K21047/05
01 October 2025

Wireless Silent Alarm Systems

for the certificate for Wireless Silent Alarm Systems for evacuation of buildings and sites.

kiwa

K21047/05
01 October 2025

Preface

This European Certification Scheme has been accepted by the Kiwa Board of Experts Fire Safety, in which all the relevant parties in the field of Fire Safety are represented. This Boards of Experts also supervises the certification activities and where necessary require the Certification Scheme to be revised. All references to Board of Experts in this Certification Scheme pertain to the Boards of Experts mentioned above. This Certification Scheme will be used by Kiwa in conjunction with the Kiwa-Regulations for Certification, in which the general rules in case of certification are registered.

The purpose of this Certification Scheme is to make clear in which way a declaration of conformity is established regarding performance-, reliability- and security requirements of the assessed Wireless Silent Alarm System (WSAS). This based on the European standards in this scope.

The basic framework for this scheme has been standard NEN 2575-4; Fire safety of buildings - Evacuation alarm installations - System and quality requirements and guidelines for locating of alarm devices - Part 4: Wireless silent alarm installation and DIN 14675; Fire detection and fire alarm systems – Design and operation.
The framework in this scheme is covering all the functions and performances of this standard based on the European standards.
Maintenance is in accordance with the NEN 2654-2 standard: Management, inspection and maintenance of fire protection systems - Part 2: Evacuation alarm systems.
Additionally are the requirements on logging, reporting, alarm transmission software more strict. It has also an additional function on positioning and counting of staff in the designated areas and in the surrounding of the designated areas.

Validation
This certification scheme has been validated by the Director Certification and Inspection of Kiwa FSS on 2025-10-01

Kiwa Fire Safety & Security
Kiwa Nederland B.V.
Kiwa FSS Certification
Dwarsweg 10
5301 KT Zaltbommel

+31 (0)88 998 51 00
NL.infocertification.fss@kiwa.com
www.kiwa.nl

Table of content

1. Introduction

1.1. General

This European certification scheme includes all relevant requirements which are employed by Kiwa when dealing with applications for the issue and maintenance of a certificate for products, (systems), processes and services used for wireless silent alarm systems.

For the performance of its certification work, Kiwa is bound to the requirements as included in EN-ISO/IEC 17065 “Conformity assessment - Requirements for bodies certifying products, processes and services”.

This certification scheme is drafted according EN-ISO/IEC 17067 “Conformity assessment - Fundamentals of product certification and guidelines for product certification schemes”. This scheme is a type 6 according to this standard.

The 5th version of this certification scheme replaces the following certification scheme:

Certification scheme	Title	Dated
K21047/04	Wireless Silent Alarm Systems (WSAS)	2024-06-15

Technological developments do not wait for laws, regulations and standards. These laws, regulations and standards are following the developments. In this document is the "Interpretation document" those embodies the technological and market developments are recorded. The purpose of this 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 5th version of the certification scheme is only about textual corrections. Below you can find the corrections in the following paragraphs:

- **1.2.4 Certification scopes**
  Chapter name is changed;
  The scope name “A” and “B” has changed. The word 'or' has been removed from this sentence.
- **1.5. Certification areas Quality declaration**
  The content has been clarified textually in accordance with the certificates.
- **5.6.1 Commissioning and delivery of the WSAS**
  The word 'flowing’ is changed into the text 'the following'.
- **11.5 Layout of quality declaration**
  The body names are changed in Annex I, II and III.
- **I Model Product certificate (example)**
  The example model has been replaced.
- **II Model Process certificate (example)**
  The example model has been replaced.
- **III Model Service certificate (example)**
  The example model has been replaced.

This version of the certification scheme can be used directly because there are no changes in the requirements.

The certificate with version 04 remains valid until 2025-10-01 and the certification body will no longer take certification decisions according to version 04 after that. The periodic assessment should take place immediately with the publication of version 05.

1.2. Field of application / scope

Figure 1 shows the demarcation of the wireless silent alarm system.

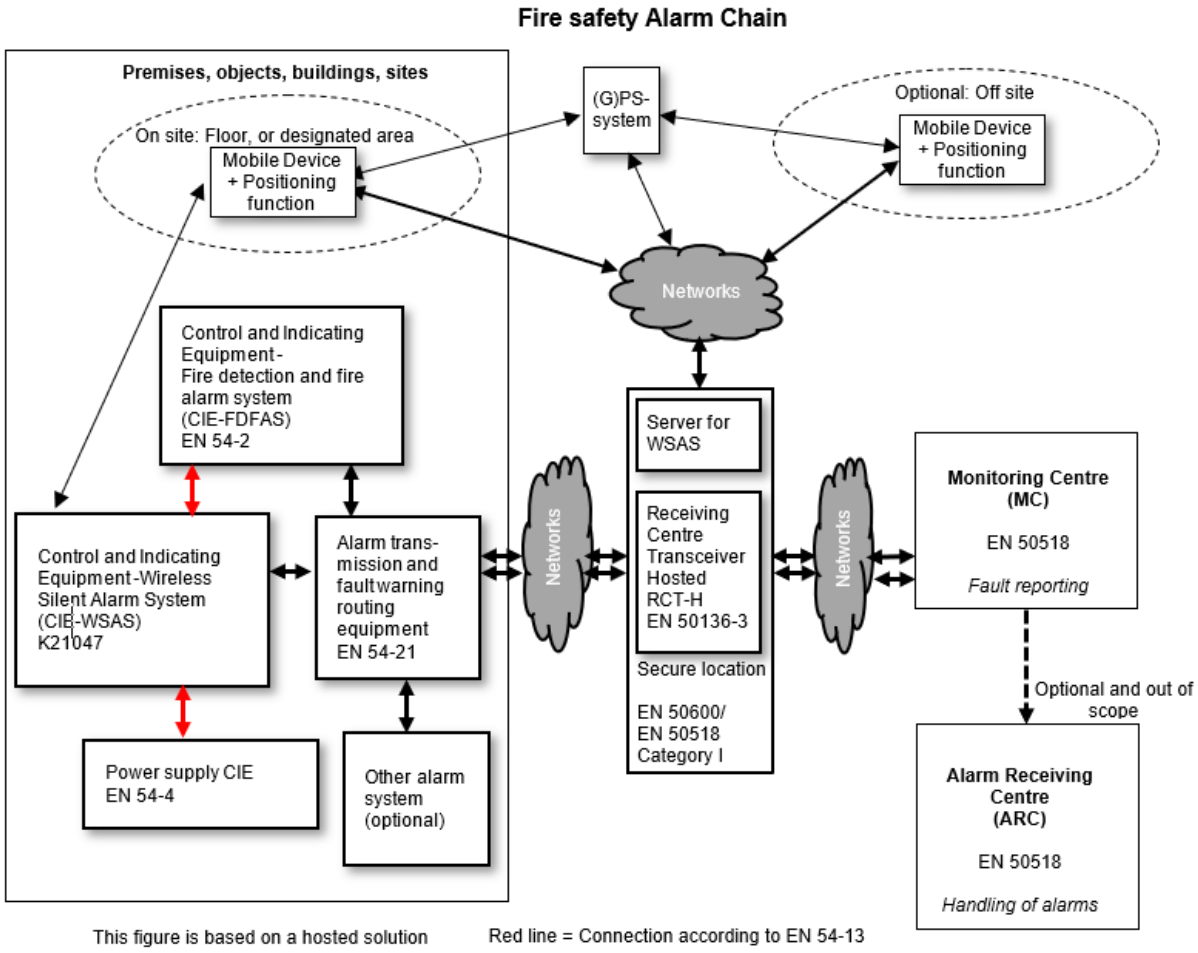

Figure 1 – infrastructure of the WSAS

1.2.1. Demarcation within scope

The wireless silent alarm system WSAS is intended to be used in buildings and/ or on sites to relay the information of the fire detection and fire alarm system (FDFAS) in a building and/or on a site to for example the emergency response team (ERT) of the building and/or site. The WSAS can be used in a hosted and non-hosted situation. Primarily the scheme is written based on a hosted situation.
The goal of the product is to inform and alarm the emergency response team in the building and/or site in a timely and secured way of the status of the fire detection system or other alarm systems. In that way, the users of mobile devices such as emergency response officers (ERO) at a location are able to start the emergency response and/or evacuation process. The reliability and availability of the system is essential.

The following elements in the demarcation are within scope:

- The CIE of the Wireless Silent Alarm System;
- The critical alarm transmission between the CIE of the fire detection system and the CIE of the WSAS;
- The critical connection to the power supply for the WSAS;
- The critical alarm transmission between the central equipment of the WSAS and the server in the secure location. The secure location can also be in the supervised premises self (non-hosted).
- The critical alarm transmission between the server in the secure location and the mobile devices (MD).
- The application performing on the mobile device with its functions to support the users on site.
- The positioning function of the WSAS for determining the number of present mobile device users.

Additionally, the critical transmission between the server in the secure location and the Monitoring Centre (MC) is in scope for at least the reporting of the faults of the WSAS. In case an optional Alarm Receiving Centre (ARC) is used, that critical transmission is also in scope.

1.2.2. Optional scope with requirements

An optional scope is the positioning function of the WSAS to users of the Mobile Devices who use their Mobile Devices off site. In this case the requirements for positioning the same as inside buildings.

1.2.3. Functions of the WSAS

The functions of the WSAS are:

- Supervised alarm transmission of the fire detection system and the mobile devices (MD) of the emergency response team at the location;
- Informing of the WSAS-user about faults in the system;
- Reporting on the availability of the system;
- Reporting on the availability of the connected number of emergency response officers within the designated area of the emergency response team;
- Optional: Reporting on the availability of the connected number of emergency response officers off site.

1.2.4. Certification scope

The Wireless Silent Alarm Systems are intended to be used in buildings and land based (indoor and outdoor) storage locations, process facilities, loading and transshipment areas.

The activities for which a manufacturer and/or system integrator can obtain a quality declaration per system are:
A. Manufacturer (at component level - product);
B. Design & - Installation (process);
C. Maintenance (service).

1.3. Technical and organizational resources

To achieve certification of a wireless silent alarm system, the assessment contains the following:

- The adoption of the demarcation and the specifications of the WSAS;
- The requirements of the product quality of relevant components;
- The requirements of the network architecture;
- The field inspection of the performance- & other requirements of the WSAS;
- The requirements of the security controls of the WSAS;
- The evaluation of the statistical data which is generated by the hardware and software of the WSAS;
- The requirements of the Monitoring Centre who collects the data and processes this according to the specifications of the WSAS;
- The requirements of the corrective actions by the WSAS on failing transmission by the system.

1.4. Acceptance of test reports provided by the supplier

With regard to the requirements laid down in this evaluation guideline, the applicant may submit, in the scope of external inspections, reports issued by conformity assessing institutions to prove that the requirements of this BRL are being satisfied. It must be demonstrated that the respective analysis/inspection/test and/or evaluation reports have been drawn up by a body that complies with the respective applicable accreditation norm with regard to the subject matter,

- NEN-EN-ISO/IEC 17020 inspection institutions;
- NEN-EN-ISO/IEC 17021-1 institutions that certify management systems;
- NEN-EN-ISO/IEC 17025 for laboratories;
- NEN-EN-ISO/IEC 17065 for institutions certifying products, processes, and service.

Explanation:
An organization will be considered as compliant with these criteria if an accreditation certificate for the respective subject matter can be submitted, issued by the Board of Accreditation (RvA) or another accreditation organization which has been accepted as a member of a multilateral agreement on the subject of mutual recognition and

acceptance of accreditation, which have been drawn up within the EA, IAF and ILAC. If no accreditation certificate can be submitted, the certification organization itself will assess if compliance is given to the accreditation criteria.

1.5. Quality declaration

The quality declaration to be issued by Kiwa with the scope is described as a:

- Product certificate for the manufacturing of the components/ systems;
- Process certificate for the delivery of installations of these systems;
- Services certificate for the delivery of maintenance of these systems.

The quality declaration to be issued by the supplier with the scope:

- For the delivery of installations of these Wireless Silent Alarm Systems provided by the supplier;
- For the delivery of maintenance of the Wireless Silent Alarm Systems provided by the supplier.

A model of these certificates to be issued based on this scheme has been included as an annex I, II en III for information.

1.6. Assessment method

The normal assessment method per installation of this certification scheme is according EN-ISO/IEC 17067 “Conformity assessment - Fundamentals of product certification and guidelines for product certification schemes” type 6.

If required by the authorities or a client, a type 1a assessment shall be performed.
This assessment shall be performed according EN-ISO/IEC 17020 “Conformity assessment - General criteria for the operation of various types of bodies performing inspection”.
In this assessment method shall the system met the requirements and conditions of the standard(s).
This method shall create a complete overview of the system and if successful shall result in a product certificate.
In this method information is used generated by the supplier of the installation and co-suppliers of the conditions.

2. Terms and definitions

2.1. Definitions general

In this certification scheme, the following terms and definitions apply.

2.1.1. Board of Experts

The Board of Experts Fire Safety

2.1.2. Certification mark

A protected trademark of which the authorization of the use is granted by Kiwa, to the supplier whose products can be considered to comply on delivery with the applicable requirements and possibly with quality information on the application of the product is added by a specially designed label which is based on the result , as stated in the report issued by Kiwa on the inspection of the prototype.

2.1.3. Certification scheme

The agreements made within the Board of Experts on the subject of certification.

2.1.4. Inspection tests

Tests carried out after the certificate has been granted in order to ascertain whether the certified products continue to meet the requirements recorded in the certification scheme.

2.1.5. IQC scheme (IQCS)

A description of the quality inspections carried out by the supplier as part of his quality system.

2.1.6. Initial assessment

Assessment in order to ascertain that all the requirements recorded in the certification scheme are met.

2.1.7. Private Label Certificate

A certificate that only pertains to processes that are also included in the certificate of a supplier that has been certified by Kiwa, the only difference being that the products and product information of the private label holder bear a brand name that belongs to the private label holder.

2.1.8. Product certificate

A document in which Kiwa declares that a product may, on delivery, be deemed to comply with the product specification recorded in the product certificate.

2.1.9. Product requirements

Concretised requirements specified by means of measures or figures, focussing on (identifiable) characteristics of products and containing a limiting value to be achieved, which can be calculated or measured in an unambiguous manner.

2.1.10. Process certificate

A document in which Kiwa declares that a process may, on delivery, be deemed to comply with the process specification recorded in the process certificate.

2.1.11. Process requirements

Requirements made specific by means of measures or figures, focussing on (identifiable) characteristics of processes and containing a limiting value to be achieved, which can be calculated or measured in an unequivocal manner.

2.1.12. Supplier

The party that is responsible for ensuring that the processes meet and continue to meet the requirements on which the certification is based.

2.1.13. Surveillance assessment
The assessment after issuing the certificate to determine that the certified processes continue to meet the requirements in this certification scheme.

Note 1: In the assessment matrix is summarized which research Kiwa will conduct at the initial and surveillance assessments and in which frequency.

2.2. Specific definitions
In this certification scheme, the following specific terms and definitions apply:

2.2.1. Wireless Silent Alarm Systems (WSAS)
Product intended to be used in buildings and/ or on sites to relay the information of the fire detection and fire alarm system in a building and/or on a site to the emergency response team of the building and/ or site (or optional off site)

2.2.2. Control and indicating equipment Wireless Silent Alarm System (CIE WSAS)
Operating possibility which, in case of fire or other emergency, can call silent alarm groups manually.

2.2.3. Control and indicating equipment Fire Detection and Fire Alarm System (CIE FDFAS)
Component of wireless silent alarm system through which other components may be supplied with power and which is used to receive signals from the connected detectors.

2.2.4. Alarm transmission and fault warning routing equipment
Intermediate equipment which routes an alarm signal or fault warning from a control and indicating equipment (CIE) to a Monitoring and Alarm Receiving Centre (MARC).

[SOURCE: EN 54-1]

2.2.5. Building / site transmission devices
For example a Wi-Fi access point at a location.

2.2.6. Monitoring Centre (MC)
Centre in which the status of one or more ATSNs is monitored.

[SOURCE: 4.1.22 EN 50136-1]

2.2.7. Alarm Receiving Centre (ARC)
Continuously manned centre where information concerning the status of one or more Alarm System (AS) is reported

[SOURCE: 4.1.2 EN 50136-1/A1]

2.2.8. Secure location
Location that is a MARC or another location that complies with a published data centre standard.

Note 1: Examples of published data centre standards or accepted best practices are: a data centre designed and maintained to EN 50600 series. Availability class 3, protection class 4 or ARC category I in accordance to EN 50518; or as best practice Uptime Institute Tier 3.

[SOURCE: 4.1.38 EN 50136-1/A1]

2.2.9. BYOD
Bring your own device.

2.2.10. Compatibility for component type 1
Ability of a component type 1 to operate with other type 1 components of the FDFAS:

- within the limits specified for each component given in the documentation;
- within the specified limits given by the relevant parts of EN 54, or given by the applicant; if no EN 54 part applies;
- within specified configurations of systems.

[SOURCE EN 54-13, 3.1.2]

2.2.11. Connectability for component type 2
Ability of component type 2 to operate without jeopardizing the performance of the fire detection and fire alarm system.

[SOURCE EN 54-13, 3.1.5]

2.2.12. Other alarm system
System that can create an alarm as start for the evacuation process as an example a system according to EN 50131.

2.2.13. Conditions
For the functioning of a WSAS, certain conditions are needed. These conditions can be for example a fire detection system or a good performing user group.

2.2.14. Emergency Response Team (ERT)
An Emergency Response Team (ERT), originally intended to evacuate employees and to fight fires, is an internal organization of typically volunteer employees designed to respond to emergencies before the arrival of public agencies.

Note 1: In Dutch you could translate this with BHV-Organisatie.
Note 2: In German you could translate this with Betriebssanitäter.

2.2.15. Emergency Response Officer (ERO)
People who are trained to be the first line of response in any emergency situation.

2.2.16. Transmission path
Physical connection between the components (external to the housing of the components) used for the transmission of information and/or power.

[SOURCE EN 54-13]

2.2.17. Mobile device
Amart mobile device (MD) with a positioning function to be used in a Wireless Silent Alarm System.

2.2.18. Dedicated mobile device
Devices which are used if needed based on the infrastructure of the Wireless Silent Alarm system.

2.2.19. Hosted RCT
RCT that consists of two parts, where one part is located in a secure location
(RCT-H) and another part is installed in the MARC (RCT-A).

[SOURCE: 4.1.41 EN 50136-1/A1]

2.2.20. Radio transmission
Radio transmission is a possibility for alarm transmission as defined in
EN 50136-1/A1.

2.2.21. Dual path Alarm Transmission System
Alarm Transmission System consisting of one primary Alarm Transmission Path and one secondary Alarm Transmission Path using diverse technology, having two transmission network interfaces at the Supervised Premise Transceiver, to connect one or more (Wireless Silent) Alarm System of one supervised premises to one or more MARCs.

[SOURCE: 4.1.16 EN 50136-1/A1]

2.2.22. Diverse technology
Technologies used in transmission paths in such a way that a single point of failure, or tampering of a single point, cannot cause both Alarm Transmission Paths of a dual path system to fail simultaneously.

[SOURCE: 4.1.15 EN EN 50136-1/A1]

2.2.23. Service provider
Organization or part of an organization delivering one or more services to a client. The service provider should be certificated based on this scheme.

2.2.24. Installation
Implementation of the design, specifically the assembling, mounting and connecting of the relevant system components.

2.2.25. Maintenance
Combination of preventive and corrective activities during the life of the system, which are intended to retain it in, or restore it to, a state in which it can perform the required function.

3. Procedure for issuing a certificate

3.1. Initial investigation

The initial investigation to be performed is based on the (process, product and system) requirements as contained in this certification scheme, including the test methods, and comprises the following:

- assessment of the quality system and the Internal Quality Control (IQC)-scheme;
- planning assessment;
- design assessment;
- assessment of the installation;
- commissioning assessment;
- assessment of the verification;
- assessment of the handover;
- assessment of maintenance;
- type testing to determine whether the products comply with the product and/ or functional requirements;
- production process assessment (if applicable);
- assessment on the presence and functioning of the remaining procedures.

3.2. Issuing certificate

After finishing the initial investigation, the results are presented to the decision maker deciding on issuing the certificate. This person evaluates the results and decides whether the certificate can be granted or if additional data and/ or tests are necessary before the certificate can be issued.

3.3. Assessment of the process and/ or performance requirements

Kiwa will assess certified products / systems by means of a valid certificate and/or quality mark. This demonstrates that the requirements set for the certification are met. The necessary samples are taken by or on behalf of Kiwa.

3.4. Production process assessment

When assessing the production process, it is investigated whether the manufacturer is capable of continuously producing products that meet the certification requirements.
The evaluation of the production process takes place during the ongoing work at the producer.
The assessment also includes at least:

- The quality of raw materials, half-finished products and end products;
- Internal transport and storage.

3.5. Contract assessment

If the supplier is not the manufacturer of the products to be certified, Kiwa will assess the agreement between the supplier and the producer.
This written agreement, which is available for Kiwa, includes at least:
That accreditation bodies, scheme managers and Kiwa will be given the opportunity to observe the certification activities carried out by Kiwa or on behalf of Kiwa at the producer.

4. Product requirements WSAS

4.1. General

This chapter contains the requirements that products have to fulfil.
The requirements for timely alarming, supervision of the transmission and the availability of the system are arranged in the product and system requirements.

4.2. Product requirements

The devices arranging the critical alarm transmission have to comply with the requirements in one of the following standards depending on the intended use:

- EN 50136-2; Alarm systems - Alarm transmission systems and equipment – Part 2: Requirements for Supervised Premises Transceiver (SPT);
- EN 50136-3; Alarm systems - Alarm transmission systems and equipment – Part 3: Requirements for Receiving Centre Transceiver (RCT);
- EN 54-21; Fire detection and fire alarm systems – Part 21: Alarm transmission and fault warning routing equipment.

The critical transmission connections are:

- CIE Fire Detection System <> CIE WSAS;
- CIE WSAS <> Server secure location;
- Server secure location <> Mobile devices users.

Note 1: These requirements are about the software of the devices.
Note 2: “<>” means a connection.
Note 3: the secure location could also be at the premises if the same requirements are fulfilled.

The connection between CIE WSAS and the CIE FDFAS, the CIE WSAS and the power supply have to comply with the requirements in EN 54-13; Fire detection and fire alarm systems - Part 13: Compatibility assessment of system components;

- CIE Fire Detection System <> CIE WSAS (type 1);
- CIE WSAS <> Power Supply of the CIE WSAS (type 1);
- CIE WSAS <> Alarm transmission and fault Warning routing equipment (type 1).

The CIE WSAS has to comply with the requirements in EN54-13 Fire detection and fire alarm systems - Part 13: Compatibility assessment of system components type 1.

The power supply of the central equipment of the WSAS has to comply with requirements in EN 54-4; Fire detection and fire alarm systems - Part 4: Power supply equipment. If the secure location is within the supervised premises, EN 54-4 is also applicable for this solution.

For other alarm systems the configuration with the WSAS shall be in according with the EN 50131.

The requirements for the software application on the mobile devices and the WSAS are specified in 4.6

4.3. System requirements

The supervised alarm transmission between the central equipment of the WSAS and the server in the secure location have to comply with the requirements in EN 50136-1/A1 / IEC 60839-5-1; Alarm and electronic security systems – Part 5-1: Alarm transmission systems – General requirements; based on certification scheme K21030 for the scope critical transmission.
The level of the secure alarm transmission is Dual Path 4 (DP 4). See EN 50136-1/A1.

The supervised alarm transmission between the mobile devices of the WSAS and the server in the secure location have to comply with the requirements in EN 50136-1/A1 / IEC 60839-5-1; Alarm and electronic security systems – Part 5-1: Alarm transmission systems – General requirements;
The level of the secure alarm transmission is Dual Path 2 (DP 2) see EN 50136-1/A1.
The reporting is accessible for the user of the system and inspection bodies.

Remark: The possible radio transmission bands are LoRa, 2G, 3G, 4G, 5G, Starlink and Wi-Fi. SMS can be used as transmission layer. This scheme does not stipulates which technology should be used for a transmission path. It does require a double path connection to al the mobile devices of the users based on divers technology. In case that divers technology is not possible in spots of the building is the use of function reliability based on the principles in NPR 2576 a possible solution.

SMS is only used as a backup when data transmission is not available.
The capacity of the used network shall be such that it has sufficient capacity in a normal and in an incident situation to interact with all the users.

The positioning function (GPS) of the WSAS per mobile device user has to meet the following specifics:

- In the building and/or site are devices (such as Wi-Fi transmitters) needed to facilitate the communication of the system of the users of the emergency response team.
- Accuracy positioning on a surface level: this has to be specified by the supplier, it needs to have a minimal accuracy of 100 meter and be determined using at least two methods of location positioning. In case of inaccurate Wi-Fi and GPS positioning there needs to be a manual input for users. The positioning function has a relation with alarm zone in the basic design of the WSAS.
- A designing and verification function tool for the determination of the number of local devices for the position function per building / floor and the verification of the function when installed. The basic criteria for this tool are accuracy positioning, adequate speed of transmission and adequate availability of transmission.

Note: The positioning function to be used off site is the same as on site.

Case studies
Specific case studies give guidance towards possible solutions.

Below are case studies shown that are not a standard requirement, but are detailing the translation of the functional and performance requirements in a possible solution.

Input	Output
1. Applying redundant WIFI networks in places where coverage is poor or worse for Public Telecom networks systems.	The scheme refers to the EN50136-1 / A1 standard, using the following principles: • Diverse technology; 2.2.22 in the scheme; • Dual path Alarm Transmission Systems; 2.2.21 in the scheme. So when using a double WIFI network, the above criteria functional shall be met. If this choice is the solutions for a specific situation has been made, it shall in any case have to be established that it concerns two different networks with their own endpoints and power supply. In these cases, NPR 2576 can be applied for obtaining Circuit integrity.
2. Applying redundant Public Telecom networks in places where coverage is poor or worse for WIFI.	The scheme refers to the EN50136-1 / A1 standard, using the following principles: • Diverse technology; 2.2.22 in the scheme; • Dual path Alarm Transmission Systems; 2.2.21 in the scheme. So when using a redundant Public Telecom network, the above criteria shall be met. The use of a second SIM card from a different Public Telecom provider is then the solution. If this choice is the solutions for a specific situation has been made, it shall in any case have to be established that it concerns two different telecom providers, each with their own network and infrastructure (antennas). If the providers use the same antenna structure, it shall be established that another antennas are present in the vicinity that shall follow-up the signal transmission to a sufficient extent if the first antenna structure fails.
3. Distinction between indoor and outdoor coverage	The minimal requirements for the availability (redundancy) of the WSAS transmission paths (2G - 5G and WIFI) is intended for inside the buildings on a site. If the WSAS use is intended for large sites with multiple buildings, there is a demarcation between indoor and outdoor areas. The outdoor areas availability of transmission paths is optional. If the basic engineering plan has additional requirements on top of the minimal requirements for communication with staff on the outdoor aeras because to alarm extra help for the evacuation should this be clearly defined in the basic engineering plan with the reason why. The plan should also define the minimal availability requirements for the outdoor areas and what the minimal performance should be of this extra help in context of the requirements of the inside evacuation.

4.3.1. Loggings of the system
According to EN 50136-1 / IEC 60839-5-1 loggings are made of the functions of all the devices within the system. The system shall have a capacity of at least 3 months to store this data.

4.4. Functional requirements wireless alarm system
In this chapter the additional functions are described that are not arranged in the product and system requirements.

4.4.1. CIE WSAS

The wireless silent alarm system must have an operating possibility (control panel) which, in case of fire or other emergency, can call silent alarm groups manually.

Remark; A control panel in accordance with the requirements of NEN 2575-3, chapter 10 meets this requirement.

4.4.2. Server WSAS– system requirements

All transmission paths of wireless silent alarm systems are intended for use by wireless silent alarm systems. Secondary application transmission pathways for wireless alarm systems must not have a negative influence on the primary purpose of the transmission paths for wireless silent alarm.

The equipment shall be a stand-alone application for alarm handling. The software application changes may only be made by trained and authorized personnel for this equipment.

The equipment shall handle a fire / evacuation alarm with the highest priority.

Note: the server of the WSAS can be at a premises (non-hosted) or at a secure location (hosted)

4.4.3. Building / site transmission devices supporting the WSAS

The local transmission devices supporting the WSAS shall provide sufficient coverage for the evacuation area. In case of failure in transmission, the reception of messages in an area may not become below the level of availability of the WSAS per week and year (based on EN 50136-1/A1) and being monitored for proper functioning and shall be controlled and indicated by the software tool of the WSAS.

The instruction of the WSAS shall specify that the local transmission devices for supporting of the WSAS shall:

- be suitable for the location where it is set up;
- comply with telecommunication legislation that applies to it.

The specifications for the building network are:

- GPS location of a smartphone must be accurate to at least 100 meter;
- Connections with technology such as WIFI & public telecom networks shall have a signal strength and speed according to technical specifications of the supplier of these networks meeting the minimal qualification “fair”.

K21047/05
01 October 2025

Case study
Specific case study give guidance towards for a possible solution.

Below is a case study shown that are not a standard requirement, but are detailing the translation of the functional and performance requirements in a possible solution.

Input	Output
1. The dB references values for example 4G and WIFI are strict in some cases.	The two transmission paths within the building should meet or exceed the qualification “fair”, according to the following industrial references: • WIFI: For a good Wi-Fi signal, we generally maintain a minimum signal strength of -67 dBm. In this case, dB stands for decibels and m for milliwatts. This number is always below zero. The closer the dBm is to zero, the better the signal can be used: ○ 0 to -40 dBm: excellent; ○ -41 to -65 dBm: good; ○ -66 to -70 dBm: fair; ○ -71 dBm and below: poor. • Mobile: https://wiki.teltonika-networks.com/view/Mobile_Signal_Strength_Recommendations If the second path does not meet the minimum requirements, the system should nevertheless works at the location with the worst coverage. This has to be inspected initially and during surveillance. A fallback from 4G to 2G is allowed if the system has a redundancy with data of Public Telecom networks systems. If there is no response through the app, the system should automatically alert the recipient by telephone.

4.5. Mobile devices supporting the WSAS

The business continuity strategy of the WSAS is such that regular mobile devices can be used supporting the functioning of the WSAS. By enforcing this strategy on a location, the possibility is created that all staff from the organisation using the WSAS present on the designated location can use their regular mobile device obtaining a high percentage of users.

This high percentage of users creates the ability to have a more direct action of the emergency response team based on the emergency response plan for the location and a higher business continuity for the WSAS.

Note: If needed within the infrastructure of the building and/or site, dedicated WSAS devices can be used. This has to stipulated within the basic engineering WSAS - plan of the building / site.

Note: Due to obtaining a proper Confidentiality, Integrity and Availability (CIA) level in terms of information security, BYOD solutions in this WSAS infrastructure are not permitted unless tested by an approved test lab.

4.5.1. Preconditions of mobile devices

The mobile devices have to been set in the following preconditions by the software tool of the WSAS on the device:

- the audible alarm signal on the receiving mobile device must be at least 65 dB (A) at 1 m and must be clearly distinguishable from other call signals. Is the sound pressure level of the ambient noise 59 dB (A) or more, the receiving mobile device must also be clearly felt through a vibrating signal;
- the acoustic signal in the event of an alarm may not interrupt the voice communication;
- the acoustic signal from the receiving device must remain active during a silent alarm call until it is manually confirmed or up to a maximum of 60 seconds if it is not manually confirmed;
- a receiving mobile device must give a text message with at least the room/location that should be evacuated (for example the alarm zone or area);

- the language of the text message must be aligned with the emergency response & evacuation team and shall be recorded in the basic engineering plan of the WSAS for the building/site;
- the text messages relating to an evacuation alarm must have the highest priority, recognizable as such and clearly distinguishable from other messages;
- the receiving mobile devices give an acoustic and visual warning when the battery capacity is too low. This warning is made when the battery capacity reaches 10% of its maximal capacity. The warning does not have to be reported to the CIE of the WSAS;
- the receiving mobile devices cannot be switched off without an acoustic and/or optical warning;
- the receiving mobile device gives “information about availability within the defined zone”, no later than 15 minutes when out of range with the WSAS if this is a control setting in the basic engineering plan based of the emergency response (evacuation) plan;
- the selection of the mobile device is such that the energy supply must be sufficient for at least 12 hours of operation. The supplier shall specify this in its instruction for the software tool.

The mobile devices shall have the following settings and shall be monitored by the WSAS:
- The Mobile Device Operating system shall be updated at least once per 2 years.
- The Push notifications shall be turned on, and on priority when possible.
- The Location services shall be turned on, and on high accuracy when possible.

The mobile devices shall have the following settings:
- Any battery savers, task killers and virus scanners need to be turned off.
- Wi-Fi and Mobile data shall be turned on.

Remark; if these settings are not met by the users this shall result in a low availability of users in a designated area. This shall be reported by the WSAS.

4.6. Mobile application and hosted web platform

This part contains the requirements that the application on the mobile device, CIE WSAS and the hosted web platform shall have to fulfil.

4.6.1. Use and access levels of the application

The mobile application is intended to be used on general mobile smart devices.
The mobile application shall connect direct by radio transmission to the WSAS.
The application requires a logical access level 2 on the smart mobile device according to EN 50131-1.
The application shall enforce a new code after first installation.

The CIE WSAS shall connect to the hosted web platform. This requires a logical access level 3 according to EN 50131-1.

4.6.2. Connections of the application

The applications shall have a secure and confidential connection to the CIE of the WSAS and meet the key management requirement of TLS1.2.
Key management shall be arranged according ISO/IEC 11770-1/2/3.
The integrity of this connection shall be arranged on cryptographic algorithms according to ISO/IEC 18033.
The hash functions according to this shall also be applied for non-repudiation.

The cryptographic algorithms shall meet the updated list of SSL labs or better.

The CIE of the WSAS shall have a secure connection to a hosted web platform according to IEC 60839-5-1 (EN 50136-1/A1).

4.6.3. Acknowledgment un/setting

The setting made on the CIE shall be acknowledged by the CIE of the WSAS and the hosted web platform. These settings shall also be communicated to the mobile devices.

The setting made in the hosted web platform shall be acknowledged by the CIE of the WSAS and the application of the mobile device.
By this the live situation is reflected by the application.

The process shall be fail-safe; that means that if during normal use the connection fails, the process is stopped and that the not completed changed settings shall fall back to the last completed settings.

4.6.4. Uptime – availability – business continuity

The availability of the hosted web platform shall meet the requirements DP4 according to IEC 60839-5-1 (EN 50136-1/A1).

The hosted web platform shall be hosted from a secure location complying with
EN 50518 or EN 50600.

4.6.5. Authenticity

The definitions and processes of ISO/IEC 29115 shall be applied.
LoA3 shall be defined in the process of getting first access (onboarding) as a user to all applications.

The mobile application shall restrict a limited time within 2 factor authentication process.

The procedure of getting access to the mobile application on the mobile device shall be the same as access to the CIE WSAS.

The procedure giving more users entrance (on different levels) to the mobile application is the same as for the CIE WSAS.

The process of remote access by the installer / supplier shall require at least 2 factor authentication.

It is allowed to use biometrics according to the standardization group ISO/IEC JTC 1 SC 37 on Biometrics.

4.6.6. Accountability

The hosted web platform and the mobile application shall apply logging.

The minimum storing time of the logs for the hosted web platform and the mobile application is 3 months.

4.6.7. Session time

A maximum session time shall be applied preventing unauthorized use for critical function(s) within the mobile application. For example: opening the mobile application function for (setting) the CIE WSAS.

Protection against hostile access (brute force) to the mobile application within the secure functions shall be tested by penetration testing in the developing stage of the application.

4.6.8. Instructions by the application towards the user

The mobile application shall warn and instruct the user to use the mobile application in a secure manner.

4.7. Secure development process for the code

This part contains the requirements that the secure development process for the code of the mobile application and the hosted web platform shall have to fulfil.

Remark; An approved process according to scheme K21048 fulfils also this requirement.

4.7.1. Process requirements

The process shall fulfil the requirements of “A.14.2 Security in development and support processes” of ISO 27001 or the secure development processes according to IEC 62443-4-1; Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements.

The manufacturer shall have an accredited certificate according to this standard for this activity or this process and it shall be assessed by an expert of Kiwa.

4.7.2. Process requirement stages

The secure development process shall contain at least the following stages:

1. Planning with project management;
2. Analyses of the epics, user stories, use cases;
3. Design with architecture & user experience;
4. Building the code by the developers;
5. Testing of the code; testing is continuous process for control and verification of the functions and the threats / weaknesses of the security;
6. Deploying of the code in a hosted solution;
7. Review of the process for improvement of the next development.

4.7.3. Testing

The security testing of the code is based on minimum requirements in “The Ten Most Critical Web Application Security Risks” according to the latest OWASP rules, laid down at; www.owasp.org/

The code shall be tested according the latest applicable version of these rules.
The testing shall be performed in the end-to-end situation in a laboratory situation.

The testing shall be performed by an expert with a validated qualification by Kiwa. The qualification shall be based on the:

- Level of general knowledge and experience of code testing (5 years);
- Level of specific knowledge and experience of the code (3 years);
- Level of general knowledge and experience of the product in its application in the specific market sector (1 year);
- Level of specific knowledge and experience of the latest OWASP rules based of the applicable specific “Vulnerability Subcategories” (2 years).

5. Requirements processes and services

5.1. General

This chapter contains the requirements that the delivery process and services have to fulfil.

5.2. Regulatory requirements

Not applicable.

5.3. Process requirements Services for fire safety systems

The requirements of the planning, design, installation, commissioning, verification, handover and maintenance are specified in EN 16763 “Services for fire safety systems and security systems”.

5.4. Design process

5.4.1. Planning (basic engineering) and detailed engineering WSAS plan

The basic engineering plan for the WSAS outlines the engineering for the WSAS at a location.
The software application of the WSAS shall be able to arrange following preconditions:

- Alarm zones; The evacuation area shall be divided into one or more alarm zones. Depending on the size of the object, there may be several silent alarm groups each be responsible for the evacuation of one or more alarm zones;
- Number of receiving mobile devices; Minimal number of receiving mobile devices that belong to the silent alarm group within in a predefined alarm zone;
- Alarm conditions; The conditions to trigger an alarm;
- These alarm zones and minimum number of silent alarm groups shall be recorded in the basic engineering plan for the system for the location and to able to be implemented in the software application of the WSAS;
- The possibilities of negative interference on the WSAS must be addressed in basic engineering plan;
- Reporting malfunctions;
- Language text on the control panel;
- Language text on the mobile devices.

Note; The basic engineering plan WSAS should be developed in conjunction with emergency response (evacuation) plan of the building and / or site. If the emergency response plan is updated this may have consequences for the basic engineering plan of the WSAS. The user of the WSAS is responsible for informing concerning parties and taking proper action if needed. It is the responsibility of the client to make the basic engineering plan available.

5.4.2. Detail design of the evacuation alarm system

The selection, assembly and installation of components in such a way that the resulting systems shall comply with the performance and the objectives of the WSAS basic plan.

Prior to the installation activities, the installation organization shall have sufficient basic information on the scope of delivery, at least:

1. Detail engineering drawing and schematics;
2. Sufficient information about the layout of the installation, the position of components and transmission paths;
3. Connection data;
4. The functional integrity based on technical redundancy of connections and components.

5.5. Installation process

5.5.1. Installation activities

The installation organization registers the controls in the quality registration for installation on following items:

1. Cables, mounting systems, fasteners and equipment to be assembled;
2. The functional integrity based on technical redundancy of connections and components;
3. Transmission paths;
4. Connection of the distribution devices.

5.5.2. Completion of installation activities

The installation organization registers the controls in the quality registration for installation on following items:

1. The organization process installation checklist;
2. Fully completed and signed statement on behalf of the installation organization.

5.6. Commissioning and verification

The WSAS shall have a reporting function providing responsible staff with information about the functioning and availability of the system components during commissioning and verification.
This report shall be the basis of the verification report needed for the handover and needed for the declaration of conformity about the installation of the WSAS.
This report and the declaration of conformity about the installation of the WSAS shall be the basis of the declaration of conformity about the system.

5.6.1. Commissioning and delivery of the WSAS

The WSAS organization delivers the system with following quality registrations:

1. Quality registration for installation and handover; [1]
2. Report field strength measurement (Wi-Fi);
3. Report field strength measurement (GPRS);
4. The documentation based on B.4 of NEN 2575-4:2013.

5.6.2. Delivery of the WSAS - wireless silent alarm system

The WSAS organization shall have sufficient information enabling the delivery of the WSAS.

The table below contains the minimum requirements for the quality registration for installation and handover.

Subjects		
	Administrator (dashboard)	Key Performance Indicator (KPI) of all monitored functions.
	General requirements for equipment	Equipment meets requirements of compatibility EN 54-13.
	Coverage Radio (Wi-Fi)	Suitable for the space. Complies with telecommunications legislation. Coverage area is adequate, see measurement report.
	Coverage network	Coverage area is adequate, see measurement report.
	Mobile Devices	Are the mobile devices conform the WSAS manufacturers listing.

[1] Preferred model in accordance with appendix B.6 of NEN 2575-4:2013, including the additional requirements completed and provided to the client.

Applied equipment			
Wireless Silent Alarm System			
Definition	**Type**	**Make, type and Product Certificate Number**	**Number**
Alarm transmission and fault warning equipment EN 54-21			
Definition	**Type**	**Make, type and Product Certificate Number**	**Number**
Mobile Devices			

5.6.3. Handover to maintenance

The user(s) of the WSAS shall be trained by the supplier of the WSAS in the correct handling of the system
After the handover of the system shall the WSAS have a reporting function providing responsible staff with information about the functioning, capacity and availability of the system components during its use and its maintenance.
This report shall be the basis of the maintenance report needed for the declaration of conformity about the maintenance.
This report and the declaration of conformity about the maintenance of the WSAS shall be the basis of the declaration of conformity about the system.

5.7. Requirements maintenance service process

The requirements of the planning, design, installation, commissioning, verification, handover and maintenance are specified in EN 16763 “Services for fire safety systems and security systems”.

5.7.1. WSAS Wireless Silent Alarm Maintenance

The maintenance organization shall have sufficient information prior to maintenance to be able to carry out the maintenance and assess the nominal condition.
Prior to the maintenance activities, the maintenance organization shall have sufficient basic information on the scope of delivery, at least:

1. Basic engineering plan for the WSAS, responsibility of the client to make available;
2. Maintenance plan;
3. Block diagram;
4. Function matrix & I/O matrix.

Other additional documentation may be used if they are not conflicting with the original documentation.
The maintenance organization shall advise the client on the corrective and preventive measures to be taken by the client in the event of (possible) deviations.

The table below contains the minimum requirements for the quality registration for maintenance.

K21047	Item	
	Administrator (dashboard)	Key Performance Indicator (KPI), of all monitored functions.
4.5	Mobile Devices (MD)	Have been checked and, if necessary, cleaned in accordance with the manufacturer's instructions, their setting has been verified and function adequately.
4.3	Central Unit	Texts are correct and easy to read, housing is intact and the internal cabling and components are undamaged and in good condition.
		Settings meet the specifications.
		Notifications of evacuation alarms, malfunctions, breakages, interruptions and short circuits in all alarm zones, control lines with line monitoring and the power supplies are functioning adequate.

4.4.3	Communication Devices	Are the dashboards showing conformity with the requirements.
5.3.1	Fault reporting	Fault messages are received by the receiving station for fault messages.
4.2	Energy supply	Connection points, texts and alerts are in good condition and working adequately. From the power supply, the voltage, charging voltage and the total current consumption at rest and alarm (with the emergency power supply at reload stage) measured and compliant. (3: Fill in measurement data)
4.4.1	Control panel	Texts are correct and easy to read, Housing is intact and in good condition.
		The operating functions of the alarm zones or silent alarm groups functions are working adequately.
		The other operable functions are working adequately.

5.7.2. Completion of the maintenance

The maintenance organization completes the maintenance based on:
Report of Maintenance being the quality registration for maintenance, and provided this to the client. [2]

The maintenance organization must advise the client on the measures to be taken by the client in the event of deviations.

5.8. Other requirements

5.8.1. Instructions and access

The supplier shall design and deliver together with its WSAS an installation, user and maintenance instruction. This instruction together with the software application shall arrange the access levels to the system according EN 50131-1.

5.8.2. Training

The supplier shall design and deliver training to the staff that has the task for the setting of the configurations of the WSAS.

5.8.3. GDPR - General Data Protection Regulation

The user registration to the WSAS and the positioning function of the system shall meet the requirements of the General Data Protection Regulation (GDPR).
The requirements in this scheme attempt to fulfil these requirements in technical way.

A contract for parties exchanging personal data is needed.

5.8.4. Monitoring Centre (MC)

The use of a Monitoring Centre (MC) is obliged for the reporting of faults. The MC must be certified according to EN 50518 in conjunction with the Alarm Transmission Service Provider certified according to certification scheme K21030.

5.8.5. Alarm Receiving Centre (ARC)

The use of an Alarm Receiving Centre is optional and out of scope for the system supplier.
The function of the ARC in this process is to act as the secondary escalation process based on manual handling by the staff of the ARC. The primary escalation process in the responsibility of the emergency response organization of the building / site. In case if the primary escalation process is insufficient shall secondary escalation process assist in this process to arrange sufficient staff for the emergency response organization.
The applicable acting and Alarm Receiving Centre has to fulfill the requirements of EN 50518.

[2] Preferred model in accordance with appendix D of NEN 2654-2:2018, including the additional requirements completed and provided to the client.

The function of the ARC may also be fulfilled by automated fallback scenarios arranging the secondary escalation process alarming additional staff to act for the emergency response organization of the building / site to arrange sufficient staff for the emergency response organization.

6. Testing the performance of the systems

6.1. General

This chapter contains the requirements for testing by Kiwa to determine the performances that the systems have to fulfil.

6.2. Specific

The products shall be tested by means of determination methods to see whether they meet the requirements in chapter 4 of this scheme.

7. Marking

7.1. General

The systems and products shall be marked with a declaration of conformity according this certification scheme and applicable standards. The declaration shall contain at least the following information:

- name or logo of the supplier or manufacturer;
- data or code indicating the date of delivery or maintenance;
- type indication;
- certification marking according this scheme.

Indications and markings shall at least fulfil the requirements in the relevant product standard.

7.2. Certification mark

After concluding a Kiwa certification agreement, the certified products shall be indelible marked with the certification mark as is detailed in this scheme.

7.2.1. Component marking - product

Essential components with an FPC of Kiwa shall be affixed with a marking according to 9.1 of this scheme.

7.2.2. Installation marking - process

Installations fulling the requirements shall be marked with an installation declaration of conformity according this certification scheme and applicable standards.

7.2.3. Maintenance marking - services

Maintenance of installations fulfilling the requirements shall be marked with a maintenance declaration of conformity according to this certification scheme and applicable standards.

8. Requirements for the quality system

This chapter contains the requirements which have to be met by the supplier's quality system.

8.1. Manager of the quality system

Within the supplier's organisational structure, an employee who will be in charge of managing the supplier's quality system must have been appointed.

8.2. Internal quality control / quality plan

The supplier shall have an internal quality control scheme/plan which is applied by them. The standard for this quality plan is the EN 16763 "Services for fire safety systems and security systems.

The following must be demonstrably recorded in this QC scheme/ plan:

- which aspects are checked by the supplier;
- according to what methods such inspections are carried out;
- how often these inspections are carried out;
- in what way the inspection results are recorded and kept.

This Internal Quality Control (IQC) scheme should at least be an equivalent derivative of the model Quality Control (QC) scheme / plan as shown in the Annex.

Note: Requirements for subcontracting are described in paragraph 3.3 of EN 16763.

8.3. Control of test and measuring equipment

The supplier shall verify the availability of necessary test and measuring equipment for demonstrating product conformity with the requirements in this evaluation guideline.
When required the equipment shall be kept calibrated (e.g. recalibration at interval).
The status of actual calibration of each equipment shall be demonstrated by traceability through a unique ID.
The supplier must keep records of the calibration results.
The supplier shall review the validity of measuring data when it is established at calibration that the equipment is not suitable anymore.

8.4. Procedures and working instructions

The supplier shall be able to submit the following:

- procedures for:
  - dealing with products showing deviations;
  - corrective actions to be taken if non-conformities are found;
  - dealing with complaints about products and/or services delivered;
- the working instructions and inspection forms used.

8.5. Other requirements for the quality system

The supplier must be able to provide the following:

- the organization's organizational chart;
- require the qualification of the personnel concerned.

8.6. Qualification requirements of staff

Staff acting in critical stages of the process needs to be qualified according the model in EN 16763 "Services for fire safety systems and security systems".
In this scheme are following roles defined:
"A" is defined for the manager responsible for the total delivery process of the fire repression system and the stages verification and handover;
"B" is defined for the staff responsible for the planning, design and commissioning process of the fire repression system.
"C" is defined for the staff responsible for the installation and maintenance process of the fire repression system.

8.6.1. Requirements exams/ diplomas

Kiwa will indicate per scope per role in its quality plan which exams or diplomas meet the requirements (technical objectives / procedures / regulations).

The quality of the work delivered is highly dependent on the professional competence of the staff: the right people have to do the right job. The organization must determine from employees involved in the process and/or product as indicated in the Wireless Silent Alarm System that the qualification requirements are met. Only qualified personnel are used to implement the Wireless Silent Alarm Systems specifications. Qualifications are tracked and recorded. An annual evaluation is carried out to ensure that the qualification requirements are still met.

Explanation
It is possible that there is no training or an examination for a specific component, such as "design engineer". Where applicable, reference is made to a training course from the manufacturer as the highest achievable and therefore to be regarded as equivalent. If a training course and examination becomes available for a specific sub-area, as intended, after the publication date of this assessment guideline, the relevant personnel must have successfully completed the examination within 3 years of the availability of this training in order to continue to be considered "qualified".

Note: If only a course becomes available, proof of participation must be submitted within 1 year after this training becomes available.

8.7. Planning audit and inspections

The supplier of the WSAS shall arrange that Kiwa can perform its yearly audit and the necessary inspections on site. The supplier shall use the registration tools of Kiwa.

9. Factory production control components

9.1. General

This chapter contains the requirements for factory production control (FPC) by Kiwa of the manufacturers of essential components (products) of wireless silent alarm systems to determine the quality of these components that the systems have to fulfil. (must wear the CE marking)
This factory production control of the manufacturer of components (products) is necessary if there is no integer information available according to these standards by acceptable approval bodies according ISO 17065 “Conformity assessment - Requirements for bodies certifying products, processes and services”.

9.2. Audit / inspection FPC

The quality system of the supplying manufacturer will be checked by Kiwa based on the IQC scheme / Quality plan.
The inspection contains at least those aspects mentioned in the Kiwa Regulations for Certification and the requirements of the applicable standards.
The quality system of the supplying manufacturer shall be audited externally by Kiwa at least once a year.
Kiwa shall witness a relevant sample of these inspections at least once a year as defined in the Kiwa Quality plan of the scheme and scope.

10. Summary of tests and inspections

This chapter contains a summary of the following tests and inspections to be carried out in the event of certification:

- **initial investigation:** tests in order to ascertain that all the requirements recorded in the evaluation guideline are met;
- **inspection test:** tests carried out after the certificate has been granted in order to ascertain whether the certified products continue to meet the requirements recorded in the evaluation guideline;
- **inspection of the quality system of the supplier:** monitoring compliance of the IQC scheme and procedures.

10.1. Test matrix

Description of requirement	**Article no. scheme**	**Tests within the scope of:**	
		Initial certification	**Inspection by Kiwa after surveillance of certificate** a) / b)
Process requirements WSAS			
Per applicable scope	5	x	x
Product- and service requirements WSAS			
If needed per applicable scope	4	x	x
Testing the performance of the WSAS			
If needed per applicable scope	6	x	x
Factory production control components			
If needed per applicable scope	9	x	x
Quality system and Certification mark			
	7 & 8	x	X

a) In case the product- service or production process changes, it must be determined whether the performance requirements are still met.

b) All product characteristics that can be determined within the visiting time (maximum 1 day) are determined by the site assessor (**SAS**) or by the supplier in the presence of the site assessor (**SAS**). In case this is not possible, an agreement will be made between the certification body and the supplier about how the inspection will take place. The frequency of inspection visits is defined in chapter 11.6 of this certification scheme.

10.2. Inspection of the quality system of the supplier

The quality system of the manufacturer, supplier (design) & installer and/or maintainer is checked by Kiwa on the basis of the IQC scheme / Quality Plan. The inspection contains at least the aspects mentioned in the Kiwa Regulations for Certification and the requirements of the applicable standards.

11. Agreements on the implementation of certification

11.1. General

The certification body must have a procedure that establishes the general rules employed for certification processes.
These rules are in particular:

- the general rules for conducting the pre-certification tests, in particular:
  - the way suppliers are to be informed about how an application is being handled;
  - how the tests are conducted;
  - the decision to be taken as a result of the pre-certification tests.
- the general rules for conducting inspections and the aspects to be audited,
- the measures to be taken by Kiwa in case of Non-Conformities,
- the measures taken by Kiwa in case of improper use of Certificates, Certification Marks, Pictograms and Logos,
- terms for termination of the certificate,
- the possibility to lodge an appeal against decisions of measures taken by Kiwa.

11.2. Certification staff

The staff involved in the certification may be sub-divided into:

- Site assessor (**SAS**): in charge of carrying out external inspections at the supplier's site(s);
- Decision maker (**DM**): in charge of taking decisions in connection with the pre-certification tests carried out, continuing the certification in connection with the inspections carried out and taking decisions on the need to take corrective actions;
- Product manager **(PM)**: in charge of act as a point of contact for the accreditation body, or other relevant third party, for requirements relating to assessment schemes;
- Unit Manager **(UM)**: in charge of establish and document policies and objectives for the assessment and/or certification activities.

11.2.1. Qualification requirements

Qualification requirements for the certification staff consist of qualification requirements for the staff executing the certification activities as laid down in the following table. The competency of the involver certification staff must be demonstrably established.

Basic requirements	Evaluation criteria
Knowledge of organization processes Requirements for conducting professional audits on products, processes, services, installations, design and management systems.	According the policies of Kiwa.
Competence for execution of site assessments. Adequate communication skills (e.g. reports, presentation skills and interviewing technique).	According the policies of Kiwa.
Execution of initial examination.	According the policies of Kiwa.
Conducting review.	According the policies of Kiwa.

Technical competences	Evaluation Criteria
Education	**General**: Education technical area: • Engineering in the context of this scheme.
Testing skills	**General:** • 1 inspection according this scheme including measuring techniques and performing tests conducted together with a qualified **SAS**. • 1 inspection according this scheme including measuring techniques and performing tests conducted self-reliant witnessed by **PM**.
Experience - specific	**SAS** • 2 inspection visits together with a qualified **SAS** • 1 inspection visits conducted self-reliant (witnessed by **PM**)
Skills in performing witnessing	**PM** Internal training witness testing.

Legend:
- Productmanager **(PM)**
- Site assessor **(SAS)**

11.2.2. Qualification
Qualification personnel must be demonstrably qualified by testing their knowledge and skills against the abovementioned requirements. If qualification takes place based on other criteria, this must be put down in writing. The authority with regard to qualification must be established in the quality system of the certification body.

The authority to qualify staff rests with the:
- **UM**: qualification **SAS** of **DM** and **PM**.

11.3. Report initial investigation
The certification body records the results of the initial investigation in a report.
This report shall comply with the following requirements:
- completeness: the report provides a verdict about all requirements included in the evaluation guideline;
- traceability: the findings on which the verdicts have been based shall be recorded and traceable;
- basis for decision: the **DM** shall be able to base his decision on the findings included in the report.

11.4. Decision for issuing the certificate
The decision on the issuing of a certificate or the imposition of measures in respect of the certificate should be based on the findings recorded in the file. The results of an admission examination and a periodic review (in case of a critical deficiency) must be reviewed by a reviewer.
On the basis of the review carried out, the decision-maker will determine whether:
- The certificate may be issued,
- Sanctions are imposed,
- The certificate must be suspended or revoked.

The reviewer and decision-maker must not have been involved in the development of the findings on which the decision is made.
The decision must be recorded in a traceable manner.

11.5. Layout of quality declaration
The Product certificate shall be in accordance with the model included in the Annex I.
The Process certificate shall be in accordance with the model included in the Annex II.
The Services certificate shall be in accordance with the model included in the Annex III.

11.6. Nature and frequency of third party audits

The certification body shall carry out surveillance audits on site at the supplier at regular intervals to check whether the supplier complies with his obligations. The Board of Experts decides on the frequency of audits.

At the time this certification scheme entered into force, the frequency of audits amounts of 1 audit on site per year for suppliers.

The audit program on site shall cover at least:

- the product requirements;
- the production process;
- the suppliers IQC scheme and the results obtained from inspections carried out by the supplier;
- the correct way of marking certified products;
- compliance with required procedures;
- handling complaints about products delivered.

For suppliers with a private label certificate the frequency of audits amounts to one audit per two years. The audits are conducted at the site of private label holder and focus on the aspects inserted in the IQC scheme and the results of the control performed by the private label holder. The IQC scheme of the private label holder shall refer to at least:

- the correct way of marking certified products;
- compliance with required procedures for receiving and final inspection;
- the storage of products and goods;
- handling complaints.

The results of each audit shall be recorded by Kiwa in a traceable manner in a report.

11.7. Non conformities

When the certification requirements are not met, measures are taken by Kiwa in accordance with the sanctions policy.
The Board of Experts has determined the following specific rules for sanctions that must be implemented when carrying out certification by Kiwa. They are informed annually about specific sanctions in the annual report.

11.7.1. Critical deficiency

A critical deficiency is one or more critical deficiencies in the quality system or in the design or product (composition) that can lead to dangerous or unsafe situations. The non-functioning or incorrect functioning of the product. The supplier presents a plan of action within a period to be determined by the certification body. Mistakes made are made immediately. The action plan shall at least consist of:

- An analysis focused on the root cause and/or root causes of the deviation(s)
- The actions to be taken that are immediately necessary to prevent more installations from failing to meet the requirements;
- An analysis focused on the installation delivered since the last assessment since the certification body that may not meet the set requirements and on the extent to which the analysed root causes have led to deviations that have not previously been detected;
- Actions to be taken to repair or repair all delivered installations that do not meet the requirements;
- Solution aimed at preventing recurrence and securing this;
- Assessing the effectiveness of the implementation of this solution.

The supplier shall fully document the corrective actions to be carried out in accordance with the action plan, so that they can be verified by the certification body. The maximum period for implementing the action plan is 3 months.

Within a period of no more than 7 working days after the agreed date of receipt, the certification body will assess the plan of action for efficiency and effectiveness in relation to the deviation found.

11.7.2. Shortcoming

A shortcoming does not directly lead to a dangerous or unsafe situation and has a lesser impact on the quality system or the product. But in such a way that the quality system / product does not meet the objective.

The supplier is given a period of time to take corrective action to be determined by the certification body. Corrective action shall consist of at least:

- An analysis focused on the root cause and/or root causes of the deviation(s);
- The actions to be taken that are immediately necessary to prevent more installations from failing to meet the requirements;
- An analysis focusing on the size of the installation delivered since the last assessment since the certification body that may not meet the set requirements and on the extent to which the analysed root causes have led to deviations not previously detected;
- Actions to be taken to repair or repair all delivered installations that do not meet the requirements;
- Solution aimed at preventing recurrence and securing this;
- Assessing the effectiveness of the implementation of this solution.

The supplier shall fully document the corrective actions to be carried out so that they are verifiable by the certification body.

The certification body assesses the implementation of the corrections and the implementation of the corrective measures within four months of the determination of the deviation.

The certification body may, on a one-off basis, extend the period for corrections and corrective measures by a period of three months.

11.8. Consequences of suspension

In the event of a suspension, the WSAS organization remains responsible for remedying defects in WSAS installations to which the certification mark has been applied.

11.9. Report to the Board of Experts

De certification body shall report annually about the performed certification activities. In this report the following aspects are included:

- mutations in number of issued certificates (granted/withdrawn);
- number of executed audits in relation to the required minimum;
- results of the inspections;
- required measures for established Non-Conformities;
- received complaints about certified products.

11.10. Interpretation of requirements

The Board of Experts may lay down the interpretation of the requirements set out in this certification scheme in one or more interpretation document(s). This interpretation document(s) will be published on the Kiwa website.

11.11. Specific rules set by the Board of Experts

The following specific rules have been laid down by the Board of Experts, which shall be followed when certification is carried out by the certification body.

12. Titles of standards

12.1. Public law rules

Not applicable

12.2. Standards / normative documents

Number	Title	Version*
ISO/IEC 17020	Conformity assessment - General criteria for the operation of various types of bodies performing inspection	
ISO/IEC 17021	Conformity assessment - Requirements for bodies providing audit and certification of management systems	
ISO/IEC 17024	Conformity assessment - General requirements for bodies operating certification of persons	
ISO/IEC 17025	General requirements for the competence of testing and calibration laboratories	
ISO/IEC 17065	Conformity assessment - Requirements for bodies certifying products, processes and services	
EN 54-13	Fire detection and fire alarm systems - Part 13: Compatibility and connectability assessment of system components	2017
EN 54-4	Fire detection and fire alarm systems - Part 4: Power supply equipment	1999/A2:2006
EN 16763	Services for fire safety systems and security systems	2017
IEC 60839-5-1	Alarm and electronic security systems – Part 5-1: Alarm transmission systems – General requirements	2014
EN 50136-1/A1	Alarm systems - Alarm transmission systems and equipment - Part 1: General requirements for alarm transmission systems	2012 + 2018
EN 50136-3	Alarm systems - Alarm transmission systems and equipment - Part 3: Requirements for Receiving Centre Transceiver (RCT)	2013
EN 50518	Monitoring & Alarm Receiving Centre	2019
EN 50131-1	Alarm systems - Intrusion and hold-up systems - Part 1: System requirements	2006
EN 50600-1	Information technology -Data centre facilities and infrastructures – Part 1: General concepts	2019
EN 50600-2-1	Information technology - Data centre facilities and infrastructures - Part 2-1: Building construction	2021
EN 50600-2-2	Information technology - Data centre facilities and infrastructures – Part 2-2: Power distribution	2019
EN 50600-2-3	Information technology - Data centre facilities and infrastructures – Part 2-3: Environmental control	2019
EN 50600-2-4	Information technology -Data centre facilities and infrastructures – Part 2-4: Telecommunications cabling infrastructure	2015
EN 50600-2-5	Information technology - Data centre facilities and infrastructures – Part 2-5: Security systems	2021
K21030	Certification of Alarm Transmission Service Providers	2020
K21048	Secure Remote Access of Alarm Systems for Remote Services / handling	2019

NEN 2575-3+A3	Fire safety of buildings - Evacuation alarm systems – System and quality requirements and projection guidelines – Part 3: Loud alarm system type B	2012 + 2023
NEN 2575-4	Fire safety of buildings – Evacuation alarm systems – System and quality requirements and guidelines for locating of alarm devices – Part 4: Wireless silent alarm installation	2013
NEN 2654-2	Management, inspection and maintenance of fire protection systems - Part 2: Evacuation alarm systems	2018
DIN 14675-1	Fire detection and fire alarm systems – Design and operation	2020
NPR 2576	Circuit integrity under fire conditions – Guideline for transmission paths	2018

*) When no date of issue has been indicated, the latest version of the document is applicable for new systems. Kiwa shall inform the certificate holders about changes in version. For design, installation and maintenance is the version of standard applicable set in the basic design.

I. Model Product certificate (example)

Certificate

Certificate
K-XXXXXXX-X

kiwa

Issued	Fill in date	Replaces	Fill in text
Valid from	Fill in date	Valid until	Fill in date
		Page	Fill in code

Wireless Silent Alarm Systems
Product

Statement from Kiwa
With this certificate, issued in accordance with the Kiwa Regulations for Certification, Kiwa declares that on the basis of assessments by Kiwa there is a justified expectation that products supplied by

Company

meet the requirements as stated in the Kiwa company scheme K21407/05 "Wireless Silent Alarm Systems" dated xxxx-xx-xx as:

A. Manufacturer

Signature

Name
Managing Director Nederland

This certificate remains the property of Kiwa. Publication of the statement is permitted.

Kiwa Nederland B.V.
Sir Winston Churchilllaan 273
Postbus 70, 2288 AB Rijswijk
Phone 088 998 44 00
www.kiwa.nl

Performed by:
Kiwa FSS Certification
NL.Infocertification.fss@kiwa.com
www.kiwafss.nl

Company
Legal entity
Address, postal code
Place
website

Location(s)
make sub-lines freely fillable

Certification process consists of initial and a at minimum yearly assessment of:
- **Quality assurance system**
- **Technical requirements**

II. Model Process certificate (example)

Certificate

Certificate
K-XXXXXXX-X

kiwa

Issued	Fill in date	Replaces	Fill in text
Valid from	Fill in date	Valid until	Fill in date
		Page	Fill in code

Wireless Silent Alarm Systems
Process

Statement from Kiwa
With this certificate, issued in accordance with the Kiwa Regulations for Certification, Kiwa declares that on the basis of assessments by Kiwa there is a justified expectation that processes supplied by

Company

meet the requirements as stated in the Kiwa certification scheme K21407/05 "Wireless Silent Alarm Systems" dated xxxx-xx-xx for:

B. Design & - Installation

Signature

Name
Managing Director Nederland

This certificate remains the property of Kiwa. Publication of the statement is permitted.

Kiwa Nederland B.V.
Sir Winston Churchilllaan 273
Postbus 70, 2288 AB Rijswijk
Phone 088 998 44 00
www.kiwa.nl

Performed by:
Kiwa FSS Certification
NL.infocertification.fss@kiwa.com
www.kiwafss.nl

Company
Legal entity
Address, postal code
Place
website

Location(s)
make sub-lines freely fillable

Certification process consists of initial and a at minimum yearly assessment of:
- **Quality assurance system**
- **Technical requirements**

III. Model Services certificate (example)

Certificate

Certificate
K-XXXXXXX-X

kiwa

Issued	Fill in date	Replaces	Fill in text
Valid from	Fill in date	Valid until	Fill in date
		Page	Fill in code

Wireless Silent Alarm Systems
Services

Statement from Kiwa
With this certificate, issued in accordance with the Kiwa Regulations for Certification, Kiwa declares that on the basis of assessments by Kiwa there is a justified expectation that services supplied by

Company

meet the requirements as stated in the Kiwa certification scheme K21407/05 "Wireless Silent Alarm Systems" dated xxxx-xx-xx for:

C. Maintenance

Signature

Name
Managing Director Nederland

This certificate remains the property of Kiwa. Publication of the statement is permitted.

Kiwa Nederland B.V.
Sir Winston Churchilllaan 273
Postbus 70, 2288 AB Rijswijk
Phone 088 998 44 00
www.kiwa.nl

Performed by:
Kiwa FSS Certification
NL.infocertification.fss@kiwa.com
www.kiwafss.nl

Company
Legal entity
Address, postal code
Place
website

Location(s)
make sub-lines freely fillable

Certification process consists of initial and a at minimum yearly assessment of:
- **Quality assurance system**
- **Technical requirements**