Interpretation document

Monitoring and Alarm Receiving Centers & Alarm Transmission Service Providers

Approved by the Board of Experts Security

27/05/2020

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” 10
3.1 A standalone (M)ARC 10
3.2 Satellite (M)ARC 10
3.3 Twin (M)ARC 10
3.4 Back-up (M)ARC 11
4 Statistics of a MARC “G” 12
4.1 Example message handling 12
4.2 Best practice for complying with the performance criteria of message handling 13
4.3 Monitoring of interconnections (Monitoring Centre) 13
4.4 Lean ATSP 14
5 Construction/system requirements 17
5.1 General 17
5.2 Resistance against physical attack - R 17
5.3 Glazed areas - R 17
5.4 Resistance against fire and smoke (construction) - R 17
5.4.1 Resistance against fire and smoke (service inlets and outlets) 17
5.5 Protection against the effect of lightning - R 18
5.6 Entrance lobby - R 18
5.7 Ventilation inlet & outlet openings - R 18
5.8 Alarm systems of the ARC 18
6 Operation of the (M)ARC 19
6.1 General 19
6.2 Daily tests - G 19
6.3 Communications - R 19
6.4 Power supplies - R 19
6.5 Access policy - G 19
6.6 Alarm verification - G 19
7 Management system of the (M)ARC 20
7.1 General 20
7.2 ICT-security - G 20
7.3 Mapping ISO 27001 Annex A controls with EN 50518 - R 21

7.4 Cross reference ISO 9001 to ISO/IEC 27001 and EN 50518 - G 23
7.5 Business Continuity - G 24
8 Alarm Transmission Service Provider 25
8.1 General - G 25
8.2 K21030 Alarm Transmission Systems - Alarm Transmission Service Providers - G 25
8.2.1 Scope 1 26
8.2.2 Scope 2 26
8.2.3 Scope 3 26
8.2.4 Scope 4 26
Annex 1: Matrix penetration seals - G 27
Annex 2: Mapping matrix EN50518 and relevant standards with additional services - G 31

Version History

Version	Change	Date
1	First setup of the document	2020/05/27

1 Introduction

This interpretation document applies to the international standards for Inspection & Certification of EN 505018 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		
Bram van den Bergen	Verisure	MARC / ATSP
Jan Bokma	Kiwa FSS Certification	Certification body
Jurjen Burghgraef	Burghgraef van Tiel & Partners	Risk assessor
Iwan Debets	ASB Security	MARC / ATSP / Supplier
Rene den Dekker	NVD Beveiligingsgroep	MARC
Ronald van Duijn	ENAI	Supplier / ATSP
Mischa van der Geld	Kiwa FSS Certification	Certification body
Rens Krijgsman	Kop Beveiliging	Installer
Sabyne van Mourik	Kiwa FSS Products	Certification body
Fred van Poelgeest	Niefra	Installer
John van Schaik	Addsecure	Supplier
Will Spoor	Europac	MARC
Mathijs de Vaal	Protify	Consulting
Peter Voshol	Kiwa FSS Certification	Certification body

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 market 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 market 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 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.

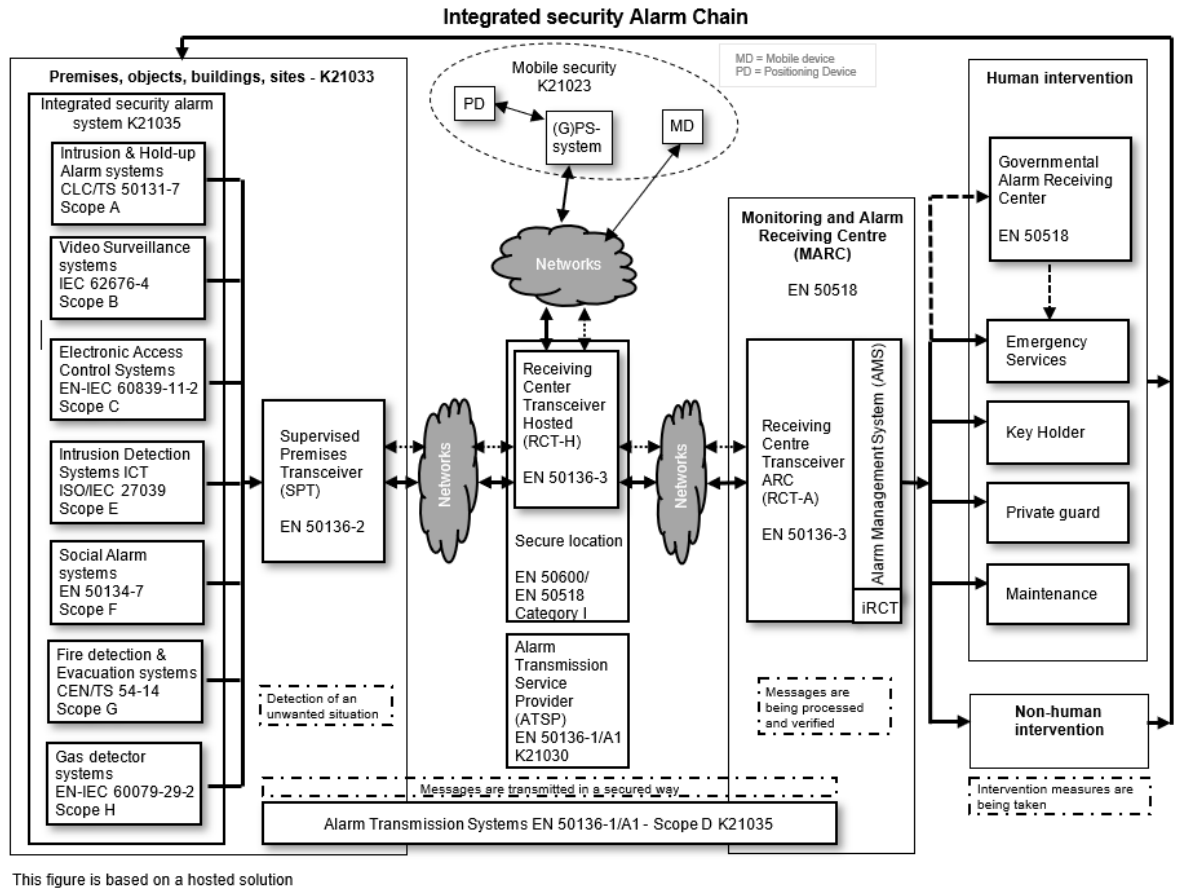


Figure 1

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

Roles defined in the security chain				
Installer		Alarm Transmission Service Provider		Monitoring and Alarm Receiving Centre
Applicable European Standards in the security alarm chain				
EN 50131 / TS54-14 / etc / Alarm systems at the premises or object	⇨	EN 50136-1/A1 Alarm transmission	⇨	EN 50518 Alarm Response by ARC
Assessment by Kiwa based on certification scheme:				
Installer integrated safety/security solutions 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

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.

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
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
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.

Not all clauses of the referenced standards are applicable. Annex 1 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 seen 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.

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 should carry out a risk assessment based on ISO 31000. The use of ISO 27005 is a best practice since the (M)ARC’s of nowadays are IT-minded. In the risk assessment, high availability of the (M)ARC must be considered. This could be done by introducing redundancy for the systems used by the (M)ARC. There are also ARC’s that are complying by working together with one or more ARC’s in their joint infrastructure. Business Continuity of an (M)ARC can furthermore be assessed additionally according to ISO 22301; Societal security - Business continuity management systems – Requirements.

The next paragraphs set some definitions to recognize different solutions of Business Continuity.

3.1 A standalone (M)ARC

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’.

Note: Only one certificate will be issued by the CB for both locations which makes them interdependent.

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).

Note: Two certificates will be issued by the CB.

3.4 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);

4 Statistics of a MARC “G”

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’:
    - from the Supervised Premises Transceiver (SPT) at the site of the Alarm System (AS) or
    - for an Alarm Transmission Service Provider (ATSP) according to EN 50136-1/A1 & certification scheme K21030 as a Monitoring Centre.

4.1 Example message handling

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)

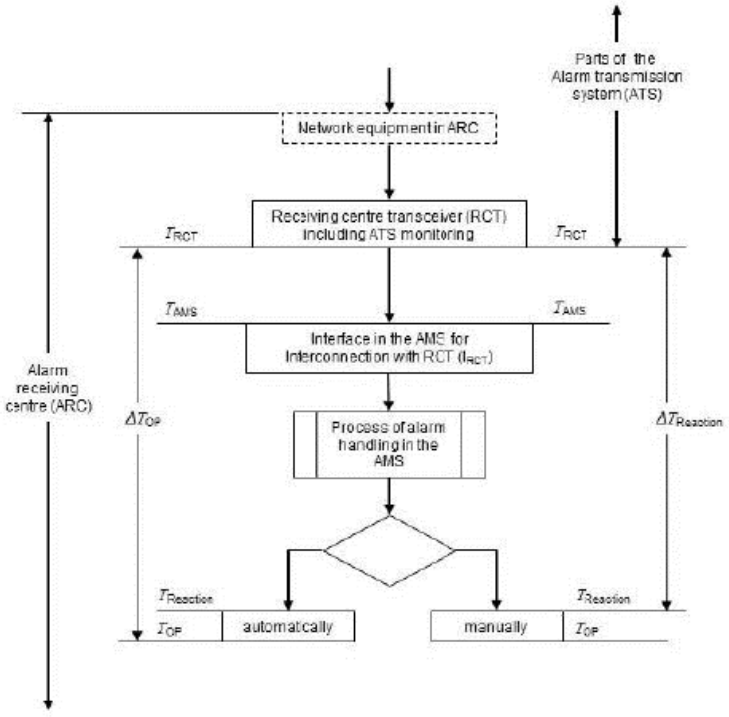


Figure 2

[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.

ΔTOP; 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 (ΔTOP = 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

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 askes 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 Monitoring of interconnections (Monitoring Centre)

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 3 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.

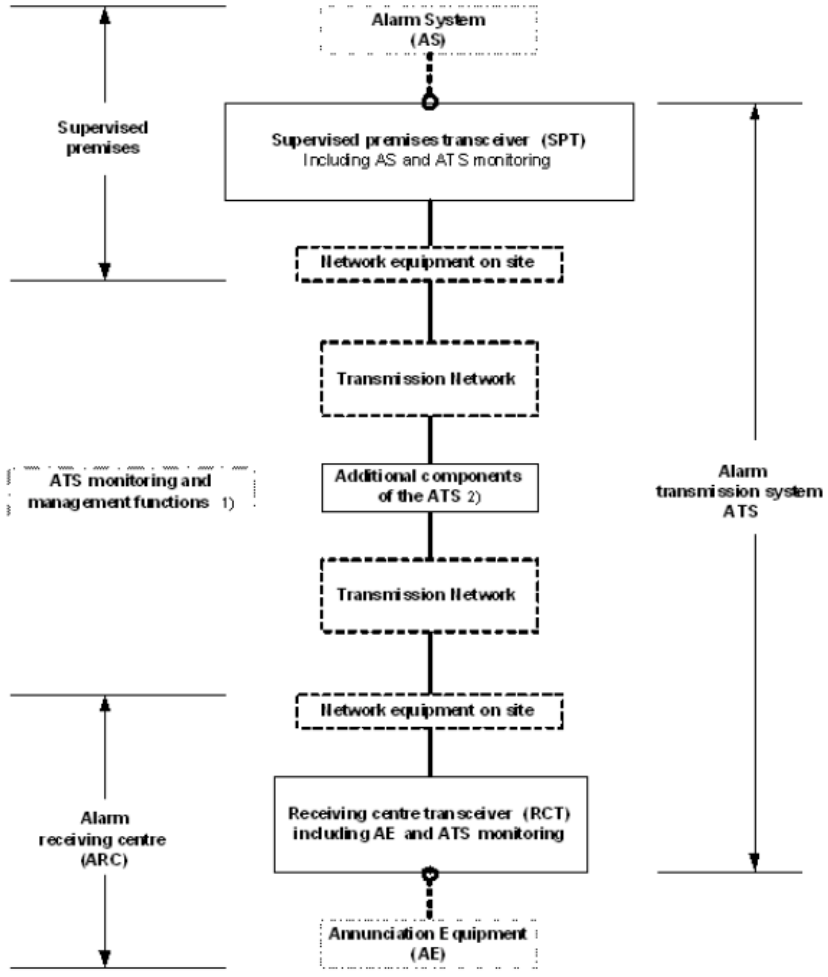


Figure 3

4.4 Lean ATSP

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 an 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 4 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**	**90 seconds after RT**		

	EN 50136-1/A1	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 5 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

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 attacks, bullet attacks 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 form 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:
    - The standard temperature/time curve (post flash-over fire);
    - The slow heating curve (smouldering fire);
    - The 'semi-natural' fire;
    - The external fire exposure curve;
    - 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
    - R - Loadbearing capacity,
    - I – Insulation,
    - 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;
    - 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 the shell of the ARC or on the shell depending 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

A risk assessment should be carried out according to EN 62305-2. If the chance of impact is higher than once every 100 years, protection against lightning must be installed.

Surge protection must be installed if no protection against lightning is installed.

Equipotential bonding must be installed for critical infrastructure.

A UPS should never be considered as a primary surge protection device.

5.6 Entrance lobby - R

- All entrance lobby doors should open outwards seen from 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 there.

5.8 Alarm systems of the ARC

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.

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 automized as possible. When components are duplicated, when only 1 component fails and the MARC keeps running on the other component, the availability is still 100%. Kiwa will verify this availability with reports according to EN 50136-1 for a weekly, monthly and yearly availability.

6.3 Communications - R

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

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

6.4 Power supplies - R

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

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

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

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

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.

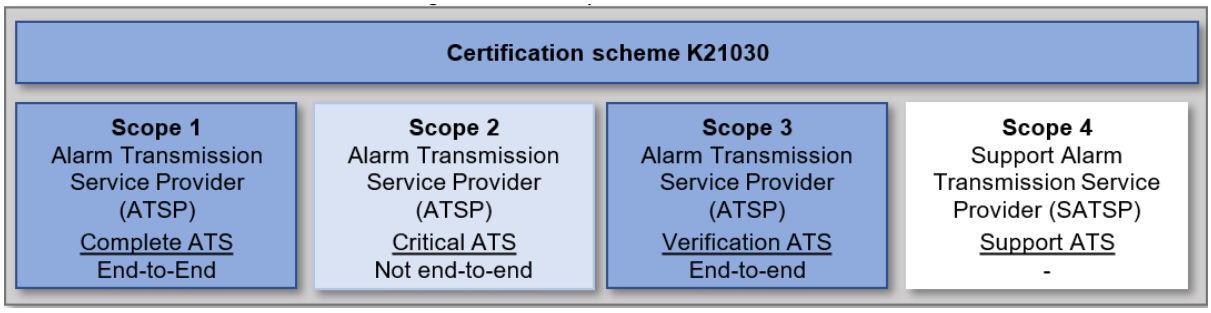
The table below shows relevancy between the standards to be noticed in the execution.

EN 50136-1/A1	TS 50136-9	EN 50518-3	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	4 Staffing 5 Operating procedures 6 Audit 7 Complaints procedure 8 Data	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) form Supervised Premises Transceiver (SPT) to Receiving Centre Transceiver (RCT) and encompasses only verification of performance and reporting to the customer. This scope is end-to-end.

8.2.4 *Scope 4*

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

Annex 1: Matrix penetration seals - G

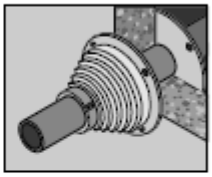
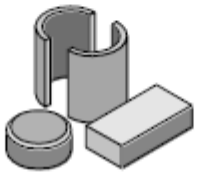
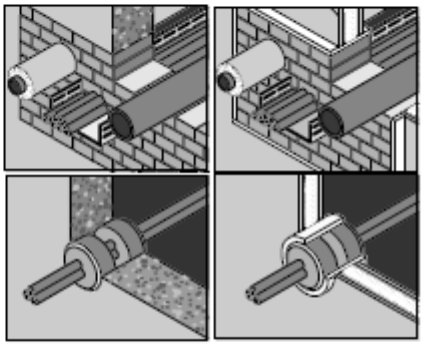
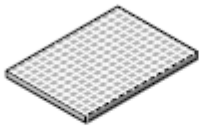
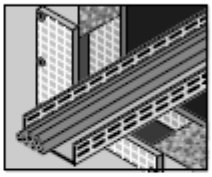
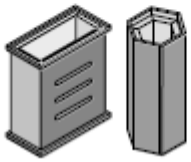
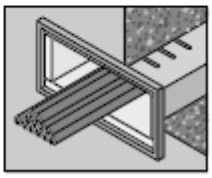
To be able to write down sufficient positive evidence, a table is given as an example to fill in per penetration seal.

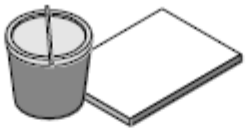
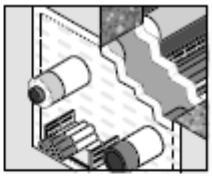
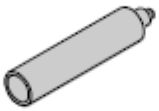
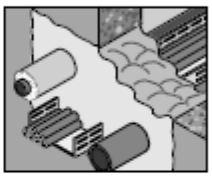
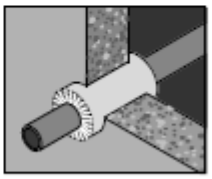
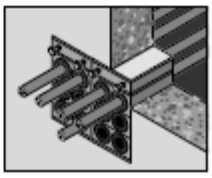
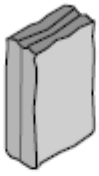
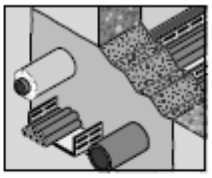
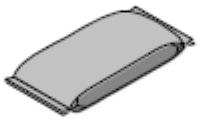
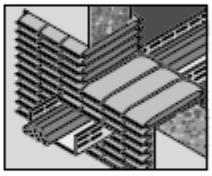
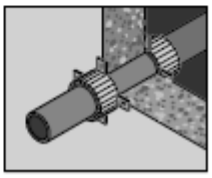
Penetration - Number		
Location	Location identification from the penetration seal on a map.	
Photo's	Before application	After application
Original seperation	Material and fire resistance.	
Penetration	Cable(s) / pipe (material) / medium in pipe.	
Type penetration seal	See table 1-1 in ETAG26-2. Caution 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.	

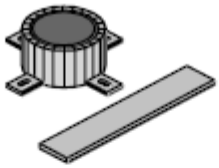
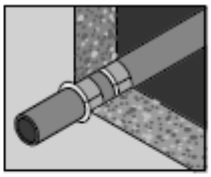
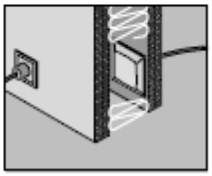
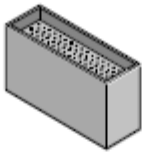
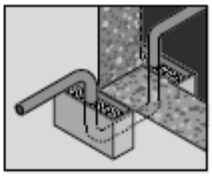
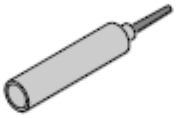
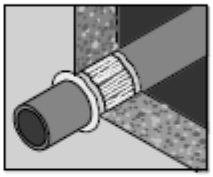
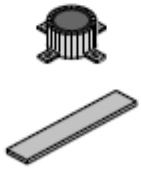
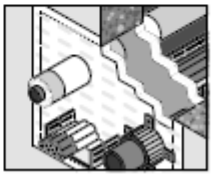
Important is the installation guideline from the used products. The instructions of the manufacturer should be followed to guarantee the same performance as during the test. Depending on the instruction of the manufacturer, the application should be done on the inside or the outside of the shell.

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		
• Collars (integrated into or outside the wall / floor)		

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

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

European standard	EN50518	EN-IEC 62676-4: 2015	IEC 60839-11-2: 2014	K21023	EN50136-1/A1 K21030	CLC/TS 50134-7:	ISO/IEC 27039; 2015	TS54-14: 2004
Name of the standard	Monitoring and alarm receiving centre	Video surveillance systems for use in security applications - Part 4: Application guidelines	Alarm & electronic security systems - Part 11-2: Electronic access control systems - Application guidelines	Mobile Security – Security of mobile objects and persons	Alarm Transmission Service Provider	Alarm systems - Social alarm systems - Part 7: Application guidelines	Information technology - Security techniques - Selection, deployment and operations of intrusion detection systems (IDPS)	Fire Alarms Systems (FAS)
Paragraph	1. Scope	P1 Scope	P1 Scope	P1 Scope	P1 scope and Responsibilities	P1 Scope	P1 Scope	P1 Scope
Paragraph	Planning 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							