

Interpretation document

Monitoring and Alarm Receiving Centers & Alarm Transmission Service Providers



Approved by the Board of Experts Security

06-06-2024

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

Tel. +31 88 998 51 00
NL.info.fss@kiwa.com
www.kiwafss.nl

© 2024 Kiwa N.V.

All rights reserved. No part of this document may be reproduced, stored in a database or retrieval system, or published, in any form or in any way, electronically, mechanically, by print, photoprint, microfilm or any other means without prior written permission from the publisher

kiwa

**Trust
Quality
Progress**



Contents

1	Introduction	4
1.1	Security alarm chain	4
2	Categories and scopes “G”	7
2.1	Referenced standards per scope	8
2.2	Monitoring of interconnections by the Monitoring Centre (MC)	8
2.3	The location of data processing equipment	9
3	Business Continuity of a (M)ARC “R”	11
3.1	A standalone (M)ARC without BC possibilities	11
3.2	Satellite (M)ARC	11
3.3	Twin (M)ARC	11
3.4	A standalone ARC with BC possibilities	12
3.5	An ARC with external IT infrastructure	12
3.6	Back-up (M)ARC	12
4	Statistics of a MARC “G and R”	14
4.1	Example message handling - G	14
4.2	Best practice for complying with the performance criteria of message handling - G	15
4.3	Listing of priorities for response times - R	16
4.4	Monitoring of interconnections (Monitoring Centre) - G	16
4.5	Lean ATSP - G	17
5	Construction/system requirements “R”	20
5.1	General	20
5.2	Resistance against physical attack - R	20
5.3	Glazed areas - R	20
5.4	Resistance against fire and smoke (construction) - R	20
5.4.1	Resistance against fire and smoke (service inlets and outlets)	20
5.5	Protection against the effect of lightning - R	21
5.6	Entrance lobby - R	21
5.7	Ventilation inlet & outlet openings - R	21
5.8	Alarm systems of the ARC – R	22
5.9	Alarm transmission – R	22
5.10	Fire detection system - R	22
6	Operation of the (M)ARC	23
6.1	General	23
6.2	Daily tests - G	23
6.3	Communications - R	23
6.4	Power supplies - R	23
6.5	Access policy - G	23



6.6	Alarm verification - G	23
7	Management system of the (M)ARC	24
7.1	General	24
7.2	ICT-security - G	24
7.3	Mapping ISO 27001 Annex A controls with EN 50518 – R	25
7.4	Cross reference ISO 9001 to ISO/IEC 27001 and EN 50518 – G	27
7.5	Business Continuity - G	28
8	Alarm Transmission Service Provider	29
8.1	General - G	29
8.2	K21030 Alarm Transmission Systems - Alarm Transmission Service Providers - G	29
8.2.1	Scope 1	30
8.2.2	Scope 2	30
8.2.3	Scope 3	30
8.2.4	Scope 4	30
9	VSS Control Room	31
9.1	Chapter 12 - Control room configuration - G	31
9.2	Connecting VSS to a VSS control room - G	31
9.2.1	Chapter 4 - General considerations - G	31
9.2.2	Chapter 5 - Operational requirements specifications - G	31
9.3	VSS control room assessment - R	32
10	Guidance op remote access/apps en portals	33
10.1	Remote access and the risks	33
10.2	Apps, appserver, webserver and webportals	34
10.3	Guidance action plan remote access	36
	Annex 1: Matrix penetration seals - G	37
	Annex 2: Mapping matrix EN50518 and relevant standards with additional services - G	41

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



1 Introduction

This interpretation document applies to the international standards for Inspection & Certification of EN 50518 Monitoring and Alarm Receiving Centers (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 are following the developments. This "Interpretation document" embodies the technological and market developments. The purpose of this document is to clarify the context by drawing up new definitions on certain themes and subjects. This clarifies to persons and market parties what the preconditions are when determining compliance with the applicable requirements. It also explains developments that play at the level of standards and how they fit the developments in the market and are in line with legislation and regulations.

This interpretation document has been drafted to set two goals:

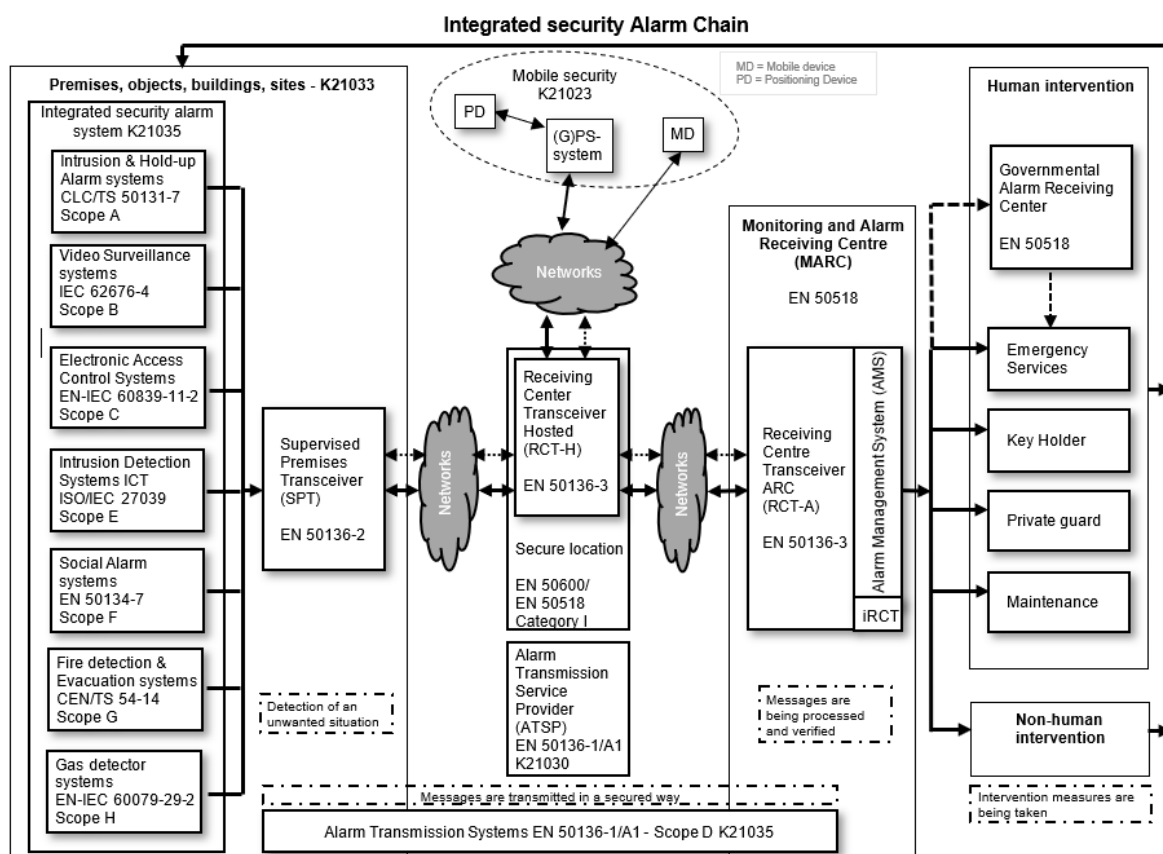
- To give guidance in the context for the design, installation and operation of systems and is marked with the letter "G";
- To give additional or alternative requirements on matters no clear defined in the standards or where the standards have not yet addressed the issue or development and is marked with the letter "R".

1.1 Security alarm chain

On the next page the integrated security alarm chain as seen by Kiwa FSS is drawn. 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.



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				
<u>Installer</u>		<u>Alarm Transmission Service Provider</u>		<u>Monitoring and Alarm Receiving Centre</u>
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



2 Categories and scopes “G”

Most countries in Europe set requirements for the operation of Alarm Receiving Centers (ARC). Almost all of these countries direct to the standard EN 50518 for 'Monitoring & Alarm Receiving Centers'. The first version of this European standard is made in 2010 and right now the EN 50518 has come to its third version.

As of August 2019 the third version of the standard EN 50518 is introduced. This will replace the EN 50518 parts 1, 2 and 3 from 2013. New Monitoring Alarm and Receiving Centers will be assessed at the new standard from 2019-6-2 on. Current (M)ARC's have to comply with the new standard at 2022-6-2 at the latest.

The standard EN 50518 requires certification under accreditation in the 2013 and 2019 version. This means that if the requirement is set to fulfill this standard, certification under accreditation is obligatory. The accreditation that applies to EN 50518 is the EN-ISO / IEC 17065. This accreditation standard states in art. 3.10 'scope of certification'. This requirement determines that certification bodies must clearly define for which products, processes or services the certification applies. This is reflected in the certification agreement, in the audit report and on the certificate.

Certification for EN 50518 is based on the standard with its requirements for the construction elements, systems and processes of an ARC. Besides that, EN 50518 offers multiple scopes for handling different kind of messages. These messages are split in two categories:

- Category I: ARC's handling messages from security applications
- Category II: ARC's handling messages from non-security applications

The EN 50518 specifies which kind of messages belong to which category. The complete overview of the scopes mentioned per category is detailed below. The second column links the scope to the applicable standard which is mentioned in EN 50518. Where no standard is mentioned, the Board of Experts has directed to a specification. The scopes which are carried out by the (M)ARC will be mentioned on their certificate.

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 2 Scopes and categories EN 50518

2.1 Referenced standards per scope

ARC's used to be mainly equipped to handle messages from Intrusion & Hold-up Alarm systems. Over the years the ARC's are able to handle all kind of messages which the EN 50518:2019 recognizes with its categories and scopes. To organise a good handling of all these different kind of scopes, the EN 50518 references to other European Standards for the handling of messages. Examples are:

The standard TS 50131-7 "Alarm systems - Intrusion and hold-up systems - Part 7: Application guidelines" gives direction to the design, installation and commission process of alarm systems.

The standard CEN/TS 54-14* gives direction for Fire detection and fire alarm systems - Part 14: Guidelines for planning, design, installation, commissioning, use and maintenance. Be aware that the standard EN54-2 for Fire detection and fire alarm systems - Part 2: Control and indicating equipment & connecting standards for components are mandatory to use according to the Construction Products Regulation (CPR) Regulation (EU) No 305/2011.

*The scope EN 54-14 only applies when there is a fully certified installation at the premises. This scope could also apply to residences on a lower level with smoke detectors based on EN 14604. This connection and handling process is then assessed in EN 50518 article 9.1.5. Smoke detectors based on EN 14604 are required.

Not all clauses of the referenced standards are applicable. Annex 2 contains the 'Matrix EN 50518 and relevant standards with additional services'. This matrix presents the applicable clauses of the referenced standards. When applicable, the ARC could supply the market with a broader portfolio of security services. By implementing these standards, the ARC is able to address international needs in the market for security services with a high business continuity and a 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 Centers' (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.

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 (M)ARC which complies 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

The interpretation of Kiwa is a verification of the remote location for data processing equipment according to the scope of certification as mentioned on the product-certificate EN 50518. This product certificate including its scopes is issued under accreditation by a IAF MLA accreditation body.

The assessment for a remote location for data processing equipment is based on the main principles for EN 50600 availability class 3 and protection class 4, but focusses on the demarcated area of the (M)ARC in context with EN 50518. In this way Kiwa verifies that the data centre is designed and maintained according to EN 50600.

Subject of the assessment is:

- Access control of the data centre and the applicable server room / server suite within the data centre,
- Cooling system,
- Redundancy principles onsite,
- Separation of power and data lines,
- (Emergency) power supplies,
- Fire detection- & fire suppression system,
- Fire resistance compartments,
- Intrusion and camera surveillance system.

The above paragraph describes a situation where all data processing equipment is managed by the (M)ARC itself within the secure location.



More and more Kiwa encounters situations where also other forms of cloud computing are used. To establish whether cloud computing is within the meaning of the standard, there must also be insight in the specifications of the cloud computing platform and geographical location(s). 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 are located in a remote location. In case also the Alarm Management System is located in a remote location, the certification scheme K21046 Hosted Alarm Solution applies. This to implement a certified and secure way of placing the AMS in 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);



* Temporary

Moving to a location to continue services can only be temporary. Plans to achieve this should always be justified in the risk analysis and detailed in a DRP and/or BCP. To make temporariness transparent and measurable, the following criteria have been established.

Time frame	Action
< 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. 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. 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 ‘alive signals’:
 - o from the Supervised Premises Transceiver (SPT) at the site of the Alarm System (AS) or
 - o 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 coming in and extra operators are needed)

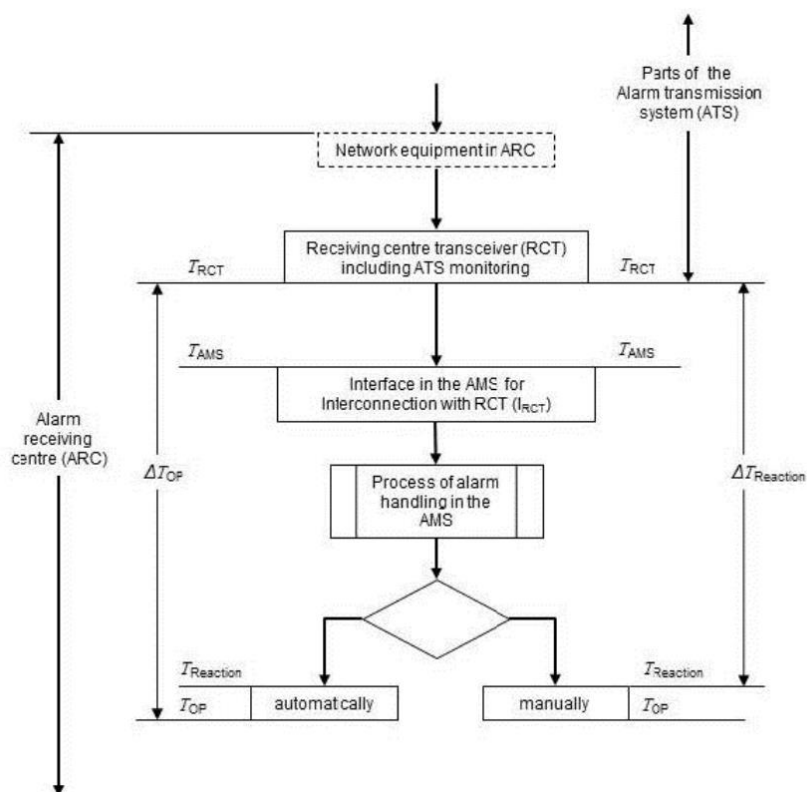


Figure 3

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



For having the right statistics, the information of the RCT, which is putting its alarms through towards the AMS, is needed.

Δ TOP; time elapsing between the moment of availability of the alarm message at the output of the RCT and the time of first action initiated by the ARC operator or the AMS (Δ TOP = TOP - TRCT).

For an ARC it is important to know:

- How many alarms are in a cue entering the MARC.
- How fast are these alarms acknowledged by the AMS. The acceptance can be done by an operator getting the alarm on its monitor. The handling time to complete the alarm by the operator is not relevant for this statistic / KPI.

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

In order to be sure to meet the priority 1 KPI for hold-up, fire, fixed firefighting systems, people monitoring and for other alarms agreed to be of highest priority level conditions: 30 s for 80 % of signals received and 60 s for 98,5 % of signals received.

Most MARC's are using a threshold of 15 until 25 seconds to comply with the performance criteria. This allows them to operate within the KPI. The threshold of 15 seconds gives the most security.

An example. A MARC daily handles 100 alarms with priority 1. The standard asks for a conformance to above criteria that shall be achieved over a rolling twelve-month period. This leads to the following criteria within a period of 30 days;

Number of prio 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 prio 1 alarms per week	80% within 30 seconds	98,5% within 60 seconds	1,5% above 60 seconds
700	560	129	11 alarms
Number of prio 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 3 Number of priority 1 alarms

If the ARC has a bad day in performing because a lot of alarms are sent to the MARC due to faults in the AS, and for example 19 alarms with priority 1 are above 60 seconds, the ARC does not meet its KPI.

In the example of a week this can lead to the next example. If 601 alarms with priority 1 are handled within a week above 30 seconds, the ARC does not meet its KPI.

The 1,5% that is allowed to be above 60 seconds is the base for further research by the ARC to improve the KPI's of their services.



4.3 Listing of priorities for response times - R

Below a table is given to clarify on EN 50518 chapter 9.2. Priority 1, 2 and individual services are mentioned. Also the possibility for automatic alarm handling and delay are added for each alarm condition/message.

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 for other alarms agreed to be of highest priority level conditions: 30 s for 80 % of alarms received and 60 s for 98,5 % of alarms received;	No No No No No Yes	No No No No No Yes/No	Hold-up Fire detection systems Firefighting systems People monitoring Social – life critical Other according to client contract
2	all other alarm conditions: 90 s for 80 % of alarms received and 180 s for 98,5 % of alarms received.	Yes Yes Yes No No Yes	Yes Yes Yes Yes Yes Yes	Burglar Video - detection Social – non life critical Tamper Double ATP failure Other according to client contract
#	Individual services by client contract EN 50518 9.1.5	Yes Yes Yes Yes Yes Yes	Yes Yes Yes Yes Yes Yes	Video Access Traffic Lift Failures also ATP Signals also technical

Table 4

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 Alarm Transmission Service Provider (ATSP). The ATSP may execute the monitoring itself or delegate it to a Monitoring Centre according to EN 50518. If the ATSP executes the monitoring itself, it should also comply with EN 50518. For more information about ATSPs, also see chapter 8.

A Monitoring Centre (MC) may be a separate centre on its own, or part of an ARC. The origin of performance monitoring is the mandatory requirement in EN 50136-1. The tasks of a Monitoring Centre are reporting and logging of faults and availability. These tasks should be undertaken for the purpose of maintaining the required performance level for each ATS of the appropriate category. The purpose of performance monitoring is to quickly identify ATS(s) that do not meet the agreed performance for the appropriate category.

It is for this reason that a MC/ATSP should continuously monitor the important performance parameters, e.g. transmission delays, faults and availability. When a fault is identified the MC/ATSP should take an action to repair the fault and restore the ATS to its fully operational state to prevent the ATS and/or ATSN from not meeting the required average delays 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 when that ARC is also the ATSP and/or MC.

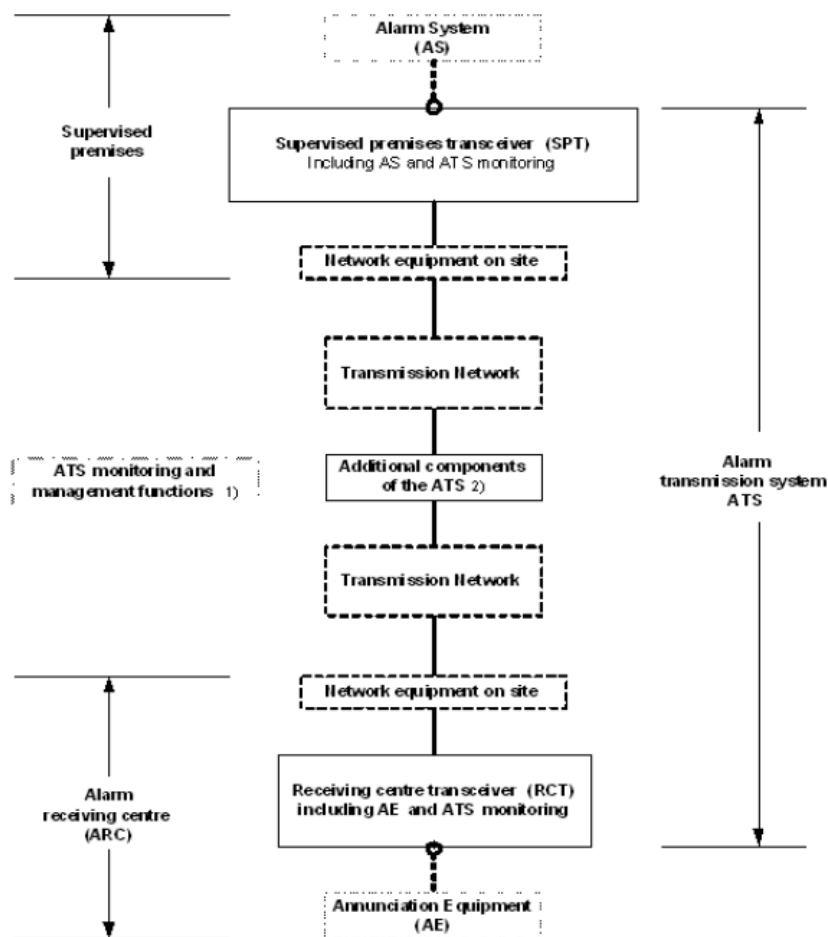


Figure 4

4.5 Lean ATSP - G

EN 50136-1/A1 specifies requirements for alarm transmission systems and monitoring of these systems in conjunction with EN 50518. The authority having jurisdiction for this are: law enforcement and insurance parties. They require a monitored alarm transmission based on the verification of performance.

EN 50136-1, -2 and -3 together with EN 50518 set requirements about this process of monitoring. In this process the Monitoring and Alarm Receiving Centre (MARC) can handle the function of Monitoring Centre (MC). We see that the MARC's are struggling with this process of fulfilling the role as MC. The purpose of Lean ATSP is to help these struggling MARC's.

The receiver according EN 50136-3 acquires the data needed to fulfill the role for dual path transmissions. The MARC needs to have standard action patterns how to behave with failing connections.

Definitions:

Polling

A common method used to monitor Alarm Transmission Paths (ATP) and/or ATS availability where the term polling means regular status message exchanges between an SPT and RCT. (EN 50136-7)



Reporting time

Period from the time a fault occurs in the ATS until the fault information is reported to the RCT, the Alarm system at the supervised premises or the Monitoring Centre transceiver (if provided) (EN 50136-1/A1)

So polling and reporting time are not the same! For more information see standard EN 50136-7.

	DP4
Primary ATP Reporting Time	90 seconds
Alternative ATP Maximum period when primary operational	5 hours
Alternative ATP Maximum period when primary failed	90 seconds
Failure of all ATP's at the same time*	3 minutes
*Where an ATS includes two or more ATPs the reporting time shall meet the requirements of this table	

Table 5 Maximum reporting time DP4

Where an ATS remains operational a single path line fault shall be presented to the ATSP, but can be delayed presenting it to the AMS where it is agreed between interested parties. The maximum delay shall not exceed 96 h.

With the information above, a suggestion for a standard action patron has been made below. The goal of this setup is to automate as much as possible in the process.

Other categories are left out of scope for this proposal.

DP 4	90 seconds EN 50136-1/A1	30 minutes after RT EN 50518	25 hours after RT EN 50518	1 week after RT EN 50518
Primary failure	Reporting time (RT)	Automatic e-mail/SMS	Automatic e-mail/SMS	Phone call
DP4	5 hours EN 50136-1/A1	30 minutes after RT EN 50518	5 hours after RT EN 50518	1 week after RT EN 50518
Alternative failure When primary is failed, alternative reporting time is 90 seconds.	Reporting time (RT)	Automatic e-mail/SMS	Automatic e-mail/SMS	Phone call
DP 4	3 minutes EN 50136-1/A1	90 seconds after RT EN 50518		
ATS failure	Reporting time (RT)	Automatic e-mail/SMS <u>and</u> a phone call		
When implementing this table to your Monitoring Centre, make sure that it is agreed between interested parties				
An automatic email / SMS is an example of a redundant form of communication towards the user / client. Other effective forms are also possible.				
All times mentioned in this table are the maximum times.				

Table 6 Lean ATSP DP4



The tables above in writing:

DP4

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 failing connection.
- When not fixed after 25 hours an automatic email / SMS* is sent to the client regarding this failing connection.
- When not fixed after 1 week a phone call to the client regarding this failing connection and that the client is fulfilling the requirements of reliable alarm transmission because the backup situation is not functioning.

Alternative path has a falling connection;

- Reporting time is 5 hours. After 30 minutes an automatic email / SMS* is sent to the client regarding this failing connection.
- When not fixed after 5 hours an automatic email / SMS* is sent to the client regarding this failing connection.
- When not fixed after 1 week a phone call to the client regarding this failing connection and that the client is fulfilling the requirements of reliable alarm transmission because the backup situation is not functioning.

Both primary and alternative path 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 to the client regarding this failing connection and that the client is fulfilling the requirements and that there is the possibility of a hostile attack on the connections and supervised premises.

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



5 Construction/system requirements “R”

5.1 General

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

5.2 Resistance against physical attack - R

- When a (M)ARC does not have test reports, production specifications and/or building drawings, destructive research must be carried out to gain compliance with the standard.
- This also applies to Sand-lime-brick 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, we assume that it is also sufficient fire resistant. In the event of close adjacent buildings, the fire resistance has more 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 attack also applies to a physical attack. Not in reverse.
- 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 shell to the inside of the shell and not in reverse.
 - Resistance against fire and smoke is depending on national regulations.
 - The shell of the ARC shall have a 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 services” with a minimum of 30 minutes. The standard mentions the following fire scenario's:
 - o The standard temperature/time curve (post flash-over fire);
 - o The slow heating curve (smouldering fire);
 - o The ‘semi-natural’ fire;
 - o The external fire exposure curve;
 - o Constant temperature attack.
 - The minimal requirement that is applicable is E – Integrity for the wall, ceiling, floor and doors.
 - National building regulations or the design of the building can obtain more performance characteristics such as
 - o R - Loadbearing capacity,
 - o I – Insulation,
 - o W – Radiation, etc.
- Do not forget to check them with the architect and/or local building authorities.
- Reinforced concrete of minimal 10 cm shall fulfil this E30 characteristic and is mentioned to fulfill the minimum resistance against physical attack for ARC.

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;
 - o 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 (1×10^{-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 be 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 (M)ARC

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 automatized 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 Access 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 Management system of the (M)ARC

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.

7.2 ICT-security - G

Applicable paragraphs EN 50518:2019

Clause	Subject	Short reference
8.2	Time synchronization of equipment	Time synchronization is required. As well as fault logs and reporting.
9.1.1	Procedures – General	Documented SOP's and KPI's required.
9.1.3	Message Handling	Statistics shall be made and analysed. For both manual and automatic messages.
9.1.7	Unexpected increase in alarms	How will the MARC deal with this?
9.1.8	Alarm transmission path failures	Alarm transmission path faults from the MARC should be signalled in the MARC.
9.1.9	Controls to maintain quality of service	How is the MARC able to 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 regularly tested
9.1.12	Fault procedures and reporting	Reporting is needed when equipment or software fails.
9.1.13	Information management	Procedure for the secure handling of information needed.
9.1.14	Data back-up	Back-up procedure needed. When are the back-ups carried out and when are they tested?
9.1.15	Confidentiality and classification of information	Authorisation matrix is needed. Labelling information and a clear desk policy
9.1.16	Relationships with essentials suppliers	Suppliers must be screened and agreements must be made about data
9.1.18	Physical Access	The access to the ARC and critical components must be restricted. An authorisation matrix must be shown.
9.1.19	Remote access	If remote access is used, this 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 energy are separate. AMS is a separate system with redundant cabling and separate cable run. (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 carried out?
10.4	Risk and contingency management	The management of IT systems as well as IT security must be organized. (See under requirements regarding ICT security) In addition, the requirements as set with regard to GDPR must be met.
10.4	Information management	See normative annex A of ISO 27001

Table 7



7.3 Mapping ISO 27001 Annex A controls with EN 50518 – R

The table below is a mapping of the controls of ISO 27001 Annex A with the requirements mentioned 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 in addition during the audit.

	Normative annex A of ISO/IEC27001:2013/2017 mapping with EN 50518	EN 50518
5	Information security policies	
5.1	<u>Management direction for information security</u> <i>Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.</i>	10.4 & 9.1
6	Organization of information security	
6.1	<u>Internal organization</u> <i>Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organization</i>	10.4 & 9.1
6.2	<u>Mobile devices and teleworking</u> <i>Objective: To ensure the security of teleworking and use of mobile devices</i>	N/A
7	Human resource security	
7.1	<u>Prior to employment</u> <i>Objective: To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered</i>	10.4 & 9.1 & 10.5
7.2	<u>During employment</u> <i>Objective: To ensure that employees and contractors are aware of and fulfill their information security responsibilities</i>	10.4 & 9.1
7.3	<u>Termination and change of employment</u> <i>Objective: To protect the organization's interests as part of the process of changing or terminating employment</i>	10.4 & 9.1
8	Asset management	
8.1	<u>Responsibility for assets</u> <i>Objective: To identify organizational assets and define appropriate protection responsibilities</i>	10.4 & 9.1
8.2	<u>Information classification</u> <i>Objective: To ensure that information receives an appropriate level of protection in accordance with its importance to the organization</i>	10.4 & 9.1
8.3	<u>Media handling</u> <i>Objective: To prevent unauthorized disclosure, modification, removal or destruction of information stored on media</i>	10.4 & 9.1
9	Access control	
9.1	<u>Business requirements of access control</u> <i>Objective: To limit access to information and information processing facilities</i>	10.4 & 9.1
9.2	<u>User access management</u> <i>Objective: To ensure authorized user access and to prevent unauthorized access to systems and services</i>	10.4 & 9.1
9.3	<u>User responsibilities</u> <i>Objective: To make users accountable for safeguarding their authentication information</i>	10.4 & 9.1
9.4	<u>System and application access control</u> <i>Objective: To prevent unauthorized access to systems and applications</i>	10.4 & 9.1
10	Cryptography	
10.1	<u>Cryptographic controls</u> <i>Objective: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information</i>	Additional
11	Physical and environmental security	
11.1	<u>Secure areas</u> <i>Objective: To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities</i>	5 & 6
11.2	<u>Equipment</u> <i>Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations</i>	5 & 6
12	Operations security	
12.1	<u>Operational procedures and responsibilities</u> <i>Objective: To ensure correct and secure operations of information processing facilities</i>	10.4 & 9.1
12.2	<u>Protection from malware</u>	Additional



	<i>Objective: To ensure that information and information processing facilities are protected against malware</i>	
12.3	<u>Backup</u> <i>Objective: To protect against loss of data</i>	10.4 & 9.1
12.4	<u>Logging and monitoring</u> <i>Objective: To record events and generate evidence</i>	10.4 & 9.1
12.5	<u>Control of operational software</u> <i>Objective: To ensure the integrity of operational systems</i>	Additional
12.6	<u>Technical vulnerability management</u> <i>Objective: To prevent exploitation of technical vulnerabilities</i>	Additional
12.7	<u>Information systems audit considerations</u> <i>Objective: To minimise the impact of audit activities on operational systems</i>	N/A
13	Communications security	
13.1	<u>Network security management</u> <i>Objective: To ensure the protection of information in networks and its supporting information processing facilities</i>	10.4 & 9.1 & 5 & 6
13.2	<u>Information transfer</u> <i>Objective: To maintain the security of information transferred within an organization and with any external entity</i>	Additional
14	System acquisition, development and maintenance	
14.1	<u>Security requirements of information systems</u> <i>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</i>	N/A
14.2	<u>Security in development and support processes</u> <i>Objective: To ensure that information security is designed and implemented within the development lifecycle of information systems</i>	N/A
14.3	<u>Test data</u> <i>Objective: To ensure the protection of data used for testing</i>	N/A
15	Supplier relationships	
15.1	<u>Information security in supplier relationships</u> <i>Objective: To ensure protection of the organization's assets that is accessible by suppliers</i>	10.4 & 9.1
15.2	<u>Supplier service delivery management</u> <i>Objective: To maintain an agreed level of information security and service delivery in line with supplier agreements</i>	10.4 & 9.1
16	Information security incident management	
16.1	<u>Management of information security incidents and improvements</u> <i>Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses</i>	Additional
17	Information security aspects of business continuity management	
17.1	<u>Information security continuity</u> <i>Objective: Information security continuity shall be embedded in the organization's business continuity management systems</i>	10.4 & 9.1
17.2	<u>Redundancies</u> <i>Objective: To ensure availability of information processing facilities</i>	10.4 & 9.1
18	Compliance	
18.1	<u>Compliance with legal and contractual requirements</u> <i>Objective: To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements</i>	10.4
18.2	<u>Information security reviews</u> <i>Objective: To ensure that information security is implemented and operated in accordance with the organizational policies and procedures</i>	10.4 & 9.1

Table 8.

This matrix brings the different standards in place in relation to service processes delivered by the alarm receiving centre to its customers. To archive the processes in a secure operation the standards for managing the business and ICT – risks are set on left site of the matrix. The correlation in the matrix gives an overview in overlapping and additional requirements between the different standards and scopes. The process shall fulfil the requirements of “A.14.2 Security in development and support processes” of ISO 27001 or the IEC 62443-4-1.



7.4 Cross reference 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 10.2 Governance and Strategy 10.3 Legal and operational set-up
6. Planning - Actions to address risks and opportunities - Quality objectives and planning to achieve them - Planning of changes	6. Planning - Actions to address risks and opportunities - Quality objectives and planning to achieve them	Planning 4.1. Categorization 4.2. Site selection 10.4 Management System. - Risk and Contingency Management. - Information Management. - Complaint Handling. - Management of the Services Portfolio. - Management of Staffing. - Client Management. - Business Partner Management.
7. Support - Resources - Competence - Awareness - Communication	7. Support - Resources - Competence - Awareness - Communication	Support – Resources & Competence 5. Construction 6. Alarm systems of the ARC 7. Electrical power supplies 10.5.1. Staffing 10.5.2. Security screening and vetting 10.6 Training
8. Operation - Quality planning and control - Requirements for products and services - Design and development of products and services - Control of externally provided processes, products and services - Production and services provision - Release of products and services - Control of nonconforming outputs	8. Operation - Operational planning and control - Information security risk assessment - Information security risk treatment	Operation 8. Alarm Management System 9. Operation of the ARC 9.1 Procedures 1. General 2. Creation, modification & cancelation 3. Message handling 4. Communication with response services 5. Individual services provided by the ARC 6. Alarm verification 7. Unexpected increase in alarm signals 8. Alarm transmission path failures 10. Installation, maintenance, protection, removal and reuse of assets under the control of the ARC 11. Monitoring & testing of equipment 12. Fault procedures and reporting 13. Information management 14. Data back-up 15. Confidentiality and classification of information 16. Relationships with essential suppliers 17. Administrative procedures 18. Physical access 19. Remote access



		20. Operational continuity and emergencies 21. Emergency evacuation and re-entry 22. Emergency entry
9. Performance evaluation - Monitoring , measurement , analyses & evaluation - Internal audit - Management review	9. Performance evaluation - Monitoring , measurement , analyses & evaluation - Internal audit - Management review	9.2 Performance criteria – message handling 9.1.9 . Controls to maintain QoS 9.1.23 KPI
10. Improvement	10. Improvement	

Table 9

7.5 Business Continuity - G

The following clauses relate to business continuity of a MARC.

Clause	Subject
5.9.1	Communication cables
9.1.9	Controls to maintain quality of service
9.1.16	Relationships with essential suppliers
9.1.20	Operational continuity and emergencies
9.1.23	Key performance indicators
9.2	Performance criteria: Message handling
10.2	Governance and strategy
10.4	Management system

Table 10



8 Alarm Transmission Service Provider

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.

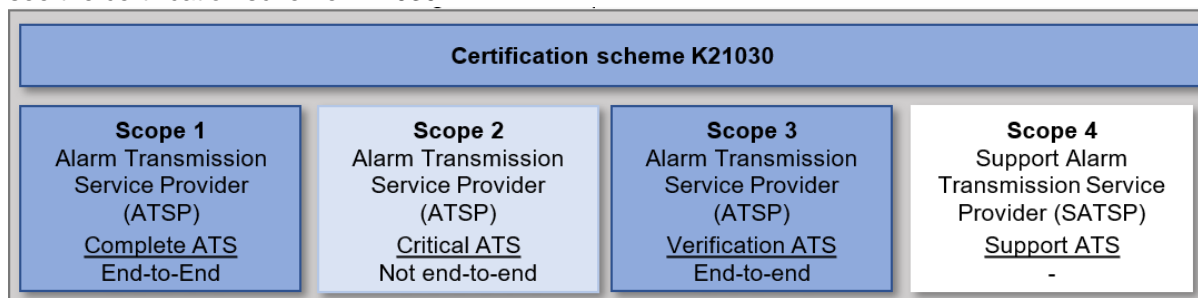
The table below shows relevancy between the standards to be noticed in the execution.

EN 50136-1/A1	TS 50136-9	EN 50518:2019
5 General requirements		
6 System requirements	4 Objective 5 Messaging 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 10.4 Compliant handling 10.4 Compliance audit 10.5 Staffing

Table 11 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.





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) from 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

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 op remote access/apps en portals

10.1 Remote access and the risks

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. This allowed the hacker to gain unauthorised access to the company's internal systems, including the XYZ.

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

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 authorized 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 action plan remote access

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 XYZ 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.


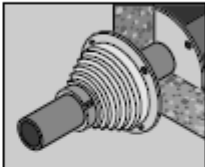
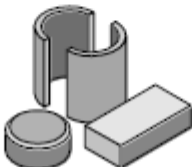
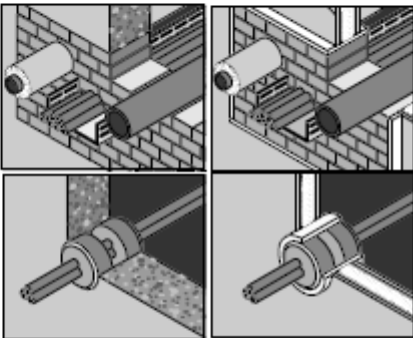
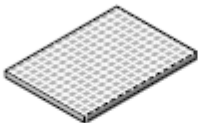
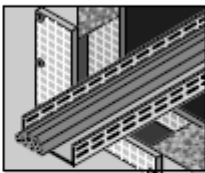
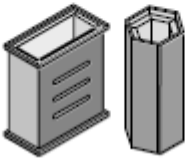
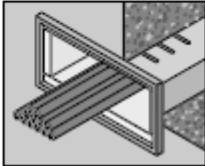
Penetration - Number					
Location	Location identification from the penetration seal on a map.				
Photo's	<table border="1" style="width: 100%;"> <tr> <td style="width: 50%; text-align: center;">Before application</td> <td style="width: 50%; text-align: center;">After application</td> </tr> <tr> <td style="background-color: #e0e0ff;"></td> <td style="background-color: #e0e0ff;"></td> </tr> </table>	Before application	After application		
Before application	After 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.

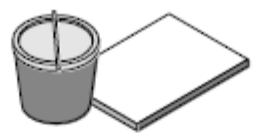
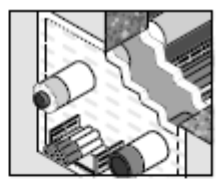
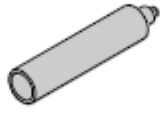
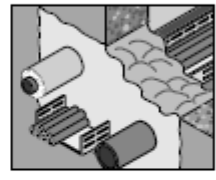

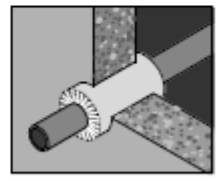

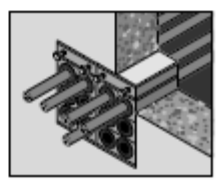
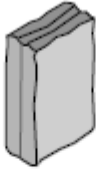
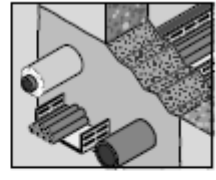
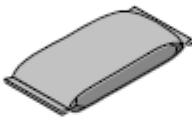
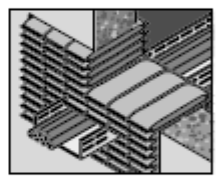

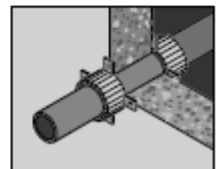
It is also important that the applicator is educated in context of the used products. The registration of the education should also be supplied.

Table 1.1 ETAG 26-2

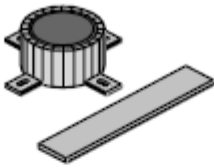
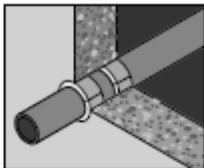

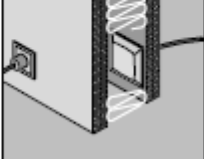
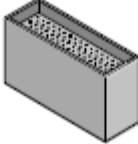
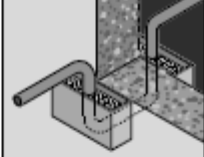

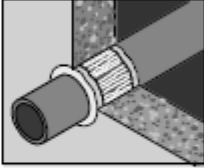
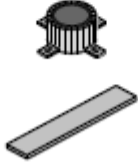
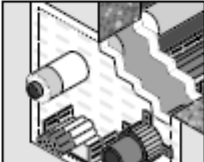


Designation	Illustration ¹ of the	
	product/component	penetration seal
Bellows seals		
Blocks, plugs		
Boards		
Cable boxes		



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		
<ul style="list-style-type: none">• Collars (integrated into or outside the wall / floor)		



<ul style="list-style-type: none"> Wraps (integrated into a wall or floor) including strips and composite strips 		
<ul style="list-style-type: none"> 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 4. Site selection							
Paragraph	Support – Resources & Competence 5. Construction 6. Alarm systems of the ARC 7. Electrical power supplies 4. Staffing	12 VSS control room configuration 12.1 Control rooms 12.2 Number, size and positioning of VSS video displays 12.3 Displays and screens mounted on or off the workstation 12.4 Recommended display sizes 12.5 Number of camera images per operator 12.6 Number of work stations 12.7 Equipment siting 12.8 Backup power supply provision 12.10 Lightning and surge protection		6 Product requirements 7 Requirements quality system	5 Requirements quality system	13 Sub-contract delivery of services 14 Staffing		
Paragraph	Operation 2013 P2: 4. Performance requirements P2: 5. Communication requirements P2: 6. Reception of signals P2: 7. Testing P2: 8. Data P2: 9. Data storage P2: 10. Availability and verification of performance of the ARC P2: 11. Contingency plan P3: 5. Operating procedures P3: 8. Data	12.9 Operating temperature	10.1 System operation	4 Performance requirements 5 Process requirements	5 Requirements quality system	8 Alarm receiving services 10 Response arrangements 12 Operational records 15 Risk management	6.4 Deployment 7 Operations	6.9 Signals to a fire alarm receiving station 8.2 Commissioning 11.2.2 Prevention of false alarms during routine testing



	2019 8. Alarm management system 9. Operation of the ARC 10. General principles, leadership, governance, management and staffing							
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							

>