**Report code**
20 February 2025

# Guidance & Interpretation-document

Monitoring and Alarm Receiving Centres & Alarm Transmission Service Providers

creating trust
***driving progress***

## Colophon

| | |
|---|---|
| Title | Guidance & Interpretation document Monitoring and Alarm Receiving Centres & Alarm Transmission Service Providers version 8.0 |
| Author | Kiwa FSS Certification |

Approved by the Board of Experts Security on 20-02-2025

**Kiwa Nederland B.V.**
Kiwa FSS Certification
Dwarsweg 10
5301 KT Zaltbommel

Tel. 088 998 51 00
NL.infocertification.fss@kiwa.com
www.kiwa.com

# Contents

## Version history

| Version | Change | Date |
|---|---|---|
| 1 | First setup of the document | 2020/05/27 |
| 2 | Adding VSS Control Room | 2020/07/31 |
| 3 | Adding input Board of Experts security | 2020/09/09 |
| 4 | Change after meeting Board of Experts security | 2021/02/10 |
| 5 | Combined changes after meetings Board of Experts security | 2022/11/17 |
| 6 | Changes in response times and Business continuity after BoE 03-2023 | 2023/03/27 |
| 7 | Change composition BoE and add guidance on remote access/apps and portals. | 2024/06/06 |
| 8 | Addition of BRLs to 1.2, inspection and expansion of Chapter 7 with 27001:2022, new corporate identity Kiwa,  addittion guidance response times (4.3) and risk assessment (7.7). | 2025/02/20 |

# 1. Introduction

This interpretation document applies to the international standards for Inspection & Certification of EN 50518 Monitoring and Alarm Receiving Centres (MARC) and K21030 Alarm Transmission Service Providers (ATSP) and has been accepted by the Board of Experts Security, in which all relevant parties in the field of Security are represented. The Board of Experts also supervises the activities and when necessary require this scope to be revised and determine when additional interpretation is needed.

The Board of Experts Security consists of the following persons:

| **Board of Experts Security** | | |
|---|---|---|
| Bert Bambach | Avans Hogeschool | Chairman |
| John van Schaik | M2M Services | Supplier |
| Ronald van Duijn | ENAI | Supplier / ATSP |
| Mathijs de Vaal | Protify | Consulting |
| Iwan Debets | ASB Security | Supplier / ATSP / MARC |
| Robèrt Wijmans | Verisure | Supplier / MARC |
| Rens Krijgsman | KOP Beveiliging | Installer |
| Jurjen Burghgraef | JBRisicobeheer | Risk assessor |
| Bram Vandenbergen | NVD Beveiligingen | MARC |
| Erwin Schoemaker | Federatie Veilig Nederland | Branche |
| Kim van Heemskerk-Grimbergen | Nationale Politie | Police |
| Jan Willem Verwoert | Kiwa FSS Testing | Certification body |
| Albertine Ibrahim | Kiwa FSS Testing | Certification body |
| Peter Voshol | Kiwa FSS Certification | Certification body |
| Mischa van der Geld | Kiwa FSS Certification | Certification body |
| Dio Kock | Kiwa FSS Certification | Certification body/Secretary |

*Table 1; Members board of experts security*

Technological developments do not wait for laws, regulations, and standards. These laws, regulations, and standards follow the developments. This 'guidance & interpretation document' embodies the technological and market developments. The purpose of this document is to clarify the context by establishing new definitions on certain themes and topics. This makes it clear for individuals and market parties what the conditions are for determining compliance with the applicable requirements. It also explains which developments are taking place at the level of standards and how these align with market developments and connect with laws and regulations

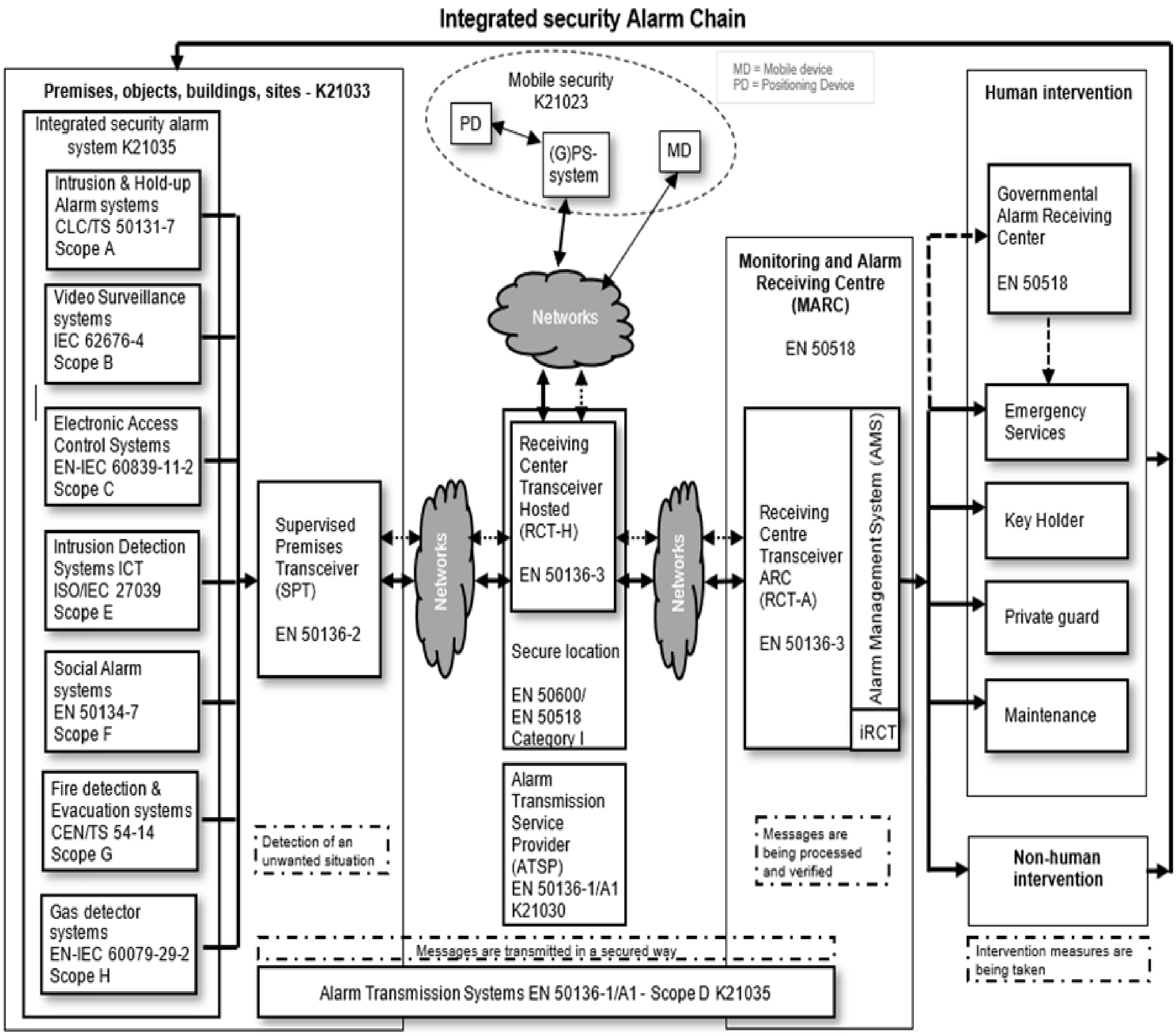
This guidance & interpretation document has been drafted with two primary goals:

- Guidance: To provide context for the design, installation, and operation of systems, marked with the letter "G".
- Requirements: To offer additional or alternative requirements on matters not clearly defined in the standards or where the standards have not yet addressed the issue or development, marked with the letter "R".

## 1.1 Security alarm chain

In Figure 1, the integrated security alarm chain as seen by Kiwa FSS is illustrated. Explanation:

1. On the left side an alarm system in a premises, object, building or site generates an alarm. This alarm is then transmitted via a Supervised Premises Transceiver (SPT). This Alarm system and SPT are installed in accordance with certification scheme K21049/K21035: Security Alarm systems.
2. In a hosted solution a secure data location applies. In that situation a Receiving Centre Transceiver-Hosted (RCT-H) communicates with an interface Receiving Centre Transceiver (iRCT). This is under responsibility of an Alarm Transmission Service Provider (ATSP).
3. The alarm now enters the MARC processes and verifies the alarm and then has two options: human intervention or non-human intervention.
4. A mobile device or a positioning device could also generate an alarm which ends up in a MARC.


Integrated security Alarm Chain
Premises, objects, buildings, sites - K21033
Integrated security alarm system K21035
Intrusion & Hold-up Alarm systems CLC/TS 50131-7 Scope A
Video Surveillance systems IEC 62676-4 Scope B
Electronic Access Control Systems EN-IEC 60839-11-2 Scope C
Intrusion Detection Systems ICT ISO/IEC 27039 Scope E
Social Alarm systems EN 50134-7 Scope F
Fire detection & Evacuation systems CEN/TS 54-14 Scope G
Gas detector systems EN-IEC 60079-29-2 Scope H
Supervised Premises Transceiver (SPT) EN 50136-2
Detection of an unwanted situation
Mobile security K21023
PD
(G)PS-system
MD
MD = Mobile device
PD = Positioning Device
Networks
Networks
Networks
Receiving Center Transceiver Hosted (RCT-H) EN 50136-3
Secure location EN 50600/ EN 50518 Category I
Alarm Transmission Service Provider (ATSP) EN 50136-1/A1 K21030
Monitoring and Alarm Receiving Centre (MARC) EN 50518
Receiving Centre Transceiver ARC (RCT-A) EN 50136-3
Alarm Management System (AMS)
iRCT
Messages are being processed and verified
Messages are transmitted in a secured way
Alarm Transmission Systems EN 50136-1/A1 - Scope D K21035
Human intervention
Governmental Alarm Receiving Center EN 50518
Emergency Services
Key Holder
Private guard
Maintenance
Non-human intervention
Intervention measures are being taken

This figure is based on a hosted solution

*Figure 1*

Below is a schedule showing the European standards and the accompanying responsibilities.

| **Roles defined in the security chain** | | | | |
|---|---|---|---|---|
| Installer | | Alarm Transmission Service Provider | | Monitoring and Alarm Receiving Centre |
| **Applicable European Standards in the security alarm chain** | | | | |
| EN 50131 / TS54-14 / etc / Alarm systems at the premises or object | ⇨ | EN 50136-1/A1 Alarm transmission | ⇨ | EN 50518 Alarm Response by ARC |
| **Assessment by Kiwa based on certification scheme:** | | | | |
| Installer integrated safety/security solutions K21049/K21035 | ⇨ | Alarm transmission service provider (ATSP) K21030 | ⇨ | EN 50518 with applicable scopes (M)ARC |
| **Responsibilities** | | | | |
| Alarm system + SPT | ⇨ | Configuration ATS, testing initial & periodic SPT & RCT & Reporting to client | ⇨ | AMS + RCT periodic reporting by the MC |

*Figure 2*

## 1.2 Related Kiwa Assessment Guideline (BRL)

| Kiwa BRL | Short reference | Link with EN 50518 |
|---|---|---|
| K21023 | The purpose of the certification scheme K21023 Mobile Security is to inform the (external) emergency organization in a timely and secure manner about the status of goods, vehicles, and/or persons in order to start the emergency process. | Certification is possible for the scope of people monitoring, lone workers, and object tracking systems for security applications based on the platform certified by K21023. With this, the supplier demonstrates higher competence. |
| K21024 | The BRL 'K21024 Security and Safety of Construction Sites' describes the process to achieve construction site security that meets the requirements as stated in the BRL K21024 and the additional wishes/requirements of the buyer or insurer. | A certified party in accordance with K21024 transfers its connections to an EN 50518-certified alarm center with the scope of Video Surveillance Systems (VSS) for security and non-security applications.<br>Scope 1 - Temporary electronic security systems<br>Scope 2 - Temporary access control systems<br>Scope 3 - Temporary fire alarm and/or evacuation systems |

| | | |
|---|---|---|
| K21035 | This international certification scheme 'K21035 Security Alarm Systems' includes all relevant requirements employed by Kiwa when dealing with applications for the issuance and maintenance of a certificate for products, processes, and services used for integrated security alarm systems. | By having the relevant scope certified, the installer can demonstrate that this security solution has been soundly realized. This allows the ARC to rely on a reliable alarm connection. |
| K21039 | The Assessment Guideline (BRL) K21039 Video Security Systems contains criteria for companies wishing to obtain and maintain certification as suppliers of video surveillance systems for use in security applications. The BRL K21039 Video Security Systems incorporates the current legislation described in the RPBR. | A certified party in accordance with K21024 transfers its connections to an EN 50518-certified alarm center with the scope of Video Surveillance Systems (VSS) for security applications. |
| K21047 | The certification scheme "K21047 Wireless Silent Alarm Systems" has been drawn up for companies that wish to obtain certification for the installation and maintenance of wireless silent alarm systems. These will mainly be applied in healthcare but can also be applied on company sites. | An EN 50518-certified alarm center is the receiving point for escalation and fault messages from wireless silent evacuation systems. This ensures the continuity of the chain. |
| K21049 | K21049 Integrated Security Alarm Solutions is the assessment scheme for testing, inspection, and certification of integrated alarm security systems. Nowadays, security companies increasingly install and combine multiple types of alarm systems in one security solution. This scheme, therefore, focuses on the integration of the various systems in a building. The structure of this scheme ensures a seamless connection of assessments between the various sub-areas. | This scheme is applicable for:<br>- Suppliers of high-end, high-risk security solutions, providing full system integrations across all security solutions available on the market and connecting to the EN 50518 alarm center.<br>- End users who want to have independently demonstrated that the supplied security systems align with their business risks and the starting point document or tender application.<br>-Insurers who require a custom solution for acceptance of high-risk (high value) customers or locations. |

*Table 2 Kiwa BRL's*

## 2. Categories and scopes "G"

Most countries in Europe impose requirements on the operation of Alarm Receiving Centers (ARCs). Almost all of these countries refer to the standard EN 50518 for 'Monitoring & Alarm Receiving Centres'. The first version of this European standard was created in 2010, and currently, EN 50518 is in its third version.

In August 2019, the third version of the EN 50518 standard was published. This replaced EN 50518 parts 1, 2, and 3 from 2013. New ARCs have been assessed according to the new standard since February 6, 2019.

The EN 50518 standard requires certification under accreditation in the 2019 version. This means that if compliance with this standard is required, certification under accreditation is mandatory. The applicable accreditation for EN 50518 is EN-ISO/IEC 17065. This accreditation standard specifies in article 3.10 the 'scope of certification'. This clarifies for which products, processes, or services the certification applies. This is reflected in the certification agreement, the audit report, and the certificate.

Certification for EN 50518 is based on the standard with its requirements for the construction elements, systems, and processes of an ARC. Additionally, EN 50518 offers multiple scopes for processing different types of notifications. These notifications are divided into two categories:

- Category I: ARCs that handle messages from security applications
- Category II: ARCs that handle messages from non-security applications

EN 50518 specifies which types of notifications belong to which category. The complete overview of the scopes mentioned per category is described below. The second column links the scope to the applicable standard mentioned in EN 50518. Where no standard is mentioned, the Board of Experts has referred to a specification. The scopes performed by the ARC are listed on their certificate after certification.

| **Scopes category I** | **Applicable standard** |
|---|---|
| Alarm Receiving Centre (ARC) for Intrusion & Holdup Alarm systems (I&HAS) | TS 50131-7 |
| Alarm Receiving Centre (ARC) for Video Surveillance Systems (VSS) for security applications | EN-IEC 62676-4 |
| Alarm Receiving Centre (ARC) for Access Control Systems (ACS) for security applications | EN-IEC 60839-11-2 |
| Alarm Receiving Centre (ARC) for people monitoring, lone workers and object tracking systems for security applications | K21023, only if the connected platform is certified according to K21023 |
| **Scopes category II** | |
| Alarm Receiving Centre (ARC) for Fire Alarms Systems (FAS) | TS 54-14* |
| Alarm Receiving Centre (ARC) for Fixed Firefighting Systems (FFS) | EN 12094-1 |

| | |
|---|---|
| Alarm Receiving Centre (ARC) for Social Alarm Systems (SAS) | TS 50134-7 |
| Alarm Receiving Centre (ARC) for audio/video door entry systems | EN 50518 |
| Alarm Receiving Centre (ARC) for Video Surveillance Systems (VSS) for non-security applications (traffic flow) | EN-IEC 62676-4 |
| Alarm Receiving Centre (ARC) for people monitoring, lone workers and object tracking systems for non-security applications | K21023, only if the connected platform is certified according to K21023 |
| Alarm Receiving Centre (ARC) for lifts emergency systems | EN 81-28 |

*Table 3 Scopes and categories EN 50518*

## 2.1 Referenced standards per scope

ARCs were originally equipped mainly to handle messages from intrusion and hold-up alarm systems. Over the years, ARCs have become capable of processing all types of messages recognized by EN 50518:2019 with its categories and scopes. To organize the proper handling of all these different types of scopes, EN 50518 refers to other European standards for message handling. Examples include:

The standard TS 50131-7 “Alarm systems - Intrusion and hold-up systems - Part 7: Application guidelines” provides direction for the design, installation, and commissioning process of alarm systems.

The standard CEN/TS 54-14* covers Automatic Fire Detection and Alarm Systems - Part 14: Guidelines for planning, design, installation, commissioning, use, and maintenance. Note that the standard EN54-2 for Automatic Fire Detection and Alarm Systems - Part 2: Control and Indicating Equipment and component connection standards are mandatory to use according to the Construction Products Regulation (CPR) Regulation (EU) No. 305/2011.

The scope of EN 54-14 only applies when a fully certified installation is present on the premises. This scope can also apply to lower-level residential properties with smoke detectors based on EN 14604. These connections and handling are then assessed in EN 50518 article 9.1.5. Smoke detectors based on EN 14604 are required.

Not all paragraphs of the mentioned standards are applicable. Annex 2 contains the ‘Matrix EN 50518 and relevant standards with additional services’. This matrix includes the applicable paragraphs of the referenced standards. If applicable, the ARC could provide the market with a broader portfolio of security services. By implementing these standards, the ARC can meet the international needs in the security services market with high business continuity and good quality of service.

## 2.2 Monitoring of interconnections by the Monitoring Centre (MC)

Although the EN 50518 is officially named as ‘Monitoring and Alarm Receiving Centres’ (MARC), most MARC’s are only operated as an ARC. The difference could be seen in the definition as described in EN 50136-1/A1:

Alarm receiving centre:
continuously manned centre to which information concerning the status of one or more AS is reported.

Monitoring and alarm receiving centre
continuously manned centre to which information concerning the status of one or more AS is reported, and additionally where the status of one or more ATS is monitored.

To recognize the end-to-end monitoring part of the MARC, Kiwa can assess the MARC as a Monitoring Centre (MC) and specify this on their certificate. To receive the recognition, an assessment in conjunction with EN 50136-1/A1 shall be carried out according to certification scheme K21030. Within EN50136-1/A1 there are requirements for the Alarm Transmission Service Providers monitoring the performances of an Alarm Transmission System (ATS) end-to-end from the Supervised Premises Transceiver (SPT) connected to the alarm system and the Receiving Centre Transceiver (RCT) at secure location of the (M)ARC. For further information see chapter 8 of this document and/or K21030.

Note: In this document, no distinction is made in terminology between an ARC and a MARC. Where a MARC is specifically meant, a Monitoring Centre (MC) is also referred to.

## 2.3 The location of data processing equipment

With the introduction of EN 50518:2019 (M)ARC's are allowed to store their data processing equipment (as mentioned in clause 5.8 EN 50518) in a secure location other than their own (M)ARC. Two possible opportunities are:

- Another certified (M)ARC based on EN 50518 category I;
- A data centre designed and maintained according to EN 50600 (availability class 3 and protection class 4 (EN 50136-1/A1 clause 4.1.38).*

The performance of the link between these two (M)ARC's or the (M)ARC and the data centre has to be a Dual Path (DP) 4 according to 50136-1/A1 and should be certified according to K21030 scope 'critical communication'. In the event a remote location of data processing equipment is applicable, Kiwa will address this on the (M)ARC's certificate.

*Explanation on EN 50600: the EN 50136-1/A1 states: *"a data centre designed and maintained according to EN 50600 (availability class 3 and protection 4)"*. This does not implicate that the data centre itself needs to be certified according to EN 50600. However, when a certificate is available it can be accepted, only when this certificate is issued under accreditation by a IAF MLA accreditation body

Kiwa's interpretation is a verification of the external location for data processing equipment. This is done with an assessment based on the main principles of EN 50600 availability class 3 and protection class 4, but focuses on the defined area of the (M)ARC. In this way, Kiwa checks whether the data center is designed and maintained according to EN 50600.

Subjects of the assessment are:

- access control of the data center,
- the cooling system,
- redundancy,
- separation of power and data lines,
- (emergency) power supplies,
- fire extinguishing system,
- intrusion and camera system.

The above paragraph describes a situation where all data processing equipment is managed by the (M)ARC itself. Kiwa increasingly encounters situations where other forms of cloud computing are also applied. To determine whether this option falls within the meaning of the standard, insight into the specifications of the cloud computing platform and geographical location(s) is also required. The assessment is also based on the main principles of EN 50600, and Kiwa could also declare 'a remote location for data processing equipment' on the EN 50518 certificate of the (M)ARC.

Note: EN 50518 chapter 5.8 describes a situation where equipment such as receivers and voice recording equipment is located at a remote location. If the Alarm Management System is also located at an external location, the certification scheme K21046 Hosted Alarm Solution applies. This is to implement a certified and secure way to place the AMS at a remote location.

# 3. Business Continuity of a (M)ARC “R”

Next to many requirements in the standard EN 50518, the (M)ARC shall have to fulfil two main goals in order to service their customers in a good way. These are:

- The availability of an (M)ARC: 24 / 7 / 365;
- The handling on the alarms within the performance requirements of the standard.

The M(ARC) shall carry out a comprehensive risk analysis. The risk analysis shall be part of a risk management process and is an integral part of management and decision-making and integrated into the structure, operations and processes of the organization. The risk management process involves the systematic application of risk identification, risk analysis, risk evaluation and risk treatment. Although the risk management process is often presented as sequential, in practice it shall be iterative and ongoing. The typical threats as given as an example in ISO 27005 Annex C shall be taken in account on top of the potential risk as given in EN 50518 article 3.1.13 and 4.2.

Level of risks shall be compared against risk evaluation criteria and risk acceptance criteria related to business continuity and include:

- Loss of business and financial value
- Legal and regulatory requirements, and contractual obligations
- Operational and business importance of availability, confidentiality and integrity
- Stakeholders expectations and perceptions, and negative consequences for goodwill and reputation

The next paragraphs set some definitions to recognize different solutions of Business Continuity. Business Continuity of an (M)ARC can furthermore be assessed additionally according to ISO 22301; Societal security - Business continuity management systems – Requirements.

## 3.1 A standalone (M)ARC without BC possibilities

EN 50518 certification of the (M)ARC. The (M)ARC requires limited DRP/BCM policies and therefore needs to inform all their customers during down time. Nevertheless, the ARC still needs to comply with a 99,9% availability according to EN 50136-1/A1.

## 3.2 Satellite (M)ARC

An operational (M)ARC that is connected to another (often larger) operational (M)ARC from the same (M)ARC organization, which is located in another region and handles some of the alarms in case of capacity problems.

Conditions; The satellite ARC is treated as a two-site by the Certification Body (CB) and must be included in the EN 50518 assessment. The satellite (M)ARC is not included in the Business Continuity Plan (BCP) of the larger (M)ARC because the other (M)ARC is not able to handle all the alarms in case of an emergency. The connection between these two (M)ARC’s has to be a DP4 according to 50136-1/A1 and should be certified according to scheme K21030 scope ‘critical transmission’.

## 3.3 Twin (M)ARC

An operational (M)ARC connected to another operational (M)ARC located in another region that handles alarms. Twin ARC’s comply with the BCP for both the ARC’s.

Conditions; The systems run completely parallel between the primary ARC and the secondary ARC. The primary and secondary ARC are fully operational ARC’s. The starting point is that the ARC’s have their own EN 50518 certificate, possibly the (M)ARC’s are treated as a two-site by the Certification Body. The (M)ARC’s can complement or replace each other in the context of their BCP. This has been tested by both the (M)ARC’s. This should be assessed by the CB at both the (M)ARC’s. The connection between these two (M)ARC’s has to be a DP4 according to 50136-1/A1 and should be certified according to K21030 scope ‘critical transmission’ (Transmission between (M)ARC’s).

## 3.4 A standalone ARC with BC possibilities

An alarm receiving center with all IT infrastructure at its own location that has capabilities to continue service partially at another location should comply with: EN50518 certification of the ARC including management system.

DRP/BCM procedures are required for the ARC and it is required to inform the part of the customers to which service cannot be provided in case of downtime. Nevertheless, the ARC must still meet the availability requirements as stated in EN50136-1 with respect to the connected ATS of the highest class (SP1 to DP4). In addition, the alarm center may temporarily* continue its services from an operational backup location. The arrangements with the operator of the backup location are formalized. The operational backup site is suitable and at least certified as EN50518- ARC Type II or is secured by private security guards during the use of the site.

## 3.5 An ARC with external IT infrastructure

An alarm receiving center with external IT infrastructure at an external location, being data center (EN50600/EN50518) can continue its service in case of disruptive events by temporarily* using an operational backup location. The alarm reception center shall comply with:

EN 50518 certification of the ARC including management system and remote location for the purpose of IT infrastructure. In addition, the IT infrastructure between the two sites complies with DP4 in accordance with EN50136-1./K21030 scope 2. The ARC has DRP/BCM procedures in place and can continue its services temporarily* from the operational backup location. The arrangements with the operator of the backup site are formalized. The operational backup site is suitable and certified as EN50518- ARC Type II or is secured by private security guards during the use of the site.

## 3.6 Back-up (M)ARC

A secondary (M)ARC which, in accordance with the Business Continuity Plan (BCP) of the primary (M)ARC, can take over the processes of a primary (M)ARC, which may not be able to meet the performance requirements due to an incident or another cause.
Conditions; The systems run completely parallel between the primary (M)ARC and the secondary back-up ARC. The backup (M)ARC is not a fully operational (M)ARC, and is only operational in the back-up situation. The back-up (M)ARC must be assessed (building- and system requirements) and evaluated by the CB within the assessment of the primary (M)ARC based on EN 50518. Possibly the (M)ARC's are treated as a two-site by the Certification Body. The BCP must be tested by the (M)ARC and verified by the CB.
There is also the possibility that a separate organization will organize this back-up (M)ARC. This situation must then be assessed by the CB within a separate certificate EN 50518, where the BCP must be tested by the (M)ARC and verified by the CB.
In either of these situations, the connection between these two (M)ARC's has to be a DP4 according to 50136-1/A1 and should be certified according to K21030 scope 'critical communication' (Communication between (M)ARC's).

Relocating to a different location to continue service can only be of a temporary nature. Plans to achieve this must always be justified in the risk analysis and elaborated in a DRP and/or BCP. To make the temporariness transparent and measurable, the following criteria have been established.

| Tijdvak | Actie |
|---|---|
| < 48 hours | Based on the DRP/BCP, a fallback is initiated. The decision for defection is recorded as an incident. All incidents are also evaluated and included in the management review.<br>In the case of working from home, reasons must be given for each shift, why there is working from home. This must also be recorded and evaluated. |
| 48 hours | After 48 hours, a decision should be made regarding the continuation of services. The decision should be recorded. All decisions are also evaluated and included in the management review. |
| < 1 week | After 1 week hours, a decision should be made regarding the continuation of services. If services are to be provided for an extended period of time outside the secure shell (Type I), a plan of action should be prepared to return within a secure shell (Type I) within 2 months.<br>The plan of action including decision(s) should be recorded. All decisions are also evaluated and included in the management review. |
| < 2 months | After 2 months, services should be continued within a secure shell (Type I). The manner in which work has resumed within the secure shell should be documented in an evaluation report. The evaluation report is evaluated and included in the management review. |

# 4. Statistics of a MARC “G and R”

A MARC has the following primary functions:

- Addressing and handling incoming messages as an Alarm Receiving Center (ARC) according to EN 50518.
- Addressing and handling failing transmissions:
  - from the Supervised Premises Transceiver (SPT) at the site of the Alarm System (AS) or
  - for an Alarm Transmission Service Provider (ATSP) according to EN 50136-1/A1 & certification scheme K21030 as a Monitoring Centre.

## 4.1 Example message handling - G

A MARC shall control its primary key performance indicators (KPI’s). In this case, the speed of handling incoming messages according to the standard. To do so, the MARC needs a function in its Alarm Management System (AMS)[1] that analyzes the meta data in this system, giving the MARC operators live insight whether they are working within their mandatory KPI’s. The management of the MARC needs these statistics to arrange corrective actions if the KPI’s are not met (for example: to train the operators additionally in doing their task more effective or to increase the number of operators handling the alarms). These statistics are also important to address preventive actions for the ARC-management (for example to recognize peak-periods during the year in which more alarms are received and extra operators are needed)

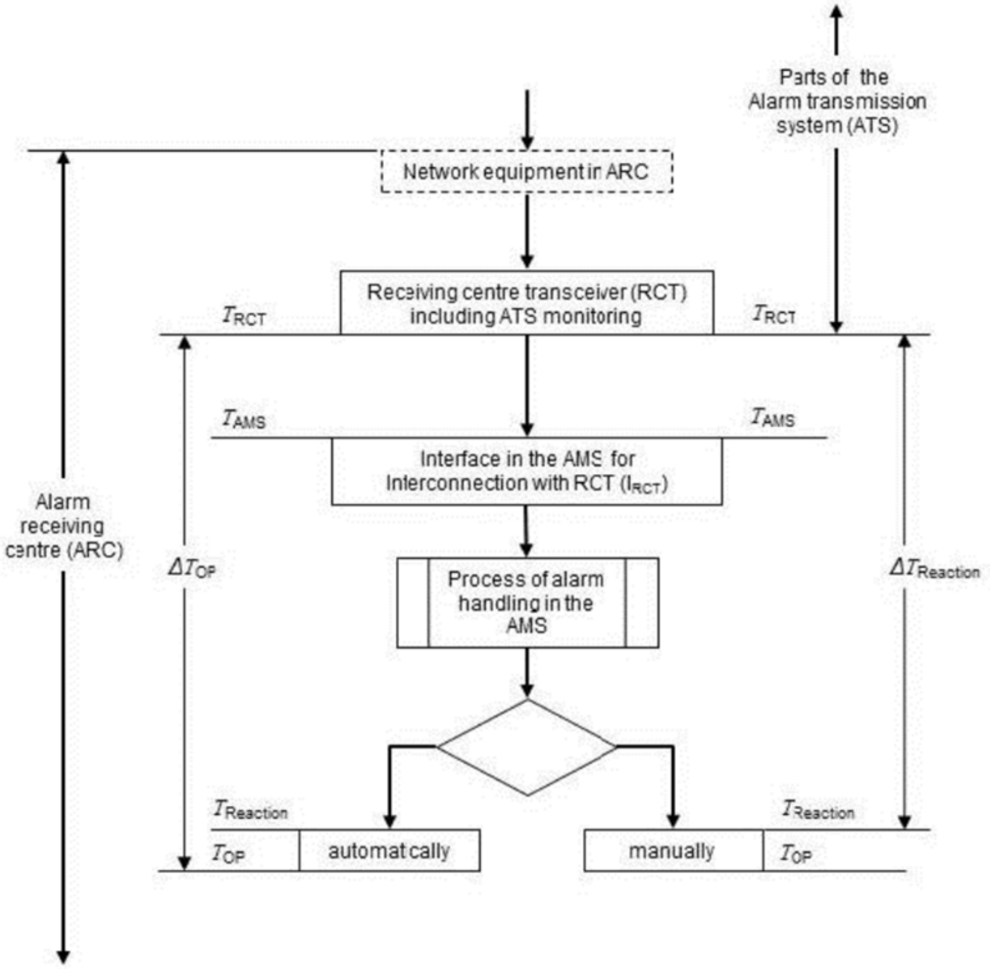

Parts of the Alarm transmission system (ATS)
Network equipment in ARC
Receiving centre transceiver (RCT) including ATS monitoring
$T_{RCT}$
$T_{RCT}$
$T_{AMS}$
$T_{AMS}$
Interface in the AMS for Interconnection with RCT ($I_{RCT}$)
Alarm receiving centre (ARC)
$\Delta T_{OP}$
Process of alarm handling in the AMS
$\Delta T_{Reaction}$
$T_{Reaction}$
$T_{Reaction}$
$T_{OP}$
automatically
manually
$T_{OP}$

*Figure 3*

[1] Annex C of the EN 50518:2019 gives an overview of requirements for an Alarm Management System

To have the correct statistics, the information from the RCT, which transmits alarms to the AMS, is needed.
ΔTOP; the time that elapses between the moment the alarm message is available at the output of the RCT and the moment of the first action initiated by the ARC operator or the AMS (ΔTOP = TOP - TRCT).
For an ARC, it is important to know:

- How many alarms enter the ARC in the queue.
- How quickly these alarms are acknowledged by the AMS. The acknowledgment can be done by an operator who receives the alarm on their monitor or by an automatic action. The processing time for the operator to complete the alarm is not relevant for this statistic/KPI

## 4.2 Best practice for complying with the performance criteria of message handling - G

To ensure they meet the KPI for priority 1 alarms for for hold-up, fire, fixed firefighting systems, people monitoring and other alarms, it has been agreed that they are of the highest priority level: 30 seconds for 80% of received signals and 60 seconds for 98.5% of received signals.
Most MARCs use a threshold of 15 to 25 seconds to meet the performance criteria. This allows them to operate within the KPI. The 15-second threshold provides the most certainty.
An example: A MARC handles 100 priority 1 alarms daily. The standard requires compliance with the above criteria over a rolling twelve-month period. This leads to the following criteria within 30 days;

| **Number of Priority 1 Alarms per Day** | **80% within 30 seconds** | **98.5% within 60 seconds** | **1.5% above 60 seconds** |
|---|---|---|---|
| 100 | 80 alarms | 18 alarms | 2 alarms |
| **Number of Priority 1 Alarms per Week** | **80% within 30 seconds** | **98.5% within 60 seconds** | **1.5% above 60 seconds** |
| 700 | 560 alarms | 129 alarms | 11 alarms |
| **Number of Priority 1 Alarms per 30 Days** | **80% within 30 seconds** | **98.5% within 60 seconds** | **1.5% above 60 seconds** |
| 3000 alarms | 2400 alarms | 555 alarms | 45 alarms |

*Table 4 Number of Priority 1 Alarms*

If the ARC has a bad day in performance because many alarms are sent to the MARC due to errors in the AS, and for example, 19 priority 1 alarms are above 60 seconds, the ARC does not meet its KPI.
In the example of a week, this can lead to the following scenario. If 601 priority 1 alarms within a week are handled above 30 seconds, the ARC does not meet its KPI.
The 1.5% that may exceed 60 seconds is the basis for further investigation by the ARC to improve the KPIs of their services.

To meet the requirements in EN 50518 H9.2, response times will have to be approached proactively at all times. Some examples of this are:
- Analyse response times daily, so NOT only analyse on a monthly or annual basis;
- Align occupancy with nominal/historical/weather influences expected load;
- Present response times (live or with a delay of e.g. 24h) in the ARC this enables anticipation in a next shift if response times are not in accordance with KPI;
- Automate lower priority calls/events .

The information below provides guidelines/handbooklets to arrive at a correct assessment of the response times:

1. Structural: The starting point is sufficient insight/analysis into one's own response times by means of:
   a. Exporting raw data of all calls/events from the database over a set period of time and analysing these;
   b. Exporting raw data of all calls/events without editing (including overruns) should always be possible on request (data in accordance with EN 50518 retention period).

2. Structural: Insight/root cause in follow-up reports of (technical) events by means of:
   a. Providing insight into the root cause based on the raw data;
   b. Being able to explain the root cause based on an accepted analysis method.

3. Structural: Correct prioritisation against the standard (interpretation document) by:
   a. Providing an overview of the classification of priorities;
   b. Making the prioritisation transparent in the raw data per type of notification/event.

4. Structural: Correct technical set-up in the control room platform on the basis of EN 50518 H9.2, EN 50518 annex C, prioritisation and measurement of follow-up reports via:
   a. Insight into supplier documentation including self-configurable variables on the basis of EN 50518.

5. Structural: Providing insight into load in relation to the number of operators via:
   a. The nominal/historical expected load must be made transparent on the basis of statistical reports;
   b. The utilisation of the number of operators must be geared to the nominal/historical expected load on the basis of rosters and statistical reports;

6. If all the above are transparent, transparent overruns can be made with at all times temporary/incidental character and not predictable through nominal/historical load.
   a. Examples of temporary character/incidental situations under explicit mention in the analysis. Consider:
   - The nuisance during non-predictable New Year's Eve incidents;
   - The nuisance during extreme non-predictable weather conditions;
   - Flu epidemic among staff;
   - Unforeseen external technical failures;

   b. Situations that are not considered temporary/incidental include:
   - Smoke breaks;
   - Fetching food;
   - Scheduled maintenance;

The analysis should be insightful both excluding and including overruns.

## 4.3 Listing of priorities for response times - R

Below is a table to clarify EN 50518, chapter 9.2. Priority 1, 2, and individual services are listed. The possibility of automatic alarm handling and delay are also included in the table per alarm condition/notification.

| Priority | EN 50518 art. 9.2 | Automatic alarm handling possible | Delay possible | Specific alarm condition/message |
|---|---|---|---|---|
| 1 | for hold-up, fire, fixed firefighting systems, people monitoring and other alarms designated as highest priority:<br>30 seconds for 80% of received alarms and 60 seconds for 98.5% of received alarms; | No<br>No<br>No<br>No<br>No<br>Yes | No<br>No<br>No<br>No<br>No<br>Yes/No | Robbery<br>Fire detection systems<br>Fire suppression systems<br>Personal monitoring<br>Social - life-threatening<br>Others according to customer contract |
| 2 | All other alarm conditions:<br>90 seconds for 80% of received alarms and 180 seconds for 98.5% of received alarms. | Yes<br>Yes<br>Yes<br>No<br>No<br>Yes | Yes<br>Yes<br>Yes<br>Yes<br>Yes<br>Yes | Burglary<br>Video detection<br>Social - non-life-threatening<br>Sabotage<br>Total outage<br>Others according to customer contract |
| # | Individual services based on a customer contract EN 50518 9.1.5 | Yes<br>Yes<br>Yes<br>Yes<br>Yes | Yes<br>Yes<br>Yes<br>Yes<br>Yes | Video<br>Access<br>Traffic<br>Lift<br>Failures also ATP<br>Signals also technical |

*Table 5 Priorities for Response Times*

Note: All alarms and notifications should be measured in the AMS. There should be no negative influence from scopes that are not under certification on the certified scope. No exclusions are possible. It must also be possible to measure automatic alarms separately.

## 4.4 Monitoring of interconnections (Monitoring Centre) - G

ATS performance monitoring is typically carried out by the ATSP (Alarm Transmission Service Provider). The ATSP can perform the monitoring itself or delegate it to a Monitoring Centre according to EN 50518. If the ATSP performs the monitoring itself, it must also comply with EN 50518. For more information about ATSPs, see also chapter 8.

A Monitoring Centre (MC) can be an independent center or part of an ARC. The origin of performance monitoring is the mandatory requirement in EN 50136-1. The tasks of a Monitoring Centre include reporting and logging failures and availability. These tasks must be undertaken to maintain the required performance level for each ATS of the respective category.

The purpose of performance monitoring is to quickly identify the ATS that does not meet the agreed performance standards for the appropriate category.

It is for this reason that an MC / ATSP must continuously monitor the key performance parameters, e.g., transmission time, availability, and error detection. When an error is identified, the MC / ATSP must take action to correct the error and restore the ATS to its fully operational state. This ensures that the ATS and/or ATSN meet the required average transmission time and availability.

Figure 4 shows the 'ATS monitoring' in the middle of the ATS between the alarm system and the ARC. In theory, the monitoring could also be carried out in the ARC if the ARC is also an ATSP and/or MC.

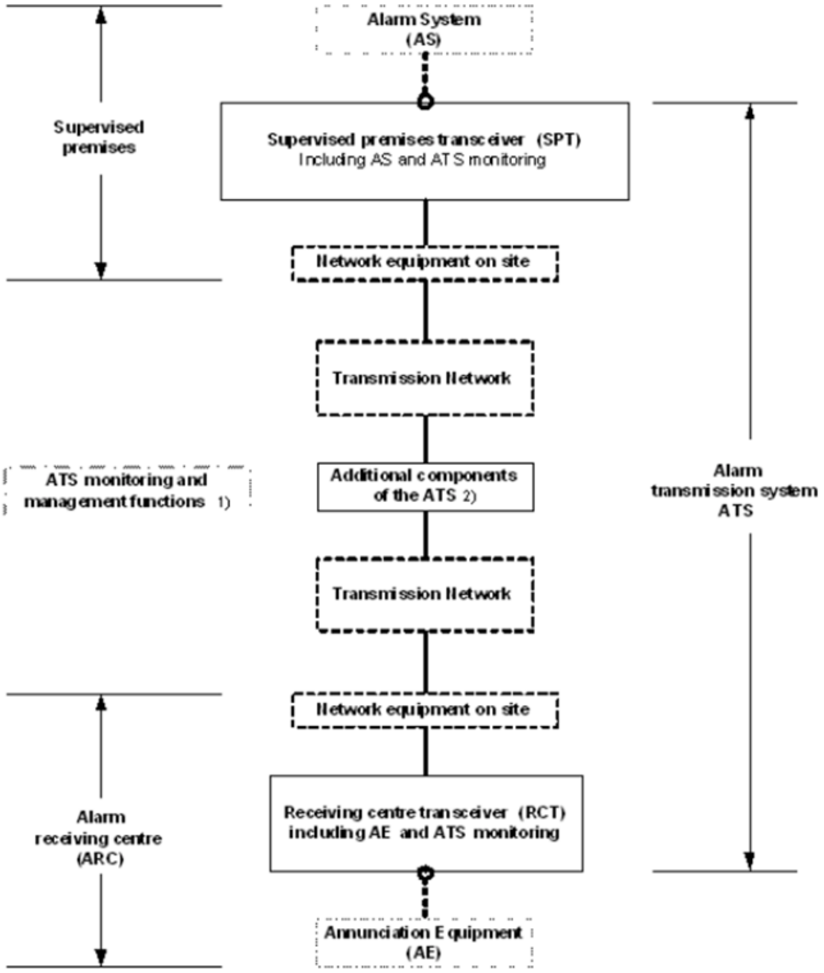

Alarm System (AS)
Supervised premises
Supervised premises transceiver (SPT)
Including AS and ATS monitoring
Network equipment on site
Transmission Network
ATS monitoring and management functions 1)
Additional components of the ATS 2)
Alarm transmission system ATS
Transmission Network
Network equipment on site
Alarm receiving centre (ARC)
Receiving centre transceiver (RCT)
including AE and ATS monitoring
Annunciation Equipment (AE)

*Figure 4*

## 4.5 Lean ATSP – G

N 50136-1 / A1 specifies requirements for alarm transmission systems and monitoring of these systems in conjunction with EN 50518. The competent authority for this is: law enforcement and insurance parties. They require monitored alarm transmission based on performance control.

EN 50136-1, -2, and -3 together with EN 50518 set requirements for this monitoring process. In this process, the Alarm Receiving Centre can perform the function of Monitoring Centre (MC). We see that ARCs struggle with this process to fulfill the role of MC. The goal of Lean ATSP is to help these struggling ARCs.

The receiver according to EN 50136-3 acquires the data needed to fulfill the role for dual-path transmissions. The ARC must have standard action patterns to behave in case of failing connections.

Definitions:
Polling
A commonly used method for monitoring alarm transmission paths (ATP) and/or ATS availability, where the term polling means that status messages are regularly exchanged between an SPT and an RCT. (EN 50136-7)

Reporting time
The period from the moment a fault occurs in the ATS until the fault information is reported to the RCT, the alarm system at the monitored site, or the receiver of the monitoring center (if present) (EN 50136-1 / A1)

Polling and reporting time are therefore not the same! See standard EN 50136-7 for more information.

| | DP4 |
|---|---|
| **Primary ATP Reporting Time** | 90 seconds |
| **Secondary ATP Maximum period when the primary is operational** | 5 hours |
| **Alternative ATP Maximum period when the primary fails** | 90 seconds |
| **Failure of all ATPs simultaneously *** | 3 minutes |
| *If an ATS contains two or more ATPs, the reporting time must meet the requirements of this table. | |

*Table 6 Maximum reporting time DP4*

If an ATS remains operational, a single line path fault is presented to the ATSP but can be delayed at the AMS if agreed upon by stakeholders. The maximum delay should not exceed 96 hours.

Based on the above information, a suggestion for a standard action is provided below. The aim of this setup is to automate as much of the process as possible.

| **DP4** | **90 seconds**<br>**EN 50136-1/A1** | **30 minutens after RT**<br>**EN 50518** | **25 hours after RT**<br>**EN 50518** | **1 week after RT**<br>**EN 50518** |
|---|---|---|---|---|
| **Failing primary connection** | **Reporting time (RT)** | **Automatic email / SMS** | **Automatic email / SMS** | **Phone call** |
| | | | | |
| **DP4** | **5 hours**<br>**EN 50136-1/A1** | **30 minutes after RT**<br>**EN 50518** | **5 hours after RT**<br>**EN 50518** | **1 week after RT**<br>**EN 50518** |
| **Failing secondary connection**<br>If the primary fails, the alternative reporting time is 90 seconds. | **Reporting time (RT)** | **Automatic email / SMS** | **Automatic email / SMS** | **Phone call** |
| | | | | |
| **DP4** | **3 minutes**<br>**EN 50136-1/A1** | **90 seconds after RT**<br>**EN 50518** | | |
| **ATS error** | **Reporting time (RT)** | **Automatic email / SMS** | | |
| Ensure that when implementing this table for your Monitoring Centre, it is agreed upon by interested parties. | | | | |
| An automatic email/SMS is an example of a redundant form of communication to the user/customer. Other effective forms are also possible. | | | | |
| All times in this table are the maximum times.<br>Other categories fall outside the scope of this proposal. | | | | |

*Talel 7 Lean ATSP DP4*

The above table in text writing:
**DP4**
**The primary path has a failing connection;**

- Reporting time is 90 seconds. After 30 minutes, an automatic email/SMS* is sent to the client regarding this failed connection.
- If not resolved after 25 hours, an automatic email/SMS* is sent to the client regarding this failing connection.
- If not fixed after 1 week, a phone call is made to the client about this failing connection and that the client does not meet the requirements for reliable alarm transmission because the backup situation is not functioning.

**Alternative path has a failing connection:**

- Reporting time is 5 hours. After 30 minutes, an automatic email/SMS* is sent to the client regarding this failed connection.
- If not fixed after 5 hours, an automatic email/SMS* is sent to the client regarding this failed connection.
- If not fixed after 1 week, a phone call is made to the client about this failing connection and that the client does not meet the requirements for reliable alarm transmission because the backup situation is not functioning.

**Both the primary and alternative paths have a failing connection:**

- Reporting time is 90 seconds. After 90 seconds, an automatic email/SMS* is sent to the client regarding this failing connection and a phone call is made to the client regarding this failing connection, informing them that they do not meet the requirements and that there is a possibility of a hostile attack on the connections and monitored buildings.

* An automatic email/SMS is an example of a redundant form of communication to the user/customer. Other effective forms are also possible.

# 5. Construction/system requirements “R”

## 5.1 General

EN 50518 sets requirements for the construction and systems of (M)ARC's. This chapter contains interpretation, additional information, and explanation of the requirements.

## 5.2 Resistance against physical attack – R

- When an (M) ARC does not have test reports, production specifications, and/or construction drawings, destructive research must be carried out to gain compliance with the standard.
- This also applies to calcium silicate bricks where its mass is most important for compliance.
- If the thickness of the wall, floor, or ceiling is in accordance with the table in EN 50518 (except steel), this is sufficient for compliance with physical resistance, bullet resistance, and fire resistance.

## 5.3 Glazed areas – R

- If the glazed area is bullet-resistant, it can be assumed that it is also sufficiently fire resistant. In the case of adjacent buildings, fire resistance has higher priority.
- The risk of buildings positioned close to the ARC shall be evaluated in the risk assessment. This is also the case with buildings with the risk of fire spread from floor to floor.
- Compliance for resistance against bullet attacks also applies to physical attacks. Not the other way around.
- Visibility of the ARC: this item should be addressed in the risk assessment. What could other people see from the outside?

## 5.4 Resistance against fire and smoke (construction) - R

- This is interpreted from outside the secure shell to the inside of the secure shell and not vice versa.
- Resistance against fire and smoke depends on national regulations.
- The secure shell of the ARC must have fire resistance according to EN 13501-2 "Fire classification of construction products and building elements – Part 2: Classification using data from fire resistance tests, excluding ventilation systems" with a minimum of 30 minutes. The standard mentions the following fire scenarios:
  - The standard temperature/time curve (after flash-over fire);
  - The slow heating curve (smoldering fire);
  - The 'semi-natural' fire;
  - The external fire exposure curve;
  - Constant temperature attack.
- The minimum applicable requirement is E – Integrity for wall, ceiling, floor, and doors.
- National building regulations or the design of the building may obtain more performance characteristics, such as:
  - R – Load-bearing capacity,
  - I – Insulation,
  - W – Radiation, etc.

  Don't forget to check these with the architect and/or local building authorities.
- Reinforced concrete of at least 10 cm is deemed to meet this E30 property according to the minimum thickness for walls mentioned in chapter 5 of the standard.

### 5.4.1 Resistance against fire and smoke (service inlets and outlets)

- Penetration seals have to fulfill the standard EN1366-3 “Fire resistance tests for service installations; Part 3: Penetration seals“ and certified according to the ETAG 26 series ”Guideline for European Technical Approvals for Fire Stopping and Fire Sealing Products”. The ETAG guidelines are replaced by EAD’s;
  - EAD 350141-00-1106; Linear Joint and Gap Seals;

  - EAD 350454-00-1104; Penetration Seals

- Fire protective Products have to be certified according to the ETAG 18 series. The ETAG guidelines are replaced by EAD's;
  - EAD 350402-00-1106; Reactive coatings for fire protection of steel elements.
  - EAD 350142-00-1106; Fire Protective Board, Slab and Mat Products and Kits.
  - EAD 350140-00-1106; Renderings and kits based on Renderings intended to fire resisting applications.
- Fire dampers in Heating, Ventilation and Air Condition systems have to fulfill the standard
  - EN1366-2 "Fire resistance tests for service installations - Part 2: Fire dampers" and
  - Classification according to EN13501-3 "Fire classification of construction products and building elements - Part 3: Classification using data from fire resistance tests on products and elements used in building service installations: fire resisting ducts and Fire dampers".
- The installation instructions of the manufacturer shall be obeyed to guarantee the same performance as during the initial type tests of these products. The products are to be installed in- or outside of the shell of the ARC, depending on the instruction of the manufacturer. The side of the shell is depending what needs protecting. Be aware that fire dampers are mostly tested mounted in the fire resistant wall.

## 5.5 Protection against the effect of lightning - R

All appropriate metallic installations/parts shall have equipotential bonding (electrical interconnection of metallic installations/parts), such that in the event of lightning currents flowing, no metallic part is at a different voltage potential with respect to one another. Bonding can also be accomplished by the use of surge protective devices (SPDs) where the direct connection with bonding conductors is not suitable. Some areas of a structure, such as a shielded room, are naturally better protected from lightning than others and it is possible to extend the more protected zones by careful design of the LPS, earth bonding of metallic services such as water and gas, and cabling techniques. However it is the correct installation of coordinated Surge Protective Devices (SPDs) that protect equipment from damage as well as ensuring continuity of its operation - critical for eliminating downtime. Therefore, proper SPD protection shall be installed accordingly when the (M)ARC is not shielded properly.

A risk analysis in accordance with EN 62305-2 or national regulations shall be carried out and appropriate action shall be taken to protect the ARC against the effects of lightning when R1 = > 1 (Loss of human life 1 in 100,000 (1 x 10-5).

## 5.6 Entrance lobby - R

- All entrance lobby doors should open outwards seen from within the (M)ARC.
- An entrance lobby could also have three doors which must also be interlocked, comply with all the construction requirements and are only operable from within the ARC.
- Key cards are not permitted for normal entry. The entrance lobby doors must be only operable from within the ARC. Key cards are accepted as emergency re-entry. Or as multi factor authentication tool.

## 5.7 Ventilation inlet & outlet openings - R

- Openings in the structure of an ARC for ventilation systems shall meet the requirements for resistance to physical attacks.
- Ventilating inlet or outlet need suitable alarm detection equipment to detect any attempt to enter the ventilation inlet.
- The ventilation inlet and outlet openings in the shell of the ARC shall be physically protected.
- Ventilation inlet and outlet openings shall be protected with air-tight flaps which can be locked in the closed position from inside the ARC.
- EN 50518 does not specify a maximum time for the closing of the air-tight flaps. This time should be seen from BCM and risk analysis perspective and must be realistic. Kiwa will assess the time and do a trend analysis.
- The fire flap must be on the fire separation. The gas flap does not have to be exactly on the fire separation.

## 5.8 Alarm systems of the ARC – R

To comply with the clauses mentioned in alarm systems of the ARC, the ARC must use certified components for their alarm system, fire alarm system, gas, hold-up buttons and Video surveillance system. The basic and detailed design must also be based on European standards: EN 50131, EN 54 and IEC 62676-4.

## 5.9 Alarm transmission – R

The alarm transmission system for the alarm system of the (M)ARC for EN 50518:2019 shall as a minimum be in accordance with EN 50136-1 category SP4 or DP3.

The ARC's own alarm system(s) including the ATS shall be monitored and tested for correct functioning. For the correct operation the following is tested and the results recorded:

- Test hold-up buttons (quarterly)
- Open emergency door and both entrance lobby doors at the same time (quarterly)
- Disconnect primary ATP (monthly)

## 5.10 Fire detection system – R

The areas of the building occupied by the company which operates the (M)ARC shall be protected by a fire detection system and include acoustic and optical warning devices in accordance with national requirements and life safety incorporating components certified according to the EN 54 series. The fire detection system shall be such that as a minimum all vital areas for business continuity, where activities are placed, technical rooms, data rooms, ups rooms, generator rooms, patch rooms are protected. The evacuation alarm systems shall comply with legislative requirements deemed necessary by a National Government and shall by such that the sounder provides a sound that is 6 dba above the ambient noise and, in case used, optical warning devices in the (M)ARC are visible for the operators within.

Special attention is needed for escape route fire detection.

# 6. Operation of the ARC “G and R’

## 6.1 General

EN 50518 sets requirements regarding the operation of (M)ARC’s. This chapter contains extra interpretation, extra information and explanation about requirements.

## 6.2 Daily tests - G

A (M)ARC should at least monitor its incoming communication lines and all critical components in the (M)ARC like the AMS, Receivers and databases to establish the availability of the MARC. This monitoring should be as automized as possible. When components are duplicated, when only 1 component fails and the MARC keeps running on the other component, the availability is still 100%. Kiwa will verify this availability with reports according to EN 50136-1 for a weekly, monthly and yearly availability.

## 6.3 Communications – R

All receivers, not being certified according to EN 50136-3 should be functionally tested by the (M)ARC itself. To execute functionally testing the (M)ARC needs the supplier. Access level-4 can’t be tested without the supplier.

Mainly the primary communication cable should be physically protected and protected against fire. The second communication cable is the redundancy.

## 6.4 Power supplies – R

To establish conformity with the standard, Kiwa is obliged to witness the testing of the power supply at least once per year including the back-up power.

## 6.5 Acces policy – G

The standard specifies the following requirements:

- Visitors of the (M)ARC should always be accompanied by an employee of the ARC
- Maintenance of critical equipment must always be supervised by an employee of the ARC

## 6.6 Alarm verification – G

For alarm verification Kiwa looks to other standard for connected systems like EN 50131, EN 50134, EN 54 etc. The system must be installed and tested in a correct way in order to be able to do a good alarm verification. The ARC should be aware of that.

The standard TS 50131-9 gives methods and principles for alarm verification of intrusion and hold-up alarm systems. Contacting the risk address for alarm verification can be based on the risk assessment of the supervised premises. This verification method can be too slow to apprehend the intruder.

There are several verification options:

- Sequential verification of intruder alarms;
- Sequential verification of hold-up alarms;
- Audible alarm verification;
- Visual alarm verification;
- ATS faults.

# 7. Managementsystem of the ARC “G and R”

## 7.1 General

The EN 50518 describes management tools that shall be in place in the ARC. This chapter gives interpretation, extra information and explanation about the connection with ISO 27001, ISO 9001 & ISO 31000. Additionally, a list has been made of the EN 50518 paragraphs in relation to ICT security and business continuity.

## 7.2 ICT-security – G

Applicable paragraphs EN 50518:2019

| Paragraph | Subject | Short reference |
|---|---|---|
| 4.2 | Site selection | Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure, should be designed and implemented |
| 5.8 | Location of data processing equipment | Areas containing information and other related assets should be protected by defining and using security zones |
| 5.9 | Communication cables | Power cables and cables used to transmit data or support information services should be protected from interception, interference or damage |
| 6.1.1 | Alarm systems of the ARC | Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure, should be designed and implemented |
| 6.1.2 | External attack | The building and grounds should be continuously monitored for unauthorised physical access |
| 6.1.10 | Video surveillance system | The building and grounds should be continuously monitored for unauthorised physical access |
| 7 | Electrical power supplies | Information processing facilities should be protected from power cuts and other disturbances caused by grid failures |
| 8.2 | Time synchronization of equipment | Time synchronisation is required. As are error logs and reporting |
| 9.1.1 | Procedures – General | Documented SOPs and KPIs required |
| 9.1.3 | Message Handling | Statistics are created and analysed. For both manual and automatic messages |
| 9.1.7 | Unexpected increase in alarms | How does MARC deal with this? |
| 9.1.8 | Alarm transmission path failures | Alarm transmission path errors from the MARC should be signalled in the MARC |
| 9.1.9 | Controls to maintain quality of service | How can MARC maintain quality of service at all times? |
| 9.1.10 | Installation, maintenance, protection, removal and reuse of assets under the control of the ARC | Asset management must be carried out |
| 9.1.11 | Monitoring and testing of equipment | All equipment must be monitored and tested regularly |
| 9.1.12 | Fault procedures and reporting | Reporting is required when equipment or software fails |
| 9.1.13 | Information management | Procedure for safe handling of required information |
| 9.1.14 | Data back-up | Backup procedure needed. When are the backups made and when are they tested? |
| 9.1.15 | Confidentiality and classification of information | Authorisation matrix is required. Labelling of information and a clear desk policy is required |

| | | |
|---|---|---|
| 9.1.16 | Relationships with essentials suppliers | Suppliers need to be vetted and agreements made on data |
| 9.1.18 | Physical Access | Access to the ARC and critical components should be restricted. An authorisation matrix should be displayed |
| 9.1.19 | Remote access | If remote access is used, it must be secure |
| 9.1.20 | Operational continuity and emergencies | Risk and continuity management. We expect an assessment based on ISO 31000 (ISO 27005). At least 2 connections, separate cable run separately, redundant receivers, CIA, within the ARC the paths of data and power are separated. AMS is a separate system with redundant cabling and separate cable runs. (EN 50136), Physical security also outside alarm centre (data centre, generator), logical access. Dirty connections? Secure remote access from suppliers. Cooling your server room. Are PEN tests performed? |
| 10.2 | Governance and Strategy | Compliance with the organisation's information security policies, subject-specific policies, rules and standards should be reviewed regularly |
| 10.3 | Legal and operational set-up | Legal, statutory, regulatory and contractual requirements relevant to information security and the organisation's approach to meeting them should be identified, documented and updated |
| 10.4 | Risk and contingency management | Management of IT systems and IT security must be organised. (See under requirements related to IT security). In addition, the requirements as stated in relation to GDPR must be met |
| 10.4 | Information management | See normative Annex A of ISO 27001 |
| 10.5.2 | Security screening and vetting | The background check of all job candidates should be conducted before they join the organisation and repeated periodically thereafter |
| 10.5.3 | Training | The organisation's staff and relevant stakeholders should be made sufficiently aware of, educated on and trained in information security and regularly updated on the organisation's information security policy, subject-specific policies and procedures, as relevant to their functions |

*Table 8 Paragraphs EN50518 related to IT*

## 7.3 Mapping ISO 27001:2013/2017 annex A controls with EN 50518 – R

The table below is a mapping of the controls of ISO 27001:2013/2017 Annex A with the requirements listed in EN 50518. Where applicable, the chapters from EN 50518 have been added. Where the link to EN 50518 is missing, this will have to be additionally demonstrated during the audit.

| | **Normative Annex A of ISO/IEC 27001:2013/2017 mapping with EN 50518** | **EN 50518** |
|---|---|---|
| 5 | Information security policies | |
| 5.1 | Management direction for information security<br>*Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.* | 10.4 & 9.1 |
| 6 | Organization of information security | |
| 6.1 | Internal organization<br>*Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organization.* | 10.4 & 9.1 |
| 6.2 | Mobile devices and teleworking<br>*Objective: To ensure the security of teleworking and use of mobile devices.* | Non applicable |
| 7 | Human resource security | |
| 7.1 | Prior to employment | 10.4 & 9.1 & 10.5 |

| | | |
|---|---|---|
| | *Objective: To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.* | |
| 7.2 | During employment<br>*Objective: To ensure that employees and contractors are aware of and fulfil their information security responsibilities.* | 10.4 & 9.1 |
| 7.3 | Termination and change of employment<br>*Objective: To protect the organization's interests as part of the process of changing or terminating employment.* | 10.4 & 9.1 |
| 8 | Asset management | |
| 8.1 | Responsibility for assets<br>*Objective: To identify organizational assets and define appropriate protection responsibilities.* | 10.4 & 9.1 |
| 8.2 | Information classification<br>*Objective: To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.* | 10.4 & 9.1 |
| 8.3 | Media handling<br>*Objective: To prevent unauthorised disclosure, modification, removal or destruction of information stored on media.* | 10.4 & 9.1 |
| 9 | Access control | |
| 9.1 | Business requirements of access control<br>*Objective: To limit access to information and information processing facilities.* | 10.4 & 9.1 |
| 9.2 | User access management<br>*Objective: To ensure authorised user access and to prevent unauthorised access to systems and services.* | 10.4 & 9.1 |
| 9.3 | User responsibilities<br>*Objective: To make users accountable for safeguarding their authentication information.* | 10.4 & 9.1 |
| 9.4 | System and application access control<br>*Objective: To prevent unauthorised access to systems and applications.* | 10.4 & 9.1 |
| 10 | Cryptography | |
| 10.1 | Cryptographic controls<br>*Objective: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.* | Additional |
| 11 | Physical and environmental security | |
| 11.1 | Secure areas<br>*Objective: To prevent unauthorised physical access, damage and interference to the organization's information and information processing facilities.* | 5 & 6 |
| 11.2 | Equipment<br>*Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.* | 5 & 6 |
| 12 | Operations security | |
| 12.1 | Operational procedures and responsibilities<br>*Doelstelling: Correcte en veilige bediening van informatieverwerkende faciliteiten waarborgen* | 10.4 & 9.1 |
| 12.2 | Protection from malware<br>*Objective: To ensure correct and secure operations of information processing facilities.* | Additional |
| 12.3 | Backup<br>*Objective: To protect against loss of data.* | 10.4 & 9.1 |
| 12.4 | Logging and monitoring<br>*Objective: To record events and generate evidence.* | 10.4 & 9.1 |
| 12.5 | Control of operational software<br>*Objective: To ensure the integrity of operational systems.* | Additional |
| 12.6 | Technical vulnerability management<br>*Objective: To prevent exploitation of technical vulnerabilities.* | Additional |
| 12.7 | Information systems audit considerations<br>*Objective: To minimise the impact of audit activities on operational systems.* | Non applicable |
| 13 | Communications security | |
| 13.1 | Network security management<br>*Objective: To ensure the protection of information in networks and its supporting information processing facilities.* | 10.4 & 9.1 & 5 & 6 |

| | | |
|---|---|---|
| 13.2 | Information transfer<br>*Objective: To maintain the security of information transferred within an organization and with any external entity.* | Additional |
| 14 | System acquisition, development and maintenance | |
| 14.1 | Security requirements of information systems<br>*Objective: To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.* | Non applicable |
| 14.2 | Security in development and support processes<br>*Objective: To ensure that information security is designed and implemented within the development lifecycle of information systems.* | Non applicable |
| 14.3 | Test data<br>*Objective: To ensure the protection of data used for testing.* | Non applicable |
| 15 | Supplier relationships | |
| 15.1 | Information security in supplier relationships<br>*Objective: To ensure protection of the organization's assets that is accessible by suppliers.* | 10.4 & 9.1 |
| 15.2 | Supplier service delivery management<br>*Objective: To maintain an agreed level of information security and service delivery in line with supplier agreements.* | 10.4 & 9.1 |
| 16 | Information security incident management | |
| 16.1 | Management of information security incidents and improvements<br>*Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.* | Additional |
| 17 | Information security aspects of business continuity management | |
| 17.1 | Information security continuity<br>*Objective: Information security continuity shall be embedded in the organization's business continuity management systems.* | 10.4 & 9.1 |
| 17.2 | Redundancies<br>*Objective: To ensure availability of information processing facilities.* | 10.4 & 9.1 |
| 18 | Compliance | |
| 18.1 | Compliance with legal and contractual requirements<br>*Objective: To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.* | 10.4 |
| 18.2 | Information security reviews<br>*Objective: To ensure that information security is implemented and operated in accordance with the organizational policies and procedures.* | 10.4 & 9.1 |

*Table 9 Mapping ISO 27001:2013/2017*

This matrix establishes the various standards related to service processes that the alarm centre provides to its customers. To archive the processes in a secure operation, the standards for managing business and ICT risks are placed to the left of the matrix. The correlation in the matrix lists overlapping and complementary requirements between the different standards and scopes. The process should meet the requirements of 'A.14.2 Security in development and support processes' of ISO 27001 or IEC 62443-4-1.

## 7.4 Mapping ISO 27001:2022 annex A controls with EN 50518 – R

The table below is a mapping of the controls of ISO 27001:2022 Annex A with the requirements listed in EN 50518. Where applicable, the chapters from EN 50518 have been added. Where the link to EN 50518 is missing, this will have to be demonstrated additionally during the audit.

| **Normative annex A of ISO/IEC 27001:2022 mapping with EN 50518** | | **EN 50518** |
|---|---|---|
| 5 Organizational control measures | | |
| A.5.1 | Policies for information security | 10.4 |
| A.5.2 | Information security roles and responsibilities | 10.4 |
| A.5.3 | Segregation of duties | 10.4 |
| A.5.4 | Management responsibilities | 10.4 |
| A.5.5 | Contact with authorities | 10.2 |
| A.5.6 | Contact with special interest groups | 10.2 |

| | | |
|---|---|---|
| A.5.7 | Threat intelligence | 10.4 |
| A.5.8 | Information security in project management | uncovered |
| A.5.9 | Inventory of information and other related assets | 9.1.10 |
| A.5.10 | Acceptable use of information and other associated assets | 10.4 & 9.1.15 |
| A.5.11 | Return of assets | 10.4 & 9.1.10 |
| A.5.12 | Classification of information | 10.4 & 9.1.15 |
| A.5.13 | Labelling of information | 10.4 & 9.1.15 |
| A.5.14 | Information transfer | 10.4 & 9.1.15 |
| A.5.15 | Access control | 10.4,  9.1.15, 9.1.18 & 9.1.19 |
| A.5.16 | Identity management | 9.1.15, 9.1.18 & 9.1.19 |
| A.5.17 | Authentication information | 10.4, 9.1.13 & 9.1.19 |
| A.5.18 | Access rights | 10.4, 9.1.13 & 9.1.19 |
| A.5.19 | Information security in supplier relations | 10.4 & 9.1.16 |
| A.5.20 | Addressing information security within supplier agreements | 10.4 |
| A.5.21 | Managing information security in the ICT supply chain | 10.4 |
| A.5.22 | Monitoring, review and change management of supplier services | 10.4 & 9.1.16 |
| A.5.23 | Information security for use of cloud services | 10.4 & 5.8 |
| A.5.24 | Information security incident management planning and preparation | 10.4 & 9.1.20 |
| A.5.25 | Assessment and decision on information security events | 10.4 |
| A.5.26 | Response to information security incidents | 10.4 |
| A.5.27 | Learning from information security incidents | 10.4 |
| A.5.28 | Collection of evidence | 10.4 |
| A.5.29 | Information security during disruption | 10.4 & 9.1.20 |
| A.5.30 | ICT readiness for business continuity | 10.4 & 9.1.20 |
| A.5.31 | Legal, statutory, regulatory and contractual requirements | 10.3 & 10.4 |
| A.5.32 | Intellectual property rights | uncovered |
| A.5.33 | Protection of records | 10.4 & 9.1.13 |
| A.5.34 | Privacy and protection of personal identifiable information (PII) | 10.4 |
| A.5.35 | Independent review of information security | 10.2 & 10.4 |
| A.5.36 | Compliance with policies, rules and standards for information security | 10.2 & 10.4 |
| A.5.37 | Documented operating procedures | 10.4 & 9.1.1 |
| 6 People-oriented management measures | | |
| A.6.1 | Screening | 10.5.2 |
| A.6.2 | Terms and conditions of employment | 10.4 |
| A.6.3 | Information security awareness, education and training | 10.5.3 |
| A.6.4 | Disciplinary process | uncovered |
| A.6.5 | Responsibilities after termination or change of employment | 10.4 |
| A.6.6 | Confidentiality or non-disclosure agreements | 10.4 & 9.1.15 |
| A.6.7 | Remote working | 9.1.19 |
| A.6.8 | Information security event reporting | 10.4 |
| 7 Physical management measures | | |
| A.7.1 | Physical security perimeters | 5.8 |
| A.7.2 | Physical entry | 5.8 & 9.1.18 |
| A.7.3 | Securing offices, rooms and facilities | chapter 5 & 6 |
| A.7.4 | Physical security monitoring | 6.1.2 & 6.1.10 |
| A.7.5 | Protecting against physical and environmental threats | 4.2 , chapter 5, 6 & 7 |
| A.7.6 | Working in secure areas | 10.4 & 9.1.15 |
| A.7.7 | Clear desk and clear screen | 9.1.15 |
| A.7.8 | Equipment siting and protection | 5.8 |
| A.7.9 | Security of assets off-premises | 5.8, 9.1.10 & 9.1.19 |
| A.7.10 | Storage media | 9.1.10 |
| A.7.11 | Supporting utilities | chapter 7 |
| A.7.12 | Cabling security | 5.9 |

| | | |
|---|---|---|
| A.7.13 | Equipment maintenance | 9.1.10 |
| A.7.14 | Secure disposal or re-use of equipment | 9.1.10 |
| 8 Technological management measures | | |
| A.8.1 | User end point devices | 10.4 & 9.1.13 |
| A.8.2 | Privileged access rights | 9.1.15 |
| A.8.3 | Information access restriction | 9.1.15 |
| A.8.4 | Access to source code | uncovered |
| A.8.5 | Secure authentication | 9.1.15 & 9.1.19 |
| A.8.6 | Capacity management | 10.2, 9.1.12 & 9.1.13 |
| A.8.7 | Protection against malware | 9.1.13 |
| A.8.8 | Magement of technical vulnerabilities | 9.1.13 |
| A.8.9 | Configuration management | 9.1.13 |
| A.8.10 | Information deletion | 9.1.13 |
| A.8.11 | Data masking | 9.1.15 |
| A.8.12 | Data leakage prevention | 9.1.13 |
| A.8.13 | Information backup | 9.1.14 |
| A.8.14 | Redundancy of information processing facilities | 9.1.12 |
| A.8.15 | Logging | 8.3 & 9.1.12 |
| A.8.16 | Monitoring activities | 9.1.12 |
| A.8.17 | Clock synchronisation | 8.2 |
| A.8.18 | Use of privileged utility programs | 10.4 & 9.1.13 |
| A.8.19 | Installation of software on operational systems | 9.1.13 |
| A.8.20 | Networks security | 9.1.13 |
| A.8.21 | Security of network services | 9.1.13 |
| A.8.22 | Segregation of networks | 9.1.13 |
| A.8.23 | Web filtering | 9.1.13 |
| A.8.24 | Use of cryptography | uncovered |
| A.8.25 | Secure development life cycle | uncovered |
| A.8.26 | Application security requirements | uncovered |
| A.8.27 | Secure system architecture and engineering principles | 10.4 |
| A.8.28 | Secure coding | uncovered |
| A.8.29 | Security testing in development and acceptance | 9.1.11 |
| A.8.30 | Outsourced development | uncovered |
| A.8.31 | Separation of development, test and production environments | uncovered |
| A.8.32 | Change management | 9.1.13 |
| A.8.33 | Test information | uncovered |
| A.8.34 | Protection of information systems during audit testing | 10.4 |

*Table 10 Mapping ISO 27001:2022*

## 7.5 Crossreference ISO 9001 to ISO/IEC 27001 and EN 50518 – G

| **EN-ISO 9001** | **ISO/IEC 27001** | **EN50518** |
|---|---|---|
| **Quality management systems – Requirements** | **Information technology - Security techniques - Information security management systems - Requirements** | **Monitoring and alarm receiving centre** |
| 4. Context of the organization | 4. Context of the organization | 1. Scope |
| 5. Leadership | 5. Leadership | 10.1 General Principles leadership<br>10.2 Governance and Strategy<br>10.3 Legal and operational set-up |
| 6. Planning<br>- Actions to address risks and opportunities | 6. Planning<br>- Actions to address risks and opportunities | Planning<br>4.1. Categorization<br>4.2. Site selection |

| | | |
|---|---|---|
| - Quality objectives and planning to achieve them<br>- Planning of changes | - Quality objectives and planning to achieve them | 10.4 Management System.<br>- Risk and Contingency Management.<br>- Information Management.<br>- Complaint Handling.<br>- Management of the Services Portfolio.<br>- Management of Staffing.<br>- Client Management.<br>- Business Partner Management. |
| 7. Support<br>- Resources<br>- Competence<br>- Awareness<br>- Communication | 7. Support<br>- Resources<br>- Competence<br>- Awareness<br>- Communication | Support – Resources & Competence<br>5. Construction<br>6. Alarm systems of the ARC<br>7. Electrical power supplies<br>10.5.1. Staffing<br>10.5.2. Security screening and vetting<br>10.6 Training |
| 8. Operation<br>- Quality planning and control<br>- Requirements for products and services<br>- Design and development of products and services<br>- Control of externally provided processes, products and services<br>- Production and services provision<br>- Release of products and services<br>- Control of nonconforming outputs | 8. Operation<br>- Operational planning and control<br>- Information security risk assessment<br>- Information security risk treatment | Operation<br>8. Alarm Management System<br>9. Operation of the ARC<br>9.1 Procedures<br>1. General<br>2. Creation, modification & cancelation<br>3. Message handling<br>4. Communication with response services<br>5. Individual services provided by the ARC<br>6. Alarm verification<br>7. Unexpected increase in alarm signals<br>8. Alarm transmission path failures<br>10. Installation, maintenance, protection, removal and reuse of assets under the control of the ARC<br>11. Monitoring & testing of equipment<br>12. Fault procedures and reporting<br>13. Information management<br>14. Data back-up<br>15. Confidentiality and classification of information<br>16. Relationships with essential suppliers<br>17. Administrative procedures<br>18. Physical access<br>19. Remote access<br>20. Operational continuity and emergencies<br>21. Emergency evacuation and re-entry<br>22. Emergency entry |
| 9. Performance evaluation<br>- Monitoring , measurement , analyses & evaluation<br>- Internal audit<br>- Management review | 9. Performance evaluation<br>- Monitoring , measurement , analyses & evaluation<br>- Internal audit<br>- Management review | 9.2 Performance criteria – message handling<br>9.1.9 . Controls to maintain QoS<br>9.1.23 KPI |
| 10. Improvement | 10. Improvement | |

*Table 11 Crossreference ISO 9001 to ISO/IEC 27001 and EN 50518*

## 7.6 Business continuity - G

The following paragraphs relate to the business continuity of a MARC.

| Paragraphs | Subject | Short reference |
|---|---|---|
| 4.2 | Site selection | The ARC should prepare a risk analysis that addresses the risks, including those that pose a threat to business continuity, and against which measures are taken to mitigate the risks. |
| 5.8 | Location of data processing equipment | By placing data processing equipment in multiple locations, the ARC is at less risk of having a complete failure of the ARC systems in case of an incident. |
| 5.9.1 | Communication cables | Having two connections from different providers entering the premises at different locations reduces the chances of a complete failure of the ARC systems. |
| 9.1.9 | Controls to maintain quality of service | Monitoring ARC systems and initiating procedures increases the chances of noticing disruptions quickly and resolving them as soon as possible. |
| 9.1.12 | Fault procedures and reporting | Monitoring ARC systems and initiating procedures increases the chances of noticing disruptions quickly and resolving them as soon as possible. |
| 9.1.13 | Information management | Protecting data reduces the risk of losing data and customer information. Systems and data can be hacked and stolen if information security is poor. |
| 9.1.14 | Data back-up | Should ARC systems do go down, backups ensure minimal loss of data and information. |
| 9.1.16 | Relationships with essential suppliers | SLA ensure good agreements that allow quick action in case of an incident. |
| 9.1.20 | Operational continuity and emergencies | Procedures for business continuity and incident recovery ensures a clear and quick response if needed. |
| 9.1.23 | Key performance indicators | Monitoring on KPI provides visibility into business performance on which the ARC can steer when the established KPI is not met. |
| 9.2 | Performance criteria: Message handling | Understanding response times and analysing them provides information to make any necessary adjustments to meet the standard. |
| 10.2 | Governance and strategy | The ARC has policies for continuous monitoring of the operating environment and performance. |
| 10.4 | Management system | The ARC has policies on business continuity and incident recovery. |

*Table 12 Paragraphs EN50518 related to business continuity*

## 7.7 ISO 31000 – Risk assessment - G

ISO 31000 provides guidelines for managing risks that organizations face. These guidelines can be tailored to fit the specific context of any organization. The document offers a generic approach to managing all types of risks and is not specific to any industry or sector. It can be used throughout the entire lifecycle of an organization and applied to all activities, including decision-making at all levels. This document is also referenced in the EN 50518 standard.

It's important to clearly define the scope and context of the risk analysis at the beginning of this process. Additionally, the necessary competencies for carrying out this process should be considered and documented in advance. If needed, extra training or personnel may be organized to ensure the effective implementation and maintenance of this process.

In the process, it's crucial to determine whether the measures taken will positively affect the reduction of the likelihood of the incident or the reduction of the impact of the incident. In other words, it's important to identify if the measures are preventive, aimed at reducing or preventing the likelihood of the incident, or if they are reactive, aimed at reducing the effect or impact after the incident has occurred.

If the measures are reactive, they should be linked to the incident recovery planning. This ensures that the organization can return to normal operations within a reasonable timeframe.

Chapter 9.1.20 of the EN 50518 standard, "Operational continuity and emergencies," requires organizations to have a Business Continuity and Disaster Recovery procedure.

The process must align with the alarm center's policy as described in Chapter 10.4, "Management System," of EN 50518. Risk and continuity management should include aspects of resilience, business continuity, and disaster recovery, supported by a comprehensive risk analysis, such as the ISO 31000 series. It should contain plans for alarm centers and procedures, considering measures to prevent, detect early, and address disruptive events at both management and technical levels.

Example case study: an alarm centre has a threat of a logical unwanted access to the alarm centre's logical domain.

The preventive measures that can be taken by the alarm centre are:
1. Technical; filtering incoming data, monitoring data traffic and filtering, encryption and code check incoming data, detection for malware / viruses / mobile codes, etc.
2. Organizational; staff training; ongoing staff awareness development; technical investments; evaluation technical monitoring , etc.

The repressive measures that may have been taken by the emergency centre after the incident occurred:
1. Organizational; the deployment of a response team with clear competences and tasks to combat this breach. Communication after relevant parties and collection of relevant information is part of the process. The deployment of possible other actions.
2. Technical; the deployment of technical means, which can defuse and remove breach of hostile code.

This above case study is an example and the measures listed are not limited.
A checklist is attached in Annex 3 to check your own process against the mentioned standard.

# 8. Alarm Transmission Service Provider “G”

## 8.1 General – G

An Alarm Transmission Service Provider (ATSP) is the entity responsible for the monitoring of the performance of the Alarm Transmission System (ATS) according EN 50136-1/A1. The task for the monitoring of the ATS is executed by a Monitoring Centre according EN 50518.

The ATSP shall maintain documentation sufficient for planning, installation, commissioning, service and operation of the ATS.

Alarm Transmission Equipment (ATE) instructions shall be structured to reflect the access levels of the different type of users. See the access levels in EN50136-1/A1 in reflection of the access levels in EN50131-1.

The MC can assist the ATSP with the commissioning, service and operation of the ATS. The MC has an Alarm Management System (AMS) to perform its tasks. The MC receives its information from the Receiving Centre Transceiver (RCT). The functions of the RCT according to EN50136-3 shall partly be fulfilled by the AMS. Check these functions according to EN50136-3 within the AMS next to the requirements of the AMS to EN50518.

If the ATSP is operating a common protocol according TS 50136-9, this shall interact with the requirements in EN50136-1/A1 about commissioning and connection setup.

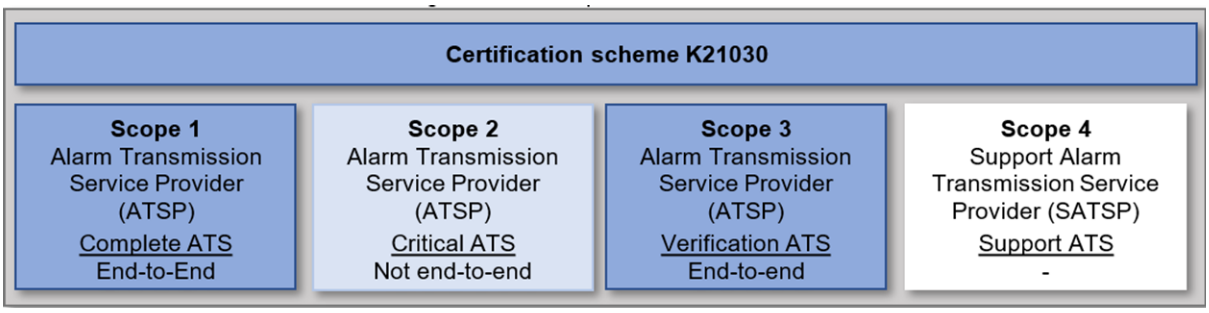
The table below shows relevancy between the standards to be noticed in the execution.

| EN 50136-1/A1 | TS 50136-9 | EN 50518:2019 |
|---|---|---|
| 5 General requirements | | |
| 6 System requirements | 4 Objective<br>5 Messaging<br>6 Message types | 8 Alarm Management System |
| 7 Verification of performance | | |
| 8 Documentation sufficient for planning, installation, commissioning, service and operation | 7 Commissioning and connection setup | 9 Operation of the ARC<br>10.4 Complaint handling<br>10.4 Compliance audit<br>10.5 Staffing |

*Tabel 13 relevancy between the standards*

## 8.2 K21030 Alarm Transmission Systems - Alarm Transmission Service Providers - G

Certification scheme K21030 is made by Kiwa for the certification of Alarm Transmission Systems and Alarm Transmission Service Providers. The scheme is divided in four scopes. For more information see the certification scheme K21030.



| Certification scheme K21030 | | | |
|---|---|---|---|
| **Scope 1**<br>Alarm Transmission Service Provider (ATSP)<br>Complete ATS<br>End-to-End | **Scope 2**<br>Alarm Transmission Service Provider (ATSP)<br>Critical ATS<br>Not end-to-end | **Scope 3**<br>Alarm Transmission Service Provider (ATSP)<br>Verification ATS<br>End-to-end | **Scope 4**<br>Support Alarm Transmission Service Provider (SATSP)<br>Support ATS<br>- |

### 8.2.1 Scope 1

Scope 1 is the certification of a complete alarm transmission system (ATS) from Supervised Premises Transceiver (SPT) to Receiving Centre Transceiver (RCT) and the full responsibility. This scope is end-to-end.

### 8.2.2 Scope 2

Scope 2 is the certification of the critical alarm transmission system (ATS). This scope is mainly applicable in hosted situations and encompasses the connection between the Receiving Centre Transceiver Hosted (RCT-H) and the Receiving Centre Transceiver part in the ARC (RCT-A) and the full responsibility. This scope is not end-to-end.

### 8.2.3 Scope 3

Scope 3 is the certification of verification alarm transmission systems (ATS) form Supervised Premises Transceiver (SPT) to Receiving Centre Transceiver (RCT) and encompasses only verification of performance and reporting to the customer. This scope is end-to-end.

### 8.2.4 Scope 4

Scope 4 is the certification of support delivered to an Alarm Transmission Service Provider.

# 9. VSS Control Room “G and R”

## 9.1 Chapter 12 - Control room configuration - G

As mentioned in chapter 2, EN 50518 directs to EN-IEC 62676-4 for Video Surveillance Systems (VSS). The purpose of this part of IEC 62676 is to provide guidance on how to ensure that video surveillance systems (VSS), meet their functional and performance requirements. Chapter 12 contains the VSS control room configuration

The EN-IEC 62676-4 states the following:
*If the VSS has a requirement for live viewing, camera control, system management, or any other human intensive tasks, a control room should be specified to house these functions. The 'control room' could be a single workstation, or a large operations centre.*

Besides the configuration of the workstations, the standard also demands back-up power and lightning and surge protection. Both of these items are already arranged in EN 50518.

## 9.2 Connecting VSS to a VSS control room - G

For connecting to a VSS control room, the purpose and parameters of the VSS should be clearly determined. This information is necessary for the VSS control room to maintain a quality of service. These requirements are stated in chapter 4 and 5 of the EN-IEC 62676-4. These chapters are obligatory for connecting a VSS to the VSS Control Room.

### 9.2.1 Chapter 4 - General considerations - G

This chapter contains general considerations before designing a VSS. This includes:

- Risk assessment;
- Security grading;
- Operational requirements;
- Site survey;
- System design and site plan;
- Developing the test plan;
- Installation, commission and hand over;
- Documenting the system.

### 9.2.2 Chapter 5 - Operational requirements specifications - G

This chapter contains operational requirements regarding the specifications of the VSS. The purpose of these operational requirements is that it is clearly stated what the customer expect that the functions of the system do. Without clearly defined operational requirements, there is no practical methodology to assess whether the system can meet its required purpose. The operational requirements include:

- Basic objective/functionalities;
- Definition of surveillance limitations;
- Definition of the site(s) under surveillance;
- Definition of activity to be captured;
- System/picture performance;
- Period of operation;
- Conditions at the location;
- Resilience;
- Monitoring and image storage;
- Exporting images;
- Routine actions;
- Operational response;

- Operator workload;
- Training;
- Expansions;
- List of any other special factors not covered by the above;
- Automation;
- Alarm response;
- System response times.

## 9.3 VSS control room assessment - R

When an assessment based on scope VSS in security applications is desired, Kiwa will assess the VSS control room configuration on chapter 12. Connected VSS will be assessed based on chapter 4 and 5. The assessment includes an initial sampling of 2 and a surveillance sampling of three projects. The sampling of projects is based on the agreed documentation and the images in the VSS control room. No location visits are needed.

# 10. Guidance on remote access/apps and portals “G”

## 10.1 Remote access and the risks - G

Remote access to IT systems also carries potential risks if its setup and configuration is inadequate. Some key risks are:

1. Security breaches: Opening remote access can potentially introduce security breaches in IT systems, allowing malicious parties to try to access sensitive data or perform malicious activities.

2. Unauthorised access: If appropriate security measures are not implemented, remote access could risk allowing unauthorised persons to access systems or data.

3. Weak passwords: Poor password security can increase the risk of malicious persons guessing, cracking or intercepting passwords to gain access to systems.

4. Malicious software: Gaining remote access can provide the opportunity for malicious persons to install or activate malicious software on the system, leading to data loss, system failures or other forms of damage.

5. Data breaches: If appropriate security measures are not in place, remote access to IT systems can lead to data breaches, exposing sensitive information to unauthorised individuals.

To mitigate these risks, it is important to implement strong security measures, such as the use of strong passwords, two-factor authentication, regular system updates, firewalls and data encryption. It is also important to use only reliable and secure connections for remote access and to manage access rights carefully.

*Example of a remote access hack with consequences:*
The fictive company ABC had enabled remote access to its IT systems for its suppliers to perform service remotely. Unfortunately, the company fell victim to a hack that could have had serious consequences.

In this scenario, a malicious hacker exploited weak security measures and an unpatched vulnerability / poorly set up Identity and Access Management (IAM) in the company's remote access infrastructure.

*The consequences of such a hack can be significant. It can lead to:*
1. Data theft: The hacker may gain access to customer databases and steal sensitive data. This may include personally identifiable information (PII) of customers, such as names, addresses, BSN numbers and financial transaction details. This data theft puts customers at risk of identity theft and potential abuse.

2. Financial damage: The hacker gains access to the company's financial systems. This allows him to perform fraudulent transactions, transfer money to external accounts and compromise the company's financial integrity. The company may suffer significant financial losses as a result of this hack.

3. Reputational damage: News of a hack spreads quickly, which can severely damage the trust of customers and business partners in the company. The company faces negative publicity, customer turnover and loss of new business opportunities. The reputational damage is significant and costs the company a lot of time and effort to restore stakeholder trust.

4. Regulatory implications: The company is subject to strict regulatory and compliance requirements. The hack may lead to violations of these requirements, resulting in investigations, fines and possible legal action by regulatory bodies.

Such an incident highlights the importance of robust security measures, regular patching and monitoring of remote access systems (SOC, SIEM, SOAR, etc), as well as the importance of an adequate incident response plan.

The company should therefore design its security measures adequately, implement additional security layers and invest in cyber security training and awareness to prevent future hacks.

Implementing ISO27001 can serve as a basis for this.

## 10.2 Apps, appserver, webserver and webportals - G

Remote access is not limited to supplier and employee access; increasingly, apps and portals are also providing remote access by servers. Where apps and web portals are mentioned below, app and web servers should also be considered in the chain. Poorly developed apps and web portals can pose several risks, including:

1. Security vulnerabilities: If an app or web portal is poorly developed, there may be vulnerabilities in the code. This can lead to security vulnerabilities, allowing malicious actors to access sensitive data or perform malicious activities.

2. Data breaches: Poorly developed apps and web portals can lead to data breaches, where unauthorised persons gain access to personal or confidential information. This can have serious consequences, such as identity theft or financial loss.

3. Poor user experience: If an app or web portal is poorly designed or insufficiently user-friendly, it can lead to frustration among users. Poor performance, unclear navigation, slow load times and other usability issues can cause users to leave the app or stop using the web portal.

4. Instability and errors: Poor development practices can result in unstable apps and web portals that frequently crash or have errors. This can negatively affect the usability of the app or web portal and reduce user trust.

5. Poor integration and compatibility issues: If an app or web portal is not developed properly with regard to integration with other systems or devices, compatibility issues may arise. This can lead to functionality loss, data loss or reduced performance.

To reduce these risks, it is important that apps and web portals are developed according to best practices in terms of security, code quality, user experience and compatibility. Regular security audits, code reviews and testing sessions can help identify vulnerabilities and errors before the app or web portal is rolled out to users. Moreover, it is crucial to safeguard users' privacy and comply with relevant laws and regulations, such as the General Data Protection Regulation (GDPR).

**Measures**

For the security of apps, app servers, web portals and web servers, several logical security measures should be applied. Here are some key measures:

1. Authentication and authorisation: Implement a robust authentication and authorisation system to ensure that only authorised users can access the app or web portal. Use strong passwords, two-factor authentication and restrict access rights based on the user's role. See EN 50518 9.1.19

2. Data encryption: Encrypt sensitive data both during storage and transmission. This helps ensure data confidentiality even if it falls into the wrong hands.

3. Input validation: Perform strict validation of user input to prevent possible attacks such as SQL injection and cross-site scripting (XSS). This prevents malicious users from injecting malicious code or exploiting weaknesses in the app or web portal.

4. Restrict access rights: Limit app or web portal access rights to what is strictly necessary. Give users access only to the functionalities and data they actually need to perform their tasks. This reduces the risk of misuse or unauthorised access. See EN 50518 Annex B.

5. Secure session management: Implement secure session management to ensure that sessions are securely authenticated and managed. For example, use unique session identifiers, ensure secure transmission of session data and set a time limit for sessions to manage inactivity. See EN 50518 Annex B.

6. Audit logs and monitoring: Implement logging and monitoring of activities within the app or web portal. This helps detect suspicious activity, security breaches or unauthorised access. Keep logs of user actions, errors and security events for analysis and forensics. See EN 50518 9.1.19

7. Regular updates and patches: Ensure regular updates and patches of the app or web portal to fix security vulnerabilities and address vulnerabilities. Keep the software frameworks, libraries and other components used up-to-date to avoid known security issues. See EN 50518 9.1.13

It is also essential to follow the security guidelines and best practices of relevant organisations and standards, such as OWASP (Open Web Application Security Project), to ensure that security measures are effective and up-to-date.

The link for the above measures is in EN 50518 article 9.1.19 it says:
*The procedure shall describe how remote access to and from any system within the ARC and to the receiving data processing equipment (see 5.8) shall be controlled by a log-in / log-out procedure recording time and date, credentials of the person involved and actions performed. Remote access can only be granted by authorization of the ARC. See annex B for further information related to remote system access.*

Let’s break down the article:
What is data processing equipment based on EN 50518 5.8:

- Interface of the AMS for interconnection with the RCT (iRCT)
  *(Front end processor/signal processor);*
- Servers of the alarm management system (databases, storages);
- Voice recording equipment;
- Active network components (routers, switches);
- Passive network components (patch panels, cabling);
- Communication equipment (PABX)
- Internal transfer point LAN / WAN

What could be seen by: authorization of the ARC
The ARC can authorize employees and/or suppliers to gain remote access by means of:
- Letting them call the ARC to gain access;
- Making a contract/SLA with preconditions to have access to the ARC in certain conditions with security arrangements;

Wat could be seen by: Log-in / Log-out procedure recording time and date, credentials of the persons involved and actions performed
The supplier or employee should be authorised by the ARC and it should be known when remote access is used. This must be logged in the application or remote access server recording time and date and the credentials.

What is: Annex B EN 50518 (informative)
EN 50518 annex B provides guidance on how to complete article 9.19 of EN 50518 with an eye also to ISO 27001 specifically for ARC data. This article therefore applies, for example, if a supplier, installer or customer can access the AMS and its functions via remote access, an app or portal. Note: this is an informative article.

## 10.3 Guidance plan of approach remote access - G

1. Identification of business-critical systems: The company first identifies the systems that are critical to their operations. This may include data storage servers, internal communication systems, financial systems and customer databases.

2. Evaluation of potential threats: The company analyses the potential threats they may face when opening up remote access. This includes threats such as unauthorised access attempts, malware infections, phishing attacks and data theft.

3. Assessment of existing security measures: The company evaluates the current security measures already implemented to protect IT systems. This includes things like firewalls, antivirus software, intrusion detection/prevention systems and data encryption.

4. Identification of vulnerabilities: The company conducts a thorough assessment of vulnerabilities in their IT infrastructure. This includes identifying any outdated software, configuration errors, weak passwords and possible misconfigurations in the systems

5. Risk assessment: The company evaluates the identified threats and vulnerabilities in terms of their impact and likelihood. This allows them to better understand the potential risks of remote access to IT systems and prioritise risk management.

6. Risk management: Based on the risk assessment, the company takes appropriate measures to manage the identified risks. This includes implementing additional security measures, such as strong authentication, network segmentation, regular system updates, security monitoring and employee awareness programmes.

7. Periodic review and revision: The company plans regular reviews and revisions of the risk assessment to ensure security measures remain up-to-date and in line with changing threat landscapes and business needs.

This risk assessment approach enables Company ABC to understand the potential risks of remote access to IT systems and implement appropriate measures.

# Annex 1: Matrix penetration seals – G

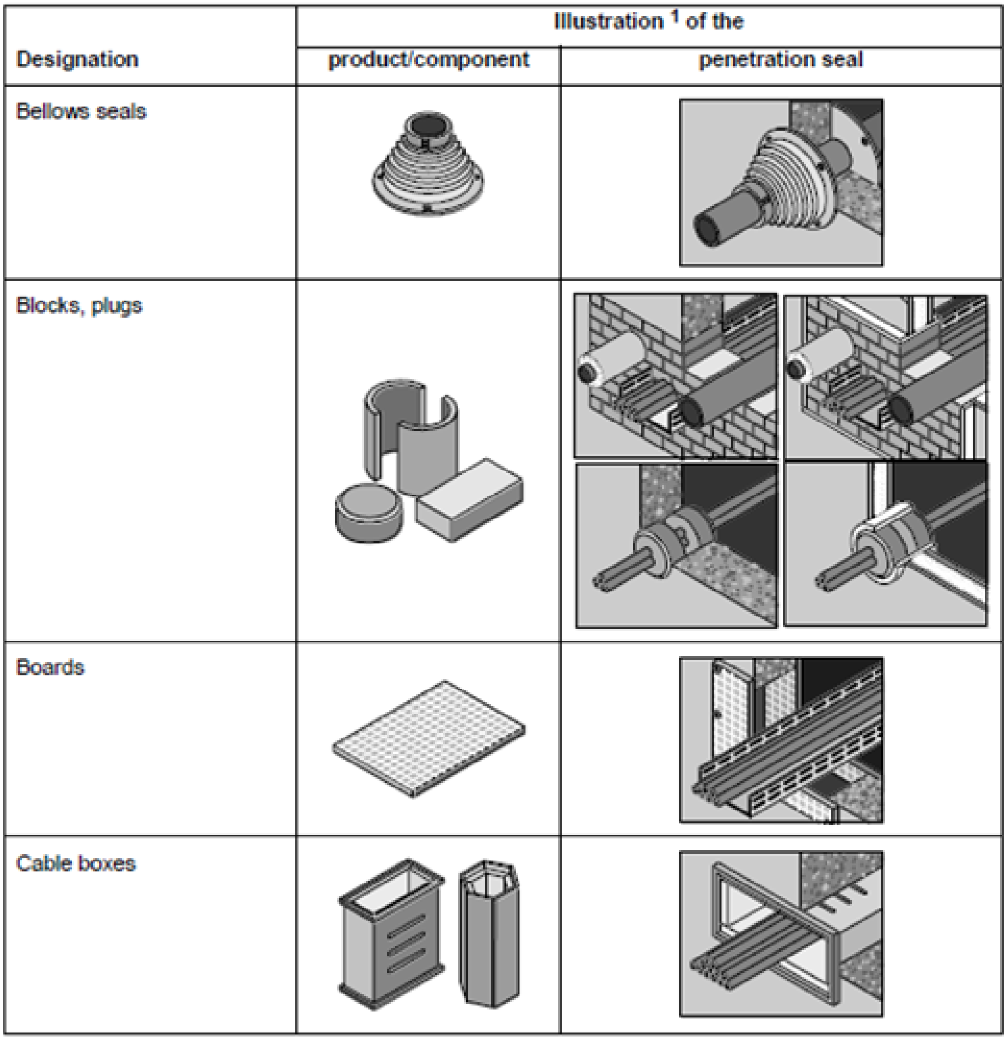
To be able to write down sufficient positive evidence, a table is given as an example to fill in per penetration seal.

| | | |
|---|---|---|
| **Penetration - Number** | | |
| **Location** | Location identification from the penetration seal on a map. | |
| **Photo's** | Before application | Before application |
| **Original seperation** | Material and fire resistance. | |
| **Penetration** | Cable(s) / pipe (material) / medium in pipe. | |
| **Type penetration seal** | See table 1-1 in ETAG26-2. Caution for pipe material. It must be clear that the type of penetration seal according to the attestation of the product certificate is able to squeeze it in case of fire. Indicate this in the matrix by referring specifically where this is stated in the certificate. | |
| **Manufacturer, product, certificate** | Name the manufacturer, the product and which certificate the product has. EAD of ETAG certificate. | |
| **Manufacturer guideline per penetration seal** | Indicate where this is specifically stated in the certificate and / or the assembly instructions of the manufacturer. Pay particular attention to the criteria for the maximum spacing between the cable (s) and / or pipes and the relevant original wall and the mounting instructions for the cables / pipes. Also make clear how far the coating must be applied to the cables / pipes per specific penetration. | |
| **The person who installed the penetration seal** | Name. | |
| **The person who checked the right application** | Name. | |

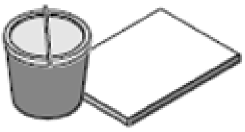
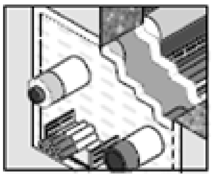
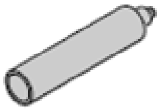
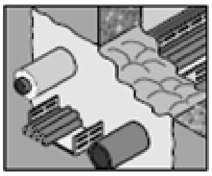
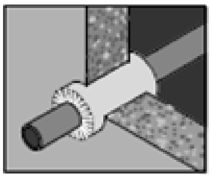
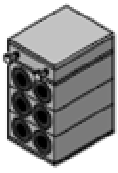
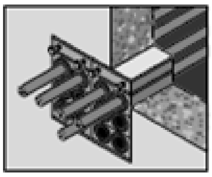
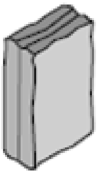
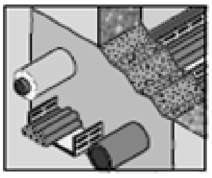
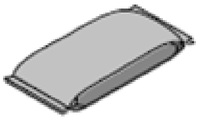
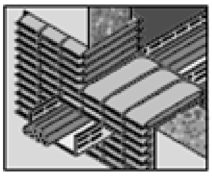
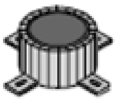
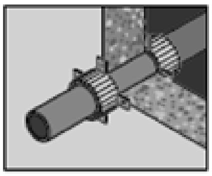
Important is the installation guideline from the used products. The instructions of the manufacturer should be followed to guarantee the same performance as during the test. Depending on the instruction of the manufacturer, the application should be done on the inside or the outside of the shell.

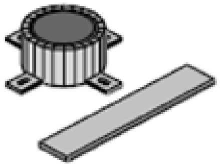
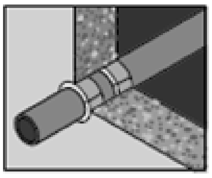
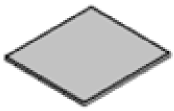
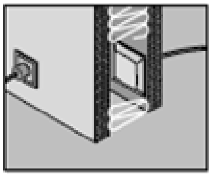
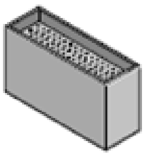
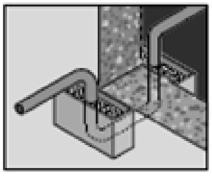
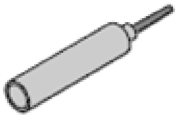
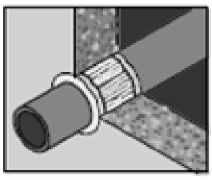
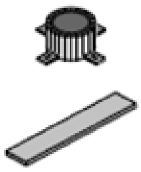
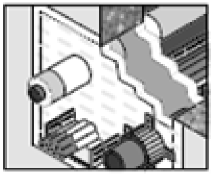
It is also important that the applicator is educated in context of the used products. The registration of the education should also be supplied.

**Table 1.1 ETAG 26-2**



| Designation | Illustration [1] of the | |
|---|---|---|
| | product/component | penetration seal |
| Bellows seals | | |
| Blocks, plugs | | |
| Boards | | |
| Cable boxes | | |

| | | |
|---|---|---|
| Coated mineral wool slabs (e.g. intumescent or ablative coating) |  |  |
| Foams |  |  |
| Mineral wool | |  |
| Modular systems |  |  |
| Mortar |  |  |
| Pillows (also referred to as "bags" or "cushions") |  |  |
| Pipe closure devices | | |
| - Collars (integrated into or outside the wall / floor) |  |  |

| | | |
|---|---|---|
| - Wraps (integrated into a wall or floor) including strips and composite strips |  |  |
| - Mechanically actuated systems for pipes | variable | variable |
| Putties |  |  |
| Sand gaskets |  |  |
| Sealants/Mastics |  |  |
| Combinations of the products named above |  |  |

# Annex 2: Mapping matrix EN50518 and relevant standards with additional services – G

| European standard | EN50518 | EN-IEC 62676-4: 2015 | IEC 60839-11-2: 2014 | K21023 | EN50136-1/A1 K21030 | CLC/TS 50134-7: | ISO/IEC 27039; 2015 | TS54-14: 2004 |
|---|---|---|---|---|---|---|---|---|
| Name of the standard | Monitoring and alarm receiving centre | Video surveillance systems for use in security applications - Part 4: Application guidelines | Alarm & electronic security systems - Part 11-2: Electronic access control systems - Application guidelines | Mobile Security – Security of mobile objects and persons | Alarm Transmission Service Provider | Alarm systems - Social alarm systems - Part 7: Application guidelines | Information technology - Security techniques - Selection, deployment and operations of intrusion detection systems (IDPS) | Fire Alarms Systems (FAS) |
| Paragraph | 1. Scope | P1 Scope | P1 Scope | P1 Scope | P1 scope and Responsibilities | P1 Scope | P1 Scope | P1 Scope |
| Paragraph | Planning<br>4. Site selection | | | | | | | |
| Paragraph | Support – Resources & Competence<br>5. Construction<br>6. Alarm systems of the ARC<br>7. Electrical power supplies<br>4. Staffing | 12 VSS control room configuration<br>12.1 Control rooms<br>12.2 Number, size and positioning of VSS video displays<br>12.3 Displays and screens mounted on or off the workstation<br>12.4 Recommended display sizes<br>12.5 Number of camera images per operator<br>12.6 Number of work stations<br>12.7 Equipment siting<br>12.8 Backup power supply provision<br>12.10 Lightning | | 6 Product requirements<br>7 Requirements quality system | 5 Requirements quality system | 13 Sub-contract delivery of services<br>14 Staffing | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | and surge protection | | | | | | |
| Paragraph | Operation<br><br>2013<br>P2: 4. Performance requirements<br>P2: 5. Communication requirements<br>P2: 6. Reception of signals<br>P2: 7. Testing<br>P2: 8. Data<br>P2: 9. Data storage<br>P2: 10. Availability and verification of performance of the ARC<br>P2: 11. Contingency plan<br>P3: 5. Operating procedures<br>P3: 8. Data<br><br>2019<br>8. Alarm management system<br>9. Operation of the ARC<br>10. General principles, leadership, governance, management and staffing | 12.9 Operating temperature | 10.1 System operation | 4 Performance requirements<br>5 Process requirements | 5 Requirements quality system | 8 Alarm receiving services<br>10 Response arrangements<br>12 Operational records<br>15 Riskmanagement | 6.4 Deployment<br>7 Operations | 6.9 Signals to a fire alarm receiving station<br>8.2 Commissioning<br>11.2.2 Prevention of false alarms during routine testing |
| Paragraph | P3: 6. Auditing | 13.3 Technical acceptance testing Annex B & C & E | | 7 Requirements quality system | | 9 Testing and maintenance | | |
| Paragraph | P3: 7. Complaints procedure | | | | | | | |

# Annex 3: Risk assessment ISO 31000

| About | c/n | Information |
|---|---|---|
| **5.1 Framework** | | |
| **5.2 Leadership and commitment** | | |
| **5.3 Integration** | | |
| **5.4 Design** | | |
| **5.5 Implementation** | | |
| **5.6 Evaluation** | | |
| **5.7 Improvement** | | |
| **6.1 Process** | | |
| **6.2 Defining the scope**<br>When planning the approach, considerations include:<br>— *objectives and decisions that need to be made;*<br>— *outcomes expected from the steps to be taken in the process;*<br>— *time, location, specific inclusions and exclusions;*<br>— *appropriate risk assessment tools and techniques;*<br>— *resources required, responsibilities and records to be kept;*<br>— *relationships with other projects, processes and activities.*<br><br>As the risk management process may be applied at different levels (e.g. strategic, operational, programme, project, or other activities), it is important to be clear about the scope under consideration, the relevant objectives to be considered and their alignment with organizational objectives. | | |
| **6.3.3 External and internal context**<br>The external and internal context is the environment in which the organization seeks to define and achieve its objectives.<br>The context of the risk management process should be established from the understanding of the external and internal environment in which the organization operates and should reflect the specific environment of the activity to which the risk management process is to be applied.<br><br>Understanding the context is important because:<br>— *risk management takes place in the context of the objectives and activities of the organization;*<br>— *organizational factors can be a source of risk;*<br>— *the purpose and scope of the risk management process may be interrelated with the objectives of the organization as a whole.*<br><br>The organization should establish the external and internal context of the risk management process by considering the factors mentioned in 5.4.1. | | |
| **6.3.4 Defining risk criteria**<br>The organization should specify the amount and type of risk that it may or may not take, relative to objectives. It should also define criteria to evaluate the significance of risk and to support decision making<br>processes. Risk criteria should be aligned with the risk management framework and customized to the specific purpose and scope of the activity under consideration. Risk criteria should reflect the organization’s values, objectives and resources and be consistent with policies and statements about risk management. The criteria should be defined taking into consideration the organization’s obligations and the views of stakeholders. While risk criteria should be established at the beginning of the risk assessment process, they are dynamic and should be continually reviewed and amended, if necessary.<br><br>To set risk criteria, the following should be considered:<br>— *the nature and type of uncertainties that can affect outcomes and objectives (both tangible and intangible);* | | |

| | | |
|---|---|---|
| *— how consequences (both positive and negative) and likelihood will be defined and measured;*<br>*— time-related factors;*<br>*— consistency in the use of measurements;*<br>*— how the level of risk is to be determined;*<br>*— how combinations and sequences of multiple risks will be taken into account;*<br>*— the organization's capacity.* | | |
| **6.4.1 Risk assessment**<br>Risk assessment is the overall process of risk identification, risk analysis and risk evaluation. Risk assessment should be conducted systematically, iteratively and collaboratively, drawing on the knowledge and views of stakeholders. It should use the best available information, supplemented by further enquiry as necessary. | | |
| **6.4.2 Risk identification**<br>The purpose of risk identification is to find, recognize and describe risks that might help or prevent an organization achieving its objectives. Relevant, appropriate and up-to-date information is important in identifying risks. The organization can use a range of techniques for identifying uncertainties that may affect one or more objectives.<br><br>The following factors, and the relationship between these factors, should be considered:<br>*— tangible and intangible sources of risk;*<br>*— causes and events;*<br>*— threats and opportunities;*<br>*— vulnerabilities and capabilities;*<br>*— changes in the external and internal context;*<br>*— indicators of emerging risks;*<br>*— the nature and value of assets and resources;*<br>*— consequences and their impact on objectives;*<br>*— limitations of knowledge and reliability of information;*<br>*— time-related factors;*<br>*— biases, assumptions and beliefs of those involved.*<br><br>The organization should identify risks, whether or not their sources are under its control. Consideration should be given that there may be more than one type of outcome, which may result in a variety of tangible or intangible consequences. | | |
| **6.4.3 Risk analysis**<br>The purpose of risk analysis is to comprehend the nature of risk and its characteristics including, where appropriate, the level of risk. Risk analysis involves a detailed consideration of uncertainties, risk sources, consequences, likelihood, events, scenarios, controls and their effectiveness. An event can have multiple causes and consequences and can affect multiple objectives.<br>Risk analysis can be undertaken with varying degrees of detail and complexity, depending on the purpose of the analysis, the availability and reliability of information, and the resources available.<br>Analysis techniques can be qualitative, quantitative or a combination of these, depending on the circumstances and intended use.<br><br>Risk analysis should consider factors such as:<br>*— the likelihood of events and consequences;*<br>*— the nature and magnitude of consequences;*<br>*— complexity and connectivity;*<br>*— time-related factors and volatility;*<br>*— the effectiveness of existing controls;*<br>*— sensitivity and confidence levels.*<br><br>The risk analysis may be influenced by any divergence of opinions, biases, perceptions of risk and judgements. Additional influences are the quality of the information used, the assumptions and exclusions made, any limitations of the | | |

| | | |
|---|---|---|
| techniques and how they are executed. These influences should be considered, documented and communicated to decision makers.<br>Highly uncertain events can be difficult to quantify. This can be an issue when analysing events with severe consequences. In such cases, using a combination of techniques generally provides greater insight.<br>Risk analysis provides an input to risk evaluation, to decisions on whether risk needs to be treated and how, and on the most appropriate risk treatment strategy and methods. The results provide insight for decisions, where choices are being made, and the options involve different types and levels of risk. | | |
| **6.4.4 Risk evaluation**<br>The purpose of risk evaluation is to support decisions. Risk evaluation involves comparing the results of the risk analysis with the established risk criteria to determine where additional action is required.<br>This can lead to a decision to:<br>— *do nothing further;*<br>— *consider risk treatment options;*<br>— *undertake further analysis to better understand the risk;*<br>— *maintain existing controls;*<br>— *reconsider objectives.*<br>Decisions should take account of the wider context and the actual and perceived consequences to external and internal stakeholders.<br>The outcome of risk evaluation should be recorded, communicated and then validated at appropriate levels of the organization. | | |
| **6.5.1 Risk treatment**<br>The purpose of risk treatment is to select and implement options for addressing risk.<br>Risk treatment involves an iterative process of:<br>— *formulating and selecting risk treatment options;*<br>— *planning and implementing risk treatment;*<br>— *assessing the effectiveness of that treatment;*<br>— *deciding whether the remaining risk is acceptable;*<br>— *if not acceptable, taking further treatment.* | | |
| **6.5.2 Selection of risk treatment options**<br>Selecting the most appropriate risk treatment option(s) involves balancing the potential benefits derived in relation to the achievement of the objectives against costs, effort or disadvantages of implementation.<br>Risk treatment options are not necessarily mutually exclusive or appropriate in all circumstances.<br>Options for treating risk may involve one or more of the following:<br>— *avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;*<br>— *taking or increasing the risk in order to pursue an opportunity;*<br>— *removing the risk source;*<br>— *changing the likelihood;*<br>— *changing the consequences;*<br>— *sharing the risk (e.g. through contracts, buying insurance);*<br>— *retaining the risk by informed decision.*<br>Justification for risk treatment is broader than solely economic considerations and should take into account all of the organization’s obligations, voluntary commitments and stakeholder views. The selection of risk treatment options should be made in accordance with the organization’s objectives, risk criteria and available resources.<br>When selecting risk treatment options, the organization should consider the values, perceptions and potential involvement of stakeholders and the most appropriate ways to communicate and consult with them. Though equally | | |

| | | |
|---|---|---|
| effective, some risk treatments can be more acceptable to some stakeholders than to others.<br>Risk treatments, even if carefully designed and implemented might not produce the expected outcomes and could produce unintended consequences. Monitoring and review need to be an integral part of the<br>risk treatment implementation to give assurance that the different forms of treatment become and remain effective.<br>Risk treatment can also introduce new risks that need to be managed. | | |
| **6.5.3 Preparing and implementing risk treatment plans**<br>The purpose of risk treatment plans is to specify how the chosen treatment options will be implemented, so that arrangements are understood by those involved, and progress against the plan can be monitored. The treatment plan should clearly identify the order in which risk treatment should be implemented.<br>Treatment plans should be integrated into the management plans and processes of the organization, in consultation with appropriate stakeholders.<br><br>The information provided in the treatment plan should include:<br>— *the rationale for selection of the treatment options, including the expected benefits to be gained;*<br>— *those who are accountable and responsible for approving and implementing the plan;*<br>— *the proposed actions;*<br>— *the resources required, including contingencies;*<br>— *the performance measures;*<br>— *the constraints;*<br>— *the required reporting and monitoring;*<br>— *when actions are expected to be undertaken and completed.* | | |
| **6.6 Monitoring and review** | | |
| **6.7 Recording and reporting** | | |