Herausgeber: Gesamtverband der Deutschen Versicherungswirtschaft e.V. (GDV)
Büro Schadenverhütung
Verlag: © VdS Schadenverhütung

VdS-Rules for Alarm Systems

Integrated Alarm Systems

Requirements

VdS 2347en : 2002-01 (02)

Contents

1 General

1.1 Scope

These rules describe requirements for integrated alarm systems and their system elements which are additionally valid respectively which are diverging from the rules valid for a dedicated system/specified application. These rules are valid in connection with the rules for the corresponding alarm system.

The test methods for additional or diverging requirements for integrated alarm systems are described in the rules for alarm systems, integrated alarm systems, test methods VdS 2348 (in preparation).

Integrated alarm systems may be a combination of clear defined alarm systems such as fire or intruder alarm systems or may be a combination of alarm system applications with other types of systems as e.g.:

- Access control systems (ACS)
- Closed circuit television (CCTV)
- Fire extinguishing systems
- Plant monitoring systems
- Time and attendance systems
- Light control systems
- Heating control systems
- Building management systems (BMS)
- Computerized processing systems
- Emergency exit management and lightning

Note: Minimum requirements for the use of detectors for hazard and emergency conditions and technical detectors in VdS approved intruder alarm systems are described in the amendment S2 to VdS 2311.

1.2 Validity

These rules are valid from 01. January 2002; they replace the edition VdS 2347 : 1997-10 DRAFT.

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 4102-12: 1998-11** Fire behaviour of building materials and elements, fire resistance of electrical cable systems
- **DIN VDE 0833-1** Alarm systems for fire, intrusion and hold-up, General requirements
- **DIN VDE 0833-2** Alarm systems for fire, intruder and hold-up, requirements for fire alarm systems
- **DIN VDE 0833-3** Alarm systems for fire, intrusion and hold-up, requirements for intrusion and hold-up alarm systems
- **VdS 2095** Rules for automatic fire detection systems, planing and installation
- **VdS 2110** Rules for alarm systems, protection against environmental influences, requirements and test methods
- **VdS 2227** Rules for intruder alarm systems, general requirements and test methods
- **VdS 2311** Rules for intruder alarm systems, planning and installation
- **VdS 2311-S2** Rules for intruder alarm systems, planning and installation, detectors for hazard and emergency conditions and technical detectors
- **VdS 2348** Rules for alarm systems, integrated alarm systems; test methods (in preparation)

3 Terms and definitions

The general terms and definitions are described in the rules for intruder alarm systems, general requirements and test methods, VdS 2227, for fire detection systems terms and definitions are given by VdS 2095. Additionally respectively different the following terms are valid for integrated alarm systems.

System: Technical realisation of a system concept.

System element: Element of an alarm system, e.g. control and indicating equipment (CIE), detectors, signalling devices, installation accessories, wiring net.

Application: Field of application of a system, e.g. for fire detection.

BUS: Summarized wiring system, which exchanges data and/or information sequentially.

Reliability of electric cable systems: According to DIN 4102-12 : 1998-11 the reliability of electric cables is guaranteed when there is no short circuit in the cable system during defined fire test and no interruption of electricity in the checked cable system.

Note: Functionability of fire detection systems regarding DIN VDE 0833 can be guaranteed by using the respective cables or by implementing an appropriate monitoring system of fire detection systems.

Building management system (BMS): Technical equipment for processing and monitoring of building management (e.g. heating, air condition, ventilation, lighting).

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

Application of alarm systems: Application for immediate protection of life and/or assets as there are

- fire detection systems,
- intruder alarm systems,
- hold-up alarm systems.

The application of alarm systems can include equipment required by the application standard as well as additional equipment.

Integrated alarm systems: A system having common facilities (like hardware, software or transmission paths) used for different applications with at least one being an alarm application.

Security relevant function: Function in which a certain event (e.g. tamper, operation error) may cause a security risk.

Security risk: An event is regarded as a security risk (e.g. disturbance of function), if the security function of an alarm system is jeopardized but not yet reduced.

Subsystem: System which is assigned to only one application (e.g. fire).

Independent system: An independent system includes all complete functions which are necessary for the defined function of the system. Additional functions which can also be part of another system are admitted when they do not adversely affect – even in case of error – the functions of each respective system.

Access level (AL): Summary of special parts or functions of an alarm system which is only reachable for special persons.

4 Classification

The classification for **performance criteria** of integrated alarm systems is defined by the respective rules for the corresponding alarm systems.

The **environmental classes** classification is made in accordance with the „Rules for intruder alarm systems, protection against environmental influences, requirements and test methods“, VdS 2110.

5 Requirements

5.1 General

It has to be differentiated between technical requirements on systems and requirements on planing, installation, operation and maintenance.

5.2 Requirements for systems

5.2.1 Requirements for system elements

All system elements shall fulfil the requirements of the according subsystem. For the common part (common used functions and devices) the respective highest standards for each single subsystem shall be fulfilled.

5.2.2 Assignment of functions

Functions as e.g. detection, processing and notification have to be assigned unambiguously to the respective application (e.g. intruder detectors have to indicate intruder signals and fire detectors have to indicate fire alarm signals).

5.2.3 Decoupling of functions and operations

Defined functions as well as non-defined ones and operations of subsystems (e.g. fire detection system) including additional elements shall not cause risks or reduction of security or further undesired effects in other subsystems (e.g. intruder alarm system).

Note: If one of the common parts fails this may lead to a total defect of one or more subsystems (example: fault of the common power supply, defect of the common BUS).

5.2.4 Indication of signals

The choice of colour and the visibility of indications shall be such that signals with the highest priority are unambiguously noticed even with different background illumination. If the rules for the respective alarm system require a coloured indication of different signals these requirements shall be fulfilled as far as they are not contradictory. In case of conflicts between the relevant standards the following colours shall apply:

RED	Alarm signals
YELLOW	Fault signals
GREEN	Normal operation

In case of conflict between the individual standards for indications the requirements with the highest priority shall be applied.

5.2.5 Priorities

Following priorities regarding processing, indication and notification of alarm signals shall be applied:

Priority 1: Signals from applications related to life protection like

- fire
- threat
- hold-up
- others (e.g. overpressure of a boiler)

Priority 2: Signals from applications related to property protection like

- intrusion
- tamper (when IAS is set)
- others (e.g. inrush of water)

Priority 3: Signals from other alarm systems

- tamper (when IAS is unset)
- fault
- status
- others

Priority 4: Other signals (e.g. temperature measuring values)

5.2.6 Indication and operation elements

Indication and operation elements shall be assigned unambiguously to the dedicated application (e.g. fire detection system) and shall be

- clearly visible,
- unambiguously to read,
- unambiguously to interpret,
- perfectly clear to understand.

5.2.7 Operation capability

The operation of integrated alarm systems shall be in a simple and unambiguous manner.

5.2.8 Multiple indication

One application (e.g. fire alarm) shall at least be able to indicate two signals at the same time, further coming signals, even from other applications, have to be indicated automatically and unambiguously by an additional signal. It shall be possible for the user to recall these further signals by an operation. After 30 s latest the indicator with the highest priority is automatically reset.

Furtheron the combination of indications from different applications is not permitted.

5.2.9 Multiple protected areas

If integrated alarm systems are designed such that transmission paths for alarm signals (e.g. intruder detection signals) may lead through areas which are not monitored by the alarm system, the functionability of the total system or the alarm-subsystem shall be ensured by appropriate measures (e.g. separated BUS for intruder detection, reliability of electric cable systems for fire detection systems).

5.2.10 Access level (AL) for the user

Integrated systems shall have various part access levels for the user to functions, e.g. AL2a for fire detection systems, AL2b for intruder alarm systems. The number of access levels depends on the number of the applications in an integrated system. Within these part access levels the access shall only be possible to the respective application.

5.3 Planing, installation, operation and maintenance

5.3.1 Rules

Planing, installation, operation and maintenance of integrated systems which include one or several alarm subsystems have to be in accordance with the respective rules for the subsystems (including the rules for wiring).

5.3.2 Installer

Planing, installation and maintenance of integrated systems which include one or several alarm subsystems have to be coordinated by **one** VdS approved installer for the corresponding applications of the alarm system. Share of responsibility is not permitted.

Note: The prospective user of the integrated alarm system has to be informed about this item by the installer.

6 Requirements for central control facilities (CCF)

6.1 General

In practice more and more alarm systems are linked to computer systems (PC); respectively computer systems are used for the combination and/or comfortable operation of alarm systems conforming to rules. The following requirements are valid for those central control and facilities (CCF).

6.2 Operation possibility for third parties

Any operation of the CCF (e.g. computer system) by third parties shall be prevented.

6.3 Indication and operation

The CCF has either to meet the requirements on the according subsystem or the system shall be equipped with an additional control and indication device system conforming to the rules of the system. In the second case all items indicated and operated in the access level AL2 of the alarm system can also be indicated and operated by the user at the CCF.

6.4 Combination of functions and events

The user of the CCF is not permitted to make any security reducing combinations or modifications of specified data, signals etc. of the alarm system within the device.

6.5 Self-start

The CCF has to be selfstarting. In this case a loss of security relevant information shall be prevented or not be distorted.

6.6 User software

Any loading of software by the user into the CCF shall be prevented (e.g. by blocked floppy drive).

6.7 Multi-using

The CCF (e.g. PC) shall not be used for other purposes (e.g. word processing programmes or bookkeeping) than for central control and indication facilities, if no negative feedback on subsystems for alarm systems of special applications (e.g. fire detection systems) or from this subsystem common used functions/system elements (e.g. BUS, power supply) shall be applied.

6.8 Faults

Faults of the CCF (e.g. PC) shall not cause a negative feedback on alarm subsystems (e.g. fire detection system) or on common used functions/system elements (e.g. BUS, power supply).

Changes

Compared with edition VdS 2347 : 1997-10 DRAFT the following changes have been made:

- Clarification in clause 1.1, that the rules are also valid for system elements of the system
- Supplementation and revision of terms and definitions in clause 3
- Update of the publishing date of DIN 4102
- Separation between tamper in the set and the unset state of an IAS in clause 5.2.5, addition of examples
- Correction of the statement in clause 5.2.9 „Multiple protected areas“
- Revision of clause 6.1, 6.5 and 6.7
- Editorial changes