Monitoring and alarm receiving center – (MARC)

Part 1: Requirements

VdS 3138-1en : 2013-12 (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

Copyright by VdS Schadenverhütung GmbH. All rights reserved.

VdS Guidelines for Security Services

Monitoring and alarm receiving center – (MARC)

Part 1: Requirements

The present product guidelines are binding only if its use in single cases has been agreed between VdS and the client. The consideration of these guidelines is not binding otherwise; the agreement on use of the guidelines is optional. Third parties may in single cases accept other security requirements or quality proofs or service providers on base of conditions that were determined at their own discretion and that do not correspond with these technical specifications.

Content

0 Introduction ... 4
1 Scope ... 5
1.1 General ... 5
1.2 Validity ... 6
2 Definitions and abbreviations ... 6
2.1 Definitions ... 6
2.2 Abbreviations ... 14
3 Normative References ... 14
4 Services of the monitoring and alarm receiving center (MARC) ... 15
4.1 Technical service (TS) ... 15
4.2 Security service – alarm service (AS) ... 18
4.3 Security service – intervention service (IS) ... 21
4.4 Additional services for improvement of efficiency of hazard defence ... 24
5 The security chain in the MARC ... 25
5.1 Process of notification ... 25
5.2 Process of intervention ... 28
5.3 Monitoring of the process steps in the security chain ... 31
5.4 Process of reporting ... 35
6 Management of the MARC ... 36
6.1 Planning of the processes ... 37
6.2 Co-operation in providing security services ... 40
Annex A (normative) Technical requirements for MCT and the forwarding of messages within the security chain ... 41
A.1 MARC comprising one ARC with integrated alarm service ... 41
A.2 Alarm provider (AP) comprising one ARC with or without integrated alarm service ... 41
Annex B (informative) The services in the security chain of the MARC ... 43

0 Introduction

A VdS-approved MARC bears the responsibility towards its customer for guaranteeing the services which are necessary for the security in and of the protected premises (according to figure 1).

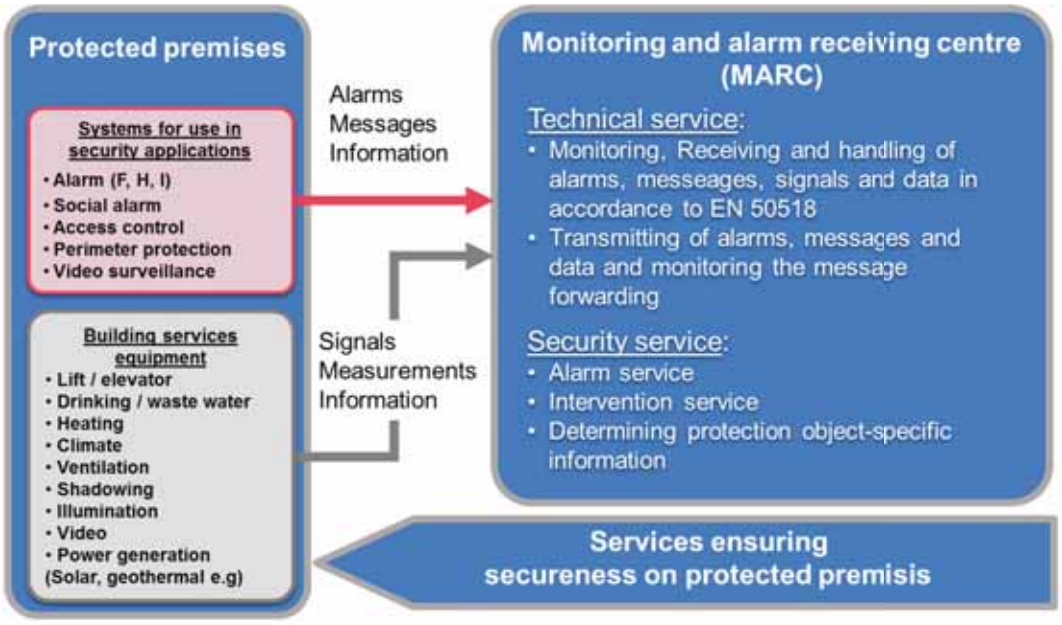


Figure 1: Services of a MARC

Alarm messages from protected premises shall immediately and securely be forwarded to the responsible locations of the technical services, to the alarm services and the intervention service in order to guarantee an optimum of protection. For securing the activities and procedures being related to this are always coped with, they are knotted in form of process steps to a security chain.

This security chain consists of the processes alarm notification, intervention, reporting including the associated process steps as well as their monitoring (see figure 2).

Figure 2: The security chain and its processes

The security chain is to be designed individually and to be adopted to protection requirements for each protected premises on base of object specific security concepts.

The processes within the security chain shall be coped with and be performed under defined conditions. The essential process steps are designed measurably so that the reaction time and availability of the respective service as well as the effectiveness on danger defence may be evaluated for each message (e.g. alarm message).

Should an increase of efficiency become necessary for keeping the protection targets at the protected premises due to this evaluation, the MARS shall offer its services for this purpose (see clause 4.4).

If the amelioration possibilities in the security chain for the respective protected premises are exhausted without reaching the protection target, the object specific security concept is to be revised. The alarm and intervention services shall be involved in this planning

The services as described in clause 4 are required for the provision of the process results.

The MARC is responsible for the planning of the processes, its effective realization as well as perpetuation (monitoring on effectiveness of the processes). The requirements for the management of the MARC are determined in clause 6.

The certification body of VdS Schadenverhütung (VdS certification body in the following) offers on base of these guidelines VdS 3138 the approval as “Monitoring and Alarm Receiving Center” (MARC).

Part 1 of the guidelines contains constructional, technical and organizational requirements.

Part 2 of the guidelines describes the procedure for the approval.

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

1 Scope

1.1 General

These guidelines contain requirements for monitoring and alarm receiving centers (MARAC) which are built up at a centralized or modular architecture.

The tasks of the MARC comprise the technical reception of messages which are transmitted from protected premises due to hazards which have there been identified, the capturing of security relevant information of the protected premises as well as the expert information processing with the quickest possible help for danger defence.

The identification of hazards in the protected premises is normally made by installed monitoring techniques (e.g. alarm systems and video surveillance systems) and necessitates alarm transmission equipment which is equipped with interconnections for notification of the MARC.

The guidelines are addressed to the following target group:

- Security providers which offer alarm and intervention services
- Authorities and organisations with security tasks (BOS), a. o. police, public fire brigade, THW and aid organisations
- Plant fire brigades and works fire brigades

- Security centers in plants for domestic and sea ports as well as airports
- Other locations and sites with security relevant tasks, as e.g. data processing service centers, mission control centers, control rooms of power supply providers and critical infrastructures

An approval as MARC on base of these guidelines (VdS 3138, part 2) is possible if at least one of the following services as per character a) or b) is offered by the approval owner independently at the site of approval. All services which are offered not independently are to be organized by co-operations with suitable service providers (cooperation partners) (see clause 6.2):

a) A technical service according to clause 4.1
b) Security service – alarm service according to clause 4.2
c) Security service – intervention service according to clause 4.3
d) Additional service for increase of efficiency of danger defence according to clause 4.4

1.2 Validity

These guidelines are valid from 01.12.2013.

2 Definitions and abbreviations

2.1 Definitions

For the purpose of these guidelines the following definitions shall apply:

2.1.1 Alarm

Warning of an existing hazard for life, property or the environment.

- **Hold-up alarm**: Signal, which is triggered by persons for calling direct help in case of hold-ups.
- **Fire alarm:** Warning of a hazard for persons or properties being caused by fire.
- **Harassment alarm:** Special type of a hold-up alarm
- **Intruder alarm:** Warning of a hazard for persons and properties being caused by an intrusion.
- **False alarm:** Alarm, underlying no hazard.
- **Remote alarm:** Indication of an alarm status to a charged service center which is not on sit (e.g. MARC).
- **Internal alarm**: Notification of the alarm triggering of an internally set IAS to persons in the monitored object.

  Note: An internal alarm may be transmitted additionally to a service center (e.g. MARC)
- **External alarm**: Alarm on site for hazard defense (e.g. by audible or optical warning devices or emergency messages)

2.1.2 Alarm notification

Calling for help for hazard defence.

Note: a MARC usually is notified by the transmission of messages and alarms (remote alarms) from the protected premises or by absence of defined messages at defined times.

2.1.3 Alarm receiving center (ARC)

Continuously manned center to which information concerning the status of one or more AS is reported and the conformity of which with the standards of series DIN EN 50518 according to DIN EN 50518-3, clause 6, is proved in form of an audit yearly by a body which is accredited according to EN 45011 or EN 17020. by an audit.

Note: The technical services in the alarm receiving center comprise the monitoring, reception and processing of signals and alarms and messages which require an immediate reaction to emergency cases (hazards).

2.1.4 Alarm service (AS)

Security service consisting of evaluation of alarms and message taking into consideration the valid protected premises relevant information and to initiate and monitor planned, i.e. with the client contractually agreed security measures for the quickest possible re-establishment of the security of the protected premises and to record the results of these activities.

Note: The alarm service may be performed within as well as outside the rooms of an alarm receiving center.

2.1.5 Alarm plan

Part of the measures for documentation of all information which is required for a proper alarm service, as e.g. name and address of the protected premises, messages to be handled and the associated agreed measures, degree of hazard, risks specific for the protected premises resp. points of risk, persons to be informed.

Note: The alarm plan is an essential fundament for the alarm service. The previously mentioned list is not exclusive.

2.1.6 Alarm provider (AP)

Alarm receiving center (ARC) which fulfils additional requirements on processing, monitoring and forwarding of signals (e.g. alarms, messages and information) according to the guidelines VdS 2471 and VdS 3534.

2.1.7 Alarm verification

Procedure for determination if the triggering cause of an alarm is based on a real hazard situation with the aim to raise the probability that it is a real alarm.

Note: the verification of an alarm is made normally by monitoring and checking of the triggering cause resp. the course of an alarm series e.g. by visual inspection. It serves especially for the differentiation between false alarm and genuine alarm, i.e. alarm which is based on a real hazard.

2.1.8 Operator

Person who is manually handling alarms and messages at the monitoring center transceiver (MCT).

2.1.9 User interface (UI)

Interface between operator and a device (e.g. MCT, DCD) at which persons perform operations (e.g. operating and indicating equipment).

2.1.10 Digital communication device (DCD)

Mobile device for data and voice communication (e.g. between IF and the MARC) which – among others – may transmit position data to the MARC.

2.1.11 Mission control system (MCS)

Control system which is used in a center (e.g. mission control center) to coordinate, to monitor and to guide mobile intervention forces in the field (e.g. in the course of the intervention service).

Note: MCS combine the resource planning of vehicles and personal with the current intervention needs and provide the communication interfaces which are necessary for this purpose. They support the person guidance during intervention.

2.1.12 Intervention means

Technical/organizational equipment/means especially for communication for the movement and the personal security of intervention forces which are necessary or helpful to perform the intervention.

2.1.13 Fault

Non-fulfilment of an agreed measure.

2.1.14 Hazard

The possible damage effect of a hazard source or the state of a threat by a hazard source as e.g. for

Attack – hazards

- Hold-up (if given with taking hostages)
- Tamper (e.g. of the message reception, at the communication devices, at the software)
- Arson, vandalism
- Intrusion
- Theft of data, properties and values

Business interruption – hazards

- Fire
- Flood, strong rain
- Lightening and overvoltage
- PC-device failure (e.g. peripherals as monitor, keypad etc.)
- Function fault of communication
- Failure of the power supply
- Fault of interconnection
- Fault of software
- Fault of security equipment
- Organisational deficiencies
- Gas leakage and ingress

2.1.15 Alarm management system (AMS)

A software system for taking over, input, generation, filing, forwarding, processing and indication of messages and data as well as for control of different security technical systems of one or several systems (according to VdS 3534).

Note: In the sense of these guidelines the AMS is a supporting tool for

- *Operator in alarm receiving centers according to DIN EN 50518*
- *Operator at alarm providers*
- *Mission control system of a monitoring and alarm receiving center as well as*
- *External bodies in the course of the performance of alarm and intervention services.*

Alarm management systems fulfil often also the requirements for mission control systems, but may also be supported by those.

2.1.16 Hazard analysis

Detailed description of all hazards which may occur at a defined reference system.

Note: A hazard analysis is normally made only for certain hazards.

2.1.17 Exposure

The degree of exposure of a protected premises which is determined by accessibility (e.g. upper floor), neighbourhood (e.g. adjacent property of third parties, third party rooms, slip road) the local situation (e.g. residential area, industrial area) and the desirousness of the existing objects.

2.1.18 Intervention

Performance of hazard defending and damage diminishing measures for the protected premises at risk. The intervention is made due to a notification.

2.1.19 Intervention service (IS)

Security service the activities of which mainly consist in performing the agreed measures for hazard defense at the protected premises and to record the results from these activities.

Note: the intervention service is performed due to a notification and is monitored by the MARC.

2.1.20 Intervention force (IF)

Person who verifiably has knowledge and skills to plan and execute the activities which are necessary for hazard defense at the protected premises.

2.1.21 Intervention plan

Documentation of all information which are necessary for a proper intervention as e.g. name and address of the protected premises, approach way, exposure, specific risks of the protected premises resp. sites of hazards, authorized persons and intervention measures.

Note: The intervention plan is the essential base for action for the intervention service. The previous list is not exclusive.

2.1.22 Intervention measures

Measures to defend hazards which are performed by an intervention service (IS).

2.1.23 Co-operation partner

An expert provider which is specialized to offer services within the security chain as agent for the MARC and which commits on base of a written, contractual agreement to fulfil and to maintain the determined quality and performance requirements and to monitor these on effectiveness.

Note: Sovereign institutions (e.g. police, fire brigade, civil protection, crime commissions) or associations are not agents for services within the security chain and thus no co-operation partner in the sense of these guidelines.

2.1.24 Client

Juridical or natural person (e.g. operator of a protected premises) who receives contractually agreed services from the MARC.

2.1.25 Performance feature

A characteristic which specifies the quality of a service or a process.

2.1.26 Performance criteria

Requirement which is to be kept for fulfilment of a performance feature.

2.1.27 Performance category

A category which is assigned to a performance criteria (in the sense of rank, grade, graduation) which determines the demand (e.g. target value) of requirement.

Note: Performance categories are used in these guidelines to determine the difference between the demands of performance criteria. Normally, each performance category fulfils other performance demands.

2.1.28 Leading MARC expert (L-NSL-FK)

Employee of a monitoring and alarm receiving center which has sufficient qualification according to VdS 2237 and competence to manage and monitor the works of the monitoring and alarm receiving center and – if given – the intervention service.

2.1.29 Deficit

Non-fulfilment of a requirement of these guidelines.

2.1.30 Action plan

Generic term for the complete action planning within the security chain starting with the protected premises to the alarm receiving center / alarm provider (technical measures), the alarm service (alarmplan) to the intervention service (intervention plan) for determination of the measures to be initiated due to incoming alarms and messages.

Note: The action plan is the essential base for the services to be brought by the MARC.

2.1.31 Message

The information given by a system (e.g. alarm system), software (e.g. alarm management system) or person (e.g. alarm message, fault message or status message).

Note: In the sense of this term the information generated by the alarm management system (software) on the absence or issue failure of an anticipated message also a message.

2.1.32 Emergency service

Standby of third parties to accept and perform commissioned activities for 24 hours on all days of a week (24/7).

2.1.33 Monitoring and alarm receiving center (MARC)

An organization which offers technical services and security services for hazard defence on base of a monitored security chain in discharge of the contractual agreements and action plans.

Note: The organization may consist of several co-operation partners.

2.1.34 MARC expert (MARC E)

Employee in a monitoring and alarm receiving center which has sufficient qualification according to VdS 2237 to perform the activities accruing in a monitoring and alarm receiving center especially for the alarm and intervention service.

2.1.35 Interface (Sx)

Imaginary or real passage at the border of two function units with agreed rules for the handover of data and signals.

Interfaces normally are standardized handover sites within a system or network which serves for communication.

Note: The index x used with the acronym S stands for a digit sequence or number by which the interface is unambiguously identified.

2.1.36 Locking secret

Information in any form (mental, material or biological) which renders access to secured areas possible without bypassing or overriding the security techniques being used for the protection of the secured areas.

2.1.37 Protection target

A protection target describes the required or aimed security status and considers the complete range of potential risks. As a consequence of the hazard and risk evaluation protection targets are to be determined. Protection targets are referring to persons and/or properties and/or the environment.

Note: Protection targets are to be expressed such that the aimed security state is presented, however leave open the way by which this state is reached.

2.1.38 Protected premises

The premises to be protected in case of an alarm (real estate, property with associated space and traffic routes, buildings, infrastructure and properties) as well as the persons and the specific environmental conditions of the object.

2.1.39 Security information relevant for the protected premises

Information that is regularly to be collected previously to the alarm and intervention services which are suitable for the establishment of up-to-date hazard evaluations specific to the protected premises and for the presentation of the security status, as e.g.

- Regional crime development, crime trend, crime methods
- Weather situation, traffic and street situation, infrastructure changes
- Requirements of authorities /measures
- Information specific to the protected premises (e.g. plant holidays, assembled scaffoldings, hazard focuses)
- Environmental conditions and environmental hazards
- Exposure of persons
- Determination on design (e.g. type, monitoring extent, notification, operation) of the used alarm systems
- Information on employment protection and accident prevention in the framework of intervention measures

2.1.40 Security situation (overview of situation)

Current status of the security of the protected premises. The compilation of the state is made on base of circumstances which arise from the timely, spatial and by persons caused correlations and present a threat or hazard for the protected premises.

Note: Counting to the security status are e.g. the regional crime development, crime trends, crime methods, weather situation, traffic and street situation, infrastructure changes, authority measures.

2.1.41 Security status

Actual condition of the functions of security equipment of the premises to be protected at the protected object.

2.1.42 Security chain

Sum of processes – including their interdependency – for a protected premises, for detection and notification of unwanted statuses and for the defence /remedy of these unwanted statuses on base of the existing security concept.

2.1.43 Security equipment

Technical equipment which is installed in protected premises in order to fulfil the protection targets for the hazard defence.

Note: Type and extent of installed security equipment is usually determined in the framework of a security concept for a protected premises. Security equipment is divided on base of its main functions into mechanical (e.g. intrusion-, fire-, shell-retardant doors), electroni-

cal (monitoring equipment as e.g. alarm detection and video surveillance system) and mechatronic (e.g. access control systems, fire extinguishing systems) security equipment.

2.1.44 Security concept

Totality of the determined organisational, personal, technical and constructional measures for securing a protected premises and / or defence of hazards.

Note: Written analysis of possible attack and damage scenarios with the aim to reach a defined protection level. Hereby, it shall be differentiated between the security against malicious attacks (security) and the security against human or technical failure (safety).

Security concepts are based on a structural procedure which normally comprises the following criteria:

- *Determination of the object to be protected and the protection targets*
- *Analysis of threats /damage scenario*
- *Evaluation of occurrence probability and potential extent of damages*
- *Development of measures for reducing damages and their occurrence probability*
- *Development of measures with the aim to initiate the hazard defence as early as possible (e.g. matching of electronical and mechanical security equipment*
- *Planning of measures and provision of means for damage combating and diminishing in case of damage*
- *Analysis of the own risk acceptability and evaluation of the remaining risk*

Even a sophisticated security concept is not able to completely eliminate the remaining risk. Due to this, a crisis and catastrophe management is implemented often, in order to protect as far as possible life and properties in case of emergency.

2.1.45 Security measures

Organisational, personal, technical and/or constructional measure for securing a protected premises and/or hazard defence.

Note: Security measures are determined for realization of the protection targets.

2.1.46 Master file data

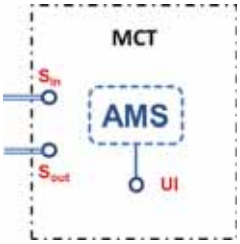
Generic term for all data and information regarding a protected premises which are necessary for monitoring, planning and realisation of measures for hazard defence including measurement plans.

Note: Master file data are for example:

- *Name, address and phone number of the protected premises*
- *Object identification number and all special agreements*
- *Name, address and phone number of the user*
- *Actions to be performed due to messages resp. alarms received at the MARC, e.g. alarm and intervention plan*
- *Actions to be performed due to absence of messages which are anticipated in the MARC, e.g. messages on setting/unsetting of the intruder alarm system*

2.1.47 Monitoring center transceiver (MCT)

Equipment/function for automatic processing, manual handling and forwarding of alarms and messages received as well as for monitoring of the connected transmission paths within the security chain.



S_{in}	Dual Path (DP)-Interface in
S_{out}	Single Path (SP)-Interface out
UI	User interface
AMS	Alarm management system

Note: The MCT may realise different function depending on its purpose (e.g. monitoring of the transmission paths between responsibility fields of co-operation partners).

2.2 Abbreviations

The following abbreviations are used in these guidelines:

AS	Alarm service
ARC	Alarm receiving center
AP	Alarm provider
ACE	Ancillary control equipment
UI	User Interface
DP	Dual Path (two path-connection)
DCD	Digital communication device
MCS	Mission control system
AMS	Alarm management system
IS	Intervention service
IF	Intervention force
MARC	Monitoring and alarm receiving center
S_X	Interface
SP	Single Path (one-way connection)
SPT	Supervised premises transceiver
TS	Technical service
ATE	Alarm transmission equipment
MCT	Monitoring center transceiver
T-CIE	transmission control and indicating equipment

3 Normative References

These guidelines contain dated and undated references to other publications. The fulfilment of the requirements of the following standards and guidelines is base of these guidelines.

DIN EN 15602 Sicherheitsdienstleister/Sicherungsdienstleister - Terminologie

DIN EN 50136-1 Alarm systems – Alarm transmission systems and equipment – Part 1: General Requirements for alarm transmission systems

DIN EN 50136-2 Alarm systems – Alarm transmission systems and equipment – Part 2: Requirements for alarm transmission equipment (ATE)

DIN EN 50136-3 Alarm systems – Alarm transmission systems and equipment – Part 3: Requirements for transmission control and indicating equipmen (T-CIE)

DIN EN 50136-4 Alarm systems – Alarm transmission systems and equipment – Part 4: Indicating and operation equipment in alarm receiving centers

DIN EN 50518-1 Monitoring and alarm receiving centers - Part 1: Location and construction requirements

DIN EN 50518-2 Monitoring and alarm receiving centers, Part 2: technical requirements

DIN EN 50518-3 Monitoring and alarm receiving centers - Part 3: Procedures and requirements for operation

VdS 2172 Guidelines for the approval of security companies - Intervention center (IC)

VdS 2237 Examination regulations for the expert assessment of security companies

VdS 2471 Guidelines for alarm systems – transmission paths in alarm transmission systems

VdS 2529 Alarm service and intervention certificate /attestation

VdS 3534 Guidelines for computerized information systems – alarm management systems, Requirements and test methods

For undated references the last edition of the publication referred will be applied.

Note:

All VdS publications may be ordered at VdS Schadenverhütung, Verlag, Post box 10 37 53, 50477 Köln, Fax: (0221) 77 66 – 109, Internet: www.vds-shop.de.

DIN – standards may be ordered at: Beuth Verlag GmbH, Burggrafenstr. 6, 10787 Berlin, Fax: (030) 2601 – 12 60, Internet: www.beuth.de

4 Services of the monitoring and alarm receiving center (MARC)

4.1 Technical service (TS)

The technical service comprises at least the functions as follows:

a) Monitoring, reception and processing of messages from systems which are installed in protected premises (e.g. intruder and hold-up alarm systems). These services shall be brought by a certified alarm receiving center according to DIN EN 5018.
b) Measurement and recording of availability of the transmission network according to DIN EN 50136-1.
c) Monitoring of alarm transmission in the security chain (see clause 5.3).
d) Detection of faults on base of messages and organization of fault remedy in the security chain
e) Documentation of functions for a) to d)

The functions resp. activities as assigned in clause 5 of the technical service (TS), shall be offered as per determined requirements and performed in case of respective agreement. The technical services as required in the present guidelines shall be provided in the alarm receiving center (ARC).

4.1.1 Protection targets for the technical service

At least the protection targets as listed in the following chapters shall be kept for the secure performance of processes in the frame of the technical service in the alarm receiving center.

4.1.1.1 Detection of attacks

The requirements set in standard series DIN EN 50518 on the detection of attacks on the alarm receiving center shall be fulfilled. They are valid also for the alarm provider (AP):

Example for security measures for fulfilling the protection target:

- Electronic detection of attack hazards (see clause 2.1.14) e.g. intruder alarm system, fire alarm and detection system, access control system, video surveillance system, gas detection system

Furthermore, the operator of the alarm provider shall be able to detect attacks on the technical equipment which serves for the message reception and its processing if a reaction on hazard defence and aid is possible by them.

Example for security measures for fulfilling the protection target:

- Monitoring of the transmission and communication according to DIN EN 50136-1

4.1.1.2 Defence of attacks

The requirements set in standard series DIN EN 50518 on the defence of attacks shall be fulfilled by the alarm receiving center and the alarm provider.

Example for security measures for fulfilling the protection target:

- Constructional requirements against attacks with mechanical means, with firearms and fire (arson)

Furthermore, the alarm provider shall protect all technical equipment which serves for the message reception and its processing by suitable technical systems (e.g. firewall, demilitarised zone) and organisational measures (e.g. controlled forwarding of access data for the alarm reception, maintenance).

Example for security measures for fulfilling the protection target:

- Measure for the defence of denial of service attacks from the transmission network

4.1.1.3 Identity of the operator

The requirements set in DIN EN 50518-2 regarding the identity of the operator shall be fulfilled. The identification shall be performed by a secured registration procedure with an identification feature of the operator at the AMS (e.g. password, biometric characteristics).

4.1.1.4 Handling of data

The requirements set in DIN EN 50518-2, -3 regarding data administration, data processing, data integrity, data filing as well as the legal regulations of the data protection act shall be fulfilled.

4.1.1.5 Personal availability

The requirements set in DIN EN 50518-3 regarding the personal manning shall be fulfilled by the ARC and the alarm provider.

4.1.1.6 Business interruption

The hazards of a business interruption are described in clause 2.1.14 (business interruption – hazards). The requirements on the availability of the technical equipment which serves for the message reception, its processing and transmission, are to be complied with according to DIN EN 50518-1 as well as DIN EN 50136-1, tables 6 and 7.

4.1.2 Constructional, technical, organisational and personal requirements

The requirements on the transmission of messages according to DIN EN 50136-1 are to be fulfilled.

The reception of messages shall be performed at an ARC which is certified according to DIN EN 50518.

ARC in which work stations for the alarm service are established, require the communication techniques as listed in clause 4.2.2.1 for the alarm service in addition to the communication equipment according to DIN EN 50518.

If the ARC co-operates with one or several remote stations for the provision of the alarm service it shall be VdS-approved as alarm provider.

MARC (approval owner) which do not operate an own ARC shall cooperate with a co-operation partner which is approved as alarm provider according to VdS 3138, part 2.

The VdS-approval as alarm provider presumes the certification as ARC according to DIN EN 50518.

Note: The approval conditions for ARC certificates of third parties are shown in VdS 3138, part 2, annex C.

The AP is responsible for the monitoring of alarm transmission systems according to DIN EN 50136-1 and the verification of performance features of the alarm transmission system(-s) of the protected premises at least up to the monitoring center transceiver of the alarm service.

Alarm receiving centers which are approved as alarm provider require communication techniques for transmission and monitoring of messages to the alarm and intervention service in addition to the communication equipment according to DIN EN 50518.

4.1.2.1 MCT with alarm management system (AMS)

The AP shall use an alarm management system for the notification process.

Note: If a VdS-approved alarm management system according to the guidelines VdS 3534 is used, it is deemed that the state-of-the art is fulfilled and the requirements according to clause 4.1.2.1 are complied with.

The AP shall use transmission techniques resp. transmission systems for the forwarding and bidirectional monitoring of messages to the alarm and/or intervention service (see also Annex A).

For the forwarding of messages from the alarm provider up to the MCT of the alarm service, the requirements for the performance features, reliability and security characteristics of alarm transmission systems according to DIN EN 50136-1 for the respective categories according to annex A are to be fulfilled.

The AP shall dispose of a certified quality management system according to DIN EN ISO 9001 where the processes for the technical services as listed in these guidelines are described and organized.

Note: The approval conditions for the QM-certificate of third parties are shown in VdS 3138, part 2, annex B.

4.2 Security service – alarm service (AS)

The functions resp. activities which are assigned to the alarm service in clause 5, shall be offered while considering the determined requirements and performed in case of respective agreements.

4.2.1 Protection targets for the alarm service

At least the protection targets as listed in the following are to be kept for the secure performance of processes in the course of the alarm service.

4.2.1.1 Detection of attacks

Attack hazards (see 2.1.14) which lead to the interruption resp. fault of the reception of messages, their manual handling and transmission shall be detectable if a reaction on hazard defense and aid is possible by them.

Note: This may be attacks on the security reps. MARC experts or on operation facilities e.g. EDP, software, communication devices, power supply, security equipment and on the transmission paths.

4.2.1.2 Defence of attacks

Detected attacks (according to clause 4.2.1.1, with the exception of attacks on the transmission paths) shall be defenced at least as long as the intervention service is informed on time and kind of attack and the alarm service has been transmitted to another remote center.

The alarm service is to be performed by the remote center as long as the secure state of the origin center is re-established. The required data specific for the protected premises for the performance of the alarm service shall be available for the remote center in up-to-date version.

4.2.1.3 Identification of persons

The identification of the MARC expert and the person who possibly supports him shall be performed by a secured registration procedure with an identification feature medium as

operator at the AMS (e.g. password, biometric characteristic). Each change of operator at the user interface (or user interfaces) of the AMS shall be recorded with time stamp in the AMS.

4.2.1.4 Confidentiality

Messages, information and data of protected premises shall be readable and modifiable exclusively by authorized persons as e.g. leading MARC expert or MARC expert. This is valid for the access to filed data as well as during the data transmission. The authorization of persons shall be documented in writing by the operator of the MARS resp. the alarm service.

Example for security measures for fulfilling the protection target:

- AMS which fulfils this requirement by access and authorization procedures.

4.2.1.5 Non-defeasibility

The reception, transmission resp. the dispatch of messages as well as data for verification management of the activities in the frame of the alarm service are to be collected and protected against loss (confidentiality), change (integrity), unauthorized reading and forwarding (confidentiality). A violation of these protection targets shall be detected. This is valid also for master file data which are provided for the performance of the alarm and intervention service the publication or distribution of which present a hazard of the protection target or for the persons and properties of the protected premises.

Example for security measures for fulfilling the protection target:

- AMS which fulfils these requirements by access and authorisation procedures.

4.2.1.6 Integrity

All changes of the data which are provided and processed in the AMS shall be traceable and documented in the AMS (see also VdS 3534).

Example for security measures for fulfilling the protection target:

- AMS which fulfils these requirements by access and authorisation procedures.

4.2.1.7 Responsibility

Activities/operations being performed at the AMS shall be assigned unambiguously to the authorised forces.

Example for security measures for fulfilling the protection target:

- AMS which detects the operator activities with date, time, operator identity and assignment of the activity to the message resp. processed procedure.

4.2.1.8 Personnel availability

The personal manning with qualified and authorised MARC experts for the performance of the alarm service shall be guaranteed.

The alarm service is to be manned daily and without interruptions from 0 to 24 per shift with at least one MARC expert. Each MARC expert may be supported by one person being instructed in the activities of alarm handling.

In case all employees of the alarm service fall out within one shift organizational measures for guaranteeing an undisturbed operation are to be determined in writing (e.g. manning by other MARC experts, transfer to another MARC or center for assumption of the alarm service).

4.2.1.9 Technical availability (business interruption)

The technical infrastructure (MCT, etc.) being used for the alarm service shall fulfil the protection targets according to clause 4.1.1.6.

Note: This protection target may be fulfilled with an alarm service being on stand-by (e.g. within the scope of an emergency concept).

4.2.2 Constructional, technical, organisational and personal requirements

The constructional requirements are fulfilled if the alarm service is provided in an alarm receiving center which is certified according to DIN EN 50518.

The security measures for fulfilling the protection targets are to be layed down if the alarm service is provided by a body which is remote from the alarm receiving center.

4.2.2.1 MCT with alarm management system (AMS)

The alarm service shall use an alarm management system for the process of notification.

Note: If an alarm management system is used which is VdS-approved according to VdS 3534, it is anticipated that the state-of-art and the requirements according to clause 4.2.2.1 are fulfilled.

The alarm service shall use transmission techniques for the forwarding of bidirectional monitoring of messages to the alarm provider and the intervention service (see Annex A).

4.2.2.2 Voice communication

The alarm service shall provide sufficient communication means for external and internal voice-communication with the technical service (TS)/alarm provider (AP), the intervention service (IS) and the contacts as stipulated in the alarm plan, which are to be contacted in case of messages, in order to reach at every time within 3 minutes the required communication partner if he is reachable. At least two autarkic communication paths via physically separated paths (e.g. radio and wire) are to be provided.

The speech communication shall be recorded for a duration of 30 days. Here, incoming as well as outgoing unsuccessful interconnection trials are to be captures. A monthly evaluation of all incoming calls is to be performed which shows in which time the incoming calls are accepted by the alarm service.

Direct calling keys are to be established on both communication systems for the phone numbers which are dialled the most. Alternatively or as amendment, an interface for phone applications (e.g. telephony application programming interface – TAPI) may be set up to the AMS.

4.2.2.3 Leading MARC expert (L-MARC E)

The alarm service shall be managed by a nominated leading MARC expert with a qualification according to VdS 2237 and – if given a deputy. He shall be employed full-time at the MARC and is contact to VdS certification body.

The L-MARC E shall proof his qualification by an exam according to VdS 2237.

Respective proofs are to be handed in on demand at the VdS certification body.

Note: For MARC with own physically assigned intervention service, an employee may be leading MARC expert in the MARC and responsible person of the IS.

4.2.2.4 MARC expert (MARC E)

The MARC experts employed in alarm service shall give proof of their qualification for MARC expert. This qualification is to be proved by an exam according to VdS 2237.

Note: Instead of the proof as MARC expert also a proof of a completed education in the security sector as expert for security and safety or as service expert for security and safety is accepted.

Respective proofs are to be handed in on demand at VdS certification body.

4.3 Security service – intervention service (IS)

The operations resp. activities as assigned to the intervention service (IS) in clause 5, shall be offered while taking into consideration the determined requirements and performed in case of respective agreements.

4.3.1 Protection targets for the intervention service

At least the following protection targets are to be kept for the secure performance of the processes in the course of the intervention service.

4.3.1.1 Detection of attacks

The intervention service and the intervention forces shall be able to detect attack hazards (see clause 2.1.14) with the aim of removal, destruction, tamper, misuses and spying regarding the locking secret of the protected premises which have been entrusted to them (e.g. object keys) and /or intervention plans if a reaction on hazard defence and aid is possible by them.

Note: This may be attacks on the intervention forces themselves as well as on operation means as e.g. EDP, software, communication means, power supply, security equipment and on the transmission paths.

4.3.1.2 Defence of attacks

The intervention service and the intervention forces shall be able to defence attacks which lead to interruption or fault of the message and information reception, forwarding and/or processing as long until the time and type of the attack has been notified to a remote intervention center and the intervention service resp. the intervention order has been forwarded to another remote center.

Until reset in the secure state the intervention service is to be performed by the remote intervention center. The data which are necessary for performance of the intervention service at the protected premises shall be available for the remote center in valid version.

4.3.1.3 Identification of persons

The identity of interventions forces which perform the intervention service shall be verifiable at every time. The identification of the intervention forces shall be performed by a se-

cured registration procedure by an identification feature medium in the AMS resp. MCS (mission control system) of the IS (e.g. password, biometric features). The begin of work, change of work as well as the end of work of each IF is to be recorded in the AMS resp. MCS with time stamp.

4.3.1.4 Confidentiality

Messages, information and date of the protected premises shall be readable and modifiable only by authorised persons (responsible person, intervention force). This is valid for the access to stored data as well as during the data transmission. The authorization of persons is to recorded in writing by the operator of the MARC resp. the alarm service.

Example for security measures for fulfilling the protection target:

- Alarm management system (AMS) reps. mission control system (MCS) which fulfils this requirements by access and authorization procedures.

4.3.1.5 Non-defeasibility

The reception, transmission resp. the dispatch of messages as well as data for verification management of the activities in the frame of the alarm service are to be collected in the AMS resp. MCS of the IF and protected against loss (confidentiality), unauthorized reading and forwarding (confidentiality). A violation of these protection targets shall be detected by the intervention forces. This is valid also for master file data which are provided for the performance of the alarm and intervention service at the IF the publication or distribution of which present a hazard of the protection target or for the persons and properties of the protected premises or the intervention service itself.

Example for security measures for fulfilling the protection target:

- AMS resp. MCS which fulfils this requirement by access, authorisation and authentification procedures.

4.3.1.6 Integrity

Data shall not be changeable without notice. All changes shall be traceable.

Example for security measures for fulfilling the protection target:

- AMS resp. MCS which fulfils this requirement by access, authorisation and authentification procedures.

4.3.1.7 Responsibility

Activities/operations shall be unambiguously assigned to the intervention forces.

Example for security measures for fulfilling the protection target:

- AMS resp. MCS which records the operations with date, time, identity of the operator as well as assignment of the operation to the message resp. to the process dealt with.

4.3.1.8 Personnel availability

The personal manning with intervention forces for performance of the intervention service shall be guaranteed and proved for the period as agreed with the customer of the concerned protected premises or ARC.

4.3.1.9 Technical availability

a) The operating resources are calculated by the total of the measurement plans and the resulting resource planning which are necessary for the performance of the interventions, as e.g. vehicles, keys for protected premises/access codes, communication devices, monitoring techniques, self-securing techniques, defence means, fire extinguish ants, measuring devices, etc.
b) A responsible spot is determined within the ARC which monitors and documents the measures for reaching and preservation of the availability of the operating resources as listed under a).
c) A documented procedure is to be implemented in the ARC which ensures the technical availability of the operating resources within determined deadlines at the possible sites of operation.
d) The verification shall be organized such that the operations performed in the frame of the notification and the intervention may be recorded and documented in a tamper-resistant manner. This implements e.g. the traceability of the single process steps, the release and redemption of operating resources or the periodic inventory of operating recourses.

Further protection targets for the performance of the intervention service are determined in the guidelines VdS 2172. The requirements of the guidelines VdS 2172 are to be fulfilled.

4.3.2 Constructional, technical, organisational and personnel requirements

The constructional requirements are defined in the guidelines for intervention centers, VdS 2172.

If an intervention center provides the alarm service, the requirements according to clause 4.2 are to be fulfilled.

4.3.2.1 MCT with mission control system (MCS)

The interventions service shall use transmission techniques for forwarding and bidirectional monitoring of messages to the alarm service and intervention forces (see annex A).

Each intervention force is to be equipped with a DCD which supports the positioning and communication function of the MCS via an interface (see figure 2).

The DCD shall dispose of an automatic emergency function (e.g. emergency call triggered depending on position).

The intervention service shall use for the process of intervention an alarm management system (AMS) resp. a mission control system (MCS).

Note: If a VdS-approved alarm management system according to guidelines VdS 3534 is used, it may be deemed that the state-of-the-art is fulfilled and the requirements according to clause 4.3.2.1 are complied with.

Aim of the operation is normally a concrete or assumed hazard defence. For this purpose the MCS receives data of a lot of sources resp. provides data to other systems in time. These are e.g.

1. Availability and status of mobile forces and their positions
2. Availability and deposit positions of auxiliaries for hazard defence (e.g. special fire extinguishants)

3. Data of potential operation sites, e.g. storage of dangerous materials, valuables storage, events, transports, jeopardized persons
4. Connection to communication systems (telephone, radio etc.) via suitable interfaces
5. Connection to traffic supervision systems (jam warning, traffic restrictions, deviations etc.)

MCS present to the operator the current overview of resources which are available to him and collect the choice criteria/recommendations.

They shall fulfil at least the following functions:

1. Support of decision making for the operation events
2. Presentation of personal and material resources for the operation
3. Indicate recommendations for the operation event, e.g. routes to reach the object, concrete operation forces, their auxiliaries
4. Notification of the intervention forces and ensuring communication with them
5. Presentation of the security situation during operation while considering the forces which interact
6. Forwarding of information to the deployed intervention forces
7. Receiving feedback of the deployed intervention forces for documentation

4.3.2.2 Voice communication

Sufficient communication means shall be available for the voice communication with the alarm service, the intervention forces and the contacts as determined by the measuring plan which are to be contacted in the course of the processing of intervention orders, in order to be able to reach the requested communication partner if he is available.

The voice communication shall be recorded for a period of 30 days. Here, the incoming as well as the outgoing unsuccessful connection attempts shall be captured. A monthly evaluation of all incoming calls is to be performed which shows in which time incoming calls are received by the alarm service.

Direct short codes are to be established for the numbers which are dialled most frequently. Alternatively or additionally, an interface for telephony applications (e.g. the telephony application programming interface – TAPI) to the MCS shall be established.

4.4 Additional services for improvement of efficiency of hazard defence

Essential base for an efficient alarm and intervention service is the planning of a suitable hazard defence of the protected premises.

This planning implements at least the following activities:

- Capture of protected premises specific security situation (overview of situation)
- Capture, evaluation and regular actualization of protected premises specific security information (e.g. plant closures, assembled scaffoldings, hazard focuses)
- Detection and identification of concrete hazards
- Determination of necessary measures and prioritization of these measures for e quickest possible hazard defence
- Capture, evaluation and conjunction of information for alarm verification
- Determination and regular evaluation of the best possible alarm processing and intervention measures and the intervention means

5 The security chain in the MARC

The security chain serves for the quickest possible detection and defence of the hazards which are notified from the protected premises by monitoring techniques. It starts and ends at the protected premises. Detection techniques monitors and notifies, transmission techniques forwards signals to a MARC which there are received and processed. Then, on base of the available information an intervention measure is performed, e.g. by intervention forces which are sent to the protected premises.

The minimum requirements for the performance of the processes within the security chain are determined in the following clauses:

The processes are divided in steps. The following features are determined for each step:

- Triggering activities
- Necessary operations
- Responsibilities for the performance of operations (responsible service according to clause 4)
- Interface where the verification is to be made
- Time measuring values to be captures (time stamp) and
- Responsible service for capture, processing, monitoring and storage of time measuring values

Measurement requirements are not imposed to all steps within a process. However, even the process steps which are not measured are significant for reaching and keeping the respective process result and thus essential part of the service. The process steps as listed in the following – if ordered – thus are to be complied with at least.

5.1 Process of notification

The process of notification starts at the protected premises. Alarm detection and transmission techniques there installed or persons being present there monitor security areas on events/statuses and forward these in form of messages to the technical services (TS). For protection of the transmission path against tamper or other reasons, the notification may be triggered also be a missing of an anticipated message.

The technical service (TS) acknowledges receipt of the message, e.g. to the transmission system in the protected premises and assigns the received/missing messages to the measures which are agreed upon.

The alarm service takes over these messages inclusively all information related to these (e.g. current information on the protected premises as hazard/traffic information, authority measures a.o.) and derives from this an intervention order which is forwarded via the intervention service (IS) to one or several intervention forces. For the choice of the intervention force the mission control system supports with concrete proposals for an optimal operation and resource planning. As soon as the intervention force has acknowledged the receipt of the intervention order, the notification process is concluded.

Note: The notification may in exceptional cases be performed also by voice communication.

The notification process is divided in the following steps, which normally are performed in the sequence as listed underneath.

1. Alarm triggering (clause 5.1.1)
2. Alarm transmission (clause 5.1.2)
3. Alarm disposition (clause 5.1.3)

5.1.1 Alarm triggering

Activities/operations	**Service for the performance of operations**	**Measuring site/interface**	**Measuring result (time stamp)**	**Service for measuring value capture**
a) Message triggering in the protected premises	-	Interface S2 according to VdS 2471 (in the protected premises)	according to DIN EN 50136-1	TS
b) Absence of anticipated messages (the period until reaction to an absent message is not to be monitored in each case but to be agreed upon with the customer on an individual basis.)	TD	In AMS of TS	Time monitoring according to DIN EN 50136-1 and VdS 3534	TS

TS: Technical service according to clause 4.1

5.1.2 Alarm transmission

Activities/operations	**Service for the performance of operations**	**Measuring site/interface**	**Measuring result (time stamp)**	**Service for measuring value capture**
a) Transmission of messages to the MARC	-	CIE, ACE, if given SPT	Failure resp. Fault message from the ATS	TS
b) Receipt of messages from the protected premises	TD	CIE, ACE at TS	T_{Rx} according to DIN EN 50518-2	TS

TS: Technical service according to clause 4.1

5.1.3 Alarm disposition

Activities/operations	Service for the performance of operations	Measuring site/interface	Measuring result (time stamp)	Service for measuring value capture
a) Start of evaluation of received resp. internally triggered messages	TS	In AMS	$T_{Reaction}$ according to DIN EN 50518-2	TS
b) Forwarding of evaluated messages to the AS	TS	MCT - Interface S_{out} at TS	$T_{TS\text{-}forwarding}$	TS
c) Receipt of evaluated messages and information by acknowledgement[1)]	AS	MCT – UI at AS	$T_{AS\text{-}Reaction}$	AS and TS
d) Monitoring of acknowledgement of c)	TS	MCT - Interface S_{out} at TS	$T_{TS\text{-}end}$	TS
e) Evaluation and processing of messages and information by conjunction with master file data of the protected premises and the protected premises specific measuring plan	AS	No measurement necessary		
opt) Amendment of master file data with protected premises specific security information (optional operation which may be performed independently from the sequence of other operations)	AS, IS	No measurement necessary		
opt) Prioritisation of alarms, messages and information depending on the degree of risk of the protected premises (optional operation which may be performed independently from the sequence of other operations)	AS	No measurement necessary		
f) Derivation of concrete measures for hazard defence according to measuring plan (see e)) as well as provision of the operation means as situatively necessary and stipulated in the measuring plan	AS	No measurement necessary		
g) Hand-over of the intervention order to the responsible IS	AS	MCT - Interface S_{out} at AS	$T_{AS\text{-}IS\ order}$	AS and TS

Activities/operations	Service for the performance of operations	Measuring site/interface	Measuring result (time stamp)	Service for measuring value capture
h) Receipt of the intervention order by acknowledgement[1)]	IS	AMS	$T_{IS\text{-}Reaction}$	IS and TS
i) Monitoring of acknowledgement of h)	AS	MCT - Interface S_{out} at AS	$T_{AS\text{-}end}$	AS and TS
j) Assignment of helping centers (e.g. police, fire brigade, emergency units, rescue service)	AS	No measurement necessary		
k) Notification of the received and if given evaluated alarms, messages and information to third parties according to the stipulated agreements (e.g. according customer agreement)	AS	No measurement necessary		

TS: Technical service according to clause 4.1

AD: Alarm service according to clause 4.2

ID: Intervention service according to clause 4.3

1) Messages which are to be dealt with due to measuring plans by the operator at the AS or IS, shall be acknowledged always manually.

5.2 Process of intervention

The intervention process starts with the receipt of the intervention order from the alarm service (IS) by the intervention service (IS): On base of the information on the employable and suitable intervention forces currently available the IS determines who will perform the intervention operation for the protected premises. The charged intervention force (IF) receives the necessary operation information from IS, equips with the necessary operation means (e.g. keys, special protection clothes) and is normally goin the fastest possible to the protected premises.

Note: Is the operation timely critical due to the received message or conjunct with higher hazards, several intervention forces should be deployed at the same time.

The IF first performs an exterior control at the protected premises and evaluates the exterior security status. Provided, the security situation at the protected premises allows it, the IF enters the protected premises to perform an interior control.

Then, the IF evaluates the security status and informs the IS on the security situation at the protected premises.

The IF agrees with the IS how resp. how far the as-is-state of the security equipment at the protected premises may be re-established and performs the agreed measures.

The process of intervention is divided in the following steps, which normally are performed in the sequence as listed underneath.

1. Intervention disposition (see clause 5.2.1)
2. Intervention operation (see clause 5.2.2)

Note: Besides the personal intervention plant-specific technical possibilities of alarm verificatioin in the protected premises should be used as a support of the intervention force (e.g. by use of video surveillance techniques).

5.2.1 Intervention disposition

Activities/operations	**Service for the performance of operations**	**Measuring site/interface**	**Measuring result (time stamp)**	**Service for measuring value capture**
a) Receipt of intervention order by acknowledgement[1)]	IS	MCT – UI at IS	$T_{IS\text{-}Reaction}$	IS and TS
b) Monitoring of acknowledgement of a)	AS	MCT – Interface S_{out} at AS	$T_{AS\text{-}end}$	AS and TS
c) Choice of available intervention forces and operation means for an immediate and target-oriented performance of the intervention	IS	No measurement necessary		
d) Assignment of the IF	IS	MCT – Interface S_{out} at IS	$T_{IS\text{-}IF\ order}$	IS, AS, TS
e) Receipt of protected premises specific intervention order by manual acknowledgement	IF	DCD-UI of the IF	$T_{IF\text{-}Reaction}$	TS
f) Monitoring of acknowledgement of e)	IS	MCT – Interface S_{out} at IS	$T_{IS\text{-}end}$	IS and TS
g) Monitoring of intervention operation e.g. by regular positioning of the IF	IS	MCS of the IS	n x $T_{IF\text{-}monitoring}$	

AS: Alarm service according to clause 4.2

IS: Intervention service according to clause 4.3

IF: Intervention force

1) Messages which are to be dealt with due to measuring plans by the operator at the AS or IS, shall be acknowledged always manually.

5.2.2 Intervention operation

Activities/operations	**Service for the performance of operations**	**Measuring site/interface**	**Measuring result (time stamp)**	**Service for measuring value capture**
a) Acknowledgement of intervention order and drive of IF to the protected premises (see 5.2.1e))	IF	DCD-UI of the IF	$T_{IF\text{-}Reaction}$	TS
b) Arrival at protected premises and technical transmission of position to the IS	IF	DCD – S_{out} (Position determination) of IF <-> MCS in the MCT of the IS	$T_{IF\ operation}$	IS and TS
c) Determination of the security situation i the protected premises (comparison planned vs. Actual security status on base of the order modalities if given supported by the findings of the alarm verification (e.g. video images)	IF	No measurement necessary		
d) Evaluation of the security status and information of the IS on the security situation in the protected premises	IF			
e) Agreement with the IS how resp. how far the as-target state of the security equipment at the protected premises may be re-established.	IF			
f) Re-establishment of the target state according to agreement aiming to reset the security equipment into functional state.	IF			
g) Status message on the reached state of the security equipment which are concerned by the intervention order.	IF	MCS in the MCT of the IS, forwarded by the DCD	$T_{IF\text{-}Object\ status}$	IS and TS
h) Message on readiness of IF for new operation	IF	MCS in the MCT of the IS, forwarded by the DCD	$T_{IF\text{-}end}$	IS

TS: Technical service according to clause 4.1

IS: Intervention service according to clause 4.3

IF: Intervention force of the intervention service

5.3 Monitoring of the process steps in the security chain

The monitoring of the security chain serves for the determination of the efficiency of the process steps in the course of the notification and intervention. In the case of faults or dysfunctions it serves for corrective measures. The monitoring of the security chain comprises the monitoring of

- The alarm transmission system (see clause 5.3.1)
- Activities (see clause 5.3.2) and
- The performance features (see clause 5.3.3)

5.3.1 Monitoring of the alarm transmission system

This process is described in DIN EN 50136-1 and is to be performed by the alarm receiving center resp. the alarm provider.

5.3.2 Monitoring of activities

The activities as listed underneath are to be checked on compliance with the time criteria mentioned for the message transmission. If the respective activity has not started within the prescript time, it is the task of the service provider responsible for the monitoring to initiate the redundant resp. emergency measures as previously determined and agreed with the process responsible. Written records on deviating measures are always to be kept. The reason for the deviation is to be documented in written form in the records and measuring plan.

Responsible service for monitoring	Monitored criteria	Triggering criteria for deviating resp. Emergency measures
TS	TTS-end (acc. to 5.1.3 d))	TTS-end – TTS-forwarding ≤ 20s
AS	TAS-end (acc. to 5.1.3 i))	TAS-end – TAS-IS order ≤ 20s
IS	TIS-end (acc. to 5.2.1 f))	TIS-end – TIS-IF order ≤ 20s
IS	n x TIF-monitoring	Δ TIF-monitoring ≤ 420s
IS	TIF operation	TIS-end – TIF operation > planned arrival time
IS	TIF-Object status	According order specific agreement
IS	TIF - end	According order specific agreement

TS: Technical service according to clause 4.1

AS: Alarm service according to clause 4.2

IS: Intervention service according to clause 4.3

If: Intervention force at the intervention service

5.3.3 Monitoring of the performance features

The performance features as listed underneath are significant base for the planning of measures for hazard defence. They are indicators for the availability and efficiency of the processes and are to be used for the disposition of the technical and personal resources.

Performance features which are to be monitored according to DIN EN 50518 Part 2 by the ARC:

Monitored duration of activities/operations	**Service for delivering results**	**Measuring site/interface**	**Measurement results (time stamp)**	**Service for monitoring**
5.1.2 b) Receipt of messages from the protected premises	TS	CIE, ACE at the TS	T_{Rx} acc. to DIN EN 50518-2	TS
5.1.3 a) Start of evaluation of the messages received	TS	In AMS of the TS	*$T_{Reaction}$ acc. to DIN EN 50518-2*	TS

TS: Technical service according to clause 4.1

ACE: Ancillary control equipment

CIE: Control and indicating equipment

Performance features to be monitored and their efficiency:

The time between T_{Rx} and $T_{Reaktion}$ shall correspond with the following efficiencies:

Performance feature	**Efficiency**	**Efficiency category**
Hold-up alarms	$T_{Reaction} - T_{Rx} \leq 30s$	80% of the received messages
Hold-up alarms	$T_{Reaction} - T_{Rx} \leq 60s$	98,5% of the received messages
All other messages as hold-up alarms	$T_{Reaction} - T_{Rx} \leq 90s$	80% of the received messages
All other messages as hold-up alarms	$T_{Reaction} - T_{Rx} \leq 180s$	98,5% of the received messages

The compliance with the a.m. criteria shall be reached each in a completed period of 12 months.

Performance features which are to be monitored by the alarm provider:

Monitored period of activities/operations	**Service for performance of results**	**Measuring site/interface**	**Measuring result (time stamp)**	**Service for monitoring**
5.1.3 a) Start of the evaluation of received messages	TS	In AMS of the TS	$T_{Reaction}$ acc. to DIN EN 50518-2	TS
5.1.3 d) Monitoring of acknowledgement of the alarm service on the receipt of evaluated messages and information	TS	MCT – interface S_{out} at the TS	$T_{TS\text{-}end}$	TS

TS: Technical service according to clause 4.1

Performance features to be monitored and their efficiency:

The time between $T_{Reaction}$ and $T_{TS\ emd}$ shall correspond with the following efficiencies:

Performance feature	**efficiency**	**Efficiency category**
Manual acknowledgement[1)]	$T_{TS\text{-}end} - T_{Reaction} \leq 60s$	80% of the received messages independent of the protected premises
Manual acknowledgement[1)]	$T_{Ts\text{-}end} - T_{Reaction} \leq 60s$	80% of the received messages of the protected premises for which this efficiency category is agreed
Manual acknowledgement[1)]	$T_{Ts\text{-}end} - T_{Reaction} \leq 60s$	Otherwise agreed efficiency category according to measuring plan, however, more than 80 % of the received messages
Automatic acknowledgement	$T_{TS\text{-}end} - T_{Reaction} \leq 30s$	98,5% of the received messages

1) Messages which are to be dealt with by the operator of the AS due to the measuring plans, shall always be acknowledged manually.

The compliance with the a.m. criteria shall be reached each in a completed period of 12 months.

Performance features for the AS which are to be monitored:

Monitored period of activities / operations	Service for performance of results	Measuring site/interface	Measuring result (time stamp)	Service for monitoring
5.1.3 c) Receipt of messages and information evaluated by the TS and acknowledgement of the AS	AS	MCT – UI at alarm service	$T_{AS\text{-}Reaction}$	AS and TS
5.1.3 k) Monitoring of receipt acknowledgement of the intervention order	AS	MCT – Interface S_{out} at AS	$T_{AS\text{-}end}$	AS and TS

TS: Technical service according to clause 4.1

As: Alarm service according to clause 4.2

The time agreed with the customer for the performance of the alarm service is to be recorded by time stamp $T_{AS\text{-}End}$ - $T_{AD\text{-}Reaction}$.

Performance features to be monitored and their efficiency:

Performance feature	Performance criteria	Efficiency category
Manual acknowledgement[1)] Automatic acknowledgement	The time agreed with the customer for the performance of the alarm service is to be recorded by time stamp $T_{As\text{-}End}$ - $T_{AD\text{-}Reaction}$.	The customer shall be informed about an exceeding of the agreed time.

1): Messages which are to be dealt with by the operator of the AS due to the measuring plans, shall always be acknowledged manually.

Performance features for the IS which are to be monitored:

Monitored period of activities/operations	Service for performance of results	Measuring site/interface	Measuring result (time stamp)	Service for monitoring
a) Receipt of intervention order by manual acknowledgement	IS	MCT – UI at IS	$T_{IS\text{-}Reaction}$	IS and TS
f) Monitoring of acknowledgement of e)	IS	MCT– Interface S_{out} at IS	$T_{IS\text{-}end}$	IS and TS

TS: Technical Service according to clause 4.1

AS: Alarm service according to clause 4.2

IS: Intervention service according to clause 4.3

Performance features to be monitored and their efficiency:

Performance feature	Performance criteria	Efficiency category
Manual acknowledgement[1)] Automatic acknowledgement	The time agreed with the customer for the performance of the alarm service is to be recorded by time stamp $T_{IS\text{-}End}$ - $T_{IS\text{-}Reaction}$.	The customer shall be informed about an exceeding of the agreed time.

1): Messages which are to be dealt with by the intervention forces due to the measuring plans, shall always be acknowledged manually.

5.4 Process of reporting

The MARC is responsible for the correct documentation of operations in the course of the notification and intervention. All contents as listed in clauses 5.3.1 and 5.3.2. are part of this documentation. The reporting process normally comprises two steps:

1. Intervention reporting comprises the establishment of the intervention report by the intervention service and the hand-over to the alarm service
2. Alarm reporting comprises the establishment of the alarm report by the alarm service and the hand-over to the customer (applicant).

5.4.1 Intervention report

At least the process steps according to clause 5.2 which are to be captured by time stamp together with the following information are to be documented in the intervention report:

a) Unambiguous customer denomination (e.g. customer number)
b) Time of message receipt at the intervention service (date, time)
c) Message criteria (e.g. intrusion)
d) Name or personal number of the intervention forces being charged or deployed at the protected premises
e) Planned resp. necessary operation means
f) Time of hand-over of operation means to the charged IF
g) Time of arrival at the protected premises
h) Special observations around the protected premises
i) Name of the person met at the protected premises
j) Further bodies (e.g. police, fire brigade, installer) or persons being present at the protected premises for re-establishment of the security status as well as the performed measures
k) Determined causes for the alarm notification, e.g. triggering cause of the detection system
l) Determined damages at the protected premises
m) The measures being performed at the protected premises for hazard defense
n) Status on the reached state of all security equipment at the protected premises
o) If given further security measures on site after damage (e.g. security patrols)
p) Name of all persons which have been informed on the facts in the course of the intervention
q) Status report (date, time) on the reached state of the security equipment at the protected premises which are concerned by the intervention order
r) Standby state of the IF for new operations (date, time)

5.4.2 Alarm report

The process steps as indicated in clause 5.2 and 5.2 which are to be captured by time stamp including the following information are to be documented in the alarm report.

a) Time of alarm triggering (date, time)
b) Time of receipt of message at the alarm service (date, time)
c) Triggering criterion (e.g. intrusion)
d) Name or personal number of responsible operator (alarm service)
e) Unambiguous customer denomination (e. g customer number)
f) Result and time of alarm verification
g) All measures which are initiated for hazard defence at the protected premises
h) Compendium of the intervention report (see 5.4.1)
i) Time of re-establishment of the security status on the protected premises
j) Further performed measures (according to intervention plan)
k) Completion of process (date, time)

6 Management of the MARC

The MARC (approval owner) shall dispose of a certified quality management system according to DIN EN ISO 9001.

Note: The conditions of acceptance of third party QM-certifications are given in Annex B.

The processes as listed in these guidelines are to be presented in the QM-system and to be organised. Here, at least the requirements of quality assurance in the QM-system as listed underneath are to be considered:

a) The responsibilities for the processes are to be determined in writing by the MARC. For limitation of the responsibilities the interfaces as shown in Annex B, figure 1 and clause 5 may be used. A person who is responsible overall processes is to be nominated (e.g. main MARC Expert). Responsible persons are to be nominated for all processes. The responsibility for single process steps may be delegated. The overall process responsible person shall perform an internal audit once a year with the process responsibles.
b) Description of activities for the performance of the technical service and the security services of the alarm and intervention service (e.g. on base of work procedures and instructions).
c) Description of the activities and responsibilities for providing the necessary equipment and operation means
d) Description of activities and responsibilities for regular regular administration of master file data, measuring plans and protected premises relevant security information. Here, it shall be determines that the currently used measuring plans are to be presented to the customer at least once in four years to be checked on actuality.
e) Description of the activities and responsibilities for planning the intervention. To this especially the determinations on tactic operation belong, which are agreed upon for maintenance resp. re-establishment of the protection target – if given considering the protected premises relevant security information.
f) Description of the activities and responsibilities in the course of performance of intervention regarding hand-over of protected premises specific operation means and operation data as well as return of protected premises specific operation means.

g) Description of activities for maintenance (e.g. maintenance and inspection), the marking, safekeeping/deposit and the protection of protected premises specific data and operation means.
h) Qualification of the uses security forces and measures for keeping their qualification (e.g. instructions/trainings)
i) Legal as well as authority requirements and the type of verification on their fulfilment
j) Requirements on type and kind of verification on performed activities
k) Determination of suitable monitoring means and measures for their use in order to surveille the fulfillment and compliance with the requirements.
l) Type and extent of the check as well as marking of the property of the customer being included in the security service
m) Determinations for the case of loss or damage of provided property of the customer
n) Requirements on handling with faults which occur during the performance of technical services and the security services
   - Determination of responsibilities for fault handling
   - Evaluation and documentation of fault causes
   - Determination of measures for fault remedies and fault avoidance
   - Documentation of fault remedy and fault avoidance
   - Monitoring of performance of fault remedy
   - Determination and documentation of efficiency of measures for fault avoidance within an appropriate period being determined by responsible persons
   - Written information of responsibles on type of fault including agreement and release of a. m. measures by the responsible
   - Release of a. m. measures by the customer

6.1 Planning of the processes

The MARC shall establish a security concept in which the management of the processes and the necessary measures for fulfilment of the protection targets are presented and documented. For the presentation of the management of the processes the procedures in the QM-system may be indicated in the security concept. The security concept is to be checked on actuality once a year and in case of changes to be adapted accordingly. The requirements on the QM-system for the development (DIN EN ISO 9001, clause 7.3) should be considered, here.

If services within the above mentioned processes are brought by co-operation partners, a co-operation contract shall be concluded between operator of the MARC (approval owner) and the respective co-operation partner in which the restrictions of responsibilities as well as hand-over interfaces are unambiguously regulated.

The co-operation partners are to be subjected to a yearly supplier assessment according to the requirements of DIN EN ISO 9001. To this end, especially the service features as indicated in clause 5.3 on fulfilment and compliance on their efficiency are to be evaluated.

The most important task for planning of intervention measures is to develop an optimised process and to regularly upgrade it. This task is to be determined as quality aim in the management system of the MARC, to be persecuted in the processes of the security chain and to be evaluated at least once a year in the course of the management evaluation.

6.1.1 Agreement on notification measures

The MARC shall agree with the customer and if given with the responsible police department under which circumstances the police is informed. To this end, the persons being present in the object and the degree fo risk of the object are to be considered.

This may for example be an agreement which comprises that

- The MARC shall inform the police directly when receiving an alarm and the police is to be driving to the monitored object at the same time as the intervention forces
- The MARC shall inform the police when receiving an alarm and the police is to drive directly to the monitored object reclusively.
- On reception of an alarm first an alarm verification is performed and/or the intervention forces of the IS are driving to the object and perform an alarm verification on site, the police is notified only in case of a concrete intrusion suspicion.

Note: If the intervention measures are base of the insurance contract between insure and insurer, the customer shall include his insurer in time in the agreement procedure. The MARC should inform the operator on this actual situation.

6.1.2 Alarm- and intervention plan

The MARC shall elaborate and maintain a detailed alarm and intervention plan in electronic form for the monitored protected premises, in which the immediate measures for the object and cause for the activity of the alarm and intervention service are listed. The totality of the alarm and intervention plan is composed of different information which are available as text, photos, site plan etc. These data are to be provided in respective form for an optimum use by the corresponding security service provider in the alarm management system resp. the mission control system.

The alarm and intervention plan shall contain at least the following indications:

- Object data:
  - Name, address, phone number of the protected premises
  - Ground plan reps. Object sketch
  - Journey with specialities
  - Indications on AS (e.g. position of ancillary control equipment, key assignment, mounting site of the control and indicating equipment, type of monitoring, configuration of alarm points)
  - Special object/person related operation instructions (e.g. for video surveillance the positions of the cameras in the object)
- Responsible police department
- Type of risk/branch (e.g. bank, jewellery, jeopardised persons)
- Regulations of key deposit/supply with indication of key carrier (person, which has access to the monitored object)
- Particularities as e.g. key hierarchy, hazard potential
- Indications on the installer of the AS
- Intervention measures which are to be fixed for each connected alarm (e.g. hold-up, intrusion, fault, fire, set/unset, missing test alarm)
- Responsible IS reps. IFs to be deployed (if necessary)

Note: It is recommended to agree upon passwords or characters for the monitored objects so that names and addresses may be treated confidentially.

If an intervention by an IS is agreed, it must be ensured that the intervention forces are in adequate delay at the place of action (normally within 20 min measured from time stamp T_{rx} in the ARC). In agreement with the customer/insurer also other delays may be agreed upon.

Note: The time of 20 minutes must not be kept, if this is not possible due to extreme unforeseen influences, e.g. in case of black ice, other weather influences, suddenly occurring vehicle defect, traffic restrictions, deviations).

The intervention is to be performed according to VdS 2172.

The IF has as far as possible (e.g. access possibility, availability of keys) to see for the object is left in secured state after an operation (e.g. closed and locked doors and windows, externally set IAS). For the case that this is not possible, adequate and damage restrictive measures which are determined by the customer shall be foreseen (e.g. steady manning by security forces, emergency security measures).

6.1.3 Alarm- and Intervention service attestation

In case of connection of VdS-approved AS measures for the alarm and intervention service are to be documented on the alarm and intervention service attestation, VdS 2529 by the MARC. The MARC shall agree upon the measures determined in the attestation for the intervention service with the provider of the service. The MARC shall see for the necessary intervention is performed only by VdS-approved IS on site of the AS.

Note 1: In agreement with the operator of the AS (and if given with its insurer) this requirement may be varied from. The deviation is to be documented in the attestation.

Note 2: The installer of the AS shall inform the MARC on the VdS-approval of the AS.

The alarm and intervention attestation, VdS 2529 may also be used for connections of not VdS-approved AS. In these cases, the attestation may be issued also by the VdS-approved IS. The completely filled attestation shall be handed over to the operator of the AS and shall be available as copy at the MARC. In case of changes of the measures for the alarm and intervention service, a new attestation shall be issued. This regulation is valid for all AS for which an alarm and intervention attestation according to VdS 2529 is issued.

6.1.4 Planning for faults, crises and emergency cases

In case of an event leading to the MARC or parts thereof can no longer fulfil completely or partly its tasks, a written plan shall be available which shows the procedure for the effects of these events. This plan shall be preventative for all foreseeable extraordinary events at which restrictions of the operations of the MARC may be anticipated.

Extraordinary foreseeable events which are to be considered at least are:

- Failure of transmission control and indicating equipment
- Failure of transmission paths
- Failure of the AMS resp. The AMS within the security chain
- Failure of the MCS
- Failure of the DCD
- Fire, flood (water ingress), storm, overvoltage
- Internal and external tamper actions
- Pandemias
- Authority regulations (e.g. in case of bomb findings, gas leakage, harassment scenario)

The activities and measures which are to be initiated and performed after such an event, shall be defined clearly and aimed to the re-establishment of the complete operationability and shall comprise at least the following aspects:

a) Contact data, including contractual bases of (external) suppliers, service providers which are able to re-establish the normal operation
b) Necessary resources by which the operation may be continued or re-established

This plan shall be checked and evaluated on practicality, realization and possibility of occurrence of such events all 12 months the latest. The check shall be documented and signed by the responsible for alarm reception, alarm service and intervention service.

This plan shall be available at every time to the responsible of the alarm reception, the alarm service and the intervention service in valid version. The plan shall regulate unambiguously who shall dispose in single events in what time of this plan.

6.2 Co-operation in providing security services

All services which are not independently provided by the MARC (approval owner) according to these guidelines (technical services and security services) or activities within these services which are not independently provided as well as such services provided in charge of the MARC at other sites, are to be provided in co-operation with suitable co-operation partners. The co-operation shall be proved in form of a written contract with the respective co-operation partner. The contract shall comprise the following details on the charged security services and its activities:

a) Detailed description of activities in the frame of security services
b) Determination of responsibilities of the respective activities
c) Minimum requirements for the equipment and the operation means to be furnished
d) Minimum requirements on the qualification of deployed security forces
e) Legal and regulatory requirements and the type of proof on its fulfillment
f) Requirements on type and kind of proof on the activities being performed by the co-operation partner
g) Determination of suitable monitoring means and measures for its use in order to surveille the fulfilment and compliance of the requirements which are set for the co-operation partner.
h) Type and extent of the check and marking of the property of the customer and the MARC being included in the security service as well as determination of the site of deposit.
i) Determinations for the case of loss or damage of provided properties of customer and the MARC
j) Requirements on handling of faults, which occur in connection with the provision of security services of the co-operation partner
   - Determination of responsibilities for fault handling
   - Evaluation and documentation of fault causes
   - Determination of measures on fault remedy and fault avoidance
   - Documentation of fault remedy and fault avoidance
   - Monitoring of performance of fault remedy
   - Determination and documentation of the efficiency of measures for fault avoidance within an adequate time frame which is to be determined by the responsible person
   - Written information of the responsibles on type of fault inclusively agreement and release of a. m. measures by the responsible
   - Release of a. m. measures by the MARC.

Annex A (normative) Technical requirements for MCT and the forwarding of messages within the security chain

A.1 MARC comprising one ARC with integrated alarm service

Transmission equipment (TE) are connected to the ARC in alarm systems. The message transmission is made according to DIN EN 50136-1 in a category being agreed with the operator of the alarm system. The message reception is made at the ARC via transmission control and indicating equipments. The messages received are forwarded to an ancillary control equipment in the ARC via interface S4. The ancillary control equipment is normally integrated part of the alarm management system according to VdS 3534. The interface at the AMS for connection to the S_4 interface is also called S_{AMS} interface.

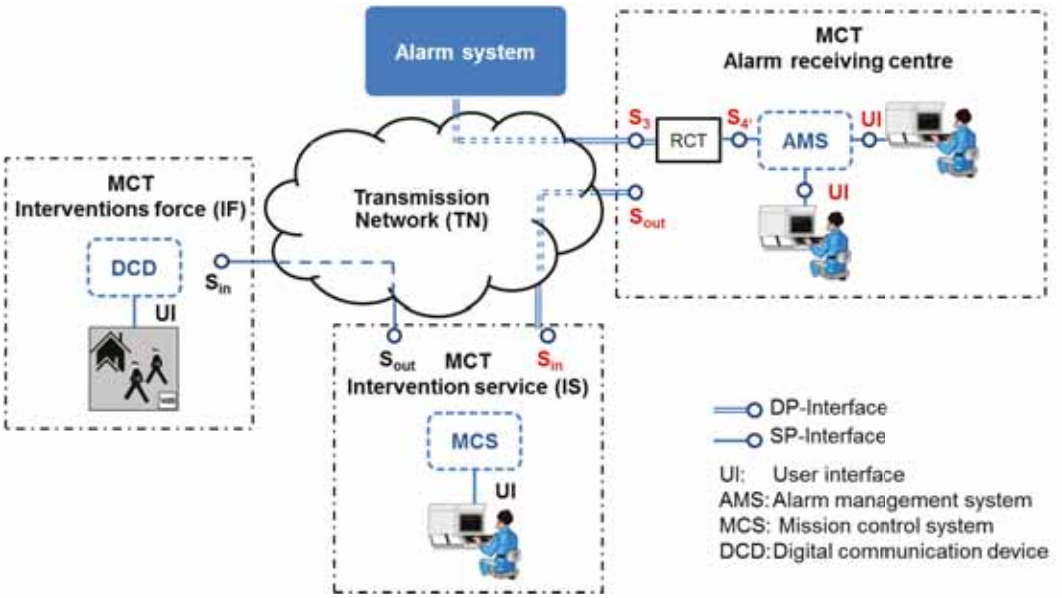


Figure 1: MCT within the security chain of a MARC comprising ARC with integrated AS and external IS

Messages are forwarded from the MCT of the alarm receiving center via S_{out} interface to the intervention service. The intervention service receives the messages at S_{in} interface, which itself is directly connected with the S_{AMS} interface of a MCS. The data are forwarded from the MCT of the intervention service via S_{out} interface to the intervention force.

Requirements on the transmission of the alarm service to the intervention service are stipulated in the guidelines VdS 2172

A.2 Alarm provider (AP) comprising one ARC with or without integrated alarm service

The alarm transmission from the alarm system to the AMS in the ARC of the alarm provider is made as described under 1. For performance of the technical services for the forwarding of messages to the MCTs in the AS as well as their bidirectional monitoring and fault detection a respective transmission techniques resp. corresponding transmission systems are available. Optionally, the AP may additionally take of the AS, e.g. for the case that the MCT of an AS cannot be reached in due time.

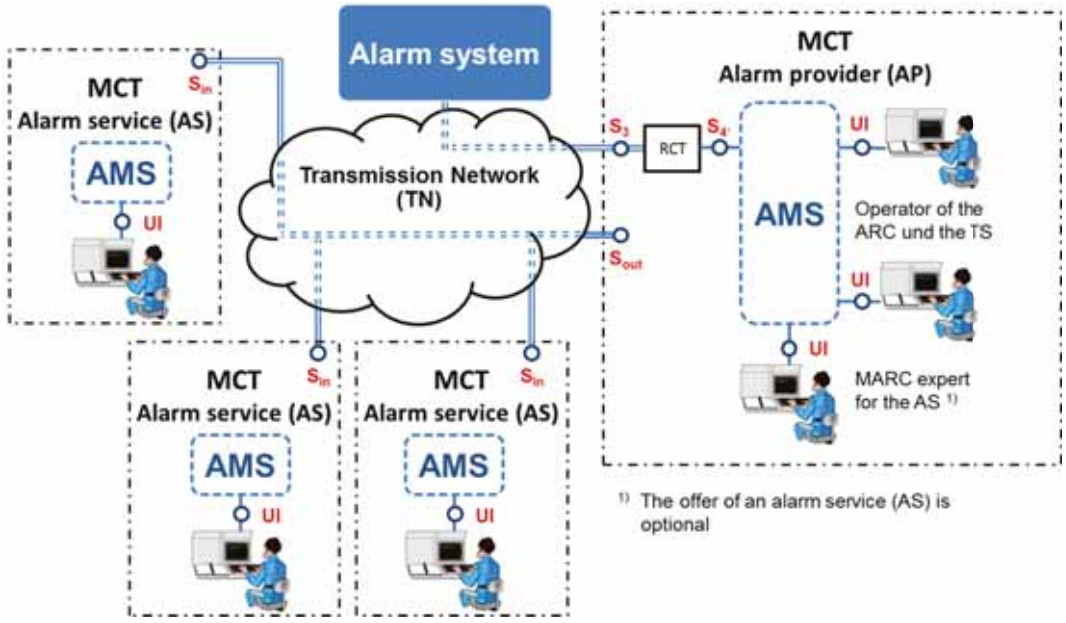
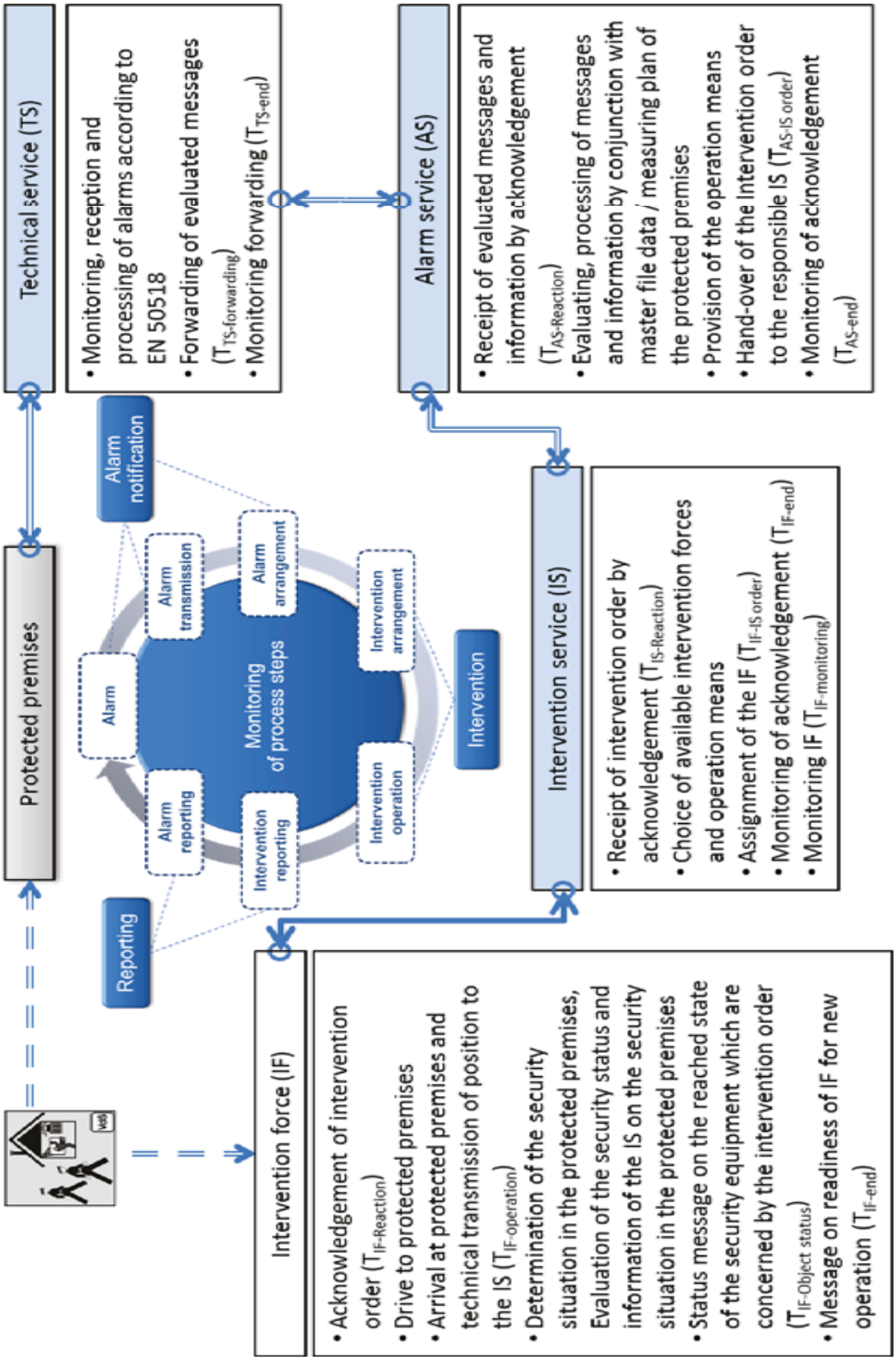


Figure 2: MCT within the security chain of an AP comprising an ARC with or without integrated AS

The requirements for alarm transmission systems according to DIN EN 50136-1:2012-08 are to be complied with for the transmission paths for forwarding messages to the MCT of the alarm service. The following configurations may be applied:

Category of the ATS	Conditions
SP 4 to MCT – AS	The AP takes over the AS for the case the MCT of the AS cannot be reached in due time. The protected premises specific current measuring plans and data for incoming messages shall be available for AP.
SP 4 to MCT – AS	Another steadily manned external AS determined as redundant takes over the AS in case that the MCT of the intended AS cannot be reached in due time. The protected premises specific current measuring plans and date for incoming messages shall be available for the AS serving as redundant. Together with his MCT, he shall be part of the network provided by the AP for alarm transmission services.
DP 4 to MCT – AS or SP 4 and SP 6 to MCT – AS	The AS disposes as redundant only a not steadily manned external AS which is manned in case of total failure of the MCT of the intended AS. The protected premises specific current measuring plans for incoming messages shall be available for the AS being redundant. Together with his MCT, he shall be part of the network provided by the AP for alarm transmission services.

Table 1: Categories for ATS from one MCT of the AP to the MCT of the AS

Annex B (informative) The services in the security chain of the MARC