Intruder Alarm Systems

General requirements and test methods

Publisher and publishing house: VdS Schadenverhütung GmbH

Amsterdamer Str. 172-174
50735 Köln, Germany
Phone: +49 221 77 66 0; Fax: +49 221 77 66 341

Rules for Intruder Alarm Systems

Intruder Alarm Systems

General requirements and test methods

CONTENT

1 General

1.1 Scope

These rules contain the minimum requirements for the functions of intruder alarm systems (IAS), a collection of terms and definitions, the performances for the classification of IAS, general requirements for system components and the relevant test methods. Separate rules are available covering the special requirements for individual system components, the relevant test methods and planning and installation of these systems (see annex A). Annex B of this English version of the rules contains a comparision of the English and German terms.

Note: The establishment of rules for pear-to-pear systems and/or master systems are in preparation.

Figure 1.01 illustrates the functions of an IAS, while figure 1.02 shows the key components.

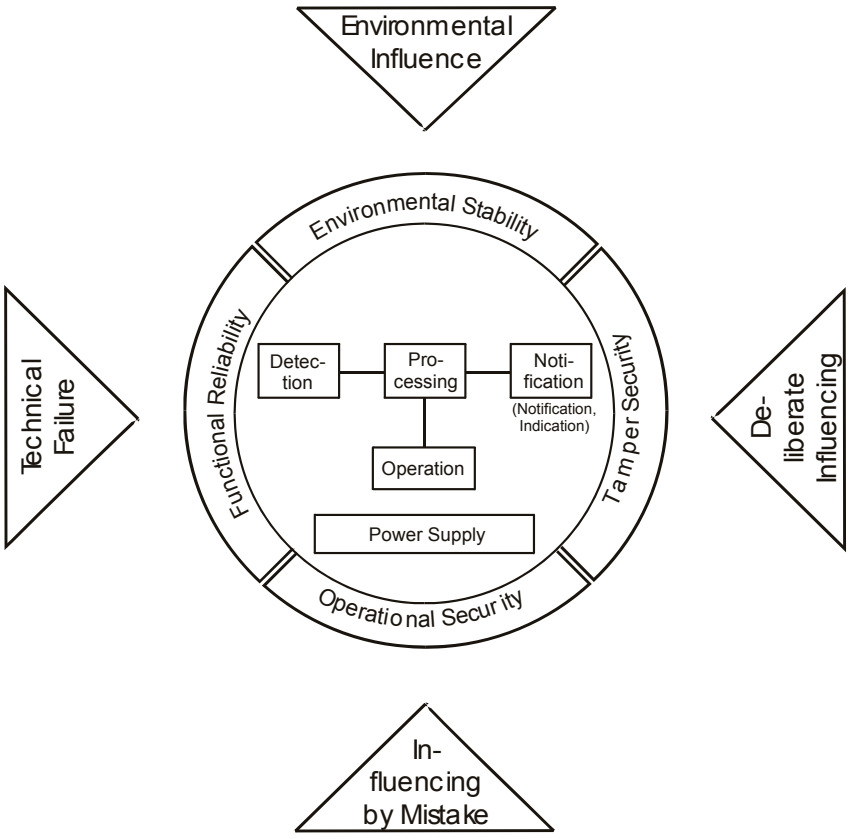

Figure 1.01: Function of an IAS

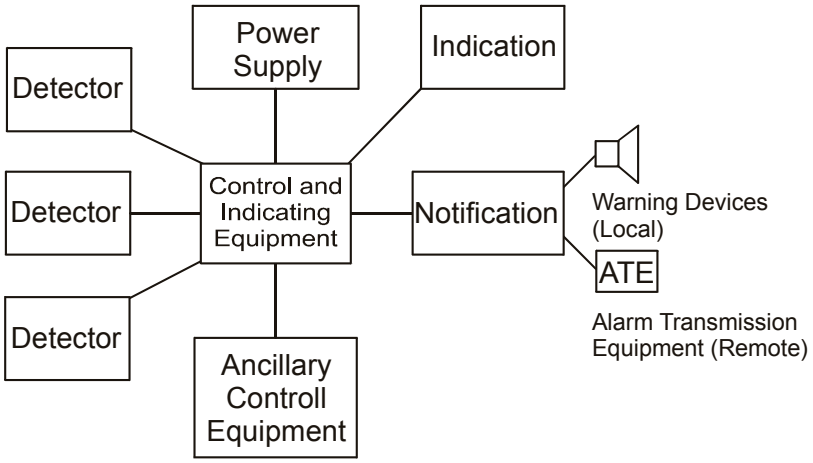

Figure 1.02: Elements of an IAS

1.2 Validity

These rules apply from 1. March 2016; they replace version VdS 2227en : 2002-05 (03).

Note: This is a translation of the German rules; if there are any discrepancies, the German version shall be binding.

2 Normative references

These rules contain dated and undated references to other publications. The normative references are cited at the appropriate places in the clauses, the publications are listed hereafter. For dated references, subsequent amendments to or revisions of any of these publications apply to these rules only when announced by a change of these rules. For undated references the latest edition of the publication referred will be applied.

- **DIN EN 50 131-1** Alarm Systems – Intruder alarm systems – Part 1: General requirements
- **DIN EN 60 065 / VDE 0860** Audio, video and similar electronic apparatus – safety requirements
- **DIN EN 60 950 / VDE 0805** Safety for information technology equipment
- **DIN IEC 721-3-3 : 1990-04** Classification of environmental conditions. Classification of groups of environmental parameters and their severities. Stationary use at weatherprotected locations
- **DIN VDE 0100** execution of power installations with rated voltages below 1000 V
- **DIN VDE 0800** Telecommunications; General concepts; requirements and tests for the safety of facilities and apparatus
- **DIN VDE 0833-1 : 1989** Alarm systems for fire, intrusion and hold-up, General requirements
- **DIN VDE 0833-3** Alarm systems for fire, intrusion and hold-up, requirements for intrusion and hold-up alarm systems
- **VdS 2110** Rules for alarm systems, protection against environmental influences, requirements and test methods

3 Terms and abbreviations

3.1 Terms and definitions

Access control system (ACS): System which automatically controls access authorizations, controls entry blocking units and logs events, including those which take place for building-related or organisational reasons.

Access control system concept (ACSC): All the system components which are tuned to function together as a whole (e.g. access control, control and indicating equipment, information media, input device for the information media and the blocking device).

Accessible stocks of bank notes: Under the terms of the German “UVV Kassen“ (Accident Prevention Regulations for Banks), stocks or bank notes are deemed to be accessible if they can be accessed without any particular difficulty. Storing the bank notes in containers with a time lock or double lock would constitute particular difficulty, for example.

Access level (AL): Group of certain components or functions of an IAS which are only accessible to certain persons.

Access protection: Protection against unauthorised access to functions, operating elements, data.

Accreditation: Formal approval of the competence e.g. of a testing laboratory, of a certification body.

Activation of a dyeing system: Function within a dyeing system, in which triggering of the system causes release of the contained colour for dyeing the objects to be protected (cash). The triggering of a dyeing system is not possible in a deactivated state.

Activation (setting of a smoke generating device): Is possible only with a smoke generating device being in operation and is made automatically with an external setting of the IAS; in case of an alarm the triggering of the smoke generating device may then be initiated by the IAS.

Adaptation of bits (German term “Bitratenadaption”): The ISDN network transmits data with a speed of 64 Kbit per second. Terminals or normal data networks are working in most of the cases with a much lower velocity rates (e.g. 9600 Bit/s). Therefore procedures had to be defined to fill “the bits left” in the 64 kbit-data streem. For asynchronous transmission (with start and stop-bit per byte) an adaptation according to V110 is applicable. As such a transmission path does not allow the transfer in the analogue network it is of more sense to use the available bandwidth for transmission of modem compatible acoustic signals.

Alarm: Signal that a status has occurred in an alarm system which requires the initiation of risk-preventive measures (intervention).

Alarm detector: Detector of an alarm system designed to detect fires, hold-ups or intruder/intruder attempts.

Alarm glass: Glass with integrated monitoring measures.

Alarm loop: Circuit which results in an alarm signal if an interruption or a defined change in resistance occurs.

Alarm plan: Plan containing the measures to be initiated for incoming alarms signals.

Alarm receiving and service centre (German term „Notruf- und Service-Leitstelle – NSL“): Physical secured, permanently manned area of a security company where Alarm receiving equipment (ARE) for alarm signals/messages are operated and from where interventions are initiated, controlled and documented.

Alarm receiving centre (ARC): Remote location which is constantly manned and to which information on the status of one or more alarm systems can be transmitted (e.g. police or security company) and which the appropriate risk-averting measures (intervention) initiated.

Alarm receiving equipment (ARE): Receiving equipment in alarm transmission systems which receives, acknowledges, processes and indicates signals/messages from alarm systems and transmits control signals to the Alarm transmission equipment (ATE). Alarm receiving equipment (ARE) consist at least of a Receiving centre transceiver (RCT) and an Annunciation equipment (AE).

Alarm room: Physical protected and 24 hours manned area of an alarm receiving centre, where alarm receiving equipment for alarm signals (ARE) are in operation.

*Remark: Term is out of date, see „**Alarm receiving and service** centre (German: NSL)“.*

Alarm signal: Signal given to indicate danger, e.g. an intrusion.

Alarm signalling equipment: Equipment which is used to summon aid with a view to averting danger or warning persons. It can be part of or supplementary to an alarm system (AS).

Alarm system (AS): System which automatically or non-automatically triggers an alarm in response to danger (e.g. intruder alarm system, fire detection system).

Alarm transmission: Transmission of a signal/message from interface S_2 to interface S_3, performed when the alarm transmission system is fully operational.

Note: The acknowledgement of receipt of a signal/message at the application level (OSI level 7) does not form part of the transmission of a signal/message.

Alarm transmission equipment for alarm signals (ATE): ATE pick up signals from alarm systems, prepare them for transmission via transmission paths and serve as an interface to these transmission paths. They also prepare the control commands issued in the alarm receiving equipment (ARE) and pass them on to the connected alarm system.

Note: Formerly known as: Transmission facility, Telephone dialling device, auto dialler

Alarm transmission system (ATS): Equipment and networks transferring information on the status of one or more alarm systems to one or more alarm receiving centres (ARC).

Alarm wire insert: Wire inserted into glass which results in an alarm signal being generated if the glass is broken.

Alternative path: Transmission path used for the transmission of signal/messages when the primary transmission path is not available, for example because of faults or tampering.

Alternative power source: Battery which is capable of supplying an alarm system (AS) with power for a certain period of time of power from the supply mains is not available.

American Standard Code for Information Interchange (ASCII): US-American data transmission code.

Ancillary control equipment (ACE): Operating device for setting/unsetting of IAS (e.g. ACE with physical identification feature).

Ancillary control equipment (ACE) with biometric identification: ACE where the setting/unsetting of an IAS is made by the identification of the operator with the necessary information being part of the operator himself (e.g. finger print, eyes background, voice).

Ancillary control equipment (ACE) with mental identification feature: ACE with which setting/unsetting of an IAS is made by input of the necessary information being in mind of the operator (e.g. numbers, figures, series of letters).

Ancillary control equipment (ACE) with physical identification feature: ACE with which setting/unsetting of an IAS is made by identification of physical features (e.g. keys, chipcards).

Ancillary control equipment (ACE) with time control: ACE with which setting/unsetting of an IAS is possible in connection with a second ACE after a programmed time respectively a in a certain time window only.

Annunciation equipment (AE) of an alarm transmission system: Device which displays the signals/messages and information from the Receiving centre transceiver (RCT), stores them if required, and allows to send control commands to the Alarm transmission equipment (ATE).

Application: Area in which a system can be used, e.g. for intruder alarms.

Approval: see **VdS-approved**

Armoured room (German term "Panzerraum"): A room protected against intrusion which is an independent construction made using pre-prepared components (room-in-room system) and which is sealed using a strongroom door. The pre-prepared components, assembly elements and strongroom door shall meet the requirements of RAL-RG 625/5.

Note: Term is out of date.

Armoured safe (German term "Gepanzerter Geldschrank"): Multiple-walled container which has not been built to the product standards of the Research and Testing Association for Safes and Strongrooms (Forschungs- und Prüfgemeinschaft Geldschränke und Tresoranlagen e. V. or FuP), and has not been tested against the testing regulations of that organisation. It shall weigh at least 300 kg, have been built after 1950 and be certified by the manufacturer as resistant to fire, shock, penetration, explosion, melting and oxyacetylene torch.

Armoured safe (German term "Panzer-Geldschrank"): Multiple-walled container weighing at least 300 kg and fulfilling the requirements of

- RAL-RG 626/10 (security level D10),
- RAL-RG 626/1 (security level D1),
- RAL-RG 626/20 (security level D20),
- RAL-RG 621 (security level D2),
- RAL-RG 621/10 (security level E10),
- RAL-RG 621 (security level E).

Note: Term is out of date.

Asymmetric injection (common-mode): Injection of the interferences between the conductors and the measuring reference potential (ground).

Asynchronous network: With an asynchronous network, each party which is connected can transfer data to the network at any time. The network transports this data to the chosen party using the specified destination number. An asynchronous network has a honeycomb networking structure and is equipped with standby paths which the network automatically uses if a path fails. Examples of asynchronous networks include ISDN, X.25 (Datex-P), Telex, analogue telecommunications networks.

ATM cell: Completely equipped facility including access control, in which an ATM system is located.

ATM-Safes: Safe intended for the build-in of an Automatic Teller Machine (ATM) or which is located around an ATM. The ATM-safe disposes of prerequisite openings necassary for the functionality of the ATM.

ATM systems: Completely equipped and surveillanced ATM in which the security technology of the deposit and dispenser components as well as the safe is regulated.

Authorised operator: Person authorised by the operator to (e.g.) set or adjust the access control system.

Authorised point: Person designated by the operator to receive signals and messages and initiate necessary measures.

Auto dialler: Telephone dialling device in which data is transmitted by voice.

Note: This term is outmoded, see „Alarm transmission equipment (ATE)"

Automatic cash safe: see **Staff-operated cash dispenser**

Automatic Teller Machine (ATM): Machine which dispenses money and/or valuables and which may also permit the deposit thereof. An ATM can be fitted with an ATM-safe to provide mechanical protection against burglary.

Note: The term "ATM " also applies to money changing machines and designs intended for exclusive use by banking staff (e.g. staff-operated ATM, in Germany called Beschäftigtenbediente Bankautomaten – BBA).

Availability: The probability of finding a system in operation order at any given time.

AWAG (German abbreviation): see **Auto dialler**

*Note: This term is outmoded, see **„Alarm transmission equipment (ATE)”***

AWUG (German abbreviation): see **Digital communicator**

*Note: This term is outmoded, see **„Alarm transmission equipment (ATE)”***

Background stocks: Background stocks are stocks of bank notes which are kept in safes or strongrooms during business hours and are not required or intended for day-to-day transactions.

Bank strongroom: Strong room used exclusively for the storage of banking valuables.

Basic rate interface (German term “Basisanschluss”): Umbrella term for ISDN multiple device access (German term “Mehrgeräteanschluss“) and ISDN system access (German term “Anlagenanschluss“). Provides two ISDN operational channels (B-channels) and one control channel (D-channel).

BBA (German abbreviation): see **Staff-operated cash dispenser**

B-channel: Operational channel of an ISDN interface with a transmission rate of 64 kbit/s.

Biometry: Biometry is decribing procedures suitable for detecting and processing unambiguous characteristics as well as aligning those characteristics certain access authorisations.

Blockade release: Absolute precedence of the alarm transmission equipment (ATE)/Receiving centre transceiver (RCT)/Sub-receiving centre transceiver (Sub-RCT) over other devices using the same communications device or network terminal. Among other things, this means the forced interruption of a connection which is being set up or already exists and which is interfering with alarm transmission.

Blocking device (German term “Sperrelement – SpE”): System component which prevents the opening of access points when an IAS is set (e.g. special blocking lock, electromechanical door opener).

Blocking period: Defined period for blocking of certain functions (e.g. bolt work of safes and strongrooms, unsetting of an IAS).

Blocking time-clock function: Mechanical and/or electrical device which uses a timer function to block certain functions (e.g. the locking mechanism on safes and strongrooms doors, unsetting an intruder alarm system) for a specified period of time.

Blockschloss-type ACE: ACE in the form of a lock comprising the input device for the setting/dissetting data medium, the associated processing device and the blocking device for access points to the protected premises in a functional unit.

Bolt: Part of a locking mechanism which e.g. moves for example when a key is turned and which is moved into the locking resp. is removed from it.

Bolt contact: see **Striking plate contact**

Bolting: Operating a device (e.g. latch on a locking mechanism) to fix a door in the closed condition.

Bolt mechanism: Device for securing a door closed so that the door cannot be opened without operating this device.

Bolt-switch-lock (German term "Riegelschaltschloss"): Ancillary Control equipment (ACE) in form of a lock for setting/unsetting IAS with simultaneous mechanical blocking/unlocking, but without locking of the blocking/unblocking operation.

Buildings management technology (BMT): Technology for the control and monitoring of specific building processes (e.g. heating, ventilation, air-conditioning, lighting).

Bullet-resistant glazing: Glass is said to be bullet-resistant if it impedes the penetration of bullets (tested to DIN 52290-2).

Burglar resistance: Feature of a component which provides resistance against attempts to damage or destroy it with the aim of breaking into the area protected by the component.

Burglar-resistant element: Complete facade element (e.g. door, window, roller blind) which, in addition to its normal functions, also counteracts burglary attempts of a defined resistance, and in which all the burglar-resistant features are tuned to one another.

BUS: Collecting-line system in which the exchange of data and/or information takes place sequentially.

Cash dispensing machine: see **Automatic Teller Machine (ATM)**

CD-protection (in Germany until now "KB"): Protection which safes and strongrooms demonstrate against a defined attack with diamond core drills. The test of CD protection includes at least on attack achieving at least one complete access or partial access.

Certificate: Document issued according to the rules of a certification system in order to give confidence that an unambiguously described product, an unambiguously described process or an unambiguously described service conform with a certain standard or other normative references (e.g. rules).

Certification: Procedure in which a third party confirms that a product, a process or a service is conform with the fixed requirements.

Certification body: Body which performs certifications.

Remark: A certification body may operate its own testing and inspection activities or overseas these activities carried out on its behalf by other bodies.

Change: Measures necessitated by operational use and security information, but not representing an extension.

Channel packaging: If a higher velocity than 64 kBit is necessary (e.g. for a transmission of photographs), several B-channels have to be used at the same time. As the signal transfer on B-channels may differ a packaging may cause severe problems.

Charging output: Output of the power supply to which the batteries are connected.

Charging voltage: Voltage delivered by the power supply to charge up batteries and maintain their charge.

Chute: Link between the input unit of an ATM or a deposit-box-system and the corresponding security container.

Circuit switching: ISDN is a network based on circuit switching. This means that after set-up up to the clearance of the connection a transparent path almost free of delays between the participants is available. For the time of the connection the full bandwidth of a B-channel is available independent of the use. This can be seen also in the tariffs of time intervals.

Closed Circuit Television (CCTV): A closed television system, see **Video-surveillance-system.**

Closed user group: Group of participants within a network who can only communicate with each other and cannot be reached by other participants of the network or from outside the network.

Closing: Operating a door or window to ensure that it is properly shut. A locking mechanism is required to close the door or window securely.

Note: A locking mechanism can also perform the function of bolting.

Combination: Series of numbers, figures or characters which permit access when entered correctly.

Comité Consultatif International des Radiocommunications (CCIR): International advisory committee for radio services.

Comité Consultatif International Télégraphique et Téléfonique (CCITT): International advisory committee of the International Telecommunications Union for telegraphy and telephony services. The CCITT drafts recommendations for telecommunications. V-series and X-series recommendations are of importance to alarm transmission.

Note: The organisation is now called ITU-T.

Communications devices: Devices within transmission paths in alarm transmission systems which do not belong to networks. Communications devices include e.g. multiplexers, concentrators, processing nodes and service transition points. They may belong to the network operator, the operator of the alarm transmission system, the operator of the alarm system or third parties.

Component, burglar resistant: Individual components (e.g. lock, belt, glazing) of a facade element which, in addition to their usual functions, counteract intruder attempts of defined resistance.

Concentrated display: A concentrated display comprises several display elements. It can display several identical and/or different operating statuses simultaneously or in sequence.

Contact surveillance: Spot surveillance of objects and components using contacts, e.g. magnet contacts.

Container: Used for the storage of cash, valuables and data media.

Container for time-controlled release of funds: These are day-safe-quality dispensers with a number of compartments with time locks. Prior to opening the tills for the day's business, the compartments are stocked with the bank notes required to top up the permitted stock of accessible bank notes. Emptied or unused compartments can be used during banking hours to store incoming payments or any bank notes exceeding the permitted stock of ready-access notes. The compartments can only be opened one after the other, and only after the pre-programmed delay time has passed. Instead of containers for staggered release of funds, staff-operated cash dispensers with modified program control can also be used provided that they comply with the required delay periods or fixed maximum payout amounts.

Container safe: see **Strongroom**

Container, simple: see **Simple container**

Container with additional security features: see **Security container**

Control and indicating equipment (CIE): Device for receiving, processing, indicating and notifying signals and information (e.g. intruder, tampering and fault signals).

Control and indicating equipment (CIE): see **Intruder control and indicating equipment (I-CIE)**

Control device: Part of an intruder alarm system which is required for the operation of the system, e.g. ancillary control equipment (ACE).

Control line: Line for the control of system components (e.g. switching displays on and off).

Circuit (German term "Meldelinie"): All detectors in a primary line brought together to form a zone.

*Note: This term is outmoded, see **"Zone"** and **"Interconnection"***

Customer-operated ATM: ATM usually installed in the exterior facade or in the porch of a bank building which is accessible to customers and is stocked with cash by the bank (container). Customers who are authorised to do so can withdraw a certain amount of cash from the ATM by using their bank card and providing additional proof of identity (e.g. entering a code).

Formerly known as: Automatic cash dispenser, cash machine, cash point, Bancomat

Data radio: In data radio systems, data is sent via a radio infrastructure and can be passed on via wired networks.

Note: Example "MODACOM" from Deutsche Telekom.

Data strongbox: Cabinet, the purpose of which is to protect data media and valuables against fire.

Note: Data strongboxes are only tested and certified with respect to the protection they provide against fire and not against burglary.

Data strongroom: Room (including door), the purpose of which is to protect data media and valuables against fire.

Note: Data strongrooms and their doors are only tested and certified with respect to the protection they provide against fire and not against burglary.

DATEX-P: Data transmission services provided by Deutsche Telekom based on the CCITT X.25-specifications.

Datex P20H: This access to the Datex-P net corresponds with the PAD-access with X.3-control directly connected to the dedicated connection (German term: ”Festverbindung“) of German Telekom. In here the packet transmission of data is no more necessary as PAD of the Deutsche Telekom offers this as service. Only one Datex-P20-h-connection is possible at the same time.

Day/night deposit-safe-system: System which allows cassettes containing cash, cheques or other items to be deposited in a strongroom or safe at any time. Day/night deposit-safe-systems consist of a lockable input device, a receiving unit and a drop-chute between input device and receiving device.

Day safe (German term “Tagestresor”): Single-walled steel cabinet, e.g. similar to single-walled steel cabinet of security level A of VDMA standard sheet 24 992.

Daytime door: Additional barrier behind a strongroom door (e.g. daytime grille door) used for access limitation when the strongroom door is open.

Daytime grille door: see **Daytime door**

D-channel: Control channel in ISDN for the transmission of control and administrative data in the connection.

DDV: Daten-Direktverbindung (Data Direct Connection) from Deutsche Telekom.

Formerly in Germany known as: Hauptanschluß for Direktruf; HfD (Main access for direct call).

Dedicated line: Physical or logical connection which, once set up or created, is constantly available for the transmission of signals/messages or for monitoring the connection.

Degree of resistance: Term for the classification of resistance to burglary.

Degree of risk: Degree of risk of an object, determined by the accessibility (e.g. uppermost storey), the neighbourhood (e.g. adjoining third-party property, third-party rooms, motorway exit), the local situation (e.g. housing, industrial area) and the covetousness of the available objects.

Deposit-box: A box located in a deposit-box system which banking customers can lease and use to deposit items. The deposit-box can usually only be opened by customers in the presence of a member of banking staff or after remote operation of a blocking device.

Deposit-box system: System in banks containing lockable boxes which can be leased by customers for the deposit of items. The boxes are usually housed in a strongroom or strongbox. Deposit-box systems are available in four different types:

- **Mechanical deposit-box system (conventional deposit-box system)**, where the deposit-box can only be opened on the spot by the banking customer accompanied by a member of banking staff.
- **Semi-automatic deposit-box system,** where the lock on the deposit-box is remotely released by a member of banking staff after confirming the identity of the banking customer; the banking customer than opens his lock himself.
- **Self-service deposit-box system**, where the lock on the deposit-box is remotely released during their business hours of a bank after the identity of the customer has been confirmed, the banking customer can access his leased box after this procedure.
- **24h-self-service deposit-box system**, where the banking customer can access to his deposit-box at any time after a respective identification procedure.

Deposit system: System in which the staff of a company (e.g. bank) can deposit cash and similar valuables in a security container at any time, without the door to the container having to be opened. The deposited cash and the like can be placed in special containers (e.g. deposits, cash boxes).

Detection: Identification of a deviation from a defined status.

Detector: see **Intruder detector, Hold-up detector, Status detector**

Detectors for hazard and emergency statuses: Detectors of an alarm system serving as early recognition of water and gas penetration, dangerous overriding or underriding temperatures or similar.

Different route: Different routes exist if transmission paths around the alarm transmission equipment (ATE) and the Receiving centre transceiver (RCT resp. Sub-RCT) are designed in such a way that attacks on one route (e.g. attack on a telecommunications cable) do not have a negative effect on the other route. Example: Different routing of two telecommunications cables in a building, transmission via telecommunications cable and radio network.

Digital Communications System (DCS): Digital mobile telephony network which operates in the 1800 MHz frequency band. In Germany this is known as the “E-Plus-Netz”.

Digital communicator: Alarm transmission equipment (ATE) for connection to switched telephone networks. Information are transmitted via coded signals. The subscriber`s device is known in Germany as AWUG-T and the receiver in the alarm receiving centre in Germany is known as AWUG-Z.

*Note: This term is outmoded, see **„Alarm transmission equipment (ATE)”***

Display element: The smallest optical element of a display which is capable of separate control (e.g. filament of an incandescent bulb, a dot in a dot matrix display, a segment of a seven-segment display).

Double-lock: see **Four-eyes principle**

Down loading: see **Remote parameterisation**

Drop-chute: Connection between the input unit and the receiving unit (container) in a day/night safe system.

DSS1: The D-channel protocol for the control and administration of ISDN connections.

Duplex safe: The term for safes which provide protection against both fire and intrusion.

Dyeing system: Equipment used to activate a smoke and/or dye system to mark objects, e.g. bank notes. in the event of a defined danger situation. The dyeing makes items stolen during a Hold-up or burglary worthless to the perpetrator, since passing on the dyed objects (e.g. bank notes) is extremely risky. In addition, the triggering of the system is also an incalculable risk for the perpetrator, and has the effect of surprising him.

Effectiveness: Security technology-related contribution made by an intruder alarm system with respect to the degree of damage limitation expected in the event of burglary or attempted burglary. This primarily depends on

- choosing the right system for the risks it will face
- the ability of the system to identify an intrusion
- the reliability of the system chosen
- the maintenance of the system
- the necessary flanking measures

Electromagnetic compatibility (EMC): The ability of an electrical device to function satisfactorily in its electromagnetic environment, without influencing this environment, which may be used by other installations, in a non-permissible manner.

Electromechanical A.C.E.: ACE device with mechanical locking function (e.g. Blockschloss-type ACE).

Electromechanical blocking device (German term "Elektromechanisches Sperrelement – SpE"): System component which prevents the opening of access points when an IAS is set (e.g. special blocking lock, electromechanical door opener).

Emergency locking system: System consisting of blocking and detection elements which prevents the operation of locking equipment once a burglary attempt has been identified.

Note: An emergency locking system can be a component of the locking system (e.g. active emergency locking system) or an independent component (e.g. passive emergency locking system).

Emergency teller: In the event of the failure of the staff-operated cash dispenser, emergency tellers are used to allow the necessary cash transactions to continue if customers cannot use the available customer-operated ATM for this purpose. Examples of emergency tellers include a lockable adjoining room in which the second staff-operated cash dispenser operator would manage the required accessible bank note stocks.

End-of-charge voltage: The voltage of a battery during charging at a specified constant current when the battery reached its full charging status.

Environmental class: According to its operation area components of alarm systems are subject to different environmental influences. Different severe requirements are to be fulfilled by the devices regarding the environmental behaviour. Difference is made between the following environmental classes:

- **I** (conditions in well-kept and air-conditioned indoor areas)
- **II** (conditions in indoor areas – e.g. stairwells – with regularly dewing)
- **III** (conditions outdoors, but weather-protected)
- **IV** (conditions outdoors, fully exposed to the elements)

Environmental stability: Ability of an IAS to resist environmental factors and function correctly within given limits.

Equipping of products: Equipped products are supplied by the manufacturer complete with intruder alarm system components, i.e. all necessary VdS-approved system components are installed, cabled, adjustment and function-tested.

Euro ISDN: ISDN in which the DSS1 protocol is used in the D-channel.

Event recorder: Device which automatically records operating events in the IAS and/or other technical equipment.

Exclusive interconnection: Interconnection for which a particular area of competence is responsible (e.g. dedicated wiring of an alarm system).

EX-protection: Protection feature exhibited by safes and strongrooms against defined attacks using explosives. The EX-protection test involves at least one attack achieving complete or partial access.

Note: This term is also used for "Explosion protection", German term "Explosionsschutz" in the sense of the German "Explosionsschutzverordnung" (EXV) and should not mixed up . EXV deals with regulations for devices and systems for the intended use in areas with explosion hazards.

Extension: Measures required by enlarged surveillance scope, modified use/operation or new perpetrator behaviour.

Exterior wall of a protected premises: see **Outer wall of a protected premises:**

External alarm: Indication of an alarm situation on site (e.g. using audible and visual warning devices or voice messaging) which is directed at the general public to call for assistance.

Note: The meaning of this term has changed

External signal: Signals which are external to the system and do not belong to the installed system.

Facade element: All the components making up an element including means for mounting and serving to close an opening in the wall of a building. Facade elements may be fixed (e.g. shop window) or fitted with an opening device, e.g. a door, window, roller blind.

Note: Facade elements in the sense of these rules may also be located inside a building – e.g. the front door to a flat in a residential block.

Fail-safe-behaviour: Characteristics of a technical equipment to be able to get into a safe state in case of a fault.

False alarm: Alarm triggered for reasons other than hazard.

False alarm signal: Alarm signal triggered for reasons other than danger, but which appears to be a security alarm signal.

Fastening: see **Locking mechanism**

Fastening device: see **Locking device**

Fastening surveillance: see **Locked state monitoring**

Fault signal: A signal given by a system component or by the intruder alarm system signifying that a fault has been identified or exists.

Fault (status): Exceeding the defined deviation from the target status and indication of this fact.

Final voltage (cut-off voltage): The specified voltage at which a discharge of a battery is considered finished and which typically shall not fall below.

Fire brigade key box: Container opened by the fire brigade to access building keys in the event of fire.

*Note: This term is outmoded, new term **Key box***

Fixed installed equipment: Equipment which is installed in a fixed manner or which does not have a carrying device or which is so large that it cannot be moved easily.

Focal-point surveillance: Surveillance of parts of a protected premises (e.g. using motion detectors) where objects at-risk (highly desirable objects) are concentrated.

Forced-entry detector: Detector which signals an early alarm when an attempt is made to force open doors, gates, windows, etc. and does so before the mechanical resistance of a mechanical security device is overcome.

Forced opening: Opening of a safe or strong room under duress, e.g. during with a Hold-up.

Force, simple manual: Physical force on a mechanical resistance without the use of tools or accessories aiming to surmount the resistance.

Four-eyes principle: Under the four-eyes principle, a certain task (e.g. opening a lock) can only be performed if it is carried out by two people with differing and complementary authorization.

Free-standing safe: Safe with burglary protection provided only by the materials used in the pre-production and construction phases and not by materials built in or added during installation.

Full penetration (full access, full breakthrough): Opening through which a rigid gauge can be inserted through the wall or door into the inside of the body of the object being tested. The following are also considered as full penetration

- Removing a Wall-mounted cabinet with inbuilt protection from the object being tested
- Removing a container door
- Opening a container door to a width of 300 mm and to at least 80 % of the internal headroom.

Fully shielded lines: Shielded lines where the shield is connected to ground on both sides or where no sections of lines exit the shielded area either fully or in part.

Function determining security: Function on which certain elements (e.g. tampering, operating error) can have the effect of endangering security.

Functional reliability: Entirety of all measures necessary to ensure uninterrupted operation of a system in accordance with requirements and to identify faults.

Furniture-mounted cabinet (German term " Einsatzschrank"): This is a

- armoured safe complying with security level D10 of RAL-RG 626/10,
- armoured safe complying with security level D1 of RAL-RG 626/1,
- strongbox for valuables complying with level C1 or C2 of RAL-RG 626/2,
- multiple-walled steel cabinet complying with security level B of VDMA 24 992

which, because of its design, is suitable for fixed installation in furniture or behind wall coverings.

German Federal Office for Telecommunications Authorisations (BZT): Competent German authority for the licensing of devices for use in telecommunications. Licences are issued on the basis of BAPT licensing provisions.

German Federal Office of Post and Telecommunications (BAPT): German authority which regulates and monitors the use of communications media and services by issuing authorisation provisions and licences under the German Telecommunications Systems Act (Fernmeldeanlagengesetz, FAG).

Note: BAPT has been replaced by „Regulierungsbehörde für Post und Telekommunikation (RegTP)".

Glass door: A window extending down to the floor/standing surface through which a person can pass.

Note: Unlike a normal window, a glass door cannot be locked from the outside.

Global System for Mobile Communications (GSM): Digital mobile telephony network which operates in the 900 MHz frequency range.

Note: Example "D-Netz" in Germany.

Hand range: For intruder alarm systems, the range up to 3 m above a freely accessible surface.

Hardware: All or part of the apparatus and equipment which makes up systems.

Hinge bolts (also called **dog bolts):** Hinge bolts are fixed on the side of the hinge of doors at the small side of the door leaf and in closed state in drill holes of an skirting plate of the door architrave (door frame) meshing metal bolts. Hinge bolts avoid that doors are opened on the frame side with violence or that doors are ejected on the doors angles (so-called protection against taking off its hinges).

Hold-up alarm system (HUAS): System which allows persons to call for help directly in the event of a Hold-up.

Hold-up signal: Signal triggered by the activation of a hold-up triggering device which leads to a remote alarm regardless of the status of the IAS.

IAE: IAE is the name for the ISDN plug connection (also known as Western plug or RJ 45).

Identification feature (ID): An identification feature is a piece of information in mental, physical or biometric form, used for an unambiguous identification (e.g. a series of figures or characters or letters existing in the memory of the operator, information existing in a magnet or chip card, a coding of a key, valuation of a finger print or an eye image).

Identification feature medium: Medium carrying information which exists in mental, physical or biological form.

- **Mental identification feature medium:** A mental information feature medium contains the information required for identification (e.g. as a series of figures, characters or letters) in the memory of the user.
- **Physical identification feature medium:** Information feature medium of a physical nature containing the information required for identification (e.g. key, chip card)
- **Biological identification feature medium:** Information feature medium in which the information required for identification is contained in the operator himself (e.g. personal characteristics such as physical features, fingerprints, iris image or other personal feature such as voice).

"Indoor" customer operated Automatic Teller Machine (ATM): Customer operated ATM integrated into the inside of a building. In order to use the ATM, the customer has to pass through a door and enter the building.

Information: Information is the content of a piece of news or message, e.g. taking the form of a compilation of characters or statuses.

Input device: Device or component of a device which takes up the information contained in its identification feature, transforms it if required (e.g. into electrical signals) and passing them on to an processing unit.

Input function: Reading/accepting of an information from the identification feature, if necessary transformation (e.g. into electrical signals) and passing-on to an processing unit.

Input unit: Part of a **Day/night safe** system in which boxes containing cash, cheques or other items can be deposited. The deposit facility is connected to a receiving unit (container) by a chute.

Integrated alarm system: A system in which the applications involved use shared equipment (e.g. hardware, software or transmission lines) and at least one application is a security application.

Integrated Services Digital Network (ISDN): Service-integrated digital communication network bringing together various communications services, e.g. telephony and data transmission.

Internal alarm: Alarm signifying the triggering of the complete or partly internal set IAS as well as voice messaging to persons in the surveilled object with the objective of self-help.

Intervention certificate: VdS-formular for the documentation of intervention measures e.g. by an Alarm receiving centre. It may form the basis of the contract of insurance taken out between insurance company and policyholder.

Intervention company (IC): Department of a security company which performs danger defence and damage reducing measures.

Intervention plan: Documentation of all information necessary for the proper surveillance and – if given – intervention as e.g. name and address of object, access route, risk, intervention measures.

Intervention measures: Intervention measures are danger defence measures, being performed by an intervention company (security company).

Intruder alarm control and indicating equipment (I-CIE): Device for receiving, processing, indication and notification of siganls/messages and informations (e.g. intrusion, tamper and fault signals).

Intruder alarm system (IAS): System for automatic surveillance of protected premises to prevent unauthorised entry.

Intruder alarm system concept (IASC): All the system components which are tuned to function together as a whole (e.g. intruder control and indicating equipment (CIE), switching devices, intruder detectors).

Intruder alarm system equipped: Equipped system components (e.g. burglar-resistant windows and doors, safes) are supplied by the manufacturer complete with intruder alarm system components, i.e. all VdS-approved intruder alarm system components are installed, cabled, set up and function tested.

Intruder alarm system preparation: Prepared system components (e.g. burglar-resistant windows and doors, safes) are especially prepared by the manufacturer so that they can accommodate intruder alarm system components. Preparation does not involve installing intruder alarm system components, but is restricted to drilling holes for fixings, for example.

Intruder detector: A component of an intruder alarm system which monitors a suitable physical parameter constantly or at regular intervals for purposes of identifying an attempted or actual intrusion to the area under surveillance.

Intruder signal: Signal signifying that intruder detectors have been triggered.

Inspection: Measures to ascertain and assess the actual condition of technical equipment in a system.

Installation certificate: VdS form (VdS 2170) for documenting security measures which have been carried out on the basis of the applicable VdS rules, e.g. installation of an intruder alarm system. The installation certificate is issued by a VdS-approved installer and forms part of the installed system. It may form the basis of the contract of insurance taken out between insurance company and policyholder.

Interconnection: Interconnections are the external connections for system components in an IAS. They are used to transfer information resp. signals/messages in an alarm system.

*Note: A distinction is made between **exclusive interconnections**, in which the responsibility for the interconnections lies with one area of competence, and **non-exclusive interconnections**, to which third parties also have access.*

Interface: Theoretical or actual transition at a boundary between two functional units with agreed rules for the for handover of data and signals.

Interface S_1: Interface between the Alarm system (AS) and the Alarm transmission equipment (ATE).

Interface S_2: Interface between the alarm transmission equipment (ATE) and the network termination point or an available communications device.

Interface $S_{2.1}$: If a communications device is located between the alarm transmission equipment (ATE) and the network termination point , its output is known as $S_{2.1}$.

Interface S_3: Interface between the network termination point and the Receiving centre transceiver (RCT) resp. Alarm receiving equipment (ARE).

Interface $S_{3.1}$: If a communications device is located between the network termination point and the Receiving centre transceiver (RCT), its input is known as $S_{3.1}$.

Interface S_4: Interface between the Receiving centre transceiver (RCT) and the Annunciation equipment (AE).

ITU Telecommunication Telecommunication Union (ITU-T): International organization responsible for private and public fields coordinating global telecommunication nets and services.

Remark: Successor organisation of the "International Telegraph and Telephone Consultative Committee" (CCITT).

Key deposit box (KDB): Stable container for the storage of building keys intended to enable authorized helping forces with the stored keys a violent-free access to buildings.

Key deposit box adapter: The key deposit box adapter comprises all the functions required to control and monitor a key deposit box.

Key deposit box adapter unit: Technical realisation of the key deposit box adapter, which may be designed as an individual device or as a slide-in unit for an C.I.E. for alarm systems.

Key-operated switch: Lock for setting/unsetting an intruder alarm system without mechanical bolting.

Knot: A knot is a exchange point in X.25-data networks. It receives data packages, searches in its transmission path table the recipient or – if this cannot be achieved on direct transmission path, the next knot to transmit the data packet to there.

Layer-1-monitoring: Monitoring of the physical layer of an transmission system according to the OSI reference model, e.g. interconnection paths, radio frequencies.

Layer-4-monitoring: Monitoring of the transporting layer of an transmission system according to the OSI reference model, e.g. by end-to-end signal transmission.

Layperson: Person without specialist knowledge with Do-it-yourself (DIY) equipment (e.g. hammer, file, voltmeter).

Light construction: see **Walls of light construction**

Linear surveillance: Linear surveillance, e.g. using the light beam from a light barrier.

Linear surveillance characteristics: Characteristic of an intruder detector which identifies and processes changes in physical parameters when a line is penetrated (e.g. light barrier).

Local alarm: see **External alarm**

Lock: Mechanism which recognises a coded input and performs the function of blocking the locking mechanism or the door.

Locked state monitoring: Surveillance of the locked status of doors, windows, etc. (e.g. with stroke plate contacts) for guaranteeing the function „Zwangsläufigkeit“.

Locking: Operating a device (e.g. locking bolt) to lock a door which is suited to close a door so that it cannot be opened without the use of an authorized identification code.

Note: A locking mechanism can also perform the function of bolting.

Locking device: Mechanical or code lock allowing the identification of authorisation of an identification feature.

Locking mechanism: Totality of all locks and locking mechanisms.

Logical (virtual) connection: Determination of a connection routing in a telecommunications network or similar over the knots between the participants. When starting a connection a suitable path is searched from knot to knot; the transmission of data packages is made automatically on this path. On a physical connection there may be a lot of logical connections which do not disturb each other.

Maintenance (German term “Wartung“): Measures for keeping the desired state of technical means of a system.

Maintenance (German term “Instandhaltung“): Measures to maintain and restore the condition of technical equipment in a system and to ascertain and assess the actual condition.

Maintenance of performance: According to DIN 4102, Part 12 (Jan. 1991), maintenance of performance is deemed to be demonstrated by an electrical wiring system when no short-circuiting or interruption of current occurs in the system when it is subjected to a defined fire test.

Note: Maintenance of performance in the meaning of DIN VDE 0833 can be achieved for Automatic fire alarm systems by using appropriate wiring or suitable surveillance measures of the system.

Mean Time Between Failures” (MTBF): Measure of the failure probability of a component.

Mechanical resistance: Degree of difficulty in breaking through a component or facility using force.

Mobile branches: Under the terms of the German Accident Prevention Regulations for Banks (“UVV Kassen”), mobile branches are moveable premises performing cash transactions.

Note: Mobile branches are not money transportation vehicles.

Modem: (artificial word for modulator/demodulator). Device which converts digital data from computers into analogue signals, e.g. for transmission via telephone lines, and vice-versa.

Money changing machine: ATM which converts the cash inserted into it (notes, coins) into cash of a different denomination or currency.

Monitored lines: Lines between the intruder control and indicating equipment (CIE) and system components which are monitored directly or indirectly (e.g. by co-routing a primary line).

*Note: This term is outmoded, see **Transmission path***

Motion detector: Intruder detector which recognises movements within its surveillance area and triggers an alarm.

Movable equipment: System components which occasionally change location; proper functioning is not expected while the parts are being moved.

Multiple device access (German term “Mehrgeräteanschluss“): With an ISDN multiple device connection, up to 12 communications sockets can be connected in parallel with up to 8 different devices at one ISDN connection. Two devices can be operated in parallel at any one time, since two operational channels (B-channels) are available in ISDN.

Multi-user-band radio: Radio network in which a participant wishing to make a call is given exclusive access by the system to an available radio channel for a limited amount of time. In addition to voice transmission, data transmission is also possible in a multi-user-band radio.

Multiple-walled steel cabinet: Double or triple-walled container weighing at least 300 kg (in households at least 200 kg), which

- fulfils the minimum requirements set out in VDMA 24 992 (security level B)
- **does not** fulfil the minimum requirements set out in VDMA 24 992 (security level B), but offers extensive or simple protection against attacks using simple burglary tools and against fire
- fulfils the requirements of RAL-RG 626/2 (security level C), see Strongbox for valuables.

Needs-based connection (dialup line): Physical or logical connection which has to be dialed-up prior to transmission of signals/messages or connection monitoring operations, and cleared again after the transmission or monitoring operation is complete.

Negative acknowledgement: Information from the alarm transmission equipment (ATE) to the alarm system to advise that an alarm signal could not be passed across interface S_2.

Network: Networks transmit information from A to B without changing it; Network-specific information may be added to or left out of the transmission process.

Network terminator (NT): Name for the network termination point of the German Telekom ISDN system.

Network termination point (NTP): Electrical (interface) and mechanical connection (e.g. socket) which the network provider makes available and which constitutes the end point of his area of responsibility.

Note: The network termination point may also contain electronic and/or energy supply equipment.

Non-exclusive interconnection: Interconnection to which third parties also have access (e.g. radio, certain BUS systems).

Non-typical hold-ups: A hold-up at a bank is regarded as non-typical if the perpetrators

- threaten the bank staff within the confines of the bank, but outside the bank's normal opening hours, to obtain money.
- overpower or threaten bank staff, their relatives or other persons outside the confines of the bank in order to obtain money.

Object surveillance: Surveillance of individual objects (e.g. safe, work of art).

Opening suitable for human entry: An opening with at least the following dimensions:

- Rectangle of 400 mm x 250 mm or
- Ellipse of 400 mm x 300 mm or
- Circle with a diameter of 350 mm.

Open Systems Interconnections (OSI layer): Layer inside the reference model for communication in open systems. The OSI reference model is divided into seven layers, which are arranged hierarchically with layer 1 at the bottom and layer 7 at the top.

Operational reliability: Entirety of all the measures taken to ensure the correct operation of the IAS by preventing operating errors.

Operator: The person responsible for operating the alarm system.

Optical space surveillance systems (German term "Optische Raumüberwachungsanlagen – ORÜA"): Camera systems (e.g. photographic cameras, video surveillance systems) which are activated by staff in the event of Hold-up and record the main events of the Hold-up in the area which they monitor. If staff see persons acting suspiciously, they can activate the systems to record events as a precautionary measure.

OSI-reference model: Within the OSI reference model, an international standardization, communication of two partners has been standardized. The sequence of the set-up and and clearing of a connection for communication has been graded in communication layers. The reference model begins with layer 1 (physical), of the hardware with is used transfering and ends with layer 7 (application), the in- and output of informaton between the machine and human-beings. Within the layers 2 (data link) and 3 (network) the procedures are specified which are necessary to specify the procedure of set-up and clearing of a connection and maintaining of a connection. The layers 4 (transport) throughout 7 are used for the structuring of the applications (e.g. software for an alarm centre). In the area of the transmission of signals/messages it is necessary to secure the transmission path against tampering. Within ISDN there are possibilities of securing the interconnection on the OSI-layers 1, 3 and 4.

"Outdoor" customer operated ATM: Customer operated ATM integrated in the exterior wall of a building. Customers use the ATM outside the building.

Outer wall of a protected premises: Wall which forms the barrier between a protected premises and other rooms or the surroundings. It may be an outer wall as well as an inner wall of a building.

Package switching: X.25 is a package transmission network. That means that from the set-up up to the end of the connection a possible transmission path from knot to knot is chosen which can be changed automatically in case of faults. Request of bandwidth and therefore costs are due only when transmitting a data package. There may be delays in the knots if several different packages are sent on the same circuit. Information need a protocol packaging for the transport, the available bandwidth is not fully usable for the user data transmission.

Packet Assembler/Disassembler (PAD): Device or function of a device which assembles or disassembles packets of data for transmission, thereby preparing the data for synchronous data transmission in the X.25 network.

PAD: see **Packet Assembler/Disassembler**

Parameterisation: The process of adjusting system-specific features of an installed alarm system (via hard- and/or software).

Partly shielded lines: Shielded lines where the shield is connected to ground just on one side or where lines desert the shielded area either fully or in part.

Part-protected premises: Closeby or also a separate situated part of a protected premises.

PCM 30: PCM 30 stands for a pulse code modulation of 30 channels and represents the technical definition for the digital transmission of information in time intervals. PCM 30 lines do not have signalling channels and are therefore a subitem of S_{2M}. S_{2M} is PCM 30 with signalling channels.

Penetration prevention: A component is said to offer penetration prevention (preventing break-in or break-out) if it increases the length of time taken to create an opening.

Penetration surveillance: Surveillance of surfaces (e.g. walls) against persons entering or reaching in.

Peripheral monitoring: Monitoring of all access points, windows or other openings as well as walls, ceilings and floors.

Permanent Virtual Circuit (PVC): Connection which is set up by the network operator and then remains in existence.

Personal Identification number (PIN): E.g. number on ID-cards of access control systems or combination of numbers which have to be inputted for use of check cards (for ATM) additionally via a code console.

Planar surveillance characteristic: Feature of an intruder detector which detects and evaluates changes in physical parameters when a surface, e.g. a wall, is penetrated (e.g. seismic detector).

Point-type surveillance characteristic: Feature of an intruder detector which identifies and processes changes in physical parameters when the position of an object under surveillance changes (e.g. magnet contact).

Portable system components: System components which frequently change location; they are expected to continue functioning properly while being moved (e.g. electronic key tags, portable Hold-up detectors).

Power supply: System component for the supply of electric power to alarm systems or parts thereof.

Power supply unit (PSU): Technical realization of the power supply, which may be realized as a single device or as a part of a system component (e.g. module of an alarm control and indicating equipment).

Power supply unit type I (mains supply and automatically rechargeable secondary battery): Fault-jeopardized power source with almost unlimited capacity (e.g. public mains power supply) in connection with a not-fault-jeopardized power source with limited capacity, which is automatically regenerable.

Power supply unit type II (mains supply and primary battery or automatically not-rechargeable secondary battery): Fault-jeopardized power source with almost unlimited capacity (e.g. public mains power supply) in connection with a not-fault-jeopardized power source with limited capacity, which is **not** automatically regenerable.

Power supply unit type III (primary battery or not automatically rechargeable secondary battery): Not-fault-jeopardized power source with limited capacity, which is not automatically regenerable.

Pre-preparation of IAS components: Pre-prepared system components (e.g. burglary-resistant doors and windows, safes) are especially prepared by the manufacturer so that they can accommodate IAS components. Preparation does not involve installing IAS components, but is restricted to drilling securing holes, for example.

Primary battery: Galvanic cell, were chemical energy is converted in electrical energy. By this energy conversion the cell will be discharged; a primary battery is not rechargeable.

Primary line (German term "Primärleitung"): Monitored connection between system components which serves to transmit messages and information and can also be used to supply power to system components.

Note: This term is outmoded, see "transmission path"

Primary multiplex access: see **S_{2M}-connection**

Private automatic branch exchange (PABX): PABX is standing for a private automatic branch exchange for telephones. Connected to ISDN not only speaking is possible but also language, data, text or photos, etc. may be transmitted. Transfer is carried out mainly via 64 kbit-paths.

Processing function: Checks the information from the data medium.

Processing unit: Device part which processes and evaluates electric parameters or signals.

Processing unit of ACE: Device or part of a device which checks authorisation and passes the result on to the intruder control and indicating equipment (CIE).

Protected premises: Closed building or closed part of building and adjacent areas in which the objects under surveillance are located.

Quality: Grade in which a set of inherent characteristics fulfils requirements.

Note 1: The definition „quality" may used in connection with adjectives as good, bad or excellent.

Note 2: „Inherent" means in contrary to „assigned" being within a unit, especially as steady characteristic.

Quality management systems (QM-System): Management system for controlling and managing an organisation regarding its quality.

RAL: Formerly known as: Reichsausschuss for Lieferbedingungen und Gütesicherung (German Committee for Supply Conditions and Quality Assurance), now: German Institute for Quality Assurance and Labelling (Deutsches Institut für Gütesicherung und Kennzeichnung e. V.).

Reach-in access: Gripping through an opening of the facade or in the facade element by hand or with auxiliary tools.

Reach-in surveillance: Surveillance of an surface against persons reaching through it. A distinction is made between:

- a person reaching a hand inside, e.g. through a hole in a window

and

- a person reaching inside using tools, e.g. reaching through a small hole in a window with a wire hook.

Ready-to-alarm: Alarm systems and their components are ready-to-alarm when information resp. signals can be processed.

Receiving centre transceiver (RCT): Receiving facility in alarm transmission systems which receives signals/messages from alarm systems, evaluates them, passes them to the Annunciation equipment (AE), stores them if necessary and passes on control signals to the Alarm transmission equipment (ATE).

Receiving unit (container): Container which takes cash boxes deposited in day/night safe systems. It is linked by a drop-chute to an input unit.

Receiving unit for day/night-deposit-systems: Containers with system-specific openings. These containers do not become fully functional until they are installed on-site when an associated input unit and transfer device (chute) is fitted and suitable security measures put in place.

Redundancy: Availability of technical components, which become necessary for the operation of a system or a device only in case a fault or a failure is given. Redundancy is an important element for increasing reliability. It is used where faults may cause great effects.

Regulierungsbehörde für Post und Telekommunikation (RegTP): German authority which regulates and monitors the use of communications media and services and postal services by issuing authorisation provisions and licences.

Release element: Facility which allows a provider of assistance to manually trigger a fire alarm from outside the object/protected premises.

Note: Release elements are components of an automatic fire alarm system (AFAS).

Reliability: The ability of an element under consideration (component, part system, system) to fulfil the requirements deriving from its purpose which are placed on the performance of its features during a set period of time and within set limits (prescribed conditions of use and maintenance).

Remote diagnosis: Technical means of checking statuses, readings, etc. of an intruder alarm system from a remote location (e.g. using an alarm transmission system).

Remote maintenance: Technical means of performing maintenance operations on an intruder alarm system from a remote location (e.g. via an alarm transmission system).

Remote parameterisation: Technical means of parameterising an intruder alarm system from a remote location (e.g. via an alarm transmission system).

Remote signalling: Indication of an alarm situation to a remote provider in charge of assistance (e.g. alarm receiving centre of the police or a security company).

Repair: Measures to restore the target condition of technical equipment in a system.

Resistance grade: The resistance grade shows the degree of burglary prevention provided by a burglar-proof facade element. The assignment of a particular resistance grade is based on static/dynamic load capacity and resistance to the effect of tools during manual tests.

Resistance Unit (RU): Resistance to burglary demonstrated when a tool with coefficient 1 and basic value 0 is used for one minute.

Roller blind: Facade element, normally made of linked moveable segments, usually arranged horizontally, which is rolled via a shaft to open or close it.

Room-in-room system (German term "Raum-in-Raum-System"): see **Strongroom**

Room with additional security features: see **Strongroom**

S_0: Technical name for the interface at the NT network termination point of an ISDN standard connection. Deutsche Telekom calls this "Basic rate interface". The S_o access point has two B-channels for actual communication and a D-channel for setting up, clearing down and controlling the connections. The S_o interface can be used

- as a BUS for connecting several devices, e.g. telephones, fax machines. The two B-channels allow a maximum of two devices to communicate independently over the network (multiple devices access or point-to-multi-point access),
- as an interface to a Private automatic branch exchange – PABX (system or point-to-point connection).

S_0-BUS: The S_0-BUS is one of the both technical performances of a basic rate interface. Up to 8 ISDN end-devices of different functionability may be connected to the S_0-BUS. Each device may be contacted from outside directly. Two of the maximum 8 devices may be active at the same time at the BUS i.e. to raise a connection or to perform a connection with an external partner.

S_0-Interface: Four-wired connection facility for ISDN terminal devices (ISDN telephones, ISDN PC cards, etc.) on the ISDN basic access.

S_0-„point to point": If a ISDN-PABX (Private automatic branch exchange) is intended to be operated at a basic rate interface, the functionability of the BUS is not necessary. Therefore the connection-point of Telecom directly (point-to-point) is directly connection to the PABX. ISDN and analog end-devices are connected to the PABX. The S_0-connection serves in this case only as connection to the network and not as distributor.

S_{2M}-connection (interface): S_{2M} is the technical description of a ISDN primary multiplex connection ISDN is also called 2 Mbit connection. The S_{2M}-connection offers 30 communication paths (B-channels) and one signalling path (D-channel). Same as in the S_0-connection up to 30 communication channels may transmit information; the signalling path serves for transmission of the relevant data (dialling information, set-up, fees and closing down).

Safe: Security container qualified according harmonized European standards. These containers perform an overall defined protection against intrusion/burglary and are intended for the storage of cash and valuables and are offered in security grades (resistance units) N ... X. They are equipped with qualified locks and may also be equipped with special protection against diamond core drills (CD) and explosives (EX). Delivered safes are completely serviceable – if given with anchorage against fast removal and are identifiable by a conformitiy mark (label).

Remark: In Germany the core drill protection „CD" was called „KB" (= Kernbohrschutz) until now.

Safe for cash dispensers: see **Safes for ATM**

Scanning connection: Physical or logical connection which is regularly available after setup or dial-up for transmitting signals/messages or for monitoring the connection.

Secondary battery: (accumulator) Galvanic cell, were chemical energy is converted into electrical energy. During this energy conversion the cell will be discharged; a secondary battery is rechargeable.

Secondary line (German term "Sekundärleitung"): Non-monitored transmission line.

Security company: Company which performs guarding and security services for protection of life and property.

Security container (German term "Wertbehältnis"): Strongrooms and safes for protection against intrusion.

Security corridor: Walking around a strongroom for control/surveillance purposes.

Security impairing: An effect is security impairing when the security function of an IAS is reduced.

Security jeopardizing: An effect (e.g. malfunction) is security jeopardizing when the security function of an IAS is put at risk but not reduced.

Security relevant function: Function where a certain influence (e.g. tampering, operating error) can have security jeopardizing effect.

Security-upgrade, mechanical: Improving the mechanical security features of windows, doors and other closing devices after installation.

Self-service safe: see **Deposit-box system**

Semi-automatic deposit-box system: see **Deposit-box system**

Setting, external: Switching the IAS or parts of the system to the external or remote alarm signalling devices.

Setting, internal: Switching the system or parts of the system to the internal alarm signalling devices.

Semi-professional: Person with specialist knowledge (e.g. fitter, precision engineer, electronics engineer) with access to high-quality tools (e.g. CNC lathe, oscilloscope).

Sensor: Component which converts physical parameters, e.g. into electrical signals.

Separate circuits for the locked state monitoring: Interconnections for informations resp. signals/messages of the locked state monitoring (e.g. from stroke plate contacts).

Separated protected premises: Part of a protected premises which has no geographic connection to the rest of the protected premises; it has to be controlled separate by the "Zwangsläufigkeit" of the IAS.

Separate route: see **Different route**

Signal: Physical embodiment of a message/information.

Silent alarm signalling: see **Remote alarm**

Shell protection: Surveillance of all access points, windows and all other openings as well as walls, ceilings and floors.

Shielded lines: see **Non-shielded lines, Partially shielded lines, Fully shielded lines**

Signal (message): The information given by a system component. A distinction is made between alarms signals, fault signals and status signals.

Simple container: Container which does not have any additional security features, e.g.

- single-walled steel cabinet,
- iron office cabinet,
- desk,
- other items of furniture, cassettes.

Single-walled steel cabinet: Simple container meeting at least the minimum requirements set out in VDMA 24 992 (security level A).

Small strongroom (German term "Kleintresorraum"): A room protected against intrusion with a solid construction in accordance with the recommendations for the building of strongrooms issued by the Research and Testing Association for Safes and Strongrooms (Forschungs- und Prüfgemeinschaft Geldschränke und Tresoranlagen e. V. or FuP) and sealed with a strongroom door meeting RAL-RG 622 (security level LT0).

Smoke generating device: Additional equipment triggered by an intruder alarm system, which impedes sight by producing aerosols in order to impede the penetrator in his intention.

Software: Programs for the control of hardware.

Specialist: Person with specialist knowledge and professional experience (e.g. key service, intruder alarm system installation engineer), who has specialist tools (e.g. locking tools).

Staff-operated cash dispenser (German abbreviation "BBA"): Device installed inside the premises of a bank which allows only bank staff to withdraw a sum of money from a container after carrying out an entry. The amount of money and the frequency of payouts are limited.

Formerly known in Germany as: "Automatischer Kassentresor (AKT)"

Stand-by-smoke generating device: All functions of the smoke generating device are available and no faults are known; once activated the smoke generating device is immediately able to be triggered in the case of an alarm.

Standby supply generator: Converts the mechanical energy of a drive unit into electrical energy.

Standby supply system: System which supplies electric power in the event of a mains failure.

Status detector: Detector which monitors the status of objects (e.g. closed status of window, doors, gates).

Status signal: Signalling of the activation of status detectors (e.g. striking plate contacts).

Striking plate contact: Device on the striking plate, e.g. contact or sensor, which is operated when the lock is secured using the bolt.

Strongroom: Security container which protects its contents against burglary and which has internal sides each over 1 m in length when closed.

Note: Strongrooms can be built in a solid construction or using entirely pre-prepared components (modular construction) or as a combination of the two (hybrid construction).

Remark: In the past, strongrooms were built in accordance with building standards. In the interests of completeness, the terms used to describe these rooms are listed below.

Small strongroom (German term "Kleintresorraum"): A room constructed on-site and protected against burglary with a solid construction in accordance with the recommendations for the building of strongrooms issued by the Research and Testing Association for Safes and Strongrooms (Forschungs- und Prüfgemeinschaft Geldschränke und Tresoranlagen e. V. or FuP) and sealed with a strongroom door meeting RAL-RG 622 (security level LT0).

Armoured strongroom (German term "Panzerraum"): A room protected against intruder which is an independent construction assembled on-site from pre-prepared components (room-in-room system) and which is sealed using a strongroom door. The pre-prepared components, assembly elements and strongroom door shall meet the requirements of RAL-RG 625/5.

Strongroom (Old German term "Tresorraum"): A room protected against burglary which is sealed with a strongroom door and which is available in the following designs:

- Small strongroom („Kleintresorraum")
- RAL-RG 622/1 (security level LT1, LT1KB), (security level LT0)
- RAL-RG 623/10 (security level T10, T10KB, T10EX, T10KBEX), (security level T1)
- RAL-RG 624/20 (security level T20, T20KB, T20EX, T20KBEX), (security level T2)

Strongrooms complying with RAL-RG 622/1, RAL-RG 623/10 and RAL-RG 624/20 are built in the following designs:

- In solid construction, if necessary using pre-prepared security elements, built on-site,
- Assembled on-site as a room-in-room system (or container safe) using pre-prepared components to form an independent construction,
- Built in solid construction according to the recommendations of the Research and Testing Association for Safes and Strongrooms (FuP) for the building of strongrooms of security levels LT0, T1 and T2 and subsequently reinforced using pre-prepared security elements (upgrade systems).

Small strongrooms and strongrooms of security levels LT0, T1 and T2 are built on-site in solid construction according to the recommendations of the FuP for the construction of strongrooms, and are sealed using the appropriate strongroom doors complying with RAL-RG 622, RAL-RG 623 or RAL-RG 624.

Strongroom door: Door with one or more locks, a bolting mechanism and a frame, which is intended as an access point to a strongroom.

Strongroom of solid construction: Strongroom walls of solid construction are built on-site in concrete by moulding (pouring the concrete into the framework) pre-prepared security elements (alarm signalling elements). The strongroom is sealed by the strongroom door and its pre-prepared frame.

Strongroom of modular construction: Strongroom walls of modular construction consist entirely of pre-prepared security elements which are assembled on-site to form an independent construction (room-in-room system). The strongroom is sealed by the strongroom door and its pre-prepared frame.

Strongroom of hybrid construction: Strongroom walls built using a combination of solid and modular construction techniques. The strongroom is sealed by the strongroom door and its pre-prepared frame.

Supply output: Output of the power supply device to which the power consumers (e.g. Control and indicating equipment – CIE, intruder detectors) are connected.

Surface surveillance: Surveillance of surfaces (e.g. walls) against persons entering and/or reaching in.

Surveillance: The term surveillance is used for the following features of an IAS:

- Surveillance of movements in a room, a window or a door of opening, an object against removal and similar
- Surveillance of availability of a function and – if given – correct operation
- Surveillance of availability of components
- Surveillance of availability of interconnections and – if given – transmission functionality

Surveillance against removal: Surveillance function of an IAS which detects and signals the removal of an object (e.g. painting, safe).

Surveillance area: Area covered by an intruder detector.

Sub-receiving centre transceiver (Sub-RCT): Processing unit for the concentration, handling, conversion and processing of signals/messages and control signals. The unit may also serve as a connection between two different networks. In the signal (alarm) direction (ATE $\Rightarrow$ alarm receiving equipment – ARE), the sub-receiving centre transceiver (Sub-RCT) has an S_3 interface at the input and an S_2 interface at the output.

Switched Virtual Call (SVC): Connection (dialup line) which is set up when required and then cleared down again when no longer needed.

Switched Virtual Call-Permanent (SVC-P): Connection (dialup line) which is set up when required and remains in existence when no longer needed.

Symmetrical injection (differential mode): Non-earthed injection of the interferences between conductors.

Synchronous network: Network with a tree-like structure and a central processor plus a processor on each branch. It is polled from above and at the same time polls all the participants or branches below it. Application: “SNA network”

System: Technical implementation of a system (that means an installed and functioning system)

System component: Part of an intruder alarm system, e.g. Control and indicating equipment (CIE), detectors, alarm signalling equipment, installation accessories, line network.

System class: A system differing from systems of another class by e.g. its performance characteristics.

System connection (German Term “Anlagenanschluss“): ISDN basic access for connecting a single telecommunications equipment, generally a telecommunications system with direct call capability.

System Network Architecture (SNA network): Company-specific synchronous data network.

System owner: The system owner is the person holding an approval for an intruder alarm system concept (IASC). This does not automatically have to be the manufacturer of the components of IASC as well.

System voltage: Voltage supplying the power supply required to operate the alarm system.

TA X.25D: A terminal adapter which is able to connect a data end device or a knot to understand and transmit data packages with the datex-p in D-channel of an ISDN basic rate interface.

Tamper contact: Contact for monitoring covers or removable casing parts of system components.

Tamper release: In contracy to the function blockade release which affects against the internal occupation of a connection the function tamper release enforces a transmission of a signal/message even in case of a tamper attempt as e.g. a permanent dialling of the connection.

Tamper security: Entirety of all the measures required to protect against deliberate attempts to interfere with the normal functioning of the intruder alarm system.

Tamper signal: Signal signifying that surveillance elements have been activated (e.g. because casings have been opened or penetrated).

Tear-off detector: Detector which detects the removal of an object (e.g. safe) at an early stage, before a defined mechanical resistance of a mechanical security device is overcome.

Technical detectors: Detectors of an alarm system which serve for an early detection of hazardous statuses e.g. overriding/falling below temperatures, deviations of rated values of machines etc.

Telecommunications connection unit (German abbreviation TAE): Sockets commonly used in Germany to connect analogue terminal devices to the traditional (analogue) telephone network.

Telephone dialling device (German term "Telefonwählgerät – TWG"): Telephone dialling devices transmit signals/messages automatically via non-monitored transmission paths (e.g. the telephone switching network of Deutsche Telekom). Depending on the manner in which the telephone dialling device works, a distinction is made between digital diallers and diallers with voice announcement.

Note: This term is outmoded, see ***Alarm transmission equipment (ATE)***

Television surveillance system: see Video surveillance system

Terminal adapter (TA): Communications device which adapts equipment using other transmission methods to a ISDN S_0 basic access, e.g.:

- Terminal adapter a/b for adapting analogue telephone service devices
- Terminal adapter V.24 for adapting devices with V.24 interface
- Terminal adapter X.25 for adapting devices which process package-based data using X.25.
- Terminal adapter X.30 for adapting devices with V.110 interface
- Terminal adapter X.75 for adapting devices with HDLC procedure

Terminating element: Component such as a end-of-line resistor which is usually located at the end of the monitored transmission path and is required for monitoring its lines.

Testing: Technical procedure representing the determination of one or several values of a certain product, procedure or a service and is to be performed according to the described procedure.

Test signal: Signal which does not contain any operational information (e.g. alarm signal) and which is used to test the transmission path and availability.

Third-party signal: Signals which are neither belong to the system nor to the installation.

Third-party signal recognition: Function of an IAS which detects and notifies the presence of third-party signals on interconnections.

Threat signal: Special type of a hold-up signal, which can, for example, be triggered without attracting attention by a person operating an IAS who comes under threat. The alarm is triggered e.g. by using an ancillary control equipment (ACE) and results independently of the status of the IAS in remote signalling.

Through access: Opening in the boundaries of a protected premises (e.g. door in a wall) for the intended access.

Time-controlled function: Physical and/or electrical device which blocks the bolt work of doors of safes and strongrooms for a definite time.

Time lock safe: Day-safe-quality safes with one or more compartments with time locks. Each compartment can be activated individually or several compartments can be activated simultaneously after the programmed delay periods. The use of time lock containers is particularly recommended for bullet-resistant and penetration-resistant counters for securing stocks of bank notes exceeding the permissible quantities of accessible bank notes. For use in offices using staff-operated ATM it is particularly recommended to use a time lock safe as an ergonomically positioned drawer with pre-sorter and several compartments for prepared stocks of bank notes and foreign currencies.

Transfer-safe: Safe with two doors intended for the controlled handover of valuables between two zones (e.g. supply with and collection of money of a bank by a value transport company). For organisational and/or security relevant reasons the valuables shall be included in additional deposits.

Transmission path (in alarm transmission system): Logical connection between interfaces S_2 and S_3.

Transmission system for alarm signals (German term "Übertragungsanlage für Gefahrenmeldungen – ÜAG"): System which picks up alarms from alarm systems, passes them on via monitored transmission lines and notifies them to an alarm receiving centre.

*Note: This term is outmoded, see **Alarm transmission system***

Transportable (mobile) system components: System components which occasionally change location; proper functioning is **not** expected while the components are being moved (e.g. personal computers, printers).

Trap protection: Surveillance of areas (e.g. using motion detectors) which have an increased probability of being entered by perpetrators.

Triggering of a smoke generating device: The smoke generating device emits the smoke, therefore the smoke generating device has to be activated and been triggered by the IAS in the case of an alarm.

Typical (robbery) Hold-up: A Hold-up of a bank is described as typical if perpetrators threaten banking staff or customers on the premises of the bank during customer banking hours with the aim of taking money or forcing persons to hand money over.

Uninterrupted power supply: Provides power for a limited period of time in the event of mains failure, without connected power consumers being affected in their operations.

Unset (status): Status of the intruder alarm system in which intruder or tampering signals **do not** lead to external and/or remote alarms.

Unsetting, external: Reversing the status in which the IAS or parts of the system are switched to the external or remote alarm signalling devices.

Unsetting, internal: Reversing the status in which the intruder alarm system or parts of the system are switched to the internal alarm signalling devices.

Up_0 and Uk_0: All S-interfaces (S_0 and S_{2M}) are 4-wire-interfaces if copper wires are used for the transmission. U-interfaces are 2-wire-interfaces in copper-wire-networks. P stands for „Ping Pong“ and K for „Compensation“. As sending and receiving devices are no more linked to copper wires on 2-wires-interfaces, the direction of the data-stream „sending and receiving“ shall be fixed differently. The expression „Ping Pong“ here describes the vice-versa-transmission similar to intercom systems: one time one side is sending and the other is receiving and at the next fixed time vice versa (like as „Ping Pong“).

For K = compensation procedure both sides do send and receive at the same time. Each side filters those data from the data-stream which were sent by itself; such way the receiving data are available as net data. Each side compensates such from the data-stream the own data and knows like that what the other side has sent.

User-to-user-info: ISDN offers a feature “user-to-user-info”. If this feature is activated, it is possible to transmit a short information to the B-participant within a connection, which may be confirmed by the A-participant to the B-participant. This short exchange of information is possible only during the set-up of the connection and is transmitted as data sentence in the signalling channel (D-channel).

This function is only specifies as a „an conversation accompanied service“, this means that an user-to-user-info has to be followed by at least one telephone conservation charged with one charge-unit. Furtheron the function is only possible when a free B-channel is available during the begin of the “dialling function”. If both B-channels are occupied by others each further connection attempt will be rejected by the telecommunication office and therefore an user-to-user-info is not possible.

UVV “Kassen” (German Accident Prevention Regulations for Banks): Independent legal standard of the German statutory accident insurance companies, for example the Administrative Employment Accident Insurance Fund (Verwaltungs-Berufsgenossenschaft) and the Statutory Accident Insurance Fund for the Prevention of Occupational Accidents and Work-Related Health Risks (GUVV zur Verhütung von Arbeitsunfällen und berufsbedingten Gesundheitsgefahren). Standard BGV C 7 resp. VBG 120 of the German Accident Prevention Regulations for Banks require that, for the protection of the insured staff, bank notes be secured in such a way that the temptation to make Hold-up attempts is sustainably reduced. It constitutes an obligation to companies when building and equipping premises and drawing up regulations, and obliges the insured to use the premises in accordance with the provisions and to comply with the instructions of their employer.

Valuables: Valuables include e.g.:

a) cash

b) certificates incl. savings books and other valuable documents

c) items of jewellery, precious stones, pearls, stamps, telephone cards, coins and medals and any item made of gold or platinum

d) furs, hand-made carpets and tapestries, works of art (e.g. paintings, collages, drawings, graphics and sculptures) and any objects made of silver and not covered by c) above

e) other items over 100 years old, with the exception of items of furniture

VdS-approved: VdS-approved products and services are fire protection and security technology products and services which have been tested and certified (approved) according to technical standards. Products and services are continually surveilled by the VdS (product surveillance). Manufacturers and service providers are also required to have a certified quality management system complying with DIN EN ISO 9000ff.

VdS rules: Technical and procedural rules for fire protection and security technology products and services. VdS rules are drawn up by the competent technical committees of the Gesamtverband der Deutschen Versicherungswirtschaft – the German Insurance association – (GDV) in close cooperation with associations and organisations in the field, the authorities, national and international bodies and the fire brigade and police.

VdS Schadenverhütung (VdS): (German) organization whose activities include the development of fire protection and security technology concepts and the testing and certification (approval) of products and services.

Vibration contact: Electromechanical vibration detector with a contact in the sensor.

Vibration detector: Intruder detector which recognises the vibrations occurring in a surface under surveillance during penetration or attempted penetration, and triggers an alarm.

Video motion detector: A device which triggers an alarm signal as a response to changes in prescribed image contents.

Video surveillance system: Installation consisting of hardware and software components of a video surveillance system concept, completely installed and in operation function for surveilling of a determined protected premises.

Volume-based surveillance characteristic: Characteristic of an intruder detector which identifies and evaluates changes in physical parameters within a volume, e.g. inside a room, (e.g. ultrasound motion detector).

Volumetric surveillance: Three-dimensional complete or partial surveillance of a protected premises, for example using motion detectors.

Wall-integrated steel wall cabinet with multiple-walled door: see **wall-mounted safe**

Wall-mounted cabinet (German term “Einmauerschrank“): A wall-integrated cabinet is a container with single steel walls and a multiple-walled door complying with security level B of VDMA 24 992 as a minimum. The container shall be firmly anchored in the wall or floor and shall not jut out. All side walls and the back wall shall be encased in a concrete sheath at least 100 mm thick.

Walls of exceptionally solid construction: Walls made of the following materials, the solidity, thickness, etc. of which provide increased resistance to entry by force:

- stone (e.g. brick, chalk sandstone, cavity block) more than 240 mm thick
- concrete more than 200 mm thick

Walls of light construction: Walls made of the following materials, the solidity, thickness, etc. of which do not provide sufficient resistance to entry by force:

- light construction panels, e.g. made of plasterboard
- wood products, wood (boards, sheets)
- sandwich panelling
- plastics
- profiled panels, corrugated panels
- clay (in half-timbered design)
- glass blocks, profiled construction glass
- foam concrete
- stone (e.g. brick, chalk sandstone, cavity block), including half-timbering design, up to 120 mm thick
- concrete up to 100 mm thick

Walls of solid construction: Walls made of the following materials, the solidity, thickness, etc. of which provide sufficient resistance to entry by force:

- stone (e.g. brick, chalk sandstone, cavity block), including half-timbering design, more than 120 mm thick
- concrete more than 100 mm thick

Wall-safe: Safe with burglary protection partly provided by materials built in or added during assembly and the way these materials are constructed.

Note: Floor-installed safes are one example of specialist forms of wall-safes.

Warning device: Alarm signalling devices which generate visible and/or audible signals.

Warning signal: Signal, that a given threshold (e.g. at a voltage, field strength) exceeded or felt below.

“Wertschrank” (Strongbox for valuables): Multiple-walled container weighing at least 300 kg and fulfilling the requirements of RAL-RG 626/2. Strongboxes are manufactured in types C 1 and C 2.

Note: This term is outmoded

Western plug: see **IAE**

Window lock fitting: Fixed and moveable parts mounted onto frames and panes which

X.25: Collective term for a packet-based data transmission procedure. The data is packed into standardised packets, which are sent one after the other and independently of one another through the network, maybe via different routes, and are assembled by the recipient to restore the original information. In colloquial terms, the term X.25 encompasses various CCITT recommendations: incl. X.3, X.25, X.28, X.29, X.31, X.75. X.25 is actually only the description of the interface to a packet-based data network.

Example: “Datex-P” from Deutsche Telekom.

X.25 in the D-channel: Alternatively to the connection over separate Datex-P10H-connections German Telekom offers since 01.09.1994 an transfer from the ISDN-network into the Datex-P-network or other (private) X.25 nets, in which the basic connection with DSS1-protocol at the same time represents a fixed connection between participant and net transfer. The transmission rate is 9600 Bit/s.

Zone: All the detectors in a zone (area) for which a dedicated display is available for the signals in the control and indicating equipment, the aim being to identify the detector location.

Zone (area): Sections of a building (e.g. rooms) which serves to clearly identify the sources of signals/messages.

„Zwangsläufigkeit“: Measure which prevents an IAS from being set when not all its components are fully functional or which prevents the operator of an set IAS from accidentally triggering an external alarm (e.g. by entering the room without first unsetting).

- **Construction-based “Zwangsläufigkeit“:** All the construction-based measures taken to maintain “Zwangsläufigkeit“, e.g. special blocking locks, exterior doors which can be closed from one side.
- **Electrical „Zwangsläufigkeit“:** All the electrical measures taken to maintain “Zwangsläufigkeit”, e.g. fastening surveillance of exterior doors, electrical bolting of blocking decives in an set IAS, blocking of the blocking decive when the IAS is not fully functional.
- **Organizatorical „Zwangsläufigkeit“:** All the organisational measures taken to maintain „Zwangsläufigkeit“, e.g. monitoring entry and exit of persons.

3.2 Abbreviations

3.2.1 German abbreviations

AE **A**larm**e**mpfangseinrichtung

ASCII **A**merican **S**tandard **C**ode for **I**nformation **I**nterchange

AKT **A**utomatischer **K**assen**t**resor (veraltet)

AÜA **A**larm**ü**bertragungs**a**nlage

AWAG **A**utomatisches **W**ähl- und **A**nsage**g**erät

AWE **A**us**w**erte**e**inrichtung von Schalteinrichtungen

AWUG A**utomatisches** W**ähl- und** Ü**bertragungs**g**erät**

BBA **B**eschäftigtenbedienter **B**anknoten**a**utomat

BE **B**edien**e**inrichtung

BMA **B**rand**m**elde**a**nlage

CCIR **C**omité **C**onsultatif **I**nternational des **R**adiocommunication

CCITT **C**omité **C**onsultatif **I**nternational **T**élégraphique et **T**éléfonique

CCTV **C**losed **C**urcuit **T**ele**v**ision

DCS **D**igital **C**ommunications **S**ystems

DIN **D**eutsches **I**nstitut für **N**ormung

EH **E**inbruch**h**emmung

EMA **E**inbruch**m**elde**a**nlage

EMC **E**lectro**m**agnetic **C**ompatibility

EMS **E**inbruch**m**elde**s**ystem

EMZ **E**inbruch**m**elder**z**entrale

EN **E**uropäische **N**orm

ETSI **E**uropean **T**elecommunications **S**tandardization **I**nstitute

EXVO **Ex**plosionsschutz**v**er**o**rdnung

FSE **F**rei**s**chalt**e**lement

FSK **F**euerwehr**s**chlüssel**k**asten

FuP **F**orschungs- **u**nd **P**rüfgemeinschaft Geldschränke und Tresoranlagen e. V.

GAA **G**eld**a**usgabe**a**utomat

GLT **G**ebäude**l**eit**t**echnik

GMA **G**efahren**m**elde**a**nlage

GSM **G**roup **S**pecial **M**obile

GUV **G**emeinde-**U**nfallversicherungs**v**erband

IAE Bezeichnung der ISDN-Steckverbindung

IM **I**dentifikations**m**erkmal

IMT **I**dentifikations**m**erkmal**t**räger

IS **I**nterventions**s**telle

ISDN **I**ntegrated **S**ervices **D**igital **N**etwork

ISO **I**nternational **S**tandardization **O**rganization

ITU **I**nternational **T**elecommunication **U**nion

KG **K**ommunikations**g**erät

NA **N**etz**a**bschluss

NSL **N**otruf- und **S**ervice-**L**eitstelle

NT **N**etz**t**erminator

ORÜA **O**ptische **R**aum**ü**berwachungs**a**nlage

OSI **O**pen **S**ystems **I**nterconnections

PAD **P**acket **A**ssembler/**D**isassembler

PC **P**ersonal **C**omputer

PCM **P**uls **C**ode **M**odulation

PIN **P**ersönliche **I**dentifikations**n**ummer

PVC **P**ermanent **V**irtual **C**ircuit

QM **Q**ualitäts**m**angement

QS **Q**ualitäts**s**icherung

RAL früher **R**eichs**a**usschuss für **L**ieferbedingungen und Gütesicherung, heute: Deutsches Institut für Gütesicherung und Kennzeichnung e.V.

RU **R**esistance **U**nits

SD **S**chlüssel**d**epot

SDA **S**chlüssel**d**epot**a**dapter
SNA **S**ystem **N**etwork **A**rchitecture
SpE **Sp**err**e**lement
SÜZ **S**ub-**Ü**berwachungs**z**entrale
SVC **S**witched **V**irtual **C**all
SVC-P **S**witched **V**irtual **C**all-**P**ermanent
TA **T**erminal**a**dapter
TAE **T**elekommunikations-**A**nschluss**e**inheit
TK **T**ele**k**ommunikation
TNT **T**ag-/**N**acht-**T**resoranlage
TWG **T**elefon**w**ähl**g**erät
ÜG **Ü**bertra**g**ungsgerät
ÜMA **Ü**berfall**m**elde**a**nlage
UMTS **U**niversal **M**obile **T**elecommunications **S**ystem
Up_0 2-Drahtschnittstellen in Kupfernetzen, „P“ steht für „Ping Pong“
Uk_0 2-Drahtschnittstellen in Kupfernetzen, „K“ steht für „Kompensation“
USV **U**nterbrechungslose **S**trom**v**ersorgung
UVV **U**nfall**v**erhütungs**v**orschrift
ÜZ **Ü**berwachungs**z**entrale
VBG **V**erwaltungs**b**erufs**g**enossenschaft
VdS VdS Schadenverhütung
WWW **W**orld-**W**ide **W**eb
X.25 Sammelbezeichnung für eine paketorientierte Datenübertragung
ZE **Z**ugangs**e**bene
ZKA **Z**utritts**k**ontroll**a**nlage
ZKS **Z**utritts**k**ontroll**s**ystem

3.2.2 English abbreviations

ACE **A**ncillary **c**ontrol **e**quipment
ACS **A**ccess **c**ontrol **s**ystem
ACSC **A**ccess **c**ontrol **s**ystem **c**oncept
AE **A**nnunciation **e**quipment
AFDS **A**utomatic **f**ire **d**etection **s**ystem
AL **A**ccess **l**evel
ARC **A**larm **r**eceiving **c**entre
ARE **A**larm **r**eceiving **e**quipment
AS **A**larm **s**ystem
ASCII **A**merican **S**tandard **C**ode for **I**nformation **I**nterchange
ATE **A**larm **t**ransmission **e**quipment

ATM **A**utomatic **T**eller **M**aschine

ATS **A**larm **t**ransmission **s**ystem

BMT **B**uildings **m**anagement **t**echnology

CCIR **C**omité **C**onsultatif **I**nternational des **R**adiocommunication

CCITT **C**omité **C**onsultatif **I**nternational **T**élégraphique et **T**éléfonique

CCTV **C**losed **C**urcuit **T**ele**v**ision

CIE **C**ontrol and **i**ndicating **e**quipment

DCS **D**igital **c**ommunications **s**ystems

DDV **D**ata **D**irect **C**onnection

EMC **E**lectro**m**agnetic **C**ompatibility

EN **E**uropean **N**orm (standard)

ETSI **E**uropean **T**elecommunications **S**tandardization **I**nstitute

GSM **G**roup **S**pecial **M**obile

HUAS **H**old-**u**p **A**larm **S**ystem

IAE IAE is the name for the ISDN plug connection

IAS **I**ntruder **a**larm **s**ystem

IASC **I**ntruder **a**larm **s**ystem **c**oncept

I-CIE **I**ntruder **c**ontrol and **i**ndicating **e**quipment

IC **I**ntervention **c**ompany

ID **Id**entification feature

ISDN **I**ntegrated **S**ervices **D**igital **N**etwork

ISO **I**nternational **S**tandardization **O**rganization

ITU **I**nternational **T**elecommunication **U**nion

NT **N**etwork **t**erminator

NTP **N**etwork **t**erminator **p**oint

MTBF **M**ean **T**ime **B**etween **F**ailures

OSI **O**pen **S**ystems **I**nterconnections

PAD **P**acket **A**ssembler/**D**isassembler

PAXB **P**rivate **a**utomatic **b**ranch **e**xchange

PC **P**ersonal **C**omputer

PCM **P**uls **C**ode **M**odulation

PIN **P**ersonal **I**dentification **N**umber

PSU **P**ower **s**upply **u**nit

PVC **P**ermanent **V**irtual **C**ircuit

QM **Q**uality **m**anagement

RCT **R**eceiving **c**entre **e**quipment

RU **R**esistance **U**nits

SNA **S**ystem **N**etwork **A**rchitecture

Sub-RCT **Sub-R**eceiving **c**entre **e**quipment

SVC **S**witched **V**irtual **C**all

SVC-P **S**witched **V**irtual **C**all-**P**ermanent

TA **T**erminal**a**dapter

TK **T**ele**k**ommunikation (Telecommunication)

UMTS **U**niversal **M**obile **T**elecommunications **S**ystem

VdS **VdS** Schadenverhütung (VdS Loss Prevention)

WWW **W**orld-**W**ide **W**eb

X.25 Collective term for a packet-orientated data transmission

4 Classification

4.1 Performance

Class A intruder alarm systems

have basic protection against attempts to bypass them when set and unset; the detectors have a medium level of sensitivity.

Class B intruder alarm systems

have medium protection against attempts to bypass them when set and unset; the detectors have a medium level of sensitivity.

Class C intruder alarm systems

have enhanced protection against attempts to bypass them when set and unset; the detectors have an enhanced level of sensitivity. Advanced monitoring of security-related functions is provided.

4.2 Comparison of DIN EN 50 131-1 to DIN VDE 0833 and VdS requirements

The requirements for VdS-approved IAS correspond to the requirements in the standards DIN EN 50131-1, DIN VDE 0833-1 and DIN VDE 0833-3.

A detailed comparison of the respective classes and security grades can be found in the guidelines VdS 3134-2.

4.3 Environmental behaviour

Because IAS are exposed to different environmental influences depending on their location, the requirements placed on the systems in terms of their environmental behaviour differ accordingly.

Note: See also Rules for Intruder Alarm Systems, Protection against Environmental Influences and Testing Methods, VdS 2110.

A distinction is made between the following environmental classes:

Environmental class I: Conditions in well-kept and air-conditioned indoor areas

(δ_{min} = 5 °C, δ_{max} = 40 °C, relative air humidity ≤ 75 %, for 30 days per year 95 %, on the remaining days temporary 85 %).

Corresponds to DIN IEC 721-3-3 : 1990-04.

K	Climatic environment	3K3
Z	Additional climatic requirements	3Z1
B	Biological environment	3B1
C	Chemically active substances	3C2
S	Mechanically active substances	3S1
M	Mechanical environment	3M2

Environmental class II: Conditions in indoor areas (e.g. stairwells)

(as I, but with additional environmental influences – e.g. condensation on windows)

Corresponds to DIN IEC 721-3-3 :1990-04.

K	Climatic environment	3K5
Z	Additional climatic requirements	3Z1
B	Biological environment	3B1
C	Chemically active substances	3C2
S	Mechanically active substances	3S2
M	Mechanical environment	3M3

Environmental class III: Conditions outdoors, but weather-protected

(δ_{min} = -25 °C, δ_{max} = 60 °C, relative air humidity ≤ 75 %, for 30 days per year 95 %, on the remaining days temporary 85 %).

Corresponds to DIN IEC 721-3-3 :1990-04.

K	Climatic environment	3K6
Z	Additional climatic requirements	3Z4, 3Z8
B	Biological environment	3B1
C	Chemically active substances	3C3
S	Mechanically active substances	3S3
M	Mechanical environment	3M4

Environmental class IV: Conditions outdoors, fully exposed to the elements

(δ_{min} = -25 °C, δ_{max} = 60 °C, relative air humidity ≤ 75 %, for 30 days per year 95 %, on the remaining days temporary 85 %).

Corresponds to DIN IEC 721-3-3 :1990-04.

K	Climatic environment	4K2
Z	Additional climatic requirements	4Z1, 4Z3, 4Z7
B	Biological environment	3B1
C	Chemically active substances	4C3
S	Mechanically active substances	4S3
M	Mechanical environment	4M4

Note: DIN IEC 721 is listed here merely to describe the environmental conditions.

5 Requirements

5.1 General

Intruder alarm systems (IAS) convert the physical parameters typical of an intrusion or an attempted intrusion into electrical signals, evaluate these signals and notify the intrusion or attempted intrusion as external alarm to an assistance provider such as the police, a guarding and security company or, in exceptional circumstances, via local audible and visible warning devices to the anonymous public.

If an IAS is to reliably signal hazards while remaining largely immune to false alarms, it shall fulfil particularly stringent requirements.

5.2 Function requirements

5.2.1 Basic functions

For a safe detection and signalling of intrusions/intrusion attempts IAS shall fulfil the following basic functions:

Detection – for detecting intrusions/intrusion attempts early.

Processing – for controlling and monitoring all processes within an IAS.

Output (Notification/Indication) – for delivering all relevant information and for initiating risk-reducing measures.

Operation – for enable the operation and parametration.

Furthermore a **Power supply** is necessary.

5.2.2 Protection functions

For a safe and reliable function the IAS shall fulfil the following protection functions:

Operational reliability as the entirety of all measures to ensure the correct operation of the IAS by preventing operating errors.

Functional reliability as the entirety of all measures to ensure uninterrupted operation of a system in accordance with requirements and to identify faults.

Tamper protection as the entirety of all measures to protect against deliberate attempts to interfere with the normal functioning of the IAS.

Environmental resistance as an quality of an IAS to resist environmental influences and to function correctly within defined limits.

5.3 DIN VDE standards

IAS shall, as a minimum, comply with the regulations of DIN VDE 0100, VDE 0800, DIN VDE 60 950 resp. 60 065. IAS of **classes B and C** shall also comply with DIN VDE 0833-1 and -3.

5.4 Marking

System components shall be clearly and durable marked with the name or symbol of the manufacturer and the type name. Where the size and shape of system components permit, the following data shall also be shown:

- Series marking,
- Time of manufacture (month, year),
- Electrical data, e.g. operating voltage, current consumption.

In addition, VdS-approved system components shall be marked externally as follows:

or VdS

If the required data cannot or cannot fully be marked on the component, it shall appear on the packaging of the system component or in an instruction sheet provided with the packaging. It shall nevertheless be possible to identify system components clearly.

5.5 User safety

System components of IAS shall be constructed in such a way that their use does not pose any hazard to the operator (user).

5.6 Requirements of the authorities

If system components (e.g. radio transmission systems) require a licence from the competent authorities, this licence shall be available.

6 Test methods

6.1 Prior conditions

6.1.1 Ambient conditions for tests

Unless otherwise stated in the rules governing the system component to be tested, all tests shall be carried out under the following environmental conditions:

- Temperature 15 ... 35° C
- Relative air humidity 45 ... 75 %
- Air pressure 86 ...106 hPa

6.1.2 Test setup

Tests are only carried out on complete and fully functional system components. The connections required for correct functioning (e.g. displays) shall be available or replaced by simulations. Deviations from this rule may be agreed in individual cases.

6.1.3 Documents

As a general rule, the following documents are required for tests:

- Technical data
- Circuit diagrams
- Part lists
- Equipment plans
- Description of major functions
- Operating instructions
- Installation and mounting instructions

6.1.4 Number of test samples

The manufacturer shall provide the number of devices required for testing purposes, as specified in the testing methods for the specific system components.

6.1.5 Determination of the test extent

If system components can fulfil functions other than those set out in the rules for the system components (for example through re-programming), the status (programming) in which the test is to take place shall be clearly established prior to the test.

6.2 Test matrix

The assignment of test samples to the individual tests is set out in the individual rules with the testing methods for the system components.

6.3 Initial inspection

A check is made to ensure that

- the system component has been provided in the correct design and is fully equipped for the test,
- all the necessary connections are present and the documents required by clause 6.1.3 are complete and in German language and are sufficient for the purposes of the test,
- the system component works and all the functions described in the operating instructions are fulfilled.

6.4 DIN VDE standards

The system components are tested in accordance with the requirements of DIN VDE 0100, DIN VDE 60 950 resp. 60 065 System components for IAS of **classes B and C** are also tested according to DIN VDE 0833 parts 1 and 3.

6.5 Marking

A visual inspection is performed to check whether the system component bears a company and type mark. The marking shall make clear who manufactured the device or who markets it and what type of device it is.

A visual inspection is performed to check whether the system component bears a series mark. The series mark shall make clear for the manufacturer of the device the time (month and year) when the device was manufactured. If the marking is encoded, the manufacturer shall explain the marking in writing.

A visual inspection is performed to check whether the system component is marked “VdS-approved” in accordance with the requirements and whether the marking is situated in an accessible position.

Note: If necessary, a repeat test should be conducted once the approval procedure is complete.

A check is also made to see whether the markings are durable.

6.6 User safety

A visual and function test is carried out to check whether system components are designed in such a way that their use does not pose any hazard to the operator (e.g. no sharp edges).

6.7 Requirements of the authorities

A check is made to see whether any required licences from the authorities are available.

Changes

Compared with edition VdS 2227en : 2002-05 (03) the following changes have been made:

- Table 4.01 Comparision of classes has been replaced by a reference to VdS 3134-2

Annex A Overview about the VdS rules for IAS (informative)

General rules

- Requirements and test methods for maintenance-free batteries, VdS 2102
- Software requirements, VdS 2203
- Protection against environmental influences, VdS 2110

Rules for Planing and installation

- Planning and installation of intruder alarm systems, VdS 2311

Rules for Intruder alarm System concepts

- Requirements and test methods for Intruder alarm System concepts, VdS 2469

Rules for system components of Intruder alarm Systems

- Requirements for alarm glass, VdS 2270
- Test methods for alarm glass, VdS 2317
- Requirements for motion detectors, VdS 2312
- Test methods for motion detectors, VdS 2326
- Requirements for class A control and indicating equipment, VdS 2194
- Test methods for class A control and indicating equipment, VdS 2196
- Requirements for class B and C control and indicating equipment, VdS 2252
- Test methods for class B and C control and indicating equipment, VdS 2319
- Requirements for class A power supply units, VdS 2195
- Test methods for class A power supply units, VdS 2197
- Requirements for class B and C power supply units, VdS 2115
- Test methods for class B and C power supply units, VdS 2122
- Requirements for vibration detectors, VdS 2480
- Test methods for vibration detectors, VdS 2481
- Requirements for capacitive proximity detectors, VdS 2482
- Test methods for capacitive proximity detectors, VdS 2483
- Requirements for penetration detection for safes and strongrooms, VdS 2264
- Test methods for penetration detection for safes and strongrooms, VdS 2477
- Requirements for foils on windows, VdS 2478
- Test methods for foils on windows, VdS 2479

- Requirements for glass-break detectors, VdS 2332
- Test methods for glass-break detectors, VdS 2468
- Requirements for seismic detectors, VdS 2331
- Test methods for seismic detectors, VdS 2484
- Requirements for infrared light beams, VdS 2117
- Test methods for infrared light beams, VdS 2485
- Requirements for opening detectors, VdS 2120
- Test methods for opening detectors, VdS 2233
- Requirements for ancillary control equipment (ACE), VdS 2119
- Test methods for ancillary control equipment (ACE), VdS 2476
- Requirements for stroke plate contacts, VdS 2269
- Test methods for stroke plate contacts, VdS 2315
- Requirements for audible warning devices, VdS 2300
- Test methods for audible warning devices, VdS 2329
- Requirements for visual warning devices, VdS 2301
- Test methods for visual warning devices, VdS 2330
- Requirements for Hold-up trigger devices, VdS 2271
- Test methods for Hold-up trigger devices, VdS 2314
- Requirements for junction boxes, VdS 2116
- Test methods for junction boxes, VdS 2166

Rules for alarm transmission systems

- Requirements an alarm transmission receiving equipment, VdS 2466
- Test methods for alarm transmission receiving equipment, VdS 2467
- Transmission systems for alarm signals, VdS 2471
- Requirements for the alarm protocol, VdS 2465
- Requirements for telephone dialling devices, VdS 2112
- Requirements for alarm transmission equipment, VdS 2463
- Test methods for alarm transmission equipment, VdS 2464

Annex B Comparision of the English and German terms (informative)

B.1 German – English

German	English
24h-Selbstbedienungs-Mietfachanlagen (24h-SB-Mietfachanlagen)	24h-self-service deposit-box system
Abfragende Verbindung	Scanning connection
Abgesetzter Sicherungsbereich	Separated protected premises
Abreißmelder	Tear-off detector
Abschlusselement	Terminating element
Ändern	Change
Akkreditierung	Accreditation
Aktivierung eines Einfärbesystems	Activation of a dyeing system
Aktivierung eines Nebelgerätes	Activation (setting) of a smoke generating device
Alarm	Alarm
Alarmdrahteinlage	Alarm wire insert
Alarmempfangseinrichtung (AE)	Alarm receiving equipment (ARE)
Alarmempfangsstelle	Alarm receiving centre (ARC)
Alarmglas	Alarm glass
Alarmierungseinrichtung	Alarm signalling equipment
Alarmplan	Alarm plan
Alarmschleife	Alarm loop
Alarmübertragungsanlage (AÜA)	Alarm transmission system (ATS)
Anlage	System
Anlagenanschluss	System connection
Anlagenklasse	System class
Anlagenspannung	System voltage
Anlageteil	System component
Anzeigeelement	Display element
Applikation	Application
ASCII (American Standard Code for Information Interchange)	ASCII (American Standard Code for Information Interchange)
Asymmetrische Einkopplung (Gleichtaktstörung, Com.-Mode)	Asymmetric Injection (common-mode)
Asynchrones Netz	Asynchronous network
Atypischer (Raub-)Überfall	Non-typical hold-ups
Aufbruchmelder	Forced-entry detector

Aufnahmeschrank für Tag-/Nacht-Tresoranlagen (Kassettenaufnahmebehältnis)	Receiving unit for day/night-deposit-systems
Auslösung eines Nebelgerätes	Triggering of a smoke generating device
Ausrüstung von Einrichtungen	Equipping of products
Außenhautüberwachung	Shell protection
Außenwand eines Sicherungsbereiches	Outer wall of a protected premises
Auswerteeinheit	Processing unit
Auswerteeinrichtung von Schalteinrichtungen (AWE)	Processing unit of ACE (Ancillary control equipment)
Auswertefunktion	Processing function
Automatisches Wähl- und Ansagegerät (AWAG)	Auto dialler
Automatisches Wähl- und Übertragungsgerät (AWUG)	Digital communicator
B-Kanal	B-channel
Banktresor	Bank strongroom
BAPT (Bundesamt für Post und Telekommunikation)	German Federal Office of Post and Telecommunications
Basisanschluss	Basic rate interface
Bauliche Zwangsläufigkeit	Construction-based „Zwangsläufigkeit“
Bauteil, einbruchhemmendes	Component, burglar resistant
Beauftragte Stelle	Authorised point
Bedarfsgesteuerte Verbindung (Wählverbindung)	Needs-based connection (dialup line)
Bedieneinrichtung (BE)	Control device
Bedieneinrichtung (BE) einer AÜA	Annunciation equipment (AE) of an alarm transmission system
Bedienungssicherheit	Operational reliability
Bedrohungsmeldung	Threat signal
Behältnis	Container
Behältnis für zeitlich gestaffelte Betragsfreigabe	Container for time-controlled release of funds
Berechtigter Betreiber	Authorised operator
Beschäftigtenbedienter Banknotenautomat (BBA)	Staff-operated cash dispenser
Betreiber	Operator
Betriebsbereites Nebelgerät	Stand-by-smoke generating device
Bewegliche Anlageteile (Movable Equipment)	Movable Equipment
Bewegungsmelder	Motion detector
Biologischer Identifikationsmerkmalträger	Biological identification feature medium

Biometrie	Biometry
Bitratenadaption	Adaptation of bits
Blockadefreischaltung	Blockade release
Blockschloss	Blockschloss-type ACE
Bündelfunk	Multi-user-band radio
BUS	BUS
BZT (Bundesamt für Zulassungen in der Telekommunikation)	German Federal Office for Telecommunications Authorisations
CCIR	CCIR (International advisory committee for radio services)
CCITT (Comité Consultatif International Télégraphique et Téléfonique)	CCITT (Comité Consultatif International Télégraphique et Téléfonique)
CCTV	CCTV – Closed Circuit Television
D-Kanal	D-channel
Datenfunk	Data radio
Datensicherungsraum	Data strongroom
Datensicherungsschrank	Data strongbox
Datex-P	Datex-P
Datex-P20H	Datex-P20H
DCS (Digital Communications System)	DCS (Digital Communications System)
DDV	DDV
Deckelkontakt	Tamper contact
Depositsystem	Deposit system
Detektion	Detection
DSS1	DSS1
Duplexschrank	Duplex safe
Durchbruchhemmung	Penetration prevention
Durchbruchüberwachung	Penetration surveillance
Durchgang	Through access
Durchgriff	Reach-in access
Durchgriffüberwachung	Reach-in surveillance
Durchschusshemmende Verglasung	Bullet-resistant glazing
Durchstiegsfähige Öffnung	Opening suitable for human entry
Durchstiegüberwachung	Penetration surveillance
EH-Element (Einbruchhemmendes Element)	Burglar-resistant element
Einbau-Wertschutzschrank	Wall-safe
Einbruchhemmung (EH)	Burglar resistance
Einbruchmeldeanlage (EMA)	Intruder alarm system (IAS)
Einbruchmelder	Intruder detector

Einbruchmelderzentrale (EMZ)	Intruder control and indicating equipment (I-CIE)
Einbruchmeldesystem (EMS)	Intruder alarm system concept (IASC)
Einbruchmeldung	Intruder signal
Einfaches Behältnis	Simple container
Einfärbesystem	Dyeing system
Eingabeeinheit	Input device
Eingabefunktion	Input function
Einmauerschrank	Wall-mounted cabinet
Einsatzschrank	Furniture-mounted cabinet
Einwandiger Stahlschrank	Single-walled steel cabinet
Einwurfvorrichtung	Input unit
Elektrische Zwangsläufigkeit	Electrical „Zwangsläufigkeit“
Elektromagnetische Verträglichkeit	Electromagnetic compatibility (EMC)
Elektromechanische Schalteinrichtung	Electromechanical A.C.E.
Elektromechanisches Sperrelement (SpE)	Electromechanical blocking device
EMA-Ausrüstung	Intruder alarm system equipped
EMA-Vorrüstung	Intruder alarm system preparation
Energieversorgung	Power supply
Energieversorgungsgerät	Power supply unit (PSU)
Energieversorgungsgerät Typ I (Netzversorgung und automatisch wiederaufladbare Sekundärbatterie)	Power supply unit type I (mains supply and automatically rechargeable secondary battery)
Energieversorgungsgerät Typ II (Netzversorgung und Primärbatterie oder Netzversorgung und nicht automatisch wiederaufladbarer Sekundärbatterie)	Power supply unit type II (mains supply and primary battery or automatically not-rechargeable secondary battery)
Energieversorgungsgerät Typ III (Primärbatterie oder nicht automatisch wiederaufladbare Sekundärbatterie)	Power supply unit type III (primary battery or not-automatically rechargeable secondary battery)
Entladeschlussspannung	Final voltage (cut-off voltage)
Ersatzstromanlage	Standby supply system
Ersatzstromerzeuger	Standby supply generator
Ersatzweg	Alternative path
Erschütterungsmelder	Vibration detector
Erweiterung	Extension
Euro-ISDN	Euro-ISDN
EX-Schutz	EX-protection
Exklusiver Übertragungsweg	Exclusive interconnection
Externalarm	External alarm
Fachmann	Specialist

Fahrbare Zweigstellen	Mobile branches
Fail-Safe-Verhalten	Fail-safe-behaviour
Fallenmäßige Überwachung	Trap protection
Fallschacht	Drop-chute
Falschalarm	False alarm
Falschmeldung	False alarm signal
Fassadenelement	Facade element
Fensterbeschlag	Window lock fitting
Fenstertür	Glass door
Fernabfrage	Remote control
Fernalarm	Remote signalling
Ferninstandhaltung (Fernwartung)	Remote maintenance
Fernparametrierung	Remote parameterisation
Fest installierte Anlageteile (Fixed Installed Equipment)	Fixed installed equipment
Feuerwehrschlüsselkasten (FSK)	Fire brigade key box
Flächenmäßige Überwachung	Surface surveillance
Flächenförmige Überwachungscharakteristik	Planar surveillance characteristic
Freischaltelement (FSE)	Release element
Freistehender Wertschutzschrank	Free-standing safe
Fremdsignal	Third-party signal
Fremdsignalerkennung	Third-party signal recognition
Funktionserhalt	Maintenance of performance
Funktionssicherheit	Functional reliability
Gebäudeleittechnik (GLT)	Buildings management technology (BMT)
Gefährdungsgrad	Degree of risk
Gefahrenmeldeanlage (GMA)	Alarm system (AS)
Gefahrenmelder	Alarm detector
Gefahrenmeldung	Alarm signal
Geistiger Identifikationsmerkmalträger	Mental identification feature medium
Geldautomat (GAA)	Automatic Teller Machine (ATM)
Geldautomatensysteme	ATM systems
Geldautomatenzelle	ATM cell
Geldwechselautomat	Money changing machine
Gepanzerter Geldschrank	Armoured safe
Geschlossene Benutzergruppe (Closed-User-Group)	Closed user group
Gewalt, einfache	Force, simple manual

Griffbereite Banknotenbestände	Accessible stocks of bank notes
GSM (Global System für Mobile Communication)	GSM (Global System for Mobile Communications)
Halbautomatische Mietfachanlage	Semi-automatic deposit-box system
Handbereich	Hand range
Hardware	Hardware
Hintergrundbestände	Background stocks
Hinterhaken	Hinge bolts (dog bolts)
IAE	IAE
Identifikationsmerkmal (IM)	Identification feature (ID)
Identifikationsmerkmalträger (IMT)	Identification feature medium
Indoor-KBA	„Indoor“ customer operated Automatic Teller Machine (ATM)
Information	Information
Inspektion	Inspection
Installationsattest	Installation certificate
Instandhaltung	Maintenance
Instandsetzung	Repair
Integrierte Gefahrenmeldeanlage	Integrated alarm system
Internalarm	Internal alarm
Interventionsattest	Intervention certificate
Interventionsmaßnahmen	Intervention measures
Interventionsplan	Intervention plan
Interventionsstelle (IS)	Intervention company (IC)
ISDN	ISDN (Integrated Services Digital Network)
ITU International Telecommunication Union (ITU-T)	ITU International Telecommunication Union (ITU-T)
Kanalbündelung	Channel packaging
Kassettenaufnahmebehältnis	Receiving unit (container)
KB-Schutz	CD-protection
Kleintresorraum	Small strongroom
Knoten	Knot
Kombination	Combination
Kommunikationsgeräte (KG)	Communications devices
Kontaktüberwachung	Contact surveillance
Kontrollgang	Security corridor
Konzentrierte Anzeige (Display)	Concentrated display
Kundenbedienter Banknotenautomat (KBA)	Customer-operated ATM

Kundenmietfach	Deposit-box
Ladeausgang	Charging output
Ladeschlussspannung	End-of-charge voltage
Ladespannung	Charging voltage
Laie	Layperson
Leitungsvermittlung	Circuit switching
Linienförmige Überwachungscharakteristik	Linear surveillance characteristics
Logische Verbindung	Logical (virtual) connection
Materieller Identifikationsmerkmalträger	Physical identification feature medium
Mechanische Mietfachanlage (Konventionelle Mietfachanlage)	Mechanical deposit-box system (conventional deposit-box system)
Mechanische Widerstandsfähigkeit	Mechanical resistance
Mehrgeräteanschluss	Multiple device access
Mehrwandiger Stahlschrank	Multiple-walled steel cabinet
Meldebereich	Zone (area)
Meldebereit	Ready-to-alarm
Meldelinie	Circuit
Melder für Gefahren- und Notzustände	Detector for hazard and emergency statuses
Meldergruppe	Zone
Meldung	Signal (message)
Meldungsübertragung	Alarm transmission
Mietfachanlage	Deposit-box system
Modem	Modem (artificial word for modulator/demodulator)
MTBF	MTBF
Nachrüstung	Security-upgrade, mechanical
Nebelgerät	Smoke generating device
Negativquittung	Negative acknowledgement
Netz	Network
Netzabschluss (NA)	Network termination point (NTP)
Netzterminator (NT)	Network terminator (NT)
Nicht-Exklusiver Übertragungsweg	Non-exclusive interconnection
Notkassen	Emergency teller
Notruf- und Service-Leitstelle (NSL)	Alarm receiving and service centre (German term “Notruf- und Service-Leitstelle – NSL”)
Notrufzentrale	Alarm room
Notstromversorgung	Alternative power source
Notverschluss	Emergency locking system

Objektüberwachung	Object surveillance
Optische Raumüberwachungsanlagen (ORÜA)	Optical space surveillance systems
Organisatorische Zwangsläufigkeit	Organizatorical „Zwangsläufigkeit“
OSI-Schicht (Open Systems Interconnections)	OSI layer (Open System Interconnections)
OSI Schichtenmodell	OSI-reference model
Outdoor-KBA	“Outdoor” customer operated ATM
Packet Assembler/Disassembler (PAD)	Packet Assembler/Disassembler (PAD)
Paketvermittlung	Package switching
Panzer-Geldschrank	Armoured safe
Panzerraum	Armoured room
Parametrierung	Parameterisation
PCM 30	PCM 30
Persönliche Identifikationsnummer (PIN)	Personal Identification number (PIN)
Primärbatterie	Primary battery
Primärleitung	Primary line
Prüfung	Testing
Punktförmige Überwachungscharakteristik	Point-type surveillance characteristic
PVC (Permanent Virtual Circuit)	PVC (Permanent Virtual Circuit)
Qualität	Quality
Qualitätsmanagementsystem (QM-System)	Quality management system (QM-System)
RAL	RAL
Räumliche Überwachung	Volumetric surveillance
Redundanz	Redundancy
Registriereinrichtung	Event recorder
Riegel	Bolt
Riegelschaltschloss	Bolt-switch-lock
Riegelwerk	Bolt mechanism
Rollladen	Roller blind
S_0	S_0
S_0-BUS	S_0-BUS
S_0-Schnittstelle	S_0-Interface
S_0 “Point to point”	S_0-„point to point“
S_{2M} Anschluss	S_{2M}-connection (interface)
Sabotagefreischaltung	Tamper release
Sabotagemeldung	Tamper signal

Sabotagesicherheit	Tamper security
Schalteinrichtung	Ancillary control equipment (ACE)
Schalteinrichtung mit biologischem Identifikationsmerkmal (IM)	Ancillary control equipment (ACE) with biometric identification
Schalteinrichtung mit geistigem Identifikationsmerkmal (IM)	Ancillary control equipment (ACE) with mental identification feature
Schalteinrichtung mit materiellem Identifikationsmerkmal (IM)	Ancillary control equipment (ACE) with physical identification feature
Schalteinrichtung mit Zeitsteuerung	Ancillary control equipment (ACE) with time control
Scharfschalten, extern	Setting, external
Scharfschalten, intern	Setting, internal
Schicht-1-Überwachung	Layer-1-monitoring
Schicht-4-Überwachung	Layer-4-monitoring
Schleusen-Wertschutzschrank	Transfer-safe
Schließblechkontakt	Striking plate contact
Schließen	Closing
Schloss	Lock
Schlüsseldepot (SD)	Key deposit box
Schlüsseldepot-Adapter (SD-Adapter)	Key deposit box adapter unit
Schlüsseldepot-Anschaltung (SDA)	Key deposit box adapter
Schlüsselschalter	Key-operated switch
Schnittstelle	Interface
Schnittstelle S_1	Interface S_1
Schnittstelle S_2	Interface S_2
Schnittstelle $S_{2.1}$	Interface $S_{2.1}$
Schnittstelle S_3	Interface S_3
Schnittstelle $S_{3.1}$	Interface $S_{3.1}$
Schnittstelle S_4	Interface S_4
Schwerpunktmäßige Überwachung	Focal-point surveillance
Sekundärbatterie	Secondary battery
Sekundärleitung	Secondary line
Selbstbedienungs-Mietfachanlage (SB-Mietfachanlage)	Self-service deposit-box system
Semi-Profi	Semi-professional
Sensor	Sensor
Separate Stromkreise für die Verschlussüberwachung	Separate circuits for the locked state monitoring
Sicherheitsbestimmende Funktion	Function determining security
Sicherheitsgefährdend	Security jeopardizing

Sicherheitsmindernd	Security impairing
Sicherheitsrelevante Funktion	Security relevant function
Sicherungsbereich	Protected premises
Signal	Signal
Signalgeber	Warning device
SNA-Netz (System Network Architecture)	SNA network
Software	Software
Sperrelement (SpE)	Blocking device
Sperrzeit	Blocking period
Sperrzeitschaltuhrfunktion	Blocking time-clock function
Stehende Verbindung (Festverbindung)	Dedicated line
Steuerleitung	Control line
Störung (Zustand)	Fault (status)
Störungsmeldung	Fault signal
Streckenüberwachung	Linear surveillance
Sub-Übertragungszentrale (SÜZ)	Sub-receiving centre transceiver (Sub-RCT)
SVC (Switched Virtual Call)	SVC (Switched Virtual Call)
SVC-P (Switched Virtual Call-Permanent)	SVC-P (Switched Virtual Call-Permanent)
Symmetrische Einkopplung (Gegentaktstörung, Diff.-Mode)	Symmetrical injection (differential mode)
Synchrones Netz	Synchronous network
Systeminhaber	System owner
TA X.25D	TA X.25D
TAE (Telekommunikations-Anschlusseinheit)	Telecommunications connection unit
Tag-/Nacht-Tresoranlage (TNT)	Day/night deposit-safe-system
Tagestresor	Day safe
Tagestür	Daytime door
Technische Melder	Technical detectors
Teilgeschirmte Leitungen	Partly shielded lines
Teil-Sicherungsbereich	Part-protected premises
Telefonwählgerät (TWG)	Telephone dialling device
Telekommunikationsanlage (TK-Anlage)	Private automatic branch exchange (PABX)
Terminaladapter	Terminal adapter (TA)
Testmeldung	Test signal
Tragbare Anlageteile (Portable Equipment)	Portable system components

Transportable Anlageteile (Mobile Equipment)	Transportable (mobile) system components
Transportschacht	Chute
Tresorraum	Strongroom
Typischer (Raub-)Überfall	Typical (robbery) Hold-up
Überfallmeldeanlage (ÜMA)	Hold-up alarm system (HUAS)
Überfallmeldung	Hold-up signal
Übertragungsanlage für Gefahrenmeldungen (ÜAG)	Transmission system for alarm signals
Übertragungsgerät für Gefahrenmeldungen (ÜG)	Alarm transmission equipment for alarm signals (ATE)
Übertragungsweg	Interconnection
Übertragungsweg in AÜA	Transmission path in alarm transmission system
Übertragungszentrale (ÜZ)	Receiving centre transceiver (RCT)
Überwachte Verbindungen	Monitored lines
Überwachung	Surveillance
Überwachung gegen Wegnahme	Surveillance against removal
Überwachungsbereich	Surveillance area
Umweltklasse	Environmental class
Umweltverträglichkeit	Environmental stability
Unscharf (Zustand)	Unset (status)
Unscharfschalten, extern	Unsetting, external
Unscharfschalten, intern	Unsetting, internal
Unterbrechungslose Stromversorgung (USV)	Uninterrupted power supply
Unterschiedliche Trasse	Different route
Up_0 und Uk_0	Up_O and Uk_O
User-to-User-Info	User-to-User-Info
UVV “Kassen”	“UVV Kassen” (German Accident Prevention Regulations for Banks)
VdS Schadenverhütung (VdS)	VdS Schadenverhütung (VdS)
VdS-anerkannt	VdS-approved
VdS-Richtlinien	VdS rules
Verfügbarkeit	Availability
Verriegeln	Bolting
Verschließen	Locking
Verschluss	Locking mechanism
Verschlusseinrichtung	Locking device
Verschlussüberwachung	Locked state monitoring
Versorgungsausgang	Supply output

Vibrationskontakt	Vibration contact
Video-Bewegungsmelder	Video motion detector
Video-Überwachungsanlage	Video surveillance system
Vieraugenprinzip	Four-eyes principle
Vollgeschirmte Leitungen	Fully shielded lines
Vollständiger Durchbruch (Vollzugriff, Volldurchbruch)	Full penetration (full access, full break-through)
Volumenförmige Überwachungscharakteristik	Volume-based surveillance characteristic
Vorrüstung von Einrichtungen	Pre-preparation of system components
Wach- und Sicherheitsunternehmen	Security company
Wände in besonders fester Bauweise	Walls of exceptionally solid construction
Wände in fester Bauweise	Walls of solid construction
Wände in Leichtbauweise	Walls of light construction
Warnmeldung	Warning signal
Wartung	Maintenance
Wertbehältnis	Security container
Wertschutzraum	Strongroom
Wertschutzraum in Massivbauweise	Strongroom of solid construction
Wertschutzraum in Modulbauweise	Strongroom of modular construction
Wertschutzraum in Mischbauweise	Strongroom of hybrid construction
Wertschutzraumtür	Strongroom door
Wertsachen	Valuables
Wertschrank	Strongbox for valuables
Wertschutzschrank	Safe
Wertschutzschrank für Geldautomaten	ATM-safes
Widerstandseinheit (RU = Resistance Unit)	Resistance Unit (RU)
Widerstandsgrad	Degree of resistance
Widerstandsklasse	Resistance grade
Wirksamkeit	Effectiveness
X.25	X.25
X.25 im D-Kanal	X.25 in the D-channel
Zeitschlossfunktion	Time-controlled function
Zeitverschlussbehältnis	Time lock safe
Zertifikat	Certificate
Zertifizierung	Certification
Zertifizierungsstelle	Certification body
Zugangsebene (ZE)	Access level (AL)

Zugriffsschutz	Access protection
Zustandsmelder	Status detector
Zustandsmeldung	Status signal
Zutrittskontrollanlage (ZKA)	Access control system (ACS)
Zutrittskontrollsystem (ZKS)	Access control system concept (ACSC)
Zuverlässigkeit	Reliability
Zwangsläufigkeit	„Zwangsläufigkeit“
Zwangsöffnung	Forced opening

B.2 English – German

English	**German**
24h-self-service deposit-box system	24h-Selbstbedienungs-Mietfachanlagen (24h-SB-Mietfachanlagen)
Access control system (ACS)	Zutrittskontrollanlage (ZKA)
Access control system concept (ACSC)	Zutrittskontrollsystem (ZKS)
Accessible stocks of bank notes	Griffbereite Banknotenbestände
Access level (AL)	Zugangsebene (ZE)
Access protection	Zugriffsschutz
Accreditation	Akkreditierung
Activation of a dyeing system	Aktivierung eines Einfärbesystems
Activation (setting) of a smoke generating device	Aktivierung eines Nebelgerätes
Adaptation of bits	Bitratenadaption
Alarm	Alarm
Alarm detector	Gefahrenmelder
Alarm glass	Alarmglas
Alarm loop	Alarmschleife
Alarm plan	Alarmplan
Alarm receiving and service centre	Notruf- und Service-Leitstelle (NSL)
Alarm receiving centre (ARC)	Alarmempfangsstelle
Alarm receiving equipment (ARE)	Alarmempfangseinrichtung (AE)
Alarm room	Notrufzentrale
Alarm signal	Gefahrenmeldung
Alarm signalling equipment	Alarmierungseinrichtung
Alarm system (AS)	Gefahrenmeldeanlage (GMA)
Alarm transmission	Meldungsübertragung
Alarm transmission equipment for alarm signals (ATE)	Übertragungsgerät für Gefahrenmeldungen (ÜG)
Alarm transmission system (ATS)	Alarmübertragungsanlage (AÜA)

Alarm wire insert	Alarmdrahteinlage
Alternative path	Ersatzweg
Alternative power source	Notstromversorgung
American Standard Code for Information Interchange (ASCII)	ASCII (American Standard Code for Information Interchange)
Ancillary control equipment (ACE)	Schalteinrichtung
Ancillary control equipment (ACE) with biometric identification	Schalteinrichtung mit biologischem Identifikationsmerkmal (IM)
Ancillary control equipment (ACE) with mental identification feature	Schalteinrichtung mit geistigem Identifikationsmerkmal (IM)
Ancillary control equipment (ACE with physical identification feature	Schalteinrichtung mit materiellem Identifikationsmerkmal (IM)
Ancillary control equipment (ACE) with time control	Schalteinrichtung mit Zeitsteuerung
Annunciation equipment (AE) of an alarm transmission system	Bedieneinrichtung (BE) einer AÜA
Application	Applikation
Armoured strongroom	Panzerraum
Armoured safe	Gepanzerter Geldschrank Panzer Geldschrank
Asymmetric injection (common-mode)	Asymmetrische Einkopplung (Gleichtaktstörung, Com.-Mode)
Asynchronous network	Asynchrones Netz
ATM cell	Geldautomatenzelle
ATM-safe	Wertschutzschrank für Geldautomaten
ATM systems	Geldautomatensysteme
Authorised operator	Berechtigter Betreiber
Authorised point	Beauftragte Stelle
Auto dialler	Automatisches Wähl- und Ansagegerät (AWAG)
Automatic Teller Maschine (ATM)	Geldautomat (GAA)
Availability	Verfügbarkeit
Background stocks	Hintergrundbestände
Bank strongroom	Banktresor
Basic rate interface	Basisanschluss
B-channel	B-Kanal
Biological identification feature medium	Biologischer Identifikationsmerkmalträger
Biometry	Biometrie
Blockade release	Blockadefreischaltung
Blocking device	Sperrelement (SpE)
Blocking period	Sperrzeit

Blocking time-clock function	Sperrzeitschaltuhrfunktion
Blockschloss-type ACE	Blockschloss
Bolt	Riegel
Bolting	Verriegeln
Bolt mechanism	Riegelwerk
Bolt-switch-lock	Riegelschaltschloss
Buildings management technology (BMT)	Gebäudeleittechnik (GLT)
Bullet-resistant glazing	Durchschusshemmende Verglasung
Burglar resistance	Einbruchhemmung (EH)
Burglar-resistant element	EH-Element (Einbruchhemmendes Element)
BUS	BUS
CD-protection (in Germany until now “KB-protection”)	KB-Schutz
Certificate	Zertifikat
Certification	Zertifizierung
Certification body	Zertifizierungsstelle
Change	Ändern
Channel packaging	Kanalbündelung
Charging output	Ladeausgang
Charging voltage	Ladespannung
Chute	Transportschacht
Circuit switching	Leitungsvermittlung
Closed user group	Geschlossene Benutzergruppe (Closed-User-Group)
Closing	Schließen
Combination	Kombination
Comité Consultatif International des Radiocommunications (CCIR)	Comité Consultatif International des Radiocommunications (CCIR)
Comité Consultatif International Télé-graphique et Téléfonique(CCITT)	Comité consultatif International Télé-graphique et Téléfonique (CCITT)
Communications devices	Kommunikationsgeräte (KG)
Component, burglar resistant	Bauteil, einbruchhemmendes
Concentrated display	Konzentrierte Anzeige (Display)
Construction-based „Zwangsläufigkeit„	Bauliche Zwangsläufigkeit
Contact surveillance	Kontaktüberwachung
Container	Behältnis
Container for time-controlled release of funds	Behältnis für zeitlich gestaffelte Be-tragsfreigabe
Control and indicating equipment (CIE)	Zentrale

Control device	Bedieneinrichtung (BE)
Control line	Steuerleitung
Circuit	Meldelinie
Customer-operated ATM	Kundenbedienter Banknotenautomat (KBA)
Data radio	Datenfunk
Data strongbox	Datensicherungsschrank
Data strongroom	Datensicherungsraum
DATEX-P	Datex-P
Datex P20H	Datex P20H
Day/night deposit-safe-system	Tag-/Nacht-Tresoranlagen (TNT)
Day safe	Tagestresor
Daytime door	Tagestür
D-channel	D-Kanal
DDV	DDV
Dedicated line	Stehende Verbindung (Festverbindung)
Degree of resistance	Widerstandsgrad
Degree of risk	Gefährdungsgrad
Deposit-box	Kundenmietfach
Deposit-box system	Mietfachanlage
Deposit system	Depositsystem
Detection	Detektion
Detectors for hazard and emergency statuses	Melder für Gefahren- und Notzustände
Different route	Unterschiedliche Trasse
Digital Communications System (DCS)	DCS (Digital Communications System)
Digital communicator	Automatisches Wähl- und Übertragungsgerät (AWUG)
Display element	Anzeigeelement
Dissetting, internal	Unscharfschalten, intern
Drop-chute	Fallschacht
DSS1	DSS1
Duplex safe	Duplexschrank
Dyeing system	Einfärbesystem
Effectiveness	Wirksamkeit
Electrical “Zwangsläufigkeit”	Elektrische Zwangsläufigkeit
Electromagnetic compatibility (EMC)	Elektromagnetische Verträglichkeit
Electromechanical A.C.E.	Elektromechanische Schalteinrichtung
Electromechanical blocking device	Elektromechanisches Sperrelement (SpE)

Emergency locking system	Notverschluss
Emergency teller	Notkassen
End-of-charge voltage	Ladeschlussspannung
Environmental class	Umweltklasse
Environmental stability	Umweltverträglichkeit
Equipping of products	Ausrüstung von Einrichtungen
Euro ISDN	Euro-ISDN
Event recorder	Registriereinrichtung
Exclusive interconnection	Exklusiver Übertragungsweg
EX-protection	EX-Schutz
Extension	Erweiterung
External alarm	Externalarm
External signal	Fremdsignal
Facade element	Fassadenelement
Fail-safe-behaviour	Fail-Safe-Verhalten
False alarm	Falschalarm
False alarm signal	Falschmeldung
Fault signal	Störungsmeldung
Fault (status)	Störung (Zustand)
Final voltage (cut-off voltage)	Entladeschlussspannung
Fire brigade key box	Feuerwehrschlüsselkasten (FSK)
Fixed installed equipment	Fest installierte Anlageteile
Focal-point surveillance	Schwerpunktmäßige Überwachung
Forced-entry detector	Aufbruchmelder
Forced opening	Zwangsöffnung
Force, simple manual	Gewalt, einfache
Four-eyes principle	Vieraugenprinzip
Free-standing safe	Freistehender Wertschutzschrank
Full penetration (full access, full break-through)	Vollständiger Durchbruch (Vollzugriff, Volldurchbruch)
Fully shielded lines	Vollgeschirmte Leitungen
Function determining security	Sicherheitsbestimmende Funktion
Functional reliability	Funktionssicherheit
Furniture-mounted cabinet	Einsatzschrank

German Federal Office for Telecommunications Authorisations (BZT)	BZT (Bundesamt für Zulassungen in der Telekommunikation)
German Federal Office of Post and Telecommunications (BAPT)	BAPT (Bundesamt für Post und Telekommunikation)
Glass door	Fenstertür
Global System for Mobile Communications (GSM)	GSM (Global System für Mobile Communication)
Hand range	Handbereich
Hardware	Hardware
Hinge bolts (dog bolts)	Hinterhaken
Hold-up alarm system (HUAS)	Überfallmeldeanlage (ÜMA)
Hold-up signal	Überfallmeldung
IAE	IAE
Identification feature (ID)	Identifikationsmerkmal (IM)
Identification feature medium	Identifikationsmerkmalträger (IMT)
“Indoor” customer operated Automatic Teller Machine (ATM)	Indoor-KBA
Information	Information
Input device	Einfärbesystem
Input function	Eingabeeinheit
Input unit	Eingabefunktion
Integrated alarm system	Integrierte Gefahrenmeldeanlage
Integrated Services Digital Network (ISDN)	ISDN
Internal alarm	Internalarm
Intervention certification	Interventionsattest
Intervention company (IC)	Interventionsstelle (IS)
Intervention plan	Interventionsplan
Intervention measures	Interventionsmaßnahmen
Intruder control and indicating equipment (I-CIE)	Einbruchmelderzentrale (EMZ)
Intruder alarm system (IAS)	Einbruchmeldeanlagen (EMA)
Intruder alarm system concept (IASC)	Einbruchmeldesystem (EMS)
Intruder alarm system equipment	EMA-Ausrüstung
Intruder alarm system preparation	EMA-Vorrüstung
Intruder detector	Einbruchmelder
Intruder signal	Einbruchmeldung
Inspection	Inspektion
Installation certificate	Installationsattest
Interconnection	Übertragungsweg
Interface	Schnittstelle

Interface S_1	Schnittstelle S_1
Interface S_2	Schnittstelle S_2
Interface $S_{2.1}$	Schnittstelle $S_{2.1}$
Interface S_3	Schnittstelle S_3
Interface $S_{3.1}$	Schnittstelle $S_{3.1}$
Interface S_4	Schnittstelle S_4
ITU Telecommunication Union (ITU-T)	ITU Telecommunication Telecommunication Union (ITU-T)
Key deposit box (KDB)	Schlüsseldepot (SD)
Key deposit box adapter	Schlüsseldepot-Anschaltung (SDA)
Key deposit box adapter unit	Schlüsseldepot-Adapter (SD-Adapter)
Key-operated switch	Schlüsselschalter
Knot	Knoten
Layer-1-monitoring	Schicht-1-Überwachung
Layer-4-monitoring	Schicht-4-Überwachung
Layperson	Laie
Linear surveillance	Streckenüberwachung
Linear surveillance characteristics	Linienförmige Überwachungscharakteristik
Lock	Schloss
Locked state monitoring	Verschlussüberwachung
Locking	Verschließen
Locking device	Verschlusseinrichtung
Locking mechanism	Verschluss
Logical (virtual) connection	Logische Verbindung
Maintenance	Wartung, Instandhaltung
Maintenance of performance	Funktionserhalt
Mean Time Between Failures” (MTBF)	MTBF
Mechanical deposit-box system (conventional deposit-box system)	Mechanische Mietfachanlage (Konventionelle Mietfachanlage)
Mechanical resistance	Mechanische Widerstandsfähigkeit
Mental identification feature medium	Geistiger Identifikationsmerkmalträger
Mobile branches	Fahrbare Zweigstellen
Modem	Modem
Money changing machine	Geldwechselautomat
Monitored lines	Überwachte Verbindungen
Motion detector	Bewegungsmelder
Movable equipment	Bewegliche Anlageteile
Multiple device access	Mehrgeräteanschluss

Multi-user-band radio	Bündelfunk
Multiple-walled steel cabinet	Mehrwandiger Stahlschrank
Needs-based connection (dialup line)	Bedarfsgesteuerte Verbindung (Wählverbindung)
Negative acknowledgement	Negativquittung
Network	Netz
Network terminator (NT)	Netzterminator (NT)
Network termination point (NTP)	Netzabschluss (NA)
Non-exclusive interconnection	Nicht-Exlusiver Übertragungsweg
Non-typical hold-ups	Atypischer (Raub-)Überfall
Object surveillance	Objektüberwachung
Opening suitable for human entry	Durchstiegsfähige Öffnung
Open Systems Interconnections (OSI layer)	OSI-Schicht (Open Systems Interconnections)
Operational reliability	Bedienungssicherheit
Operator	Betreiber
Optical space surveillance systems	Optische Raumüberwachungsanlage (ORÜA)
Organisatorical “Zwangsläufigkeit”	Organisatorische Zwangsläufigkeit
OSI-reference model	OSI Schichtenmodell
Outdoor customer operated ATM	Outdoor-KBA
Outer wall of a protected premises	Außenwand eines Sicherungsbereiches
Package switching	Paketvermittlung
Packet Assembler/Disassembler (PAD)	Packet Assembler/Disassembler (PAD)
Parameterisation	Parametrierung
Partly shielded lines	Teilgeschirmte Leitungen
Part-protected premises	Teil-Sicherungsbereich
PCM 30	PCM 30
Penetration prevention	Durchbruchhemmung
Penetration surveillance	Durchbruchüberwachung
Peripheral monitoring	Außenhautüberwachung
Permanent virtual circuit (PVC)	PVC (Permanent virtual circuit)
Personal identification number (PIN)	Persönliche Identifikationsnummer (PIN)
Physical identification feature medium	Materieller Identifikationsmerkmalträger
Planar surveillance characteristique	Flächenförmige Überwachungscharakteristik
Point-type surveillance characteristic	Punktförmige Überwachungscharakteristik
Portable system components	Tragbare Anlageteile
Power supply	Energieversorgung

Power supply unit (PSU)	Energieversorgungsgerät
Power supply unit type I (mains supply and automatically rechargeable secondary battery)	Energieversorgungsgerät Typ I (Netzversorgung und automatisch wiederaufladbare Sekundärbatterie)
Power supply unit type II (mains supply and primary battery or automatically not-rechargeable secondary battery)	Energieversorgungsgerät Typ II (Netzversorgung und Primärbatterie oder Netzversorgung und nicht automatisch wiederaufladbarer Sekundärbatterie)
Power supply unit type III (primary battery or not automatically rechargeable secondary battery)	Energieversorgungsgerät Typ III (Primärbatterie oder nicht automatisch wiederaufladbare Sekundärbatterie)
Pre-preparation of IAS components	Vorrüstung von Einrichtungen
Primary battery	Primärbatterie
Primary line	Primärleitung
Private automatic branch exchange (PABX)	Telekommunikationsanlage (TK-Anlage)
Processing function	Auswertefunktion
Processing unit	Auswerteeinheit
Processing unit of ACE	Auswerteeinrichtung von Schalteinrichtungen (AWE)
Protected premises	Sicherungsbereich
Quality	Qualität
Quality management systems (QM-System)	Qualitätsmanagementsystem (QM-System)
RAL	RAL
Reach-in access	Durchgriff
Reach-in surveillance	Durchgriffüberwachung
Ready-to-alarm	Meldebereit
Receiving centre transceiver (RCT)	Übertragungszentrale (ÜZ)
Receiving unit (container)	Kassettenaufnahmebehältnis
Receiving unit for day/night-deposit-systems	Aufnahmeschrank für Tag-/Nacht-Tresoranlagen (Kassettenaufnahmebehältnis)
Redundancy	Redundanz
Regulierungsbehörde für Post und Telekommunikation (RegTP)	Regulierungsbehörde für Post und Telekommunikation (RegTP)
Release element	Freischaltelement (FSE)
Reliability	Zuverlässigkeit
Remote diagnosis	Ferndiagnose
Remote maintenance	Ferninstandhaltung (Fernwartung)
Remote parameterisation	Fernparametrierung
Remote signalling	Fernalarm
Repair	Instandsetzung

Resistance grade	Widerstandsklasse
Resistance Unit (RU)	Widerstandseinheit (RU = Resistance Unit)
Roller blind	Rollladen
S_0	S_0
S_0-BUS	S_0-BUS
S_0-Interface	S_0-Schnittstelle
S_0-„point to point“	S_0-„point to point“
S_{2M}-connection (interface)	S_{2M} Anschluss
Safe	Wertschutzschrank
Scanning connection	Abfragende Verbindung
Secondary battery	Sekundärbatterie
Secondary line	Sekundärleitung
Security company	Wach- und Sicherheitsunternehmen
Security container	Wertbehältnis
Security corridor	Kontrollgang
Security impairing	Sicherheitsmindernd
Security jeopardizing	Sicherheitsgefährdend
Security relevant function	Sicherheitsrelevante Funktion
Security-upgrade, mechanical	Nachrüstung
Self-service deposit-box system	Selbstbedienungs-Mietfachanlage (SB-Mietfachanlage)
Setting, external	Scharfschalten, extern
Setting, internal	Scharfschalten, intern
Semi-automatic deposit-box system	Halbautomatische Mietfachanlage
Semi-professional	Semi-Profi
Sensor	Sensor
Separate circuits for the locked state monitoring	Separate Stromkreise für die Verschlussüberwachung
Separated protected premises	Abgesetzter Sicherungsbereich
Signal	Signal
Shell protection	Außenhautüberwachung
Signal (message)	Meldung
Simple container	Behältnis, einfaches
Single-walled steel cabinet	Einwandiger Stahlschrank
Small strongroom	Kleintresorraum
Smoke generating device	Nebelgerät
Software	Software
Specialist	Fachmann

Staff-operated cash dispenser	Beschäftigtenbedienter Banknotenautomat (BBA)
Stand-by-smoke generating device	Betriebsbereites Nebelgerät
Standby supply generator	Ersatzstromerzeuger
Standby supply system	Ersatzstromanlage
Status detector	Zustandsmelder
Status signal	Zustandsmeldung
Striking plate contact	Schließblechkontakt
Strongroom	Wertschutzraum
Strongroom (old Germn term „Tresorraum“)	Wertschutzraum
Strongroom door	Wertschutzraumtür
Strongroom of solid construction	Wertschutzraum in Massivbauweise
Strongroom of modular construction	Wertschutzraum in Modulbauweise
Strongroom of hybrid construction	Wertschutzraum in Mischbauweise
Supply output	Versorgungsausgang
Surface surveillance	Flächenmäßige Überwachung
Surveillance	Überwachung
Surveillance against removal	Überwachung gegen Wegnahme
Surveillance area	Überwachungsbereich
Sub-receiving centre transceiver (Sub-RCT)	Sub-Übertragungszentrale (SÜZ)
Switched Virtual Call (SVC)	SVC (Switched Virtual Call)
Switched Virtual Call-Permanent (SVC-P)	SVC-P (Switched Virtual Call-Permanent)
Symmetrical injection (differential mode)	Symmetrische Einkopplung (Gegentaktstörung, Diff.-Mode)
Synchronous network	Synchrones Netz
System	System
System component	Anlageteil
System class	Anlagenklasse
System connection	Anlagenanschluss
System Network Architecture (SNA network)	SNA-Netz (System Network Architecture)
System owner	Systeminhaber
System voltage	Anlagenspannung
TA X.25D	TA X.25D
Tamper contact	Deckelkontakt
Tamper release	Sabotagefreischaltung
Tamper security	Sabotagesicherheit
Tamper signal	Sabotagemeldung

Tear-off detector	Abreißmelder
Technical detectors	Technische Melder
Telecommunications connection unit	TAE (Telekommunikations-Anschlusseinheit)
Telephone dialling device	Telefonwählgerät (TWG)
Terminal adapter (TA)	Terminaladapter
Terminating element	Abschlusselement
Testing	Prüfung
Test signal	Testmeldung
Third-party signal	Fremdsignal
Third-party signal recognition	Fremdsignalerkennung
Threat signal	Bedrohungsmeldung
Through access	Durchgang
Time-controlled function	Zeitschlossfunktion
Time lock safe	Zeitverschlussbehältnis
Transfer-safe	Schleusen-Wertschutzschrank
Transmission path (in alarm transmission system)	Übertragungsweg in AÜA
Transmission system for alarm signals	Übertragungsgerät für Gefahrenmeldungen (ÜG)
Transportable (mobile) system components	Transportable Anlageteile (Mobile Equipment)
Trap protection	Fallenmäßige Überwachung
Triggering of a smoke generating device	Auslösung eines Nebelgerätes
Typical (robbery) Hold-up	Typischer (Raub-)Überfall
Uninterrupted power supply	Unterbrechungslose Stromversorgung (USV)
Unset (status)	Unscharf (Zustand)
Unsetting, external	Unscharfschalten, extern
Unsetting, internal	Unscharfschalten, intern
Up_0 and Uk_0	Up_0 und Uk_0
User-to-user-info	User-to-User-Info
UVV “Kassen” (German Accident Prevention Regulations for Banks)	UVV “Kassen”
Valuables	Wertsachen
VdS-approved	VdS-anerkannt
VdS rules	VdS-Richtlinien
VdS Schadenverhütung (VdS)	VdS Schadenverhütung (VdS)
Vibration contact	Vibrationskontakt
Vibration detector	Erschütterungsmelder

Video motion detector	Video-Bewegungsmelder
Video surveillance system	Video-Überwachungsanlage
Volume-based surveillance characteristic	Volumenförmige Überwachungscharakteristik
Volumetric surveillance	Räumliche Überwachung
Wall-mounted cabinet	Einmauerschrank
Walls of exceptionally solid construction	Wände in besonders fester Bauweise
Walls of light construction	Wände in Leichtbauweise
Walls of solid contruction	Wände in fester Bauweise
Wall-safe	Einbau-Wertschutzschrank
Warning device	Signalgeber
Warning signal	Warnmeldung
“Wertschrank” (Strongbox for valuables)	Wertschrank
Window lock fitting	Fensterbeschlag
X.25	X.25
X.25 in the D-channel	X.25 im D-Kanal
Zone	Meldergruppe
Zone (area)	Meldebereich
“Zwangsläufigkeit”	Zwangsläufigkeit