Control and Indicating Equipment (CIE) of classes B and C

Requirements

(Including draft amendment VdS 2252en-S1: 2006-12 (01))

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

Guidelines for Intruder Alarm Systems

Control and Indicating Equipment (CIE) of classes B and C

Requirements

(Including draft amendment VdS 2252en-S1: 2006-12 (01))

CONTENT

1 General

1.1 Scope

These guidelines contain requirements for class B and C control and indicating equipment (CIE). They shall be applied in conjunction with the “Guidelines for intruder alarm systems, general requirements and test methods“; VdS 2227 and the “Guidelines for intruder alarm systems, protection against environmental influences, requirements and test methods“, VdS 2110. The “Guidelines for alarm systems, software controlled system components, requirements and test methods“, VdS 2203, also apply for system components controlled by software.

CIE receive signals/messages generated a. o. by intruder detectors and – if applicable – by hold-up devices, process these and notify these via remote signalling to an alarm receiving centre (ARC) (e.g. the police, a security company) or as external alarm via local warning devices to the anonymous public.

Note: Class B CIE according to these guidelines may dispose of exclusive interconnections (e.g. wired) as well as of non-exclusive interconnections (e.g. radio). It is not intended to elaborate guidelines for non-exclusive interconnections for CIE class C.

The test methods for class B and C CIE are described in the guidelines VdS 2319 (at present draft).

1.2 Validity

These guidelines are valid from 01. June 2003; they replace the edition VdS 2252 : 1996-01 (02). For practical reasons the draft amendment S1 December 2006 is incorporated into the guidelines (clause 12.1.1).

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

2 Normative references

These guidelines 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 guidelines only when announced by a change of these guidelines. For undated references the latest edition of the publication referred will be applied.

- **CCITT V.31bis** Electrical characteristics for single-current interchange using optocouplers
- **DIN 41 636** Sensitve switches for communication technology
- **DIN EN 60 529 : 2000-09** Degrees of protection provided by enclosures (IP-Code)
- **DIN EN 60 651** Sound level meters
- **DIN EN ISO 75-1** Plastics; Determination of temperature deflection under load; Part 1: General test methods

- **DIN EN ISO 75-2** Plastics; Determination of temperature deflection under load; Part 2: Plastics and ebonite
- **DIN EN ISO 527-1** Plastics; Determination of tensile properties; Part 1: General principles
- **DIN EN ISO 527-2** Plastics; Determination of tensile properties; Part 2: Test conditions for moulding and extrusion plastics
- **DIN EN ISO 2039-1** Plastics; Determination of hardness; Part 1: Ball indentation method
- **DIN EN ISO 6988 : 1997-03** Metallic and other non-organic coatings - sulfur dioxide - test with general condensation of moisture
- **DIN IEC 65A/179/CDV : 1995** Functional safety – Safety-relevant systems – Part 1: General requirements – corresponds with VDE 0801 part 1 : 1995-12
- **DIN VDE 0100** Execution of power installations with rated voltages below 1000 V
- **DIN VDE 0833-1 : 1989-01** Alarm systems for fire, intrusion and hold-up, General requirements
- **EN 50131-1 : 1997-03** Alarm Systems – Intruder alarm systems - Part 1: General requirements
- **EN 61000-4-2 : 1995-03** Electromagnetic compatibility (EMC) - Part 4: Testing and measurement techniques – Section 2: Electrostatic discharge immunity test – Basic EMC publication
- **EN 61000-4-2/A1 : 1998-04** Electromagnetic compatibility (EMC) - Part 4 - 2: Testing and measurement techniques - Electrostatic discharge immunity test; Amendment A1
- **EN 61000-4-3 : 1996-09** Electromagnetic compatibility (EMC) - Part 4 -3: Testing and measurement techniques – Radiated, radio-frequency, electromagnetic field immunity test, Amendment A1
- **EN 61000-4-3/A1 : 1998-08** Electromagnetic compatibility (EMC); Testing and measurement techniques; Radiated, radio-frequency, electromagnetic field immunity test, Amendment A1
- **EN 61000-4-4 : 1995-03** Electromagnetic compatibility (EMC) - Part 4-4: Testing and measurement techniques, Electrical fast transient/burst immunity test
- **EN 61000-4-5 : 1995-03** Electromagnetic compatibility (EMC) - Part 4: Testing and measurement techniques – Section 5: Surge immunity test
- **EN 61000-4-6 : 1996-07** Electromagnetic compatibility (EMC) - Part 4: Testing and measurement techniques – Section 6: Immunity to conducted disturbances, induced by radio-frequency fields
- **EN 61 000-4-11 : 1994-08** Electromagnetic compatibility (EMC) - Part 4: Testing and measurement techniques – Section 11: Voltage dips, short interruptions and Voltage variations immunity test
- **EN ISO 179** Plastics; Determination of Charpy impact properties
- **EN 60068-2-1 : 1993-03** Environmental testing - Part 2: Tests, tests A: Cold;
- **EN 60068-2-1/A1 : 1993-03** Environmental testing; Tests; tests A: Cold
- **EN 60068-2-1/A2 : 1994-07** Environmental testing; Tests; tests A: Cold

- **EN 60068-2-2 : 1973-03** Basic environmental testing procedures - Part 2: Tests; tests B: Dry heat
- **EN 60068-2-2/A1 : 1993-03** Basic environmental testing - Part 2: Tests; tests B: Dry heat
- **EN 60068-2-2/A2 : 1994-07** Basic environmental testing - Part 2: Tests, tests B: Dry heat
- **IEC 60 068-2-6 : 1995-03** Environmental testing - Part 2: Tests; test Fc: Vibration (sinusoidal)
- **EN 60068-2-6 : 1995-04** Environmental testing - Part 2: Tests; test Fc: Vibration (sinusoidal)
- **EN 60068-2-6 : 1995-04** Environmental testing - Part 2: Tests; test Fc: Vibration (sinusoidal)
- **EN 60068-2-6 : 1995-04** Environmental testing - Part 2: Tests; test Fc: Vibration (sinusoidal)
- **IEC 60 068-2-27 : 1987** Basic environmental testing - Part 2: Tests, tests Ea: shock
- **IEC 60 068-2-56 : 1988** Environmental testing - Part 2: Tests; test Cb: Damp heat, steady state. Primarily for equipment
- **IEC 60 068-2-63 : 1991** Environmental testing - Part 2: Tests; test Eg: Impact, spring hammer
- **VdS 2110** Guidelines for intruder alarm systems, protection against environmental influences, requirements and test methods
- **VdS 2119** Guidelines for intruder alarm systems, ancillary control equipment (ACE)
- **VdS 2203** Guidelines for alarm systems, software controlled system components, requirements and test methods
- **VdS 2227** Guidelines for intruder alarm systems, general requirements and test methods
- **VdS 2311** Guidelines for intruder alarm systems, planning and installation
- **VdS 2319** Guidelines for intruder alarm systems, class B and C Control and Indicating Equipment (CIE), test methods (at present draft)
- **VdS 2463** Guidelines for alarm systems, alarm transmission equipment for alarm signals (ATE), requirements
- **VdS 2465** Guidelines for alarm systems, transmission protocol for alarm signals, requirements

3 Terms and definitions

For general terms and definitions refer to the “Guidelines for intruder alarm systems, general requirements and test methods“, VdS 2227.

Important Note: For a better understanding of these guidelines the definition of “Zwangsläufigkeit” according to VdS 2227 is included below:

*“**Zwangsläufigkeit**”: Measure which prevents an IAS from being set when not all its components are fully functional or which prevents the operator of a 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. 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 devices in a set IAS, blocking of the blocking device when the IAS is not fully functional.*

***Organisational “Zwangsläufigkeit”:** All the organisational measures taken to maintain “Zwangsläufigkeit”, e.g. monitoring entry and exit of persons.*

4 Classification

The **performance criteria** for different classes are defined in the „Guidelines for intruder alarm systems, general requirements and test methods“, VdS 2227.

The **environmental classes** are set in accordance with the “Guidelines for intruder alarm systems, protection against environmental influences, requirements and test methods“, VdS 2110.

5 Protection against environmental influences

5.1 Limits of application

Environmental influences shall not affect the function of CIE. Environmental influences can have various effects on operating characteristics, depending on the nature of the function applied. The manufacturer shall therefore specify the limits of the application (e.g. climate).

5.2 Climates

The function of CIE shall not be adversely affected by the thermal conditions described in table 5.01, appropriate to its environmental class.

Test	**Functional test**	**Endurance test**	**Degree of severity, abbreviated description of conditions**	
			I	II
Dry heat (T1) as spec. in EN 60068-2-2	x		+40 °C, 16 h	+55 °C, 16 h
Cold (T3) as spec. in EN 60068-2-1	x		+5 °C, 16 h	-10 °C, 16 h
Damp heat, steady (T4) as spec. in IEC 60068-2-3	x		+40 °C, 4 d, 93 % rel. humidity	

Table 5.01: Climates

5.3 Protection against corrosion

CIE shall have adequate resistance to corrosion as specified in table 5.02.

Test	**Functional test**	**Endurance test**	**Degree of severity, abbreviated description of conditions**	
			I	II
SO_2-corrosion as spec. in DIN EN ISO 6988 (K3)		X	No test	0.2 l SO_2, 5 cycles

Table 5.02: Protection against corrosion

5.4 Mechanical influences

The function of CIE shall not be adversely affected by mechanical influences as described in table 5.03.

Test	**Functional test**	**Endurance test**	**Degree of severity, abbreviated description of conditions**	
			I	II
Shock (M1) as spec. in EN 60068-2-27	X		Â(m/s²) = 1000 - (200 x M) 6 x 3 shocks, duration 6 times 6 ms	
Impact (M2) as spec. in EN 60068-2-75	X		0.5 J, 3 impacts per point	
Vibration sinus (M3) as spec. in EN 60068-2-6	X		10-150 Hz, 0.2 g, 1 cycle/axis	10-150 Hz, 0.5 g, 1 cycle/axis

Â = peak acceleration, M = kilogram value of the mass of the test specimen

Table 5.03: Mechanical influences

5.5 Electromagnetic compatibility (EMC)

The function of CIE shall not be adversely affected by electromagnetic influences (EMC) as specified in table 5.04.

Test	**Functional test**	**Endurance test**	**Degree of severity, abbreviated description of conditions**	
			I	II
Electrostatic discharge of low energy (E1b) acc. to EN 61 000-4-2	x		Each 10 times pos. and neg. contact discharge 2, 4 and 6 kV resp. air discharge 2, 4 and 8 kV	
Radiated, radio-frequency, electromagnetic field (E2a) acc. to EN 61 000-4-3	x		80 – 2000 MHz, 10 V/m as well as 415-466 and 890-960 MHz, 30 V/m Modulation: AM 80 % (modulated with 1 kHz sinus) for at least 3 s and in addition 3 times switching on/off of the carrier with 1 Hz and 1 kHz	
Conducted radio-frequency (E2b) acc. to EN 61 000-4-6	x		150 kHz-100 MHz, 140 dBµV Modulation: AM 80 % (modulated with 1 kHz sinus) for at least 3 s and in addition 3 times switching on/off of the carrier with 1 Hz and 1 kHz	
Conducted electrical fast transient with low energy – burst - (E3a) acc. to EN 61 000-4-4	x		Each for a period of 1 min pos. and neg. mains 0.5, 1 and 2 kV, other circuits 0.25, 0.5 and 1 kV	
Conducted slow surge with high energy - (E4a) acc. to EN 61 000-4-5	x		Mains 20 times pos. and neg. cl. 4 diff. 0.5, 1, 2 kV Other circuits 5 times pos. and neg. cl. 3: line-to-line 0,5, 1 kV and line-to-ground 0.5, 1, 2 kV	
Static magnetic fields (E6)	x		150 mT	

Table 5.04: Electromagnetic compatibility (EMC)

6 Functional reliability

6.1 Provision of functions

6.1.1 Technical data

Technical data describing the CIE shall be provided in the German language. This data shall include all information and parameters necessary for the correct and reliable operation of the CIE.

6.1.2 Installation instructions

Installation instructions written in German language shall be provided for CIE. These instructions shall include a clear illustration of the assembly and installation procedures and information describing the applications for which the CIE is suitable (including an indication of the class according to clause 4). Further on instructions are necessary for adjustment (setting) and maintenance. Adjustments not allowed shall be marked unambiguously.

6.1.3 Operating voltage behaviour

Nominal voltage, operating voltage range (at least nominal voltage U_N ± 15 %) and maximum permitted ripple of the operating voltage shall be specified by the manufacturer. CIE shall function correctly within these specified values. Variations in the voltage as specified in table 6.01 shall not adversely affect the function of CIE.

Test	**Functional test**	**Endurance test**	**Degree of severity, abbreviated description of conditions**	
			I	II
Operating voltage changes mains supply (B1a)	x		U_N + 10 % - U_N - 15 %	
Operating voltage range system-voltage (B1b)	x		U_N ± 15 % or system-relevant	
Operating voltage dips of the mains supply (B2a) acc. to EN 61 000-4-11	x		For 0.5, 1, 5 and 10 periods the voltage shall be reduced by 60 % for 3 times as well as for 0.5, 1, 5 and 10 periods the voltage shall be reduced by 100 % for 3 times, duration between the reductions ≥ 10 s	
Operating voltage surge system voltage (B2b)	x		10 cycles from U_N +15 % to U_N –15 % and back or system-relevant	

Table 6.01: Operating voltage behaviour

6.1.4 Ripple of the operating voltage

As a minimum requirement CIE shall function correctly with a voltage ripple of ≤ 1.0 V_{SS} if a nominal voltage of 12 V is specified. For a nominal voltage of 24 V the ripple value is ≤ 2.0 V_{SS}. For other nominal voltages the specifications of the manufacturer shall apply.

6.1.5 Reliability

The selection of components for CIE shall be such that they are suitable for the selected environmental class.

6.1.6 Components

Only components using a technology that has proven to be reliable in various applications, with an unmodified specification over a period of 2 years, may be used. For components of unproven reliability, other means of demonstrating reliability may be considered on an individual basis.

All components shall be operated within the limits specified by the component manufacturer while taking into consideration the effect of ambient temperature (including inherent warming) (see also DIN IEC 65A/179/CDV).

6.1.7 Relays

Relays shall be protected against the effects of dust at least to the degree of protection specified by DIN EN 60 529 (identical with DIN VDE 0470-1) - IP 5x. Relay contacts shall be designed for at least 10,000 switching cycles at a corresponding connected load.

6.1.8 Switches

Switches shall be fitted with self-cleaning contacts or be enclosed in dust-protected casings complying at least with the degree of protection specified by DIN EN 60 529 (identical with DIN VDE 0470-1) - IP 5x.

6.1.9 Access to assemblies and components

CIE shall be constructed to ensure that assemblies and components are easy accessible only for the installer and maintenance service (AL 3) and replacement is easily possible. Provisions shall be made to reduce handling errors to a minimum.

Note: AL = Access level, see clause 7.10.

6.1.10 Connecting and adjustment elements

Connecting and adjustment elements shall be marked and easily accessible to installer and maintenance service (AL 3). For the operator (AL 2) and third parties (AL 1) access shall not be possible; the elements shall be secured e.g. by covers against unauthorised access.

6.1.11 Connection of external power consumers

External power consumers shall be connected such that a short circuit cannot negatively influence the complete function of the IAS. If CIE are intended for use of monitoring of several protected premises, the connection of power consumers shall be made such that a short circuit in one protected premises shall not negatively influence the other protected premises.

Note: This protection function may also be located in another system component (e.g. power supply).

6.1.12 Isolation of fundamental functions

It shall not be possible for third parties (AL 1) or the user (AL 2) to switch off fundamental security relevant functions (e.g. monitoring of transmission paths) at all. For installer and maintenance service (AL 3) the possibility to switch off fundamental security functions shall be limited.

6.1.13 Failure of fundamental functions

Faults of transmission paths (e.g. short circuit and interruption of transmission paths for intruder and hold-up signals/messages, connections to warning devices etc.) shall not lead to a breakdown/failure of fundamental security relevant functions.

6.2 Function monitoring

Class B:

The failure of central processing units (e.g. microprocessors) shall cause a remote or external alarm. In the unset state of the IAS instead of the remote alarm the signalling of a fault condition is also possible.

Class C:

The failure of central processing units (e.g. microprocessors) shall cause a remote alarm. In the unset state of the IAS besides the remote alarm the signalling of a fault condition is also possible.

7 Operation security

7.1 Operation

Actions to be executed by the operator shall be simple. Indicators shall be designed to be clear and easily understood.

7.2 Operation instructions

Operation instructions written in the German language shall be available to the operator of the IAS. The instructions shall include a clear illustration and description of all control and display elements of importance to the operator and shall incorporate clear instructions for all operating states of the installation.

7.3 Marking

The function of indication and operation elements shall be unambiguously highlighted on the CIE inscription. Indications and abbreviations, especially such of alphanumeric type, shall be designed logically and easily to be assigned to.

7.4 Degree of protection

CIE shall, if installed, be constructed at least to the degree of protection as specified by DIN EN 60 529 (identical with DIN VDE 0470-1) - IP 3x.

7.5 Protection against access

Parts affecting the function of CIE as well as connecting elements and adjustment elements shall not be freely accessible; they shall be protected e.g. by covers.

7.6 Sealing capability

CIE shall be designed so that the sealing of parts which are not accessible to the user of the CIE (AL 3 resp. AL 4) is possible.

7.7 Error tolerance

CIE shall be constructed such that they cannot be adversely affected by incorrect operations executed by the operator (AL 2).

7.8 Setting of parameters

Facilities for the setting of the parameters of CIE shall be designed to allow parameter setting by the installer (AL 3) after commissioning only with the consent of the operator – (AL 2) and only in the unset state of the IAS.

For remote parameterisation the same requirements for access levels are valid as for parameterisation on site. A remote parameterisation may be possible only, if an employee of the installation company (AL 3) is on site, there releasing the remote parameterisation actively and changes made in parameterisation are checked on site by the installer (check of changes according to DIN VDE 0833-1 resp. the VdS-guidelines for planning and installation of IAS, VdS 2311).

Information to be transmitted shall be secured such, that faulty setting of parameters is excluded. Furthermore measurers shall be taken, that a released possibility for remote parameterisation is not steadily given by mistake (e.g. time limitation – at maximum 30 min, automatic restoring during the next setting procedure).

In addition measures shall be taken, that a faulty remote parameterisation may be set in the previous (former) version of the parameterisation (e.g. by making of a copy in the CIE or somewhere else).

Each remote parameterisation shall be recorded automatically in the event recorder according to clause 12.4 together with the type of setting of parameters, date and time.

7.9 Remote diagnosis

A remote diagnosis of the CIE (e.g. for determination of failures, reading of a fitted background memory) may be performed taking into consideration access levels AL 2 or AL 3, an active single release on site and only in the unset state of the IAS. It must be assured that by a remote diagnosis

- the function of the CIE as intended is not negatively influenced,
- no changes within the CIE are possible,
- no unauthorised persons have access to the CIE.

Each remote diagnosis action shall be recorded automatically together with date and time in an event recorder according to clause 12.4.

Note: The mandatory regularly inspection and maintenance of IAS cannot be compensated by a remote control.

7.10 Access limitation

7.10.1 Access level (AL)

For regulating the access for different authorized persons to different components and functions of an IAS, a division is made in access levels (AL). CIE shall provide access levels according to table 7.01.

Access level (AL)	**Definition**
1	Access for everybody possible
2	Access possible for operator of the IAS
3	Access possible for installer and maintenance personal [1)]
4	Access possible for manufacturer [1)]

[1)] The access levels 3 and 4 are only accessible if an authorization (e.g. by technical and/or organisational measures) of access level 2 is available.

Table 7.01: Definition of the access levels

Within the different access levels further subdivisions are possible (e.g. for AL 2, if the operator of the IAS intends to provide to the users different access authorizations for the internal setting/unsetting procedure).

7.10.2 Access authorization

The authorized access to the single access levels shall be achieved according to the measures in table 7.02.

Access level (AL)	**Measures**
1	None
2	Technical (e.g. lock, code) as well as organisational measures are possible (e.g. installation of the system component in an area which is not freely accessible for third-parties).
3	Lock or code (for both at least 1,000 combinations) or sealed screwing, whereas an opening shall lead to a tamper signal/message; the access to AL 3 requires in each case a pre-release (e.g. by technical and/or organisational measures) of AL 2.
4	Suitable measures by the manufacturer (e.g. special equipment, codes); the access to AL 4 requires in each case a pre-release (e.g. by technical and/or organisational measures) of AL 2.

Table 7.02: Securing of the access levels

8 Tamper

8.1 Tamper protection

Indication and operating elements shall be designed such that they do not weaken the stability of the housing or permit access into the device without leaving changes of form.

Housings shall not have stamped pre-determined breaking points except those at the mounting side. Hinges shall be provided with extricable bolts if accessible from the outside. Mounting screws of assemblies shall not be visible from the outside once mounted properly. Furthermore it shall not be possible to see inside of the housing in intended operation.

Opening of the CIE shall be possible only to installer and maintenance service (AL 3) except for those parts which do not have security relevant functions and which have to be accessible to the user for operation.

Attacks aiming to get inside of the CIE shall lead to a remaining form change. The opening of a part of the CIE which is not accessible to the user and which contains fundamental functions (e.g. forwarding alarms) shall be possible with tools only.

8.2 Tamper detection

8.2.1 Monitoring of opening

Opening of the CIE shall be detected and signalled in the set state of the IAS as well as in the unset state of the IAS, if security relevant functions become accessible by the opening (is to be included in the measurements of tamper monitoring of the CIE or a zone for tamper signals/messages).

The inside of the components and the monitoring of the opening shall be protected against access as long until the monitoring system has responded.

Only micro-“snap”-switches according to DIN 41636 or equivalent parts shall be used for cover contacts. The contact area of the contacts shall be gold-plated or of equivalent finish. Alternatively, reed contacts may be used as long as they cannot be influenced from the outside.

8.2.2 Penetration monitoring

According to the guidelines for planning and installation of IAS, VdS 2311, CIE shall be within the supervised area in the set state of the IAS. This supervision may be processed either by separate intruder detectors (e.g. motion detectors) or directly by the CIE itself.

If the CIE is supervised directly, an opening wherever of ∅ > 15 mm shall lead to a signal/message. In order to fulfil the requirements for the „Zwangsläufigkeit“ it shall no more be possible to operate the parts of the CIE which are set externally. At the same time the opening of the CIE shall be inhibited in all access levels, if security relevant functions are accessible (e.g. by using of an electromagnetic blocking device).

Note: For use of a lockable housing which is included in the „Zwangsläufigkeit“ via a blocking device, this shall be monitored on opening, locked state and penetration (e.g. by an alarm wire insert with a maximum distance of the alarm wires of 15 mm).

8.3 External voltage

The connection of external voltage to the transmission paths shall not influence the function of the IAS or shall generate an intruder, hold-up or tamper signal/message.

9 Construction

9.1 Stability

Class B

Housings of CIE shall be of sufficient mechanical strength. Covers shall be mounted mechanically stable, e.g. by screwing.

Accessible elements, serving as interface for the interconnections (e.g. antennas) shall be designed such stable and mounted as the housing of the CIE. If this is not possible an interference (e.g. complete or part taking off) shall be detected and triggered as tamper according to clause 8.2.1.

Class C

Housings of CIE shall be of metal or material with similar stability characteristics. They shall prove sufficient mechanical stability and shall be temperature consistent. Covers shall be mounted mechanically stable, e.g. by screwing.

Class B and C

Plastic housings shall be stable and consistent against environmental influences and temperature. They shall furthermore prove good viscosity, stability and stiffness. Minimal values according to table 9.01 are to be maintained.

Characteristics	**Minimal value**
Impact strength	10 kJ/m^2 in acc. with DIN EN ISO 179
Notched impact strength	5 kJ/m^2 in acc. with DIN EN ISO 179
Deformation resistance	55 °C in acc. with DIN EN ISO 75-1 and –2
Ball indention hardness	95 N/mm^2 in acc. with DIN EN ISO 2039-1
Tensile strength	50 N/mm^2 in acc. with DIN EN ISO 527-1 and -2
Table 9.01: Minimum values for plastics	

9.2 Stationary installation

CIE shall be designed that a stationary installation is possible.

9.3 Freedom of potential, isolation resistance

The housing and all parts of the housing of CIE should be free from electrical potential (with the exception of electrical protective measures and/or EMC protection measures). The isolation resistance shall be at least 500 kΩ.

For the equi-potential bonding it shall be possible to connect a wire with a sectional view of 1.5 mm^2 to 4 mm^2 to the CIE.

Note: For protection of class I devices according to DIN VDE 0100 it is permitted to use the existing protective earth conductor with a sectional view of 1.5 mm^2. In this case the additional terminal is not necessary.

9.4 Shielded cables

CIE shall be constructed so that the shielded cables can be joined together in a reliable manner.

9.5 Strain relief

Connecting and contact areas of cables and wires are to be relieved of mechanical strains if such strains can be anticipated.

9.6 Fastening and calibration

CIE shall be constructed to allow proper installation and calibration. Any special tools required shall be supplied by the manufacturer of the device.

9.7 Indicators

9.7.1 Design of visible indicators

All visible indicators – except concentrated displays – shall be marked by different colours and – if their meaning is not clearly identifiable – by a respective inscription. All abbreviations shall be in alphanumeric order, logically designed and easily to be assigned to.

The following colours shall be selected:

- GREEN = Operation
- RED = Alarm signal, e.g. intrusion signal/message
- YELLOW = Fault; state, e.g. unset

9.7.2 Concentrated displays

If concentrated displays are used, at least the following higher indicators (collective displays) shall be provided:

- Operation
- (collective) Alarm
- (collective) Fault
- if necessary Technical signals/messages (see clause 10.5)

If concentrated displays are used alarm signals have priority to other signals/ messages, e.g. "fault" and further information, e.g. "isolation". It shall be possible to recognize if more information is given than the concentrated display is able to indicate. It shall be possible to recall this information; such a recall shall not lead to a loss of information.

9.7.3 Testibility of indicators

All visible and acoustic indicators shall be identifiable unambiguously and testable on function by the operator (AL 2) in a simple way (e.g. by an indicators test-button). A test may be possible also for access level 1 (AL 1).

9.7.4 Loudness of audible indicators

Sounders for audible indicators shall have a minimum volume of 60 dB(A) - measured in accordance with DIN 45 631 - at a distance of 1 m from the signal emitter.

9.7.4 Reliability of visible indicators

Visible indicators shall be long-lasting; their life cycle shall at least be 30,000 h.

9.7.6 Recognizability of visible indicators

Visible collective indicators shall be recognisable unambiguously at a lightening between 0 - 200 Lux with a distance of 3 m and radiating angle of $\pm$ 22.5°. The radiating angle is measured from the vertical to the front of the CIE.

All other indicators shall be recognisable unambiguously at a lightening of 50 to 1000 Lux with a distance of 1 m and a radiating angle of $\pm$ 22.5°.

10 Inputs for signals/messages and monitoring measures

10.1 Required inputs

CIE shall have at least the required inputs and their associated features as described in table 10.01. For class B CIE with non-exclusive interconnections (e.g. radio links) these requirements are valid accordingly.

Inputs for	Number at least	Monitoring of the associated interconnections	Assignment to zones
Intrusion signals/messages	1	according to clause 14	required
Hold-up signals/messages	1	according to clause 14	required
Tamper signals/messages	1	according to clause 14	Required
Tamper monitoring for CIE [2)]	1	according to clause 14 [1)]	not required [3)]
Tamper monitoring for ACE [2)]	1	according to clause 14	not required [3)]
Tamper monitoring for warning devices [2)]	1	according to clause 14	not required [3)]
Locked state monitoring	1	not required	required
Pre-warning end-of-capacity of the power supply (≥ 50 days)[6)]	1	not required	not required [4)]
Signal end-of-capacity of the power supply (≥ 30 days)[6)]	1	not required	not required [4)]
Fault signal of the power supply [5)]	1	not required	not required [4)]
Fault signal of the alarm transmission system (ATS) [5)]	1	not required	not required [4)]
Fault signal of other system components (e.g. detectors)	1	not required	not required [4)]

1) Monitoring according to clause 14 is necessary only for external parts of the CIE (e.g. remote operation panel, remote concentrators).

2) Including tamper monitoring of these parts (e.g. opening monitoring).

3) At least an indication is necessary, e.g. as „Tamper“.

4) At least an indication is necessary, e.g. as „Fault“.

5) If ATS/power supply are not part of the CIE.

6) Only for IAS with non-exclusive interconnections.

Table 10.01: Inputs

10.2 Limitations of the connected system components

Not more than 1,024 system components (e.g. detectors) shall be connected to one input and the associated interconnection as a reasonable technical limitation. If a common failure of all components caused by **one** simple fault in the area of the interconnections (e.g. interruption of a wire, short circuit, third party carrier) is possible, this number has to be reduced to 128 system components. A system component which has several in- or outputs, counts as **one** system component.

The fault shall be signalled as fault if it does not cause an intruder or tamper signal/message.

Note: Guidelines for CIE connected via networks are in preparation.

If the IAS may be designed such that interconnections of protected premises of IAS which are externally set, can be lead through security protected premises which are completely or partly in unset state, it shall be guaranteed that for simple faults of these interconnections not more than one protected premises or 128 system components of one protected premises fail (see annex A).

10.3 Recognition of signals/messages

Signals/messages of detectors with conventional interfaces (contact outputs) shall be detected reliably within 1 s. Other interfaces, e.g. for BUS-structured IAS, shall be designed such that a specified transmission of the signals/messages is assured; a signal/message shall be detected, however, within 1 s at the latest.

Note: Depending on the design of the interface a common test of CIE and detectors can be required.

10.4 Loss of signals/messages

Inputs/input functions for signals/messages shall be designed such that a loss or change of signals/messages and information is not possible.

10.5 Additional inputs

CIE may have inputs for additional signals/messages (e.g. for so-called technical signals/messages), if it is assured that not negative effects are possible on the alarm signalling part.

11 Control inputs and operation functions

11.1 Required control inputs

CIE shall dispose at least of the required control inputs according to table 11.01 as well as the respective performance features.

Inputs/input functions for	**Number**	**Possibility to connect**	**Monitoring of the related interconnections**
First (basic) ACE for external setting/unsetting	At least 1 per protected premises	class B resp. class C ACE with physical identification feature according to VdS 2119[2)]	In accordance with clause 14
Additional ACE for external setting/unsetting	For class C[3)] at least 1, but it has to be allocated to each protected premises	class B resp. class C ACE with mental identification feature or with time control according to VdS 2119[2)]	In accordance with clause 14
Internal setting/unsetting	No requirement	No requirement	No requirement
Negative acknowledgement from the ATE	At least 1	ATE	No requirement (however „fail-safe-behaviour" according to clause 15.2.1.2) [1)]
Functional testing of the interconnections [4)] (e.g. before an external setting)	At least 1, unless not performed as a control function according to table 11.02 and layer-4-monitoring is not performed every 100 s.	Control function	Not necessary

ACE: Ancillary control equipment ATE: Alarm transmission equipment for alarm signals

1) Monitoring of the interconnection may not apply if the ATE is part of the CIE.

2) Draft at present time.

3) For **class B** CIE it is recommended that at least an additional ACE, designed as ACE with a mental identification feature or with time control, is connectible.

4) Only for **class B** IAS with non-exclusive interconnections.

Table 11.01: Control inputs

11.2 Required operation functions

CIE shall provide at least the operation functions listed in table 11.02 as well as the respective performance features.

Operation functions	Number	Operable for
Restore of latched indications for		
– Intrusion/Hold-up signals/ messages	At least 1	Operator (AL 2)/Installer (AL 3) [1)]
– Tamper signals/messages	At least 1	Installer (AL 3)
– Tamper monitoring of CIE, ACE and warning devices	At least 1	Installer (AL 3)
Test of indicators	At least 1	Operator (AL 2, but also permitted in AL 1)
Test of detectors	At least 1	Operator (AL 2)
Bypassing of the preventing of the setting procedure in IAS with non-exclusive interconnections according to clause 13.2.2 [2)]	At least 1	Operator (AL 2)
Functional testing of the interconnections[2)] (e.g. before external setting)	At least 1, if not designed as input according to clause 11.1 and layer 4 monitoring is not performed every 100 s.	Operator (AL 2)
Restoring of "self-latching" detectors	Function is recommended	Operator (AL 2)

[1)] The type of restoring should be adjustable for the installer between AL 2 and AL 3, at least it has to be performed as AL 2.

[2)] Only in **class B** IAS with non-exclusive interconnections.

Table 11.02: Operation functions

11.3 Isolation of zones

Zones for intruder, tamper and hold-up signals/messages as well as the monitoring measures for CIE, housings of power supply, ACE and warning devices shall not be able to be isolated by the operator of the IAS.

In connection with the internal setting/unsetting procedure the isolation of zones for intrusion signals/messages, however, is admitted.

*Note: The admittance of the isolation of zones for intrusion signals/messages for **class B** IAS is in discussion.*

11.4 Restoring of latched zones in the externally set state of the CIE (option)

Class C

If in special cases for organisational reasons (e.g. security risk for the key holder, several key holders) IAS cannot be unset after an external/remote alarm, deviating from the requirements according to clause 11.3, zones and detectors with latched alarms may be restored (cancelled) once at an ancillary control equipment (ACE) after the external/remote alarm has expired in order to be ready for signalling again. Zones at which the trial of restoring fails (e.g. because a detector is signalling steadily) shall not cause further alarms.

Note: The indicator of the triggered zone shall be kept latched according to clause 12.1.1.

This ACE may be operational after an external alarm and/or remote alarm, triggered/caused by an intruder zone only by the operator (AL 2) after authorisation resp. indicators may be accessible. Furthermore no security relevant functions shall be included which e.g. allow an unauthorised unsetting of the IAS. For the restoring of the zones at least the operation of one lock with at least 5^4 variations or the input of a code of a least 10^4 possible combinations is necessary. The isolation of zones shall not be indicated steadily.

After unsetting of the IAS all previous mentioned operations shall be restored. The use of the equipment shall be indicated (recorded) and included into the "Zwangsläufigkeit". The restoring of this indicator shall be possible only by the maintenance service of the IAS (AL 3).

11.5 Restoring of tamper signals/messages

Latched tamper signals/messages (optical indicators) shall only be restored manually by the installer or maintenance service (AL 3).

Note: CIE which can control several protected premises (see annex A), should be designed such that for the restoring of tamper signals/messages only those protected premises are unset, which are necessary to be entered for the identification of the cause of the tamper signal/message.

11.6 Operation in the externally set state of the IAS

In the externally set state of the IAS besides the unsetting and operation in connection with clauses 11.4 and 11.5 as well as by additional inputs and functions (see clause 11.7) no commands on control inputs or operation elements shall be accepted. However, indicators may be activated by operation elements.

11.7 Additional control inputs and operation functions

CIE may dispose of additional control inputs and operation functions (e.g. input for activating the control function "additional alarm lightening"), if it is secured that no negative influences are possible on the alarm detection part.

11.8 Remote control

A remote control of CIE (e.g. isolation, restoring of zones) from the outside of the protected premises is not permitted.

12 Outputs and event recorder

12.1 Indications

12.1.1 Indications required

CIE shall at least dispose of the indications and respective performance features as shown in table 12.01. CIE may dispose of indications for additional operational conditions and signals/messages if these indications are separated (except concentrated indications) and if it is ensured that they do not negatively influence the alarm detection part.

Indications	**Type of indica-tion**	**Indication depending of the state of the IAS**		**Conditions for indications**	**Latching (freezing) of the indications**	**Restoring of latched optical indications (Restoring audible indications: AL 2)**
		external set	unset			
Function (Operation)	visible	(x)	X	At least presence of U_B	Not applicable	Not applicable
Alarm [1)]	visible	N	X	Alarm generated in external set state of IAS	After EA/RS	Manually after EA/RS by AL 2/AL 3 [5)]
Zone for intrusion signals/messages	visible	N	Xa	Response of a zone for IS	After EA/RS [2)]	Manually after EA/RS by AL 2/AL 3 [5)]
Signal/message of the monitoring of the CIE, ACE and the warning devices	visible and audible	N	X	Triggering of tamper monitoring	After each signal/ message	Manually by AL 3 only
Zone for tamper signals/messages	visible and audible	N	X	Triggering of a zone for TS	After each signal/ message	Manually by AL 3 only
Zone for hold-up signals/messages	visible	N	Xa[6)]	Triggering of a zone for HS	After EA/RS [8)]	Manually after EA/RS by AL 2/AL 3 [5)]
Signal/message of the monitoring of the intercon-nections [3)] as well as the monitoring of interconnection functions [7)]	visible and audible	N	X	Triggering of monitoring of interconnections acc. to clause 14	After triggering of monitoring (if own indicator is provided)	Manually by AL 3 only
Locked state monitoring	visible	N	Xa	Response of locked state monitoring	Not applicable	not applicable
Fault	visible and audible	N (except for system faults)	X	- Faults of the power supply - fault of central processing units	Not required	Manually by operator (AL 2) after end of fault [3)]
				- external faults - Fault ATS - Tamper moni-toring for CIE, WD and ACE, if not allocated to zones for TS	After each signal/ message	Manually by AL 3 only
Warning (class B CIE only [7)])	visible	N	X	Warning signal/ message of a power supply	After each signal/ message	Manually by operator (AL 2)
Third-party signal (class B CIE only [7)])	visible and audible	N	X	Recognition of a third-party signal > 10 s (see clause 14.3)	After each signal/ message	Manually by operator (AL 2)
Setting confirmation	visible and/or audible	X[4)]	Not applica ble	CIE accepted external set state	Not applicable	Not applicable

Table 12.01: Indications required

Abbreviations used in table 12.01:

EA	External alarm	TS	Tamper signals/messages
IS	Intrusion signals/messages	U_B	Operation voltage
PS	Power Supply	HS	Hold-up signals/messages
RS	Remote signalling	(x)	Indication may occur
N	Indication may not happen	X	Indication shall occur automatically
ACE	Ancillary control equipment	Xa	Indication shall occur automatically or on request of the operator
WD	Warning device	AL	Access level

Footnotes to table 12.01:

1) Only required, if not all signals/messages can be indicated at the same time (e.g. for concentrated displays).

2) After unsetting no further signals/messages shall be latched.

3) The visible fault indications shall remain until the cause of the fault has been remedied. If the fault does no more exist, the audible fault indication may be resored automatically, however, it must be possible to restore it manually (AL 2). In this case a repeat of the signal for further faults shall be possible.

4) Only time-limited recognisable nearby the ACE (maximal 30 s).

5) Kind of restoring should be adjustable by installer at AL 2 or AL 3.

6) If indication is processed automatically, the instruction manual should show clearly that the CIE is to be installed such that the indication is not visible for an intruder.

7) Only for IAS with non-exclusive interconnections.

8) For hold-up signals/messages an external alarm shall be generated only in exceptional cases, see clause 13.4.

12.1.2 Allocation of indications

All indications as required in table 12.01 shall be configured together at least at one place such way that optical indications can be seen with one sight and acoustic indications can be heard (e.g. at the CIE or a remote indications panel).

Note: The design of the indicators is described in clause 9.7.

12.1.3 First-to-alarm indication

After unsetting it must be detected which zones have triggered in the external set state of the IAS.

12.1.4 Indication of tamper signals/messages

In the unset state of the IAS triggering of zones for tamper signals/messages as well as tamper monitoring for CIE, ACE and WD shall be indicated optically and audible (see table 12.01). The optical indicators may be designed as collective indicator. It must, however, be visible for installer and maintenance service (AL 3) which tamper monitoring (e.g. the one of the ACE) has caused the signal/message.

The visible indicator (collective) shall be stored even if the criteria causing the indication is no more given. It shall be possible for the operator (AL 2) to restore the audible indication manually. The visible indicator shall be restorable by installer or maintenance service (AL 3).

12.1.5 Access to indicators

Indicators of CIE shall not be accessible to everybody, but have to be allocated to AL 2.

Note: This requirement can be realised either technically (e.g. key switch or code) or organisationally by respective installation of the CIE (see VdS 2311).

12.1.6 Indications in case of several protected premises

If a formation of several protected premises is possible with the CIE, for each protected premises indication boards shall be available for

- faults,
- tamper and
- operational state of zones (e.g. collective indication)

as well as – if given – with test of indication and restore button being connected to the CIE. These shall be visible according to clause 12.1.5 only for AL 2.

12.2 Outputs for the notification of signals/messages as well as for detector testing/cancellation

12.2.1 Required outputs

CIE shall dispose of the outputs and respective performance features as in table 12.02 (description of interfaces see clause 15).

Outputs/ Output functions	**Freedom of potential of output required**	**Unlimited function for faults of mains power supply required**	**Monitoring of associated interconnec-tion**	**Condition for triggering of output**	**Duration of function**
Audible external WD No 1 and 2[1)]	No	Yes	Acc. to clause 14	EA	Adjustable between 20 s and 180 s[4)]
Visible external WD[1)]	No	Yes	Acc. to clause 14	EA	Until restoring of triggering (automatically together with or manually after unsetting)
WD for internal alarm (if fitted)	No	Yes	No requirements	Internal alarm	No requirement
Class B AS for triggering of ATE	Yes[2)]	Yes	Is done by ATE[2)]	EA/RS (intrusion and/or hold-up)	Duration ≥ 250 ms ≤ 180 s[3)]
Class C is for triggering of ATE	Yes[2)]	Yes	Is done by ATE[2)]	EA/RS for intrusion	Duration ≥ 250 ms ≤ 180 s[3)]
Class C HS for triggering of ATE	Yes[2)]	Yes	Is done by ATE[2)]	EA/RS for hold-up	Duration ≥ 250 ms ≤ 180 s
Fault signal for triggering of ATE	Yes[2)]	Yes	No requirements *Note: Is monitored by ATE*	Fault of PS and/or central processing units (in unset state of IAS, see clause 6.2)	Duration ≥ 250 ms
"Third-party-signal"[6)] (for triggering of ATE)	Yes[2)]	Yes	No requirement; *Note: Interconnection is monitored by ATE*	Detection of a "Third-party-signal" > 30 s (see clause 14.3)	Duration ≥ 250 ms
Set/-unset status signal/ message of IAS per protected premises	Yes[2)]	Yes	No requirements	State set / unset of IAS per protected premises	≥ 250 ms
Test of detectors[5)]	Acc. to clause 14	Yes	No requirements	Operation „Detector test" (Walk test)	No requirements
Restore self-latching detector	Acc. to clause 14	Yes	No requirements	Operation „Restore detector"	No requirements

Table 12.02: Required outputs

Abbreviations to table 12.02:

EA External alarm
IS Intrusion signal/message
PS Power supply
RS Remote signalling
AS alarm signal/message
WD Warning device
ATE Alarm transmission equipment
HS Hold-up signal/message

Footnotes to table 12.02:

1) Not applicable for CIE designed exclusively for remote alarm by ATE.

2) Not applicable for ATE integrated in the housing of CIE.

3) If all power supplies of CIE fail the outputs shall be controlled at least for 250 ms.

4) Adjustable in at least four steps.

5) It must be ensured that no detector test function can be performed in the external set state of the IAS.

6) Only for IAS with non-exclusive interconnections; signal/message shall be interpreted in the external set state of the IAS as tamper.

12.2.2 Loss of signals/messages

Outputs/output functions shall be designed such that no signals/messages and no information is lost and/or falsified.

12.2.3 Additional outputs

CIE may have outputs for additional signals/messages (e.g. for so-called technical signals/messages), if it is assured that no negative influences on the alarm signalling part are possible.

12.3 Outputs for blocking devices

At least one electromechanical blocking devices per protected premises shall be connectable to the CIE. If the CIE processes more than one protected premises (see annex A), connection interfaces for further electromechanical blocking devices shall be available (e.g. blocking locks), in order to be able to include all protected premises in the “Zwangsläufigkeit” of the IAS.

External setting shall be possible only if all blocking devices associated to a protected premises are blocked; after external setting the blocking devices shall inhibit the access to the respective protected premises for the duration of the setting.

12.4 Recording of events

12.4.1 Operational events

Class B

CIE should have at least the measures for recording events according to the content of table 12.03.

Note: Remote parameterisation resp. remote diagnosis according to clause 7.8 for CIE of class B is admitted only if an event storage is available.

Class C

CIE shall have at least the measures for recording events according to the content of table 12.03.

Devices	Events to be recorded	Capacity	Marking with date and time	Keeping of memory contents in case of total failure of the power supply	Reading of memory contents	Access to the adjust-ment of date and time	Altering of memory contents
Alarm-counting device	External and remote alarms	≥ 100 events [3]	None	≥ 8 days	Operator (AL 2) and installer (AL 3)	Not applicable	Not allowed [2]
Event recorder	– External and remote alarms, if given with indication of zone – Isolations – Tamper signals/ messages – Ext. Setting/ unsetting – Fault – Recognised third-party-signal[5]	≥ 1,000 events [3]	Yes	≥ 8 days	Operator (AL 2) and installer (AL 3)	Only installer (AL 3) [1]	Not allowed [2]
Event recording in case of remote paramete-risation	– Remote paramete-risation [4] – Remote diagnosis [4]	≥ 1,000 events [3]	Yes	≥ 8 days	Operator (AL 2) and installer (AL 3)	Only installer (AL 3) [1]	Not allowed [2]

[1] Except the change from summer to winter time.

[2] For the installer an influence shall at least be difficult.

[3] After these events old filed events may be overwritten.

[4] If function is available.

[5] Only for IAS with non-exclusive interconnections.

Table 12.03: Recording of events

12.4.2 Changes of date and time

Class B

If an event storage is available, all changes on date and time shall be recorded in this event storage.

Class C

All changes on date and time shall be recorded in the event storage.

13 Processing of signals/messages

13.1 General

CIE shall process received signals/messages and depending on the state of the system indicate and/or notify them.

13.2 Setting/Unsetting

13.2.1 General

The external setting/unsetting shall be possible for the operator (AL 2) via an Ancillary Control Equipment (ACE) with physical identification feature of the relevant class according to the guidelines for ACE, VdS 2119.

Class B

A further – additional - ACE is recommended additionally.

Class C

It shall be possible for external setting/unsetting to use an additonal ACE (e.g. an ACE with mental identification feature and/or ACE with time control).

13.2.2 External setting

It shall be possible to externally set the CIE respectively the CIE shall adopt the externally set state only if

- it is fully operational (except admitted isolations),
- no intruder/hold-up signals/messages are pending,
- no fault signals/messages are pending,
- no warning alarms of power supply are pending (only for IAS **class B** with non-exclusiv interconnections and power supply type III),
- no tamper signals/messages are pending,
- no signals/messages on tamper monitoring of the CIE, Warning Devices and ACE are pending,
- no signals/messages of the monitoring of interconnections are pending,
- no signals/messages of the “third-party-monitoring” are pending (only for IAS **class B** with non-exclusive interconnections),
- the interconnections have been checked in a period of ≤ 100 s before setting with a positive result (only for IAS **class B** with non-exclusive interconnections),
- no signals/messages are pending from the blocking monitoring,
- no remote diagnosis /remote parameterisation is performed.

An inhibit of the setting caused by warning signals of the power supply type II may be bypassed by a deliberate action of the operator (see also clause 11.2). This deliberate action shall be performed at each setting procedure.

If the operation of the respective ACE does not ensure that the IAS has adopted its set state after switching the ACE (e.g. if key-used ACE with material identification feature inhibit the removal of the key until the setting of the IAS really is effected), the setting made shall be indicated in the surroundings of the ACE by a timely restricted visible or audible signal.

A setting of the IAS in connection with the ACE with mental identification feature shall be possible only if the adjusted combination of the ACE is discarded and for ACE with time control the blocking time is set.

Note: This logical conjunction may also be included in the ACE, see VdS 2119.

13.2.3 External Unsetting

The unsetting of the CIE shall be possible only, if all ACE (e.g. when an ACE with material and mental identification feature is available) have been properly activated - respectively the ACE with time control has released the unsetting procedure.

13.2.4 Access to protected premises after external alarm

For IAS with ACE with mental identification feature and/or time control the access to protected premises shall be possible after an external/remote alarm independent of the state of this ACE after expiry of a time adjustable by the installer (AL 3) of 0 – 30 min. For IAS with several protected premises (see annex A) only access to the affected protected premises should be released.

Note: By this requirement it is only guaranteed, that the access to protected premises after an external/remote alarm is eased; the IAS shall still leave in the externally set state.

13.2.5 Internal setting/unsetting

For the internal setting of the IAS when persons could be present in the protected premises, the IAS should be internally settable for part of the protected premises as well as for the complete protected premises.

The internal setting may be made on the CIE or a remote ACE within the protected premises. If an intruder alarm is triggered when the IAS is internally set, only WD shall be addressed for the internal alarm (see also table 12.02).

13.3 Reaction time, loss of signals/messages

After receipt of a signal/message (see clause 10.3) an indication shall be shown within 10 s (see clause 12.1) respectively the outputs for signals/messages shall be addressed (see clause 12.2). No signals/messages shall be lost or falsified.

If the IAS is in its state as intended delays caused by running and/or processing times of signals/messages within the IAS shall not lead to security relevant influences (e.g. fault signals/messages).

13.4 Hold-up signals/messages

CIE shall be designed such that hold-up signals/messages lead to remote alarm independently of the state of the ACE (see table 13.01) but **not** to external alarm. After triggering of a hold-up signal/message it shall be possible to trigger a further hold-up signal/message after 180 s the latest. If in exceptional cases IAS are provided with external alarm only, it shall then also be possible to trigger an external alarm by a hold-up signal/message.

Steady activity of hold-up detectors shall not lead to multiple triggering of the remote alarm.

Hold-up detectors being in an external set area may be isolated automatically; after unsetting of the area the detectors shall be re-joined automatically.

13.5 Fault of power supply of the CIE

No external/remote alarm shall be triggered after the fault of the power supply of the CIE and following return of the mains voltage, if no actual alarm signals/messages are pending respectively the CIE is in unset state.

13.6 Cancelling of external/remote alarm

An external/remote alarm triggered can be cancelled by the unsetting of the IAS only if this alarm has not been triggered by a zone for tamper signals/messages or by the tamper monitoring for CIE, housings of power supply, ACE and WD.

13.7 Suppression of external alarm in the case of remote alarm

For IAS with notification via remote signalling depending of the intervention time triggering of the warning devices (external alarm) may be suppressed (see VdS 2311).

In this case first the outputs for alarm signals/messages are adressed for triggering an ATE according to clause 12.2.1 (remote signalling).

If the signal/message is not or only partly transmitted by the alarm transmission system (e.g. there is no acknowlegdement from the Alarm receiving equipment (ARE)), the ARE at latest after 240 s triggers the input “negative acknowledgement from the ATE” according to clauses 11.1 and 15.2.1.2 – and the CIE generates an external alarm (see also Table 13.01).

Note: For hold-up no external alarm shall be triggered.

13.8 Alarm repetition

If in the external set state of the IAS an external/remote alarm has been triggered, a new triggering of the zone which caused the alarm shall not lead to an external/remote alarm again. Triggering of further zones may, however, lead to further external/remote alarms.

Triggering of zones for hold-up alarms can lead as often as useful to repetition of hold-up signals/messages.

13.9 Reactions of the CIE depending of the state of the system

Depending of the state of the system (unset, internally/externally set) CIE shall react according to table 13.01.

Event (triggering input)	Reaction at system condition		
	Unset	Internally set (if fitted)	Externally set
Intrusion signal/message	Indication [4], no EA/RS	Triggering of outputs for IA, no EA/RS	Triggering of outputs for EA/ RS [2]
Hold-up signal/message [1]	Triggering of outputs for RS	Triggering of outputs for RS	Triggering of outputs for RS
Tamper signal/message	Indication[4] (visible and audible), no EA/RS	Indication[4] (visible and audible), no EA/RS	Triggering of outputs for EA/RS [2]
Signal/message on tamper monitoring of ACE and WD	Indication[4] (visible and audible), no EA/RA	Indication[4], no EA/RS	Triggering of outputs for EA/RS [2]
Signal/message of tamper monitoring of CIE	Indication[4] (visible and audible), no EA/RS	Indication[4], no EA/RS	Triggering of outputs for EA/RS [2]
Signal/message of monitoring of interconnections for intruder detectors and tamper detection	Indication[4], no EA/RS	Indication[4], no EA/RS	Triggering of outputs for EA/RS [2]
Signal/message of regularly performed monitoring of interconnections [5]	Indication[4], no EA/RS	Indication[4], no EA/RSA	Triggering of outputs for EA/RS and indication after unsetting of IAS
"Third-party signal" detection triggered [5]	Indication for "third-party- signal" during > 10 s, triggering of output "third-party-signal" after > 30 s, no triggering of outputs for EA/RS	As unset	As unset, however a signal/message "third-party-signal" shall be interpreted as tamper signal/message.
Monitoring of locked state[3]	Indication[4], no EA/RS	Indication[4], no EA/RS	No EA/RS
External fault signal/ message	Indication[4], no EA/RS	Indication[4], no EA/RS	No EA/RS
Monitoring of function acc. to clause 6.2 (if given)	Indication[4], no EA	Indication[4], no EA	Triggering of outputs for EA/RS [2]
Negative acknowledgement of ATE triggered (if ATE available)	No effects	No effects	For EA/RS and triggering of input: immediate external alarm
Fault signal/message of ATS	Indication[4], no EA	Indication[4], no EA	For EA/RS and triggering of input: immediate external alarm

Abbreviations:

ATS	Alarm transmission system	IA	Internal alarm	ATE	Alarm transmission
EA	External alarm	TS	Tamper signal/message		equipment
IS	Intrusion signal/message	ACE	Ancillary control equipment	HS	Hold-up signal/message
RS	Remote signalling	WD	Warning device	IC	Interconnection

[1] For hold-up signals/messages external alarm shall be generated only in exceptional cases - see clause 13.4.

[2] If a function acc. to clause 13.7 is available, external alarm is at first not necessary when generating a remote alarm over ATS.

[3] Locked state monitoring of doors with ACE may be realised already in connection with the ACE.

[4] See table 12.01

[5] For IAS with non-exclusive interconnections only.

Table 13.01: Reactions of the CIE

13.10 Additional functions

The processing of additional functions by the CIE (e.g. processing of technical alarms) shall have no negative influence on the alarm signalling part and shall be unambiguous (e.g. a technical signal/message shall lead also to the triggering of an output for technical signals/messages; in any case it may lead to an external alarm/remote signalling).

14 Monitoring of the interconnections

14.1 General

*Remark: Non-exclusive interconnections (e.g. via radio links) may at present only be used in **class B** IAS.*

For the transmission of signals/messages and control signals exclusive as well as non-exclusive interconnections may be used. These shall be suitable for the transmission of alarm signals/messages and signals of the IAS. Furthermore they shall be designed such way, that even in the case of a high volume of signals/ messages - for IAS with non-exclusive interconnections also other users of the interconnections – no signals/messages and information get lost or are altered.

For planning, installation, commissioning and maintenance of the IAS the manufacturer of the CIE has to provide equipment for testing the interconnections.

Non-exclusive interconnections may be only used when for an intended use an availability of more than 98 % over a period of each 24 h is guaranteed and each transmitted signal/message is acknowledged (that means bi-directional transmission).

14.2 Exclusive interconnections

14.2.1 Triggering behaviour during quiescent current (End-of line-resistor-technology)

If interconnections are monitored by quiescent current (End-of line-resistor-technology) a change of criteria (e.g. end-of-line resistor for 40 % and more pending longer than 200 ms) shall be detected and indicated if the change can lead to the fact that one or several system components of the IAS (e.g. detector) would fail.

14.2.2 Triggering behaviour of other types of monitoring

Interruptions and short circuits of interconnections which are not monitored by quiescent current (end-of line-resistor-technology) as well as a partly disturbed transmission shall be detected after 10 s the latest and triggered if these would lead to the fact that one or several system components of the IAS (e.g. detector) would fail.

14.3 Non-exclusive interconnections (only for class B-IAS)

If the intended function of non-exclusive interconnections, used not exclusively by the IAS, can be influenced by third-party signals (e.g. in the case of radio communication by other radio services in the same frequency or in the same frequency range, strong radio services nearby the frequency range), measures shall be taken which guarantee an operation of the IAS as intended (e.g. for radio transmission further transmission possibilities on additional frequencies with automatic change of frequency).

Further on additional measures are necessary (e.g. a second frequency band), when these influences may also be caused deliberately (tamper).

In this case first a transmission possibility has first to be searched on another frequency. If this is not possible, the frequency band has to be changed.

In addition it shall be detected and signalled, when the interconnection in case of non-exclusive interconnections > 30 s is not more available for the transmission of signals/messages of the IAS (possible failures are e.g. third-party signal blocks the transmission in "radio-linked" IAS; overload of the interconnections in BUS-structured IAS). For a detected fault first an indication is given (e.g. third-party signal > 10 s present); for a signal present > 30 s a signal/message is generated on the output "third-party signal", but no external alarm/remote signalling (see table 13.01).

Additionally the interconnection has to be checked on function and the IAS on completeness of all system components (integrity of the IAS) by a transmission of signals/messages (layer 4 according to the OSI-7-layer model) at maximum 100 s before each external setting and at least 180 s in the external set state of the IAS. Faults revealed at this check are to be indicated as “fault of interconnection” (see table 12.01).

Note: The a.m. values may change during the revision of the European standard EN 50131-1. These changes may have effects on these guidelines.

14.4 Electric circuits for setting/unsetting

The electric circuits for the external setting/unsetting shall be monitored at least according to the requirements as described in clauses 14.2 and 14.3. Faults of these electric circuits shall not lead to an unsetting.

15 Interfaces

15.1 Interfaces to other system components of the IAS

For IAS with a third party power supply of detectors with a mains supply up to at maximum 48 V DC and a “conventional” line termination technology (end-of line-resistor-technology) the following requirements for in- and outputs are valid.

15.1.1 Parallel interface for detectors

Interfaces shall be described in detail by the manufacturer. Alternatively the proposals for a standardized parallel detector interface as described in annex C may be used.

15.1.2 Parallel interface for detectors

The input shall meet the following requirements:

- Connectable to a relais with potential-free contacts which is closed in the non-alarm state (idle state) and an open contact in the case of an event.

  Note: Corresponds with interface CCITT V.31bis.

- A pending signal/message ≥ 1 s shall be detected.

15.2 Interfaces to alarm transmission equipment

Note: Not applicable for integrated or especially for the CIE designed ATE.

15.2.1 Parallel interface

If the interface is parallel the following requirements are valid:

15.2.1.1 Input for external faults of ATS

The input shall meet the following requirements:

- Connectable to outputs where in the non-alarm state (idle state) a closed contact/electronic switch (resistance ≤ 1 kΩ), in the case of a fault an open contact/electronic switch ≥ 500 kΩ) is available.

  Note: Corresponds with interface CCITT V.31bis.

- A pending signal/message ≥ 1 s shall be detected.

15.2.1.2 Input for negative acknowledgement of ATS

The input shall meet the following requirements:

- Connectable to outputs where in the non-alarm state (idle state) a closed contact/ electronic switch (resistor ≤ 1 kΩ), in the case of missing acknowledgement an open contact/electronic switch (resistor ≥ 500 kΩ) is available.

  Note: Corresponds with interface CCITT V.31bis.

The triggering occurs in the range of ≥ 1 s ≤ 3 s and shall result in a reaction according to clause 13.6.

15.2.1.3 Output for alarm signals/messages for CIE of class B resp. intruder alarm signals/messages for CIE of class C

The output shall meet the following requirements:

- Potential free
- Closed in the non-alarm state (low resistance), opening in the event of a signal/ message (high resistance)
- Response time ≥ 250 ms ... ≤ 180 s

15.2.1.4 Output for hold-up signals/messages (required only for CIE of class C)

The output shall meet the following requirements:

- Potential free
- Closed in the non-alarm state (low resistance), opens in the event of a signal/message (high resistance)
- Response time ≥ 250 ms ... ≤ 180 s

15.2.1.5 Output for fault signals/messages

The output shall meet the following requirements:

- Potential free
- Closed in the non-alarm state (low resistance), opens in the event of a signal/ message (high resistance)
- Response time at least 250 ms, at maximum as long a fault condition is pending

Further features shall be specified by the manufacturer.

15.2.1.6 Output for signals/messages „Third-party signal“

The output shall meet the following requirements:

- Potential free
- Closed in the non-alarm state (low resistance), opening in the event of a signal/message (high resistance)
- Response time at least 250 ms, at maximum as long a fault condition is pending

Further features shall be specified by the manufacturer.

15.2.1.7 Output for signal/message „Set/Unset“

The output shall meet the following requirements:

- Potential free
- Closed in the non-alarm state (low resistance), opening in the set state (high resistance)

Further features shall be specified by the manufacturer.

15.2.2 Serial interface (S_1)

Serial interfaces shall comply with the requirements of the guidelines for alarm transmission equipment for alarm signals/messages, VdS 2463 and the transmission protocol for alarm signals/messages, VdS 2465. If a serial interface according to the requirements is available, a parallel interface according to clause 15.2.1 is not necessary.

15.3 Other interfaces

The performance shall be specified by the manufacturer.

16 Power supply

For the power supply of the CIE only a power supply for alarm systems according to VdS 2115 shall be used.

17 Options

Options shall have no adverse effect on the functions required for CIE. The performances of the options shall be specified by the manufacturer.

Changes

Compared with version VdS 2252 : 1996-01 (02) the following changes were made:

- Completion of requirements for remote CIE of class B
- Including clause 2 (new) “Normative references”
- Revision of complete clause 3 “Definitions”
- Revision of complete clause 5 “Protection against environmental influences”
- Revision of clause 6.2 „Function monitoring“ regarding different requirements for classes B and C
- Completion of clause 6.8 with „Remote parameterisation“
- Including clause 6.9 (new) „Remote diagnosis”
- Deletion of the lower requirements for class B; deletion of requirements regarding the lock of CIE for class C
- Complete revision of clause 9.2; a. o. raise of number of system components from 512 to 1024
- Deletion of admittance of zone isolation in clause 11.3
- Clarifying in clause 12.1.5 that requirements can be fulfilled by technical as well as organisational measures
- Revision of table 12.03; in future at least 1,000 filable events are required; furthermore remote diagnosis and remote parameterisation shall be recorded.
- Completion of requirements in clause 13.3 regarding the running and/or processing times of signals/
- Complete revision of clause 14 „Monitoring of interconnections for signals/ messages“
- Adaption of Annex A to actual version of VdS 2311
- New annex B for performance of remote IAS for class B
- New annex C with a proposal for performance of parallel interfaces for detectors

Annex A Examples for design of protected premises (informativ)

The examples according figures A.01 – A.05 address the most used possibilities for the setting/unsetting of protected premises. The presented versions may be also combined (e.g. several protected premises independent from each other in connection with areas included in the “Zwangsläufigkeit” of protected premises by blocking elements).

A.1 One protected premises with on ACE

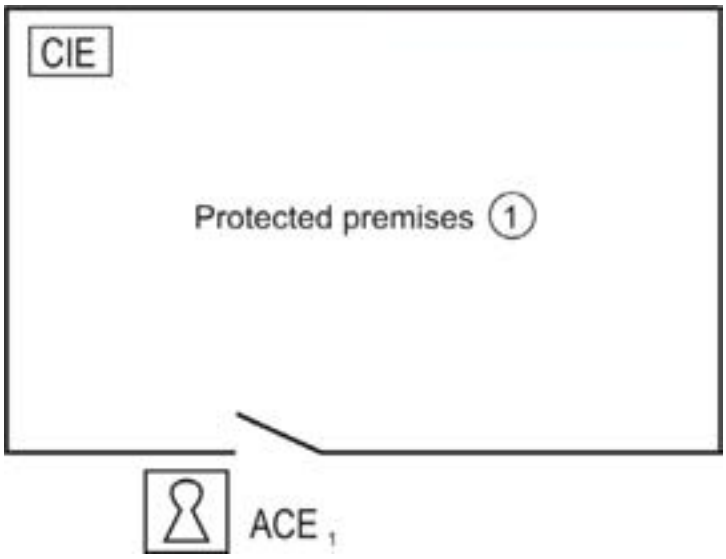

Figure A.01

A.2 One protected premises with several ACE

The example shown in figure A.02 the external setting of a protected premises is made only, when all ACE (here ACE 1.1 and ACE 1.2) are operated; the unsetting is made already after operation of one ACE.

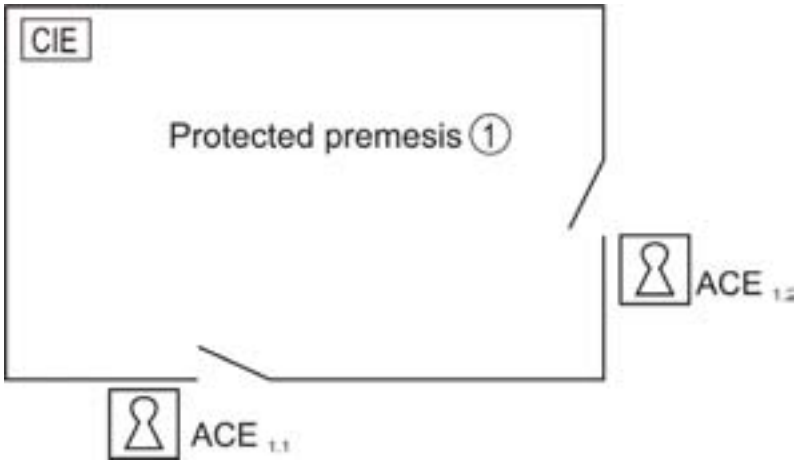

Figure A.02

A.3 One protected premises with remote protected premises

The example in figure A.03 show protected premises 1 and the remote seperated premises 2, 3 being set/unset together by the ACE. The remote protected premises 2 and 3 are included in the “Zwangsläufigkeit” by the blocking elements SpE 1.2 and SpE 1.3.

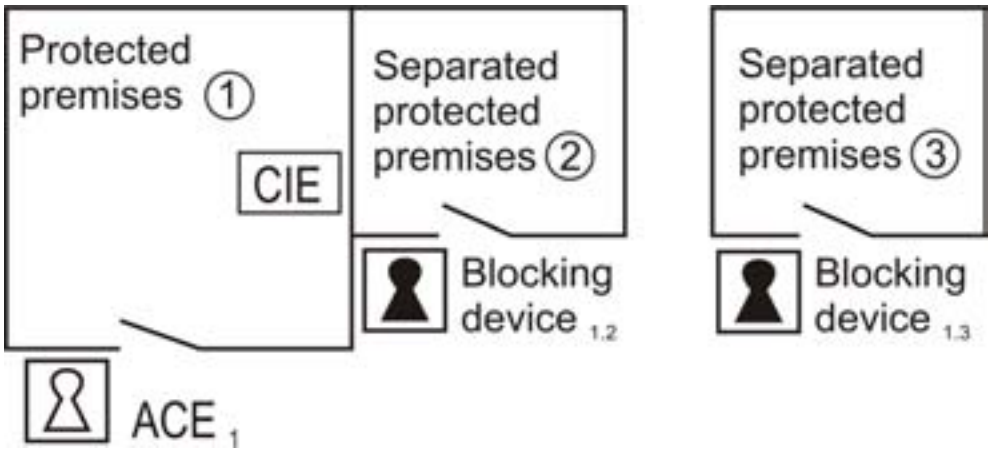

Figure A.03

A.4 Several protected premises

For IAS with several protected premises areas being independant from each other, the CIE shall be located in an external set area if one or several part areas are externally set (e.g. own monitored “CIE-area” (protected premises) which is included in the “Zwangsläufigkeit”, a monitored housing for the CIE which is monitored for locked-state, opening and penetration).

Figure A.04 shows an example with two protected premises depending on each other where protected premises 2 may be set externally alone by ACE2. Additionally protected premises 1 can be set by ACE1 if protected premises 2 has already been externally set. The unsetting of protected premises 1 may be made independently from protected premises 2.

Depending on the design of the IAS and ACE2 the protected premises 1 and 2 may be externally set/unset together.

The CIE shall be located in protected premises 2.

In order to recognise the operation state of protected premises 2, faults, tamper as well as operation state of the respective zones shall be indicated in the surroundings of ACE1 (e.g. by collective indication) and, if necessary a button for testing the indicator and restoring shall be assigned too.

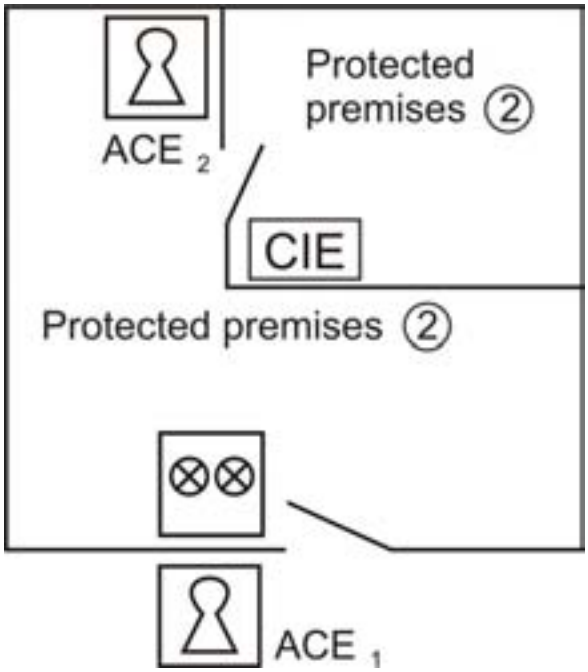

Figure A.04

The example in figure A.05 shows several protected premises which may be set/unset externally independent from each other.

The CIE shall be located in protected premises 4 (room or monitored housing).

In order to recognise the operation state of protected premises to be externally set (e.g. 1) and the protected premises 4 of the CIE and to be able to operate the IAS, faults, tamper as well as operation state of the respective zones shall be indicated in the surroundings of respective ACE (e.g. by collective indication) and a bottom for indicator-testing and restoring shall be assigned to.

Note 1: This example is admitted only for a common user for all protected premises.

Note 2: For IAS with several protected premises which are independent from each other the unsetting of all protected premises incl. an own CIE- protected premises may be released after an alarm by the IAS in the externally set state (i. e. required is only an identification feature for the unsetting and available ACE with mental identification feature or time control are bypassed.

Note 3: For faults and the triggering of tamper zones depending on the design of the IAS it may be necessary to unset several or all protected premises for the remedy of faults resp. restoring of tamper zones.

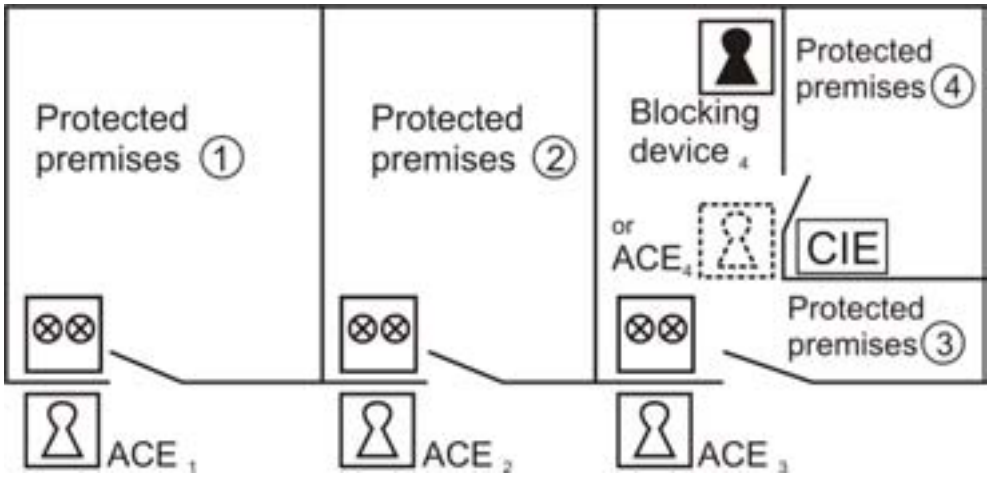

Figure A.05

The example in figure A.06 with several protected premises shows that assignment of the CIE-zone 4 (protected premises 4) is such that without moving into another protected premises it may be reached.

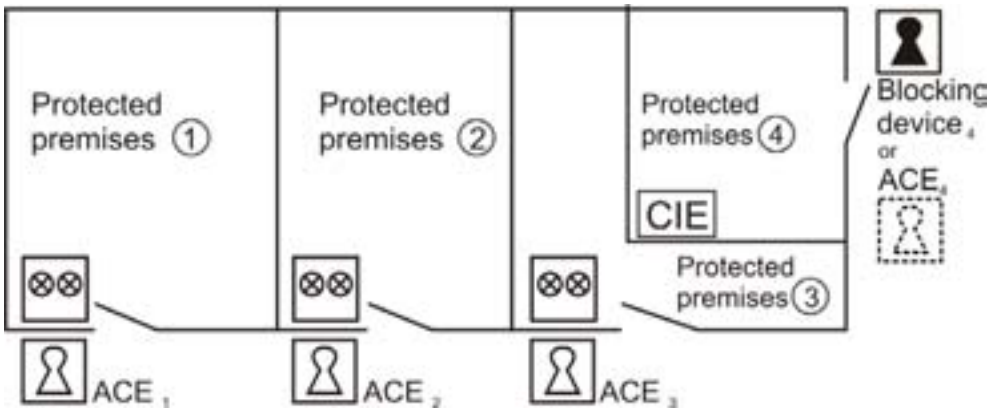

Figure A.06

Annex B Class B „radio-linked IAS“ (normative)

If radio communication is used as a non-exclusive interconnection the requirements depend very much of the use of the single frequency bands, which are at the time subject to steady changes. Due to this fact the concrete requirements and test methods for radio-based transmission may change in short time.

According to the actual knowledge the following guidelines in table B.01 for radio communication are valid in addition to the requirements in clause 14.3:

Characteristic/Function	**Design**
Frequency bands:	At least two bands (e.g. 433 and 868 MHz)
„Channels“:	≥ 20 channels within 433 MHz and ≥ 4 within 868 MHz
Directions of the communications:	Technical solution: today only bi-directional
Monitoring of the interconnections on availability (layer 1 according to the OSI-7-Layer model) for each frequency band („Third-party signal monitoring“):	In case of a fault ≥ 10 s indication „third-party signal“ according to table 13.01, in case of a fault ≥ 30 s triggering [1)] of the output „third-party signal“ according to table 13.01
Monitoring of the interconnections for function by a signal/message transmission (layer 4 according to the OSI-7-layer-model) for each frequency band („Function monitoring of interconnections“):	At least every 180 s as well as automatically ≤ 100 s before every external setting procedure; in case of a failure indication/preventing of external setting resp. external alarm/remote signalling according to table 13.01

[1)] Signal/message is triggered only if the attempt to change to other available "channels" and if necessary bands was not successful. In the unset state of the IAS a fault signal/message is generated, in the external set state external alarm and/or remote signalling.

Table B.01: Radio-linked transmission

Note: The values mentioned in table B.01 may change during the revision of the European standard EN 50131-1. These changes may have effects on these guidelines.

Annex C Parallel interface for detectors (informativ) (Options with requirements)

For a standardized parallel Interface for detectors the following requirements are proposed for the time being.

C.1 Supply voltage for detectors

For the supply of detectors a separate protected (fused) output with sufficient loading capacity with a voltage of 12 V= ± 25 % shall be provided.

Remark: Depending of the design of the der IAS this output may also be located in another system component (e.g. a power supply unit).

C.2 Input for intrusion signals/messages

The input shall meet the following conditions:

- Operation voltage (output voltage) maximum 48 V DC
- Operation current (output current) maximum 50 mA
- Defined flow of current means non alarm state
- Open state or deviation from the defined flow of current means signal/message
- An open state or a deviation from a defined condition shall be detected within ≥ 200 ms

C.3 Inputs for hold-up signals/messages

The input shall meet the following conditions:

- Operation voltage (output voltage) maximum 48 V DC
- Operation current (output current) maximum 50 mA
- Defined flow of current means non alarm state
- Open state or deviation from the defined flow of current means signal/message
- An open state or a deviation from a defined condition shall be detected within ≥ 200 ms

C.4 Inputs for tamper signals/messages

The input shall meet the following conditions:

- Operation voltage (output voltage) maximum 48 V DC
- Operation current (output current) maximum 50 mA
- Defined flow of current means non alarm state
- Open state or deviation from the defined flow of current means signal/message
- An open state or a deviation from a defined condition shall be detected within ≥ 200 ms

C.5 Input for external faults from detectors (e.g. fault, masking of mouvement detectors)

The input shall meet the following conditions:

- Connectable to a relay with potential free contacts switch were in the normal (non-alarm) state a closed contact and in case of a fault an open contact is available.

  Note: Corresponds with interface CCITT V.31bis.

- A pending signal/message available ≥ 1 s shall be detected

C.6 Output for the control of logical (memory) controls of detectors (indication, freezing of memory)

For the control of logical controls of detectors an output shall be available which is designed as follows:

Enabled (input LOW or logical 0)

	Minimum	**Maximum**
– Output voltage	0 V	1,5 V

Disabled (input HIGH or logical 1)

	Minimum	**Maximum**
– Output voltage	3.5 V	U_{Bmax}

The output shall dispose of a nominal voltage of at maximum 48 V DC, shall be short-circuit-proof and shall be able to deliver a current of 1 – 20 mA.

C.7 Output for detector testing (test)

For enabling/disabling of the testing functions of detectors an output shall be available, which is designed as follows:

Enabled (input LOW or logical 0)

	Minimum	**Maximum**
– Output voltage	0 V	1.5 V

Disabled (input HIGH or logical 1)

	Minimum	**Maximum**
– Output voltage	3.5 V	U_{Bmax}

The duration of triggering shall be ≥ 1 s.

C.8 Output for the control of operation modes

For enabling/disabling of operation modes (e.g. of detectors) an output shall be availabe designed as follows:

Operation function switched off (input LOW or logical 0), e.g. emitter set, transmitter switched on, motion detector fully operational,

Memory enabled (IAS set)

	Minimum	**Maximum**
– Output voltage	0 V	1.5 V

Operation function switched off (input HIGH or logical 1)

	Minimum	**Maximum**
– Output voltage	3.5 V	U_{Bmax}

The duration of triggering shall be ≥ 1 s.

C.9 Output for restoring of self-latching detectors

For the restoring of self-latching detectors an output shall be available designed as follows:

Restoring (input LOW or logical 0)

	Minimum	**Maximum**
– Output voltage	0 V	1.5 V

Idle state (input HIGH or logical 1)

	Minimum	**Maximum**
– Output voltage	3.5 V	U_{Bmax}

The duration of the triggering shall be ≥ 1 s.

Amendment VdS 2252en-S1 : 2006-12 (01): Revision of table 12.01 „Required indications“

Warning note

This draft of an amendment of the guidelines for Intruder Alarm Systems, class B and C Control and Indicating Equipment (CIE) VdS 2252 : 2003-06 (03) contains corrections in table 12.01 „required indications“ caused by a printing fault in columns indication of faults. The draft of this new table is due for approval.

Changes during the approval procedure may have effects on these guidelines.

1.2 Validity*; the clause 2.1 of VdS 2252 : 2003-12 will be amended with the following sentence:*

The guidelines VdS 2252en : 2003-06 (03) are applicable starting from 01. December 2006 only in connection with amendment VdS 2252-S1en : 2006-12 (01). For prolongations/changes of a certificate of a VdS-approved product the guidelines VdS 2252en : 2003-06 (03) are to be applied at the latest starting from 01 January 2008 only together with the amendment VdS 2252-S1en : 2006-12.

12.1 Indications

12.1.1 Indications required, *the table 12.01 of VdS 2252 : 2003-12 is replaced by the following table*

CIE shall at least dispose of the indications and respective performance features as shown in table 12.01. CIE may dispose of indications for additional operational conditions and signals/messages if these indications are separated (except concentrated indications) and if it is ensured that they do not negatively influence the alarm detection part.

Indications	Type of indication	Indication depending of the state of the IAS		Conditions for indications	Latching (freezing) of the indications	Restoring of latched visible indications (restoring audible indications: AL 2)
		external set	unset			
Function (Operation)	visible	(x)	X	At least presence of U_B	Not applicable	Not applicable
Alarm[1)]	visible	N	X	Alarm generated in external set state of IAS	After EA/RS	Manually after EA/RS by AL 2/AL 3 [5)]
Zone for intrusion signals/messages	visible	N	Xa	Response of a zone for IS	After EA/RS [2)]	Manually after EA/RS by AL 2/AL 3 [5)]
Signal/message of the monitoring of the CIE, ACE and the warning devices	visible and audible	N	X	Triggering of tamper monitoring	After each signal/ message	Manually by AL 3 only
Zone for tamper signals/messages	visible and audible	N	X	Triggering of a zone for TS	After each signal/ message	Manually by AL 3 only
Zone for hold-up signals/messages	visible	N	Xa[6)]	Triggering of a zone for HS	After EA/RS [8)]	Manually after EA/RS by AL 2/AL 3 [5)]
Signal/message of the monitoring of the intercon- nections [3)] as well as the monitoring of interconnection functions [7)]	visible and audible	N	X	Triggering of monitoring of interconnections acc. to clause 14	After triggering of monitoring (if own indicator is provided)	Manually by AL 3 only
Locked state monitoring	visible	N	Xa	Response of locked state monitoring	Not applicable	not applicable
Fault	visible and audible	N (except for system faults)	X	- Faults of the PS - Fault of central processing units	Not required	Manually by operator (AL 2) after end of fault [3)]
				- external faults - Fault ATS	After each signal/ message	Manually by operator (AL 2) after end of fault [3)]
				Tamper monitoring for CIE, WD and ACE, if not allocated to zone for TS	After each signal/ message	Manually by operator (AL 3)
Warning (class B CIE only [7)])	visible	N	X	Warning signal/ message of a power supply	After each signal/message	Manually by operator (AL 2)
Third-party signal (class B CIE only[7)])	visible and audible	N	X	Recognition of a third-party signal > 10 s (see clause 14.3)	After each signal/ message	Manually by operator (AL 2)
Setting confirmation	visible and/or audible	X[4)]	Not applic-able	CIE accepted external set state	Not applicable	Not applicable

Abbreviations used in table 12.01:

ACE Ancillary control equipment
AL Access level
ATS Alarm transmission system
CIE Control an indicating equipment
EA External alarm
HS Hold-up signals/messages
IAS Intruder alarm system
IS Intrusion signals/messages
Nz Indication may not happen
PS Power Supply
RS Remote signalling
TS Tamper signals/messages
U_B Operation voltage
WD Warning device
(x) Indication may occur
X Indication shall occur automatically
Xa Indication shall occur automatically or on request of the operator

Footnotes to table 12.01:

1) Only required, if not all signals/messages can be indicated at the same time (e.g. for concentrated displays).
2) After unsetting no further signals/messages shall be latched.
3) The visible fault indications shall remain until the cause of the fault has been remedied. If the fault does no more exist, the audible fault indication may be restored automatically, however, it must be possible to restore it manually (AL 2). In this case a repeat of the signal for further faults shall be possible.
4) Only time-limited recognisable nearby the ACE (maximal 30 s).
5) Kind of restoring should be adjustable by installer at AL 2 or AL 3.
6) If indication is processed automatically, the instruction manual should show clearly that the CIE is to be installed such that the indication is not visible for an intruder.
7) Only for IAS with non-exclusive interconnections.
8) For hold-up signals/messages an external alarm shall be generated only in exceptional cases, see clause 13.4.

Table 12.01: Indications required