy which can generally not be provided by the emergency power supply. In case of a voltage loss and battery-operated power supply, it is therefore admissible to shed the heating load. This is not a problem in case of short voltage loss since sufficient residual heat is still available or the loss occurs at a time when heating is not necessary. However, if the temperature drops below a certain level in the course of that, a fault message is generated. In analogy, the same applies to cooling.

11.3.4 Sabotage surveillance

If parts of the perimeter detection system feature sabotage contacts (preferably only parts with sabotage surveillance should be installed), messages generated by these contacts have to be evaluated appropriately and transferred. If the cause for a sabotage alarm cannot be identified, the part in question, after resetting the sabotage alarm (to be done by the installer only), should be checked for proper functioning.

Sabotage surveillance of parts of the perimeter detection system must not be connected to groups of sabotage detectors from the intruder alarm system. If it is connected to the IAS, the sabotage message from the perimeter detection system must be evaluated and transferred as a technical message.

12 Addition by organisational measures and personnel resources

12.1 Basics

Aside from structural, mechanical and electronic measures, the protection concept should be complemented by organisational and personnel measures.

Implementation of organisational measures may require considerable investment. Economic aspects also determine which measures are included in the security concept. Therefore, measures that are not costly yet very useful and effective are particularly interesting.

In view of the large number of possible organisational measures, special attention should be drawn to security management. It may be transferred to several persons. Depending on the scope of protection measures, it might be useful to dedicate a separate organisational unit to security management. Tasks include risk management and responsibility for installation and operation of the relevant security systems and measures.

It is not possible to provide a conclusive list of all possible organisational measures. Some important measures will be outlined below.

12.2 Intervention measures

Security facilities for perimeter protection have to be designed in such a way that intrusions or attempted intrusions are detected and indicated as early as possible. For this purpose, physical safeguards and electronic surveillance need to be coordinated (cf. chapter 5.4).

The aim is for the operator of the system and a certified intervention company in conjunction with a tested and certified alarm receiving and service centre to agree on intervention measures by surveillance facilities. Certification attests that the prerequisites for competent service provision are fulfilled. In response to an alarm, the intervention company should perform a qualified preliminary technical or personnel check. The police shall be informed only in case of reasonable suspicion. All measures must be documented by the alarm receiving centre.

12.3 Lighting

Lighting may have a deterrent effect. However, the effect neither on amateurs nor on professionals should be overestimated (cf. chapter 5.2.2) implying for instance, that automatically-operated lighting systems are only given secondary importance in the context of the security concept. However, aside from the deterrent effect, lighting is of special technical importance for the application of video surveillance systems.

12.4 Guards/Patrols

Different concepts may be applied to surveillance of open areas:

- premises are protected by security guards only,
- premises are protected only by electronic safeguards in line with chapter 8,
- premises are protected by a combination of personnel and technical measures.

The benefits of protection by security guards have to do with man's outstanding capacity for recognising and adequately assessing different risk situations. The high expense for adequately qualified staff may be a disadvantage. Moreover, man's natural limited capacity for concentration and tendency towards distraction must also be considered.

The benefits of electronic measures are their reliability (no fatigue and lapse of concentration compared with human resources) and the costs which are often low. The sensors' one-dimensional detection and the strict interpretation of signals are generally pitfalls.

A combination of personnel and technical measures is able to achieve a high security standard.

13 System documentation and operation

13.1 Design documentation

Proper documentation is an integral part of a perimeter detection system. At least one complete set of all relevant documents should be available at the installation site of the perimeter detection system to the extent that this is deemed useful. Since such documentation generally contains confidential information, it is necessary to ensure that only authorised persons have access to the documentation. The documentation must at least contain the following:

- layout plans that indicate the locations of devices and equipment⁸ relevant for interaction of physical and electronic safeguards,
- layout plans or other illustrations of surveillance sectors and dedication of detection systems to groups of detectors
- plans of groups of detectors
- plans of distribution panels
- plans of installations and cables
- logic diagrams
- manufacturer's manual
- assembly/installation manual
- programming/parameter setting instructions
- documentation of the technical function of interfaces to neighbouring systems (e.g. IAS, HMS)
- documentation of responsibilities and accountabilities for interfaces as well as up-to-date contact details
- operating references of the installer
- operator's documentation (operating manual for the entire system).

It is necessary to ensure that maintenance or repair on the perimeter detection system installed can be performed on the basis of this documentation at any time.

⁸ If possible, the plans should be supplemented by photos.

13.2 Operator's documentation

Every perimeter protection and detection system is individually geared towards the local conditions of the object and the requirements of the risk carrier and the operator as well as the technical conditions. Consequently, instructions by the manufacturer or supplier of the perimeter protection and detection system are generally not adequate to provide the operator with all information relevant for operating and handling of the system. Therefore, the installer of the perimeter protection and detection system should compile customised "operating manuals" for the entire perimeter protection and detection system which is also part of the design documentation (cf. chapter 13.1). One copy must be deposited with the operating manual (cf. chapter 13.7).

13.3 Acceptance and acceptance protocol

Before the perimeter protection and detection system is commissioned, the installer and the client will jointly carry out a documented inspection that consists of a visual inspection and functional test as well as checking availability of all documents required for subsequent hand-over of the system to the operator and commissioning (acceptance).

The inspection includes:

- a visual inspection and functional test of the perimeter protection and detection system installed in every part including the alarm transmission system and intervention
- a check of the operating manual, design documents, in particular the system description and, if necessary, technical documents with performance parameters and limits required for the operation of the perimeter protection and detection system for completeness
- the acceptance protocol with signatures of the parties responsible for acceptance testing.

In the course of construction progress, acceptance of parts of the perimeter protection and detection system is also possible. Following every extension or change, the new function of the perimeter protection and detection system has to be verified immediately by an acceptance test. This test can be confined to the equipment affected and/or influenced by the extension or change and to equipment newly added. Moreover, the design documents, in particular the system description need to be updated.

13.4 Trial operation

Initially, perimeter protection and detection systems have to be operational for a trial phase of at least 8 days (trial operation) without their alarm systems being activated and/or any intervention taking place. The system will be permanently commissioned only if it has worked as intended during the trial operation and if any available not exclusive transmission lines (e.g. radio) achieved the minimum requirements for availability of the transmission route.

Note: The manufacturer supplies suitable tools to measure availability and specifies minimum requirements. If these requirements for the transmission route (e.g. availability $\geq 98\%$ for a specified time) are not met, the system either has to be modified for different transmission routes or it must not be commissioned.

13.5 Handover to operator and commissioning

Following successful acceptance and trial operation as outlined in chapter 13.4, the perimeter protection and detection system is handed over to the operator. When the perimeter protection and detection system is handed over to the operator for commissioning, the installer must brief the operator and responsible person(s) authorised by the operator on the required and intended functions and operation of the system.

Commissioning marks the point in time when the operator starts using the required function of the perimeter protection and detection system.

The events “handover“ and “commissioning“ must be documented in the operating manual. All relevant groups of people have to be notified of the perimeter protection and detection systems being commissioned.

13.6 Maintenance

13.6.1 General

In order to meet the protection goals in line with this Security Manual, the operator is obliged to operate and service the perimeter protection and detection system in line with the manufacturer’s specifications. He has to notify the maintenance service of any defects identified or any other problem and have them repaired.

In agreement with the risk carrier, it is possible to deviate from the intervals specified in chapter 13.6.5, in particular to define shorter intervals or special advanced compensation measures.

13.6.2 Survey

In regular intervals, the perimeter protection and detection system must be properly inspected by a qualified person designated by the operating manual (or several persons) with a view to abnormalities. The aim of such surveys is a timely identification of adverse influence that jeopardises the detection quality and false alarm resistance of the perimeter detection system or reliable function of the perimeter protection and detection system. Special attention must be drawn to:

- (imminent) influence by vegetation and trees as well as roots,
- impurities and damage,
- sub-standard assembly of system components,
- excessive depletion of stocks of spare parts for components subject to mechanical loads,
- sabotage attempts,
- system compliance with the goals defined in the security concept, in particular review of any change in occupancy or structural modifications
- completeness and accuracy of operating manual.

The installer has to enable the operator to carry out a proper survey and specify a reasonable interval for such inspections.

13.6.3 Inspection

Perimeter protection and detection systems should be inspected at least four times a year in regular intervals. The following aspects should be inspected for proper function:

- transmission routes,
- at least one detector for every transmission route, however, only detectors that can be subjected to non-destructive testing,
- warning devices,
- indicating and control equipment
- ancillary control equipment
- power supply(ies)
- actuators in conjunction with alarm transmission, control units and alarm devices,
- read-out the event recorder and check for special events.

In addition, the following should be checked:

- possible limitations or imminent medium-term limitations to detection reliability or fail-safety caused by vegetation, roots or other environmental influences,
- all system components for assembly as intended

- all system components for external mechanical damage and soiling
- surveillance range of detectors by way of suitable measures to determine any deviation from the surveillance range documented in the installation certificate,
- the entire system for disturbing influence (e.g. resulting from a change in occupancy or structural modifications) that is not evaluated as part of standard operating procedure,
- fault message transmission to a contracted receiving unit.

13.6.4 Maintenance

The perimeter protection and detection system must be maintained at least once a year, if necessary in combination with an inspection as described in chapter 13.6.3. In addition to the points described in chapter 13.6.3, the following operations must be carried out:

- battery test if the system uses a power supply with emergency power generation. Unless otherwise specified in the approval certificate, the battery(ies) must be exchanged four years after its/their manufacturing date at the latest.

Note: When batteries are exchanged, they should be marked with the date when they are fitted. In addition, this date should also be documented in the operating manual.

- functional check of all detectors that can be subjected to non-destructive testing and all transmission routes of detectors that cannot be checked this way,
- functional check of all contacts subject to wear and tear,
- trimming and adjustment of system components
- functional check of the clearance of movable mechanical components,
- maintenance operations in line with manufacturer's documentation
- checking documentation for completeness and accuracy.

13.6.5 Repair

All defects (e.g. faults, defective or system components which are no longer properly assembled) found during the inspection or maintenance must be repaired immediately.

The installer's maintenance service should be accessible at any time and should respond to the operator within two hours of the latter's call. Problems should be solved in 24 hours provided the perimeter protection and detection system is regularly maintained by the installer (this does not apply to major destruction by vandalism or natural phenomena such as e.g. strike of lightning or snow storm). For this purpose, the installer has to provide for sufficient stocks of spare parts and maintenance tools. If need be, these prerequisites need to be checked and documented in advance.

13.7 Operating manual

The regular maintenance operations (e.g. replacing detectors, time of battery exchange), changes, expansion, remote alarm (with current status of alarm recorder), tamper and fault signals must be documented in an operating manual in line with the template given in VdS 3144 which must be updated regularly.

The operating manual must be handed over and transferred to the operator. The latter must be informed that he has to keep the operating manual and have it at hand and that he and/or the installer/maintenance company has to document all operating events (e.g. alarms, fault alarm signals) including details on their causes as well as all maintenance activities and modifications required. The operator is obliged to keep the operating manual for at least 5 years (which also applies to operating manuals that have been completed/replaced).

Operating events that do not require any details on their causes or origins may be automatically documented in an internal event recording system.

14 Examples of security concepts

14.1 General

When developing a concept for perimeter protection and detection systems, physical safeguards should be specified before electronic measures are defined.

This makes sense for several reasons:

- physical safeguards discourage intruders' determination,
- a sufficiently high mechanical quality of the barrier is the basis for electronic detection in sector 1 (no audio cable at the wooden lattice fence),
- reducing the number of unwanted alarms, e.g. through a fence: electronic detection behind the fence enhances the significance of alarms,
- electronic safeguards are not able to prevent any loss, they merely indicate a loss,
- all messages from electronic security systems have to be transmitted to a control unit manned 24/7 (e.g. connection to an alarm receiving and service centre),
- if alarm verification on the basis of video images is possible, these images should be transmitted to a control unit manned 24/7.

An intervention, for instance, could be carried out as a subsequent organisational measure.

All measures in this context have to be seen regardless of necessary electronic surveillance of buildings by intruder alarm systems pursuant to Guidelines VdS 2311. **Perimeter protection and detection systems may complement intruder alarm systems, however, they do not replace them.**

The operator has to weigh and plan the entire perimeter security system taking into account the assets to be protected and the loss to be expected relative to the investment to be made.

14.2 Key for the examples

The overview presented in chapter 14.3 should be read as follows:

Type of risk	Describes the risk
Classification of the protection level	Assumed classification of the protection level
Risk analysis	Possible threats identified in the context of the risk analysis
Analysis of perpetrator profile	Profile of perpetrators expected against which protection is required
Protection goal	Define threats against which protective measures are to be taken

Protective measures	Structural-physical	Electronic	Organisational
Sector 0			
Sector 1			
Sector 2			
Sector 3			

The measures are designated to the relevant sector⁹ and divided into categories structural-physical, electronic and organisational.

⁹ Cf. chapter 6.1

14.3 Examples of security concepts

14.3.1 Car park supermarket

Description:

A standard fence prevents spontaneous intrusion effectively; additional measures are not required to achieve the protection goal.

Type of risk	Car park supermarket
Classification of the protection level	basic
Risk analysis	Vandalism
Analysis of perpetrator profile	Single perpetrator, casual perpetrator
Protection goal	Prevent unauthorised access, spontaneous vandalism

Protective measures	Structural-physical	Electronic	Organisational
Sector 0	---	---	---
Sector 1	Fence, wall, gate, height 1.2 m	---	---
Sector 2	---	---	---
Sector 3	---	---	---

14.3.2 Community facility, e.g. outdoor swimming pool

Description:

Spontaneous intrusion is prevented. Although a low protection level is assumed, a fence of 2.0 m height must nevertheless be installed pursuant to accident prevention regulations, which is also conducive to other protection goals.

Type of risk	Community facility, e.g. outdoor swimming pool
Classification of the protection level	basic
Risk analysis	Vandalism, theft
Analysis of perpetrator profile	Single perpetrator, casual perpetrator
Protection goal	Prevent unauthorised access, vandalism, damage to building/object

Protective measures	Structural-physical	Electronic	Organisational
Sector 0	---	---	---
Sector 1	Fence, wall, gate, height 2.0 m	---	---
Sector 2	---	---	---
Sector 3	---	---	---

14.3.3 Open depots

Description:

Due to the great appeal of the goods stored, a fence of 4.0 m height is envisaged deviating from the recommendations of table 7-1. This structural-physical measure in sector 1 prevents intrusion in the perimeter area effectively. Premium/profitable goods are protected by an additional barrier, i.e. wire mesh crates. In combination with electronic surveillance, this can buy time for intervention measures. Video technology available can be used for alarm verification.

Type of risk	Open depot
Classification of protection level	increased
Risk analysis	Theft, arson, vandalism
Analysis of perpetrator profile	Groups of perpetrators, organised crime
Protection goal	Prevent theft, unauthorised access, vandalism

Protective measures	Structural-physical	Electronic	Organisational
Sector 0	---	---	---
Sector 1	Fence, wall, gate, height \geq 4.0 m	---	---
Sector 2	Wire mesh create as additional physical barrier for premium/profitable goods (also empties)	Focal point as well as surface surveillance, e.g. motion detectors	Use video technology available for verification
Sector 3	---	---	---

14.3.4 Tiling/galvanising shop

Description:

Structural-physical measures in sector 1 prevent intrusion into the perimeter area effectively. Premium/profitable goods are protected by an additional barrier, i.e. wire mesh crates. In combination with electronic surveillance, this can buy time for intervention measures. As an alternative to the measures in sector 1, surveillance of focal points and as traps, e.g. installing motion detectors may be realised in sector 2. Video technology can be used for alarm verification.

Type of risk	Tiling/galvanising shop
Classification of protection level	increased
Risk analysis	Theft, arson, vandalism
Analysis of perpetrator profile	Groups of perpetrators, organised crime
Protection goal	Prevent theft, unauthorised access, vandalism, damage to building/object

Protective measures	Structural-physical	Electronic	Organisational
Sector 0	---	---	---
Sector 1	Fence, wall, gate, height \geq 2.0 m	Fence protection or volumetric-/linear surveillance or Video sensor technology with recording	---
Sector 2	Wire mesh create as additional physical barrier for premium/profitable goods	Alternatively: Focal point as well as surface surveillance, e.g. motion detectors	Use video technology available for verification
Sector 3	---	---	---

14.3.5 Photovoltaic park

Description:

The fence prevents spontaneous intrusion and vandalism effectively. Conditions obstructing access roads or transport routes already provide protection against theft of the solar panels in sector 0. The panels are also protected by physical safeguards and additionally monitored for removal. As an alternative to fence protection, volumetric / linear surveillance, video sensor technology or a floor detection system with pressure change sensors may be applied for detection of theft or sabotage in sector 2.

Type of risk	Photovoltaic park
Classification of protection level	high
Risk analysis	Theft, sabotage, vandalism
Analysis of perpetrator profile	Single perpetrators or groups of perpetrators, casual perpetrators and organised crime
Protection goal	Prevent theft of solar panels and unauthorised access, vandalism and sabotage

Protective measures	Structural-physical	Electronic	Organisational
Sector 0	Install barriers on access road (boulders etc.)	---	---
Sector 1	Fence, wall gate, height \geq 2.4 m	Gate and fence protection	---
Sector 2	---	As alternative to fence protection, volumetric / linear surveillance or video sensor technology or floor detection systems with pressure change sensors	Use video technology for verification
Sector 3	Physical safeguards against removal	Object surveillance of solar panels	---

14.3.6 Car dealer with open area (presentation area with public access)

Description:

The example only covers the presentation area of the car dealership accessible to the public. Fenced areas and the like as well as the business premises proper do not meet Zwangsläufigkeit. Due to the fact that customers should be able to see the cars at any time (including after business hours), physical barriers to hamper car theft are recommended. Electronic measures ensure early detection of removal of entire vehicles or theft of parts. If agreed, the messages from the video sensor technology and/or other detection measures in sector 2 monitoring the vehicle area can be connected to an alarm receiving and service centre. Immediate verification on the basis of images transmitted makes it possible to decide quickly whether to intervene or not.

Type of risk	Car dealer with open area (presentation area with public access)
Classification of protection level	high
Risk analysis	Theft (also theft of parts), vandalism
Analysis of perpetrator profile	Single perpetrators or groups of perpetrators, casual perpetrators and organised crime
Protection goal	Prevent theft and vandalism

Protective measures	Structural-physical	Electronic	Organisational
Sector 0	Boulders, ditches	---	---
Sector 1	Bollards	---	---
Sector 2	---	Linear surveillance or Video sensor technology for detection and video surveillance and image transmission	Use video technology for verification
Sector 3	---	---	---

14.3.7 Bank foyer with self-service terminals temporarily closed at night

Description:

If the foyer should also be accessible beyond business hours, surveillance with a classical IAS is generally not an option since correct setting/unsetting while complying with "Zwangsläufigkeit" is not possible. If low frequency can be expected during a certain time frame and access to the foyer beyond business hours cannot be avoided, the foyer could be monitored, if need be, by perimeter detection. As part of a consistent security concept, motion detectors can be installed to monitor the foyer or magnetic contacts and the like to monitor the door; a video surveillance system is installed and messages and images are transferred to an alarm receiving and service centre. A message generated during a specified time frame (e.g. between 0.00 a.m. and 5.00 a.m.) may, for instance, automatically transfer the video image or sequence to the alarm receiving and service centre and has to be verified by a member of staff. The video images will make it possible to easily ascertain whether a "genuine customer" is inside the bank or whether an ATM is being attacked. The technical evaluation and transmission of the messages can be handled by the IAS. In case the detectors are adapted as perimeter detectors, the certificate of the VdS-approved IAS will remain valid (regulations are currently planned). An interface in line with VdS Guidelines VdS 2465-S3 makes it possible to realise a smart link between IAS and VSS.

Type of risk	Bank foyer with self-service terminals temporarily closed at night
Classification of protection level	high
Risk analysis	Attacks on ATM, theft, vandalism, arson
Analysis of perpetrator profile	Single perpetrators or groups of perpetrators, casual perpetrators and organised crime
Protection goal	Prevent theft, unauthorised access, vandalism, damage to building/object

Protective measures	Structural-physical	Electronic	Organisational
Sector 0	--	--	--
Sector 1	Blocking device for the door, with time control	Monitor opening of door, e.g. by magnetic contact	--
Sector 2	--	Focal point surveillance, e.g. motion detectors and/or video analysis	Video technology for verification absolutely necessary
Sector 3	Temporary cover of object, e.g. with shutters	Monitoring of opening and closing of covers/shutters	

Annex A – Impact loads as safety standards for road blocks (informative)

A.1 General

In the past, road blocks were predominantly installed at embassies, nuclear power plants, government buildings or military sites. However, in the course of time, they have become interesting also for IT centres, big wholesale stores, industrial facilities, car dealerships as well as banks and insurances, to name but a few.

In addition to structural calculations used as a basis for testing and certification of these products, the results of tests with practical relevance (impact test with vehicles) are also included. The impact loads for the products described in chapter 7.2.6.4 are based on requirements stipulated by US (Department of State, DOS) or British standards.

A.2 Requirements in line with DOS, US specification

The ASTM (American Society for Testing and Materials) divides requirements into three different classes. The classification is based on a certain combination of a defined impact load (6.8 t) at different impact velocities. In order to pass the test, the vehicles are allowed to fly beyond the barrier at the most 1 m onto the premises to be protected.

ASTM M30: 6.8 t at approx. 50 km/h (30 mph) = 700 kJ (just about equivalent to K4*)

ASTM M40: 6.8 t at approx. 65 km/h (40 mph) = 1,108 kJ (just about equivalent to K8*)

ASTM M50: 6.8 t at approx. 80 km/h (50 mph) = 1,700 kJ (just about equivalent to K12*)

*) pursuant to British PAS 68 and 69

A.3 Requirements in line with PAS 68 and 69, British specification

The Publically Available Specifications (PAS) 68 and 69 also divide the products into three classes: K4, K8 and K12. Compared with the US requirements, the British specification is based on an impact load of 7.5 t. Impact velocities are identical. The distance the vehicle travels after the impact is the yardstick for the barrier's effectiveness. This distance must not exceed 5 m.

K 4: 7.5 t at approx. 50 km/h (30 mph) = 910 kJ

K 8: 7.5 t at approx. 65 km/h (40 mph) = 1,220 kJ

K12: 7.5 t at approx. 80 km/h (50 mph) = 1,850 kJ

Annex B – Further references (informative)

VdS 3134-3	Technical commentaries – Part 3: Glazing
DIN 18300	German construction contract procedures (VOB) – Part C: General technical specifications in construction contracts (ATV) – Earthworks
DIN EN 12433-1	Industrial, commercial and garage doors and gates – Terminology – Part 1: Types of doors;
DIN EN 12433-2	Industrial, commercial and garage doors and gates – Terminology – Part 2: Parts of doors
DIN EN 12453	Industrial, commercial and garage doors and gates – Safety in use of power operated doors – Requirements
DIN EN 12978	Industrial, commercial and garage doors and gates – Safety devices for power operated doors and gates – Requirements and test methods
DIN EN 12635	Industrial, commercial and garage doors and gates – Installation and use
DIN EN 12424	Industrial, commercial and garage doors and gates – Resistance to wind load – Classification
DIN EN 12428	Industrial, commercial and garage doors and gates – Thermal transmittance – Requirements for calculation
DIN EN 12444	Industrial, commercial and garage doors and gates – Resistance to wind load – Testing and calculation
DIN EN 12425	Industrial, commercial and garage doors and gates – Resistance to water penetration – Classification
DIN EN 12489	Industrial, commercial and garage doors and gates – Resistance to water penetration – Test methods
DIN EN 12426	Industrial, commercial and garage doors and gates – Air permeability – Classification
DIN EN 12427	Industrial, commercial and garage doors and gates – Air permeability – Test method
DIN EN 13241-1	Industrial, commercial and garage doors and gates – Product standard – Part 1: Products without fire resistance or smoke control characteristics
DIN EN 60335-1	Household and similar electrical appliances – Safety – Part 1: General requirements
DIN EN 60335-2-95	Household and similar electrical appliances – Safety – Part 2-95: Particular requirements for drives for vertically moving garage doors for residential use
DIN EN 10223-1	Steel wire and wire products for fencing and netting – Part 1: Zinc and zinc-alloy coated steel barbed wire
DIN EN 10223-2	Steel wire and wire products for fencing and netting – Part 2: Hexagonal steel wire netting for agricultural, insulation and fencing purposes
DIN EN 10223-3	Steel wire and wire products for fences – Part 3: Hexagonal steel wire netting for engineering purposes
DIN EN 10223-4	Steel wire and wire products for fencing and netting – Part 4: Steel wire welded mesh fencing

- | | |
|----------------|--|
| DIN EN 10223-5 | Steel wire and wire products for fencing and netting –
Part 5: Steel wire woven hinged joint and knotted mesh fencing |
| DIN EN 10223-6 | Steel wire and wire products for fencing and netting –
Part 6: Steel wire chain link fencing |
| DIN EN 10223-7 | Steel wire and wire products for fencing and netting –
Part 7: Steel wire welded panels for fencing |

Annex C – Dispensation with projections on metal fences up to < 1.80 m height of wire mesh cover – Recommendations for safe fencing in the sense of personal protection (informative)

**FACHVERBAND METALLZAUNTECHNIK E .V.
GÜTEGEMEINSCHAFT METALLZAUNTECHNIK E .V.**

IM FACHVERBAND INDUSTRIE VERSCHIEDENER EISEN- UND STAHLWAREN E.V.
AN DER PÖNT 48-40885 RATINGEN-FON 02102/186200- FAX 02102/186169 - E-MAIL: info@guetezaun.de

MZT Recommendation

Dispensation with projections on metal fences up to < 1.80 m height of wire mesh cover – Recommendations for safe fencing in the sense of personal protection

Based on the **recommendation** of 9 September 2010 by the working group "Technik und Normung" (Engineering and standardisation) of RAL Gütegemeinschaft MZT e.V. whose passive members include representatives of fence companies and in particular manufacturers and distributors of metal fences and their components **the following regulation shall be the norm as of 2011.**

Metal fences, in particular fencing from bar grating panels shall **not have any projections up to 1.8 m height of wire mesh cover.** What this means for manufacturers / distributors in practical terms:

- **All fast-selling types of metal fences up to 1.6 m height of wire mesh cover will have no projections as standard issue. Any deliveries up to this standard height delivered with projections will then be customised.**
- **Fences up to ≥ 1.80 m height of wire mesh cover can still be produced and delivered (as a rule).**

Background to this recommendation:

1. On the one hand, fencing is often installed on property boundaries that separate areas frequented by the public (e.g. pavements, driveways) from private property. On the other hand, **people of average height in Germany** (status: 2009) who frequent these public and/or private areas tend to be **175-180 cm (male) respectively 165-170 cm (female) tall.** With the request of fence makers to dispense with projections on fences up to < 1.80 m height as a rule, the metal fencing industry makes a voluntary contribution towards eliminating a possibly latent injury potential for people in connection with metal fences.
2. For reasons of **personal protection, in particular of children and adolescents,** manufacturers and distributors voluntarily dispense with deliveries of metal fences with so-called **projections** in general. As reported by representatives (supervisors) from municipal accident insurance associations or regional accident insurers in the past, **children, adolescents and sometimes adults, too, have suffered injuries time and again in sport and leisure facilities as well as day care centres, schools and playgrounds close to fences (e.g. when attempting to climb up or over fences).**
3. The relevant accident prevention regulations for the above establishments (at the same time also work places) therefore do not allow "fencing of any type with possible pointy or sharp edges". This **latent potential for injuries certainly also prevails in private, commercial-industrial and other public areas.**

The fence industry is taking this measure to support sponsors and/or companies that maintain such fenced areas in meeting their duty to implement safety precautions. Accordingly, fencing has to be safe enough to avoid any risks, if possible, and consider and comply with relevant safety regulations. In principle, this also

applies to owners, proprietors and operators of residential and non-residential buildings, properties and commercial as well as transport facilities.

Of course, customers may also buy and install metal fencing with projections in future. However, the **two objectives – protection of persons on the one hand and of the object on the other – need to be weighed carefully** to arrive at a definite decision. This task can be solved reasonably with a risk assessment on site, for instance, in agreement between the fence builder/manufacturer and the designer/architect/owner. In any case, fence builders and manufacturers are always prepared to contribute their consulting expertise providing support and contributing to a solution.

In the spirit of enhanced safety, many manufacturers and distributors of metal fences will hopefully use this recommendation as guidance for their conduct.

Ratingen, October 2010

Translation of the by courtesy of the Fachverband Metallzauntechnik e.V., Ratingen, printed information.

Annex D – Protection and security for areas frequented by the public by fencing and gates – Leaflet for practical implementation (informative)

FACHVERBAND METALLZAUNTECHNIK E .V.
GÜTEGEMEINSCHAFT METALLZAUNTECHNIK E .V.

IM FACHVERBAND INDUSTRIE VERSCHIEDENER EISEN- UND STAHLWAREN E.V.
AN DER PÖNT 48-40885 RATINGEN-FON 02102/186200- FAX 02102/186169 -E-MAIL: infof@guetezaun.de

Protection and security for areas frequented by the public by fencing and gates – Leaflet for practical implementation

What public, corporate and private sponsors of schools, day care centres, sports facilities, playgrounds and leisure centres, parks and zoos etc. need to focus on!

Introduction

Kids' day care centres, schools of all kinds, playgrounds as well as sport and leisure centres for children, adolescents and adults often have fencing or other enclosures and corresponding access facilities (e.g. doors and/or gates, turnstiles, barriers and blockades). Their purpose is to protect these establishments and their users from unauthorised or "uninvited guests" (e.g. animals) on the one hand and to shield adjacent areas (e.g. traffic routes) from sport equipment and toys and prevent children and adolescents from care-less departure on the other. However, these facilities must be safe (design). Time and again, there have been reports about accidents involving children and other groups of people that can be attributed to shortcomings and/or non-compliance with safety rules for fence(s) and their access. They clearly show that sponsors and operators do not necessarily meet their obligation to maintain safety in this context. The following recommendations and hints are the result of practical experience on a day-to-day basis as well as standards and regulations with a legal background.

Recommendations and hints

A. Planning and selection of fences and gates

- (1) When planning schoolyards, playgrounds, sport and leisure facilities, day care centres and similar establishments, sponsors/operators should consult "experts on industrial health and safety" on the one hand and experienced construction engineers and contractors on the other. Regarding enclosures of metal fences and metal door(s) and/or gate(s), RAL quality-approved fence companies in line with the quality and test requirements of **RAL GZ 602 "Metallzauntechnik" (issue 2007-07)** should be consulted.
- (2) The most important premise should be to apply suitable, that is, permanently safe metal fences and doors/gates/barriers only, in particular as early as the design phase. Fences and gates/barriers installed in line with RAL GZ 602 guarantee this claim through additional compliance with health and safety regulations and/or standards for doors/gates (e.g. fences with double bar grating or flat bar grating, wire mesh fences, revolving doors and/or gates).
- (3) A prior risk assessment is recommended for leisure and sport centres and public playgrounds for which there are no explicit and specific legal or other rules or regulations.

B. Installation and operation

- (4) In general, it is necessary to make sure that fences and other enclosures do not have any protruding tips or sharp edges or projecting parts.
[Source: Health and safety regulations for schools and day care centres]
- (5) It is necessary to make sure that manually or power-operated doors or gates of fences or barriers do not pose any risk of crushing, shearing, being pulled in or hit

by them due to their design. This can be achieved, for instance, by sufficient safety margins between the gate panels (e.g. between post and wings of a gate) or between a wing and the wall of a building, by keeping sufficient safety distance between a horizontal and/or vertical handle and the door's/gate's frame or sufficient clearance between the wing of a sliding door and the enclosure (in this case it depends on the wire mesh size). The main and dependent closing edge(s) of power-operated doors need to be secured and the operating force of the moving wing of the gate must be limited in line with relevant standards; in addition, detection of persons must be available (e.g. by way of a light detector) in case the door is equipped with a pulse-operated or automatic control. Incidentally, doors and gates of fences must be lockable (*GUV-V S2 2009-04*)

[Source: *Industrial, commercial and garage doors and gates - Mechanical aspects (DIN EN 12604:2000-11) and Safety in use of power operated doors (DIN EN 12453:2001 -06)*]

- (6) Pursuant to the accident prevention regulations for schools (*GUV-V S1, chapters 11 and 14*), it is necessary to ensure that enclosures (e.g. metal fences) – without height restrictions – on schoolyards and/or common areas near school properties do not have any pointy, sharp-edged or protruding parts.
- (7) Pursuant to the accident prevention regulations for children's day care centres (*GUV-V S2*), structural components like fences or other enclosures must not have any pointy, protruding or sharp parts. This prohibition applies without any height restrictions like for schools. Fences should have a minimum height of 1.0 m, better yet 1.5 m; their design should make it difficult or impossible to climb on them.
- (8) Installation of barbed wire or pointy fences (e.g. wooden lattice fences) is generally not allowed (explicitly stipulated by *GUV-V S1, § 11* resp. *GUV-V S2*). If random inspections of e.g. bar grating panels find any projections, immediate action is recommended: a fencing company should turn the fence panels with the pointy projections to the floor (ideally not leaving any or very little clearance); in the medium-term, the fence panels should be replaced by fencing with smooth top and bottom edges.
- (9) In case of particular hazards (e.g. highly frequented roads, adjoining water) in the immediate vicinity of the children's day care centres, it may be necessary to enlarge the fencing.
- (10) Since there are no specific legal provisions and regulations for establishments similar to schools and children's day care centres, e.g. leisure and sports centres, public playgrounds and football grounds, compliance in analogy with the above safety regulations for schools is highly recommended (risk assessment) and consequently select appropriate fencing and access.
- (11) Equally important: Neighbouring properties to playing and leisure facilities (e.g. playgrounds and football grounds) used for private, commercial or public purposes should also have safe fencing to the same effect in order not to have any unwanted yet possible accidents with persons playing (Example: Ball falls onto to the enclosed property next to the playground). In this case, the owner of the neighbouring property is obliged to maintain safety which also needs to be considered.

C Maintenance and inspection

- (12) As a result of improper use or other events (e.g. wear and tear), fencing and access gates to outdoor facilities (gates, doors, turnstiles) that were originally safe and designed in compliance with standards may be damaged or show functional defects that can easily lead to loss or personal injuries. Therefore, sponsors or operators need to ensure regular inspections of the outdoor facilities and fencing of schools, children's day care centres etc. by competent inspectors, e.g. on the basis of a maintenance and inspection plan.

- (13) On the basis of regular inspections (e.g. using the operating or maintenance manual of the manufacturer or fence builder as a reference, at least once every year in analogy with the Manual for workplaces ASR A1.7 2009-12), obvious deficiencies and damage in the sense of the health and safety regulations can be detected and repaired in a timely manner. Deficiencies include e.g. protruding tips of wire mesh fences, projections on bar grating fences to prevent intruders from climbing over fences (!), exceeding the operating force of power-operated doors and gates, failure of physical and/or electric safety precautions on gates/doors.
- (14) Manually operated doors and gates in fences need to be checked regularly by visual inspection in order to eliminate any risks (of crushing) or deficiencies coming up in the meantime (to be derived from § 3, Para. 1 of the relevant regional building code). Power-operated doors and gates are subject to an annual inspection/service in line with ASRA1.7 on doors and gates to be carried out only by an expert inspector commissioned by e.g. the operator of a day care centre and to be documented in a service manual providing the service protocol.
- (15) In principle, only qualified persons – in particular on the part of the sponsor/operator – should be contracted for the regular inspections and possible repair/trouble-shooting jobs of such facilities. RAL-tested fence construction companies that meet the requirements of RAL-GZ 602 and produce evidence thereof through periodic tests are particularly qualified to carry out such jobs by order of the sponsor or at least advise the latter on how to prepare for this important task. Technicians qualified for inspections of power-operated doors and gates are regularly trained through further training measures organised by the Gütergemeinschaft Metallzauntechnik e.V. in cooperation with the BVT - Verband Tore, Ratingen.
- (16) A list of members of the quality assurance association on a nationwide basis can be obtained at www.guetezaun.de. You may also request direct assistance from the association's secretariat at the above address. Your contact is Dipl.-Ökonom Friedrich Klopotek, Managing Director, Phone 02102/136-210 or Mail: klopotek@quelezaun.de.

Ratingen, 2010-01-22

Translation of the by courtesy of the Fachverband Metallzauntechnik e.V., Ratingen, printed information.

