



National Security Inspectorate

Sentinel House, 5 Reform Road, Maidenhead, SL6 8BY

E: nsi@nsi.org.uk | W: nsi.org.uk

Security.Improved

Date: 06 December 2019

To: All NSI ARC Gold approved companies and applicants for ARC Gold Approval

TECHNICAL BULLETIN No: 0050

Publication of BS EN 50518:2019 - Monitoring and Alarm Receiving Centre

BS EN 50518:2019 was published on the 31st August 2019 and is available from the BSI or NSI as an individual purchase or through the NSI Standards on Subscription service for approved companies.

Implementation timescale for applicant companies

New applicant companies will be audited against BS EN 50518:2019 with immediate effect, and any Improvement Needs recorded against clauses of the Standard will have to be satisfactorily addressed before approval can be granted.

Where an application for approval to BS 5979:2007 or the 2013 BS EN 50518 series was already in progress with the NSI before the date of this Technical Bulletin, then the approval will continue to progress against the appropriate standard i.e. BS 5979:2007 or the 2013 BS EN 50518 series.

Implementation timescale for existing approved companies

Existing NSI approved companies who are approved to BS 5979:2007 or the 2013 BS EN 50518 series will continue to be audited against BS 5979:2007 or the 2013 BS EN 50518 series.

Existing NSI approved companies requesting approval for a new ARC will be audited to BS EN 50518:2019 with immediate effect and any Improvement Needs recorded against clauses of the Standard will have to be satisfactorily addressed before approval can be granted.

Details of the changes

Where the actual wording of the Standard is quoted, it is reproduced in bold text.

Where it is considered relevant, further clarification is included in italics.

Please note this is not a definitive list of all the changes between BS EN 50518:2019 and the 2013 BS EN 50518 series of standards. Only the significant changes are detailed below.

BS EN 50518:2019 introduces two categories of ARC. Where an ARC monitors security related connections, e.g. Intruder, holdup, security CCTV, etc., the ARC must meet Category I of BS EN 50518:2019. Category I ARCs will be designed, constructed and operated to a higher standard than a Category II ARC.

Standard references have been updated to the latest editions.

Many clauses are renumbered and divided to provide separate requirements for Category I and Category II ARCS. Where a clause does not identify separate requirements for each ARC category, then the requirement applies to both ARC categories.

Many clauses found in the 2013 series of standards have been consolidated as a result of making a single part standard based on the previous 3-part series.

Annex A, B, C and NA are Informative and provide information and guidance.

A - Typical ARC layout category I.

B - Security and technical implications of remote access to ARC data.

C - Alarm management system requirements.

The National Annex NA – provides Guidance on the UK implementation of BS EN 50518:2019

Note: The National Annex NB provides requirements where the main body of the standard states there is no requirement, this annex as a national Annex is deemed to contain normative requirements,

Requirements included in Annex NB are provided within this technical bulletin and will be identified by a dashed border, each requirement will appear below the appropriate clauses, where 'no requirement' is stated.

1 Scope

This document specifies the minimum requirements for monitoring, receiving and processing of alarm messages generated by alarm systems taking place as a part of the total fire, safety and security solution.

For the purpose of this document, the term "alarm" is used in the broad sense to include fault, status and other messages received from one or more of a range of safety and security alarm systems such as, but not limited to, fire detection and fire alarm systems, fixed firefighting systems, intrusion and holdup alarm systems, access control systems, video surveillance systems, social alarms systems and combinations of such systems.

This document gives requirements for two categories of ARC, Category I and Category II. A Category I ARC will be designed, constructed and operated to a higher standard with respect to construction, security and integrity than a Category II ARC.

The categorization is determined according to the type(s) of alarm messages handled.

Category I: ARCs handling messages from security applications:

- I&HAS's;
- access control systems;
- VSS in security applications that require an emergency response (for example loss prevention);
- people monitoring, lone workers and object tracking systems for security applications;
- alarm messages handled by category II ARCs;
- combinations of the above systems.

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

- fire alarm systems;
- fixed firefighting systems;
- social alarm systems;
- audio/video door entry systems;
- VSS in non-security applications (for example traffic flow);
- people monitoring, lone workers and object tracking systems for non-security applications;
- lifts emergency systems;
- combinations of the above systems.

The requirements apply to ARC's (whether established in single or multiple sites) monitoring and processing alarms generated by systems installed at other locations and also to ARC's monitoring solely alarms from systems within their own site.

The document includes functional and specific requirements supporting the services of an ARC.

The document does NOT apply to:

- alarm systems used for non-civil purposes;
- alarm systems for medical or health applications.

The scope has widened to include monitoring of social alarms, CCTV, Lone worker systems, emergency systems in lifts, etc. the types of monitoring applicable to each category of ARC is listed in the scope.

2 Normative references

All normative standard references are undated leading to the latest edition being applicable, also a number of new standards are referenced to provide requirements for new monitoring types listed in the scope.

3.1 Terms and definitions

3.1.3

alarm handling delay

procedure whereby signalled alarm conditions are intentionally delayed at the ARC and their status reviewed for the purpose of preventing unnecessary calls to the relevant response service by cancelling certain alarm conditions, where such cancellation is authorized by the user at the supervised premises

'Alarm handling delay' is a new definition.

3.1.4

alarm management system

AMS

system which stores, organises, controls, manages and allows retrieval of client data and is interfaced to alarm receiving equipment for automatic annunciation of messages for each alarm system

'Alarm management system' is a new definition and broadly replaces Annunciation equipment used in the 2013 edition.

3.1.7

alarm receiving centre shell

ARC shell

all structural elements of the ARC perimeter (walls, entrance lobby, windows, glazed areas, floors, ceilings, entry and exit doors, entry and exits points of ventilation ducts, entry and exit points for other service cables and ducts, transfer hatches/chutes)

'Alarm receiving centre shell' is a new definition.

3.1.13

disruptive event

any natural or man-made occurrence that may cause the discontinuation of orderly ARC activities according to standard operating procedures and requires the execution of special procedures

Note 1 to entry: Such as (but not limited to):

- **failure of power supply;**
- **failure of inbound communication systems;**
- **failure of outbound communication systems;**
- **failure of IT systems, loss of data;**
- **fire;**

- **extreme weather conditions, such as storm, flooding, lightning;**
- **natural disasters such as earthquakes or landslides;**
- **damage by vehicles from land and air;**
- **hazardous gases and reduction of oxygen levels in the ambient air;**

'Disruptive event' is a new definition.

3.1.15

expected message

message which has to reach the ARC according to predefined schedules (in particular status messages from alarm systems and communication systems)

'Expected message' is a new definition.

3.1.17

fire resistance

ability of an element of building construction, component or structure to fulfil, for a stated period of time, the required stability, fire integrity and/or thermal insulation and/or other expected duty in a standard fire resistance test

'Fire resistance' is a new definition.

3.1.20

installer

legal entity which installs systems

'Installer is' a new definition.

3.1.21

key performance indicator

KPI

business statistics which measure an organization's performance

'Key performance indicator' is a new definition.

3.1.22

message

series of signals routed via interconnections which include identification, function data and the various means for providing its own integrity, immunity and proper reception

'Message' is a new definition taken from BS EN 50131-1:2006.

3.1.26

responder

organization or person which executes actions upon request by an ARC

'Responder' is a new definition.

3.1.27

security application

application(s) designed to detect a hazard which may cause harm or damage from criminal actions to humans, property, objects or assets

'Security application' is a new definition.

3.1.32

time stamp

value, which assigns a unique time to an event

'Time stamp' is a new Definition.

3.2 Abbreviations

AMS Alarm management system

KPI Key performance indicator

SOP Standard operating procedure

UPS Uninterruptible power system

UTC Coordinated Universal time

VSS Video surveillance system (formerly called CCTV)

The above are new abbreviations.

4 Planning

4.1 Categorization

The planning for the construction of an ARC should be determined by the intended categorization.

ARC's are categorized according to the type(s) of alarm messages handled and the consequent requirements for integrity and security of construction, communications, operation and information.

This standard gives recommendations for two categories of ARC as described in the scope.

Unless otherwise stated the requirements in this standard apply to both Category I and Category II ARC's'.

Categorisation defines which category should be selected dependant on the types of alarm messages being handled. NOTE the categorisation is reversed when compared with BS 5979 i.e. Category I is for security related connections.

5.2.1 Category I

The ARC shell is intended to provide equivalent protection for all structural elements of the ARC. They shall provide resistance against physical attack in compliance with Table 1.

Table 1 — Minimum resistance against physical attack for ARC shell

Construction elements	Materials	Thickness
Walls of the shell of the ARC and the walls of the entrance lobby (see Annex A)	Solid masonry Cast concrete Reinforced concrete Solid steel	≥ 200 mm ≥ 150 mm ≥ 100 mm ≥ 8 mm
Internal walls	No requirement	No requirement
Floors and ceilings	Cast concrete Reinforced concrete Solid steel	≥ 150 mm ≥ 100 mm ≥ 8 mm ^a
Where the ARC is located on an upper floor > 4 m above ground or any adjacent standing plane the wall thickness may be reduced by 50 %.		
^a Thickness of steel may be reduced by 50 % where not directly accessible to the general public		

The construction elements listed in Table 1 cover the minimum resistance against physical attack. If other construction methods or material are applied it shall be demonstrable that the resistance against physical and bullet attack is equal to that listed in Table 2.

A reduced requirement is provided for an ARC situated on upper floors (5th row of table 1) and where the general public don't have access to floors or ceilings made of steel (6th row of Table 1).

5.2.2 Category II

The ARC shell shall consist of a physical barrier able to prevent unauthorised access, such as provided by walls, doors, floor and ceiling.

Category II is a new ARC category.

This clause provides basic requirements for the construction of a category II ARC, this is then supplemented by Annex NB which as a national annex will be deemed to provide normative requirements for a category II ARC.

5.3 Perimeter doorsets – resistance against physical attack and bullet attack

The resistance against physical attack and bullet attack of at least one of the entrance lobby doors and all other perimeter doorsets shall be in compliance with Table 2.

Table 2 — Physical attack and bullet attack

	Physical Attack	Bullet Attack
Doorsets Category I	EN 1627 resistance class 3 (RC3)	EN 1522 classification FB3
Doorsets Category II	EN 1627 resistance class 2 (RC2)	No requirements

Category II is a new ARC category.

This clause defines the physical attack protection required for all external door sets and at least one entrance lobby Door set. (see the third row of Table 2).

5.4 Glazed areas

5.4.1 Category I

Windows in the ARC shell shall be locked from the inside at all times except where an emergency exit procedure has been initiated or for maintenance purposes and shall offer resistance to physical attack and bullet attack as specified in Table 3.

Table 3 — Category I physical attack and bullet attack

	Physical attack	Bullet attack
Windows	EN 1627 resistance class 3 (RC3)	EN 1522 classification FB3
Glazing	EN 356 classification P5A	EN 1063 classification BR 3 – S

The interior of the ARC shall not be visible from outside of the ARC shell.

Windows and glazing should provide a resistance to fire and smoke of not less than 30 min.

There is an additional requirement for a category I ARC which allows the use of windows, Table 3 provides protection requirements for both Physical and Bullet attack.

5.4.2 Category II

No requirements.

Annex NB provides requirements where the main body of the standard includes 'no requirement' for a category II ARC.

National Annex - NB.1.1.1 Glazed areas: Category II

Displayed information should not be visible from outside the shell of the ARC.

Accessible glazed areas in a Category II ARC should be provided with vandal-resistant glazing (e.g. laminated glass at least 7.5 mm thick or wired glass).

NOTE This recommendation relates to clause 5.4.2 of BS EN 50518:2019

5.7.2 Entrance to the ARC

5.7.2.1 Category I – Entrance Lobby

Entrance to and exit from the ARC shall be by two doors, separated by an entrance lobby the floor area of which shall not exceed 6 m². One of the doors of the entrance lobby shall have a fire resistance according to 5.5. The second door shall fulfil the requirements of Table 2 category I.

The doors shall be interlocked to prevent both being opened at the same time during normal entry and exit. The interlock may be overridden in exceptional instances such as an emergency allowing both doors to open. Both doors shall open outwards from the ARC (see Annex A) and shall be fitted with automatic self-closing and locking devices.

Both doors shall be secured by electromechanical locking/unlocking devices in compliance with EN 14846 having a classification code as a minimum of Table 4, operable only from within the ARC.

Table 4 — Electromechanical lock classification code

Digit	1	2	3	4	5	6	7	8	9
EN 14841	3	S	2	D	0	L	6	1	3

There shall be a mechanical override for emergency release, protected against accidental use. If the locking device is being fitted in the door, the electrical cable to the lock shall be contained in a metal armoured door loop, and otherwise be mechanically protected where exposed.

A means shall be provided within the ARC to allow the locking devices to be overridden in the event of emergency exit.

It is permissible to have more than one entry/exit lobby provided they comply with this clause.

5.7.2.2 Category II

Entrance doorsets shall be secured by means of a locking device to meet EN 1627 RC2.

The maximum dimensions of the lobby doors are no longer defined in this standard.

Electro mechanical locks must comply with BS EN 14846 as illustrated in table 4.

It is now permitted to have more than one Lobby to the ARC but all must comply with the requirements of this clause.

Category II is a new Category of ARC.

5.7.3 Emergency entry

Where entrance to the ARC is controlled by operators within the ARC a facility or procedure should be provided to gain entry to the ARC without the aid of persons within. Any keys, codes or cards used to gain entry should be stored in a secure location, for example in a safe, and access to this should be restricted to a list of nominated person(s). This facility should not be used as a normal means of entry only being used in exceptional circumstances such as an emergency.

This clause describes requirements for re-entry to the ARC in an emergency condition.

5.7.4 Emergency exit(s)

Emergency exit door(s) shall open outwards and shall be provided with unlocking devices in compliance with EN 179, EN 1125 or EN 13637 as appropriate, intended to be released only in the event of an emergency. The unlocking devices shall be operable only from inside the ARC.

Two additional Standards relating to compliant unlocking devices for emergency exits are now listed, providing more choice.

5.7.5 Ventilation

5.7.5.1 Category I

Ventilation systems serving an ARC shall be controlled from within the ARC. All vents shall be protected with air-tight flaps which can readily be closed either manually from inside the ARC or automatically in the event of suspicion that gas or smoke is being drawn into the ARC.

Where the cross-sectional area of a ventilating inlet or outlet exceeds 0.02 m², suitable alarm detection equipment shall be fitted to detect any attempt to enter the ventilation inlet or outlet.

This clause does not require that ventilation systems to meet or to be certified to any defined standards.

5.7.5.2 Category II

No requirement.

Annex NB provides requirements where the main body of the standard includes 'no requirement' for a category II ARC.

National Annex NB - NB.1.1.2 Ventilation: Category II
Ventilation should be controllable from within the ARC.
NOTE This recommendation relates to clause 5.7.5.2 of
BS EN 50518:2019 5.7.6 Service inlets and outlets

5.7.6.1 Category I

A breach in the ARC shell for the admission of any service cables or pipe shall not exceed 0.02 m² in cross-sectional area. All breaches in the ARC shell shall be filled with fire resistant material to minimize fire and smoke propagation into the ARC shell from outside.

This clause introduces less rigorous requirements for filling in any clearance around cables and or pipes entering or leaving the ARC.

5.7.6.2 Category II

No requirement.

Annex NB provides requirements where the main body of the standard includes 'no requirement' for a category II ARC.

National Annex NB - NB.1.1.3 Service inlets and outlets: Category II
Cable and service ducts should be sealed where they penetrate walls, floors, etc., to maintain the fire resistance of the ARC.
NOTE 1 Attention is drawn to the Regulatory Reform (Fire Safety) Order 2005 in England and Wales and equivalent legislation in Scotland and Northern Ireland
NOTE 2 This recommendation relates to clause 5.7.6.2 of BS EN 50518:2019

5.7.7 Transfer hatch / chute

5.7.7.1 Category I

A transfer hatch or chute may be located in the ARC shell.

The hatch / chute shall be constructed with material that provide a resistance to physical and bullet attack as equal to that listed in Table 2. The points of entry shall be interlocked to

prevent direct access to the ARC being available at any time and the opening and closing actions shall be controlled from within the ARC. The outer entrance shall open outwards away from the ARC.

Voice communication system(s) shall be available between the operations area of the ARC and the outer entry of the hatch/chute.

This clause adds clarification that the Transfer hatch or chute shall meet the requirements of table 2 to protect against bullet attack.

5.7.7.2 Category II

No requirement.

Annex NB provides requirements where the main body of the standard includes 'no requirement' for a category II ARC.

National Annex NB - NB.1.1.4 Transfer hatch / chute: Category II

A transfer hatch or chute may be located in the shell of the ARC.

The hatch/chute should open into a security controlled area. The hatch/chute should be constructed to a standard similar to that of the shell of the ARC. The points of entry should be interlocked to prevent direct access to the ARC being available at any time and the opening and closing actions should be controlled from within the ARC. The outer entrance should open outwards away from the ARC. Voice communication system(s) should be available from inside the ARC and the outer entry of the hatch/chute.

NOTE This recommendation relates to clause 5.7.7.2 of BS EN 50518:2019

5.8 Location of data processing equipment

5.8.1 Category I

5.8.1.1 General

The following receiving centre equipment shall be under the responsibility of the ARC and should be located within the ARC shell:

- **interface of the AMS for interconnection with RCT (IRCT);**
- **servers of the alarm management system (databases, storages);**
- **voice recording equipment;**
- **active network components (routers, switches);**
- **passive network components (patch panels, cabling);**
- **communication equipment (Private Automatic Branch Exchange, PABX);**
- **internal transfer point LAN / WAN (Network provider).**

NOTE The necessity of RCTs within an ARC of category I and the responsibility for these RCTs may depend on a so called hosted or non-hosted solution provided by the alarm transmission system provider (ATSP) as described in EN 50136-1.

Clause 9.1.12 and 9.1.20 should be considered.

This clause defines equipment that must be located inside the shell of the ARC.

5.8.1.2 Equipment room located in the same building or premises at the ARC

Where all or part of the equipment in 5.8.1 is not located inside the ARC shell the following shall be provided in the same building or on the same premises where the ARC is located:

- a documented risk assessment shall be completed in accordance with 4.2;
- construction requirements shall provide a resistance to physical attack in accordance with 5.2.1, 5.3, Table 2 and 5.4.1;
- resistance against fire and smoke in compliance with 5.5;
- protection against lightning in compliance with 5.6;
- alarm systems in compliance with 6.1.2, 6.1.3, 6.1.4 and 6.1.9;
- electrical power supplies in compliance with Clause 7;

NOTE The standby power supplies of the ARC as described in 7.2 can also be used for the location of data processing equipment.

- external power cables and communication cabling to the ARC shell should be protected against physical and fire damage.

An entrance lobby is not required, access to this area shall be controlled and authorized by the ARC and include a video surveillance system whose images are viewable from within the ARC to identify authorized persons before permitting them to enter the location of data processing equipment.

This is a new clause providing requirements for equipment rooms located within the same building or premises as the ARC shell.

5.8.1.3 Equipment room located at a remote location from the ARC

Where all or part of the equipment in 5.8.1 is not located inside the ARC shell and is in a remote location from the ARC, the following shall be provided:

- a data centre designed and maintained according to EN 50600 or another category I ARC in accordance to EN 50518;
- the performance of the link between the remote location and the ARC in terms of the data security, substitution protection and availability shall be equal or higher than defined in EN 50136- 1 category DP4.

If the ARC as a redundancy has a secondary location for data processing equipment it shall fulfill the requirements of a category I equipment room.

This new clause provides requirements for equipment rooms located remotely from the building or premises where the ARC is located.

5.8.2 Category II

The following receiving centre equipment shall be under the responsibility of the ARC:

- **receiving centre transceiver (RCT);**
- **interface in the AMS for interconnection with RCT (IRCT);**
- **servers of the alarm management system (databases, storages);**
- **voice recording equipment;**
- **active network components (routers, switches);**
- **passive network components (patch panels, cabling);**
- **communication equipment (Private Automatic Branch Exchange, PABX);**
- **internal transfer point LAN / WAN (Network provider).**

Where all or part of the above equipment is not located inside the ARC shell the following shall be provided in a secure location that complies with one of the following published standards for data centres:

- **a data centre designed and maintained to EN 50600, or;**
- **ARC in accordance to EN 50518 in category I or II which has its equipment room located in the same building or premises where it is located in.**

The performance of the link between the secure location and the ARC in terms of the data security, substitution protection and availability shall be equal or higher than defined in EN 50136-1 category DP4.

Category II is a new Category of ARC.

5.9 Communication cables

5.9.1 Category I

All communication cables between the point of entry into the building and the shell should be protected against physical and fire damage.

All cable based connections and wireless connections carrying alarm messages to and from the ARC and the remote I&HAS connected to the ARC shall be protected in accordance with EN 50136-1.

There shall be a 24 h support service that can be called on for all telecommunications circuits, the failure of which would affect the monitoring of alarm signals or the extension of alarm signals or alarm messages to the emergency services.

Requirements for communications cables have been expanded to require protection against physical attack and fire damage. Also a 24hr support service should be in place for any telecommunications

circuits, where failure of these circuits would have an impact on any incoming alarm signals or outgoing alarm response messages for the emergency services.

5.9.2 Category II

No requirements.

Annex NB provides requirements where the main body of the standard includes 'no requirement' for a category II ARC.

National Annex NB - NB.1.1.5 Communication cables: Category II

All communication cables between the point of entry into the building and the shell should be protected against physical and fire damage.

All cable based connections and wireless connections carrying alarm messages to and from the ARC and the remote alarm systems connected to the ARC should be protected in accordance with BS EN 50136-1:2012+A1:2018.

There should be a 24 h support service that can be called on for all telecommunications circuits, the failure of which would affect the monitoring of alarm signals or the extension of alarm signals or alarm messages to the emergency services.

NOTE This recommendation relates to clause 5.9.2 of BS EN 50518:2019

5.10 Facilities

5.10.1 Category I

Toilet and washing facilities shall be provided within the ARC shell.

The location of any cooking facilities is no longer restricted.

5.10.2 Category II

No requirements.

Annex NB provides requirements where the main body of the standard includes 'no requirement' for a category II ARC.

National Annex NB - NB.1.1.6 Facilities: Category II

Toilet and washing facilities should be provided within the ARC shell.

NOTE This recommendation relates to clause 5.10.2 of BS EN 50518:2019

6 Alarm systems of the ARC

6.1 Category I

6.1.4 Fire

The areas of the building occupied by the company which operates the ARC, and in which the ARC is located, shall be protected by a fire detection system in accordance with national requirements for the highest level of property protection and life safety incorporating components certified according to the EN 54 series.

A fire alarm shall be installed to national requirements i.e. compliant with BS 5839-1 at category L1/P1, rather than to EN54-14 as was required by the 2013 edition of BS EN 50518.

6.1.5 Entry / exit

An audible or visible alarm shall operate within the ARC to notify the operators when any entrance or exit door to the ARC or lobby is not secured, except where the entrance lobby doors have been opened for authorized entry / exit.

An alarm condition shall be signalled when an emergency exit door is opened or both of the entry doors to the lobby and ARC are open at the same time.

This clause provides clarification that where an entrance lobby door is opened for authorized entry or exit an audible alarm is not required.

There is also a new requirement for an alarm condition to be signalled where an emergency exit door is opened, and or both lobby entry doors are opened simultaneously in any lobby.

6.1.8 Safety monitoring

The safety and security of the ARC operators shall be automatically checked at a maximum of 60 min intervals. When the check is made if there is no response within 60 s an alarm shall be automatically extended to another ARC meeting the requirements for category I of this standard.

Failure of the 'safety monitoring' check must be signalled to another category I ARC.

6.1.9 Messages from the ARC alarm systems

Messages from the ARC alarm system (see 6.1.1) shall be notified to another ARC meeting the requirements of category I of this standard. The ARC receiving the messages shall not be

located in the same building. The alarm transmission system for the alarm system shall as a minimum be in accordance with EN 50136-1 category SP4 or DP3.

The category of ATS used to signal alarm messages from the ARC alarm systems shall meet the requirements of SP4 or DP3 as defined in BS EN 50136-1.

6.1.10 Video surveillance system

Video surveillance systems shall be provided so that:

- a) All approaches to the building in which the ARC is located can be monitored from within the ARC in accordance with the application guidelines in EN 62676-4.**
- b) ARC employees can identify authorized persons before permitting them to enter the entrance lobby, to view any activity therein and to ensure a safe exit.**
- c) ARC employees can identify any personnel using a transfer hatch / chute.**

Reference to the CCTV application guidelines standard is updated to BS EN 62676-4.

6.2 Category II

The ARC shall be fitted with an I&HAS in accordance with EN 50131-1 minimum grade 2 and shall include at least one hold-up device.

The areas of the building occupied by the company which operates the ARC, and in which the ARC is located, shall be protected by a fire detection system in accordance with national requirements for the highest level of property protection and life safety incorporating components certified according to the EN 54 series.

Category II is a new Category of ARC.

7 Electrical power supplies

7.1 Mains supply

The mains supply shall be used as the principal source of electrical power, although reliable alternatives can be used. There shall be an indication in the operations area of the current source of power. If the mains supply fails an audible or visible alarm sufficient to alert operators should be signalled in the operations area. The mains supply shall be such that it is capable of providing sufficient power for the normal load of the ARC and for simultaneously recharging the UPS standby energy storage devices (batteries) to the required capacity within 24 h.

In the event of a mains power fail an audible a visual alarm must be available to the ARC operators in the operations area.

7.2 Standby power supplies

7.2.1 General

A standby power supply shall be of sufficient capacity for the uninterrupted operation of all communication, signalling, monitoring, recording, electrically operated door locks, essential ventilation and essential lighting equipment, including that required for the necessary surveillance for a period of 24 h based on a demand of 1.2 times the maximum expected load.

Changeover to, or from, a standby power supply shall not affect the normal operation of equipment.

The standby power supply shall be by a generator or generators supported by an UPS according to EN 62040-1.

A Stand by Power supply must in addition to the requirement of the 2013 edition of BS EN 50518, provide power to electrically operated door locks. There must be sufficient backup power to maintain defined systems for 1.2 times the total load.

7.2.2 UPS

The UPS and any automatic changeover equipment should be located within the shell of the ARC. As an exception, if the UPS and/or automatic changeover equipment is not installed within the ARC shell the following shall apply:

- a) Category I — the UPS and/or automatic changeover equipment shall be in an area complying with the construction requirements of a category I ARC as described in 5.2.1, 5.3, 5.4.1, 5.5, 5.6 and alarm system in accordance with 6.1.2, 6.1.4 and 6.1.5;**
- b) Category II — the UPS and/or automatic changeover equipment shall be in an area complying with the construction requirements of a category II ARC as described in Clause 5 and alarm system as 6.2.**

Where the UPS is located outside the shell of the ARC access to this area shall be authorized by the ARC and include a VSS whose images are viewable from within the ARC.

The UPS shall be brought into use automatically immediately after the primary voltage falls below the level required to operate the ARC. The ARC shall return to primary power operation and the energy storage devices of the UPS shall recharge automatically when the primary voltage is restored.

Battery installations shall conform to EN 50272-2.

Where a standby generator is used, the UPS capacity shall be sufficient to power the ARC equipment as described in 7.2.1 for at least 10 min.

Category II is a new Category of ARC.

Where by exception a UPS is fitted outside the shell of the ARC, VSS images of the entrances to the UPS shall be available from within the ARC to aide authorised entry.

8 Alarm Management System

8.1 General

An AMS is a system which stores, organizes, controls, manages and allows retrieval of client data and is interfaced to alarm receiving equipment for automatic annunciation of messages for each alarm system. The main purpose of an AMS is receiving and presentation of alarm information and messages. A typical AMS is described in Annex C.

Figure 2 shows the sequence of events under ARC responsibility applicable for any alarm message generated by an alarm system as detailed within the scope of this standard after completion of processing by the RCT. Where applicable this should be interpreted together with EN 50136-1:2012, Figure 1. This standard applies to an AMS handling the events from TRCT to TReaction.

8.2 Time synchronization of equipment

Any item of equipment where a time reference is recorded for the purpose of providing the ARC service shall be synchronised to a UTC time source. The synchronization can be achieved by the AMS itself, by ARC personnel, or by an internal or external source.

Synchronization shall be carried out at least every 24 h. The lack of synchronization over 24 h should be treated in the AMS as a fault. When a specific difference of more than 5 s occurs in the synchronization of the AMS time with UTC time, it shall be treated as a fault.

For components with a GUI (graphical user interface) for alarm processing, the local time used by the ARC shall additionally always be available.

Failure of time synchronisation or where the time difference between the AMS and UTC time is greater than 5 seconds should be recognised as faults by the AMS.

Components with a GUI for alarm processing shall have the ARC time always available.

8.4 Storage of master data

The master data for each alarm system connected to the ARC shall be stored and easily available on an “as-needed basis” to management and to ARC operators. The master data shall be kept current at all times. Changes in master data shall be date and time stamped. Master data changed due to a contractual change, due to a change in the client organization, or becoming obsolete following a contract cancellation or amendment shall be retained for a minimum period of three years.

Master data shall include:

- **unique AS reference number;**
- **name, address, phone numbers of supervised premises;**
- **actions to be taken for each alarm message;**
- **contact details for responder(s) (emergency services, Key Holder);**
- **any other specific data required for the ARC to handle alarm messages and carry out agreed actions;**
- **definition of priority level alarms and of related response times (if different from default performance defined above).**

Retention of master data records for each connection shall be for 3 years beyond the cancellation of the related connection.

Additional data shall be recorded as part of the master data for each connection, i.e. contact information for responders, actions to be taken for each alarm message, definition of alarm event priority if not set to the default value.

9 Operation of the ARC

9.1 Procedures – General

9.1.1 General

Standard Operating Procedures (SOP's) shall be established and made available to all staff as required by their function. Each SOP shall identify those responsible for its design, implementation, execution, evaluation and maintenance. Where KPI's are required to measure SOP execution and quality levels they shall be identified together with the method of measurement. An overview documenting the valid release date of each SOP shall be maintained at all times. Documented SOP's shall exist for the following:

Provision of SOPs should be made available to all staff appropriate to their role.

9.1.2 Creation, modification and cancellation of services or customer accounts

The procedure shall include how master data are modified and how master data as described in 8.3 and 8.4 is archived.

9.1.4 Communication with response services

Procedures shall include any specific information as agreed or required by the response services such as police, fire, guards and key holders.

9.1.5 Individual services provided by the ARC

The procedure shall include each one of the services provided by the ARC including performance or other KPI's.

9.1.7 Unexpected increase in alarm signals

The procedure shall describe contingency measures in place to accommodate unexpected increases in alarm activity caused by for example bad weather, communication outages.

9.1.8 Alarm transmission path failures

The procedure shall describe how alarm transmission path (ATP) failures are handled and include performance indicators.

9.1.9 Controls to maintain quality of service

The procedure shall include the control measures that are in place to prevent poor response by the ARC towards protected persons or objects. It should include monitoring of execution (technical/human) of response according to the agreed action plan.

9.1.10 Installation, maintenance, protection, removal and reuse of assets under the control of the ARC

The procedure shall describe who is allowed to approve and execute installation, maintenance, removal and disposal/reuse of assets. This shall take into account the specific risks related to the data and licensed software that may be included in the assets. The procedure shall ensure that unattended assets have appropriate protection.

9.1.11 Monitoring and testing of equipment

For the correct operation of the ARC the following regular monitoring and testing of all equipment are required and the results recorded:

— Daily

RCT's, AMS, the annunciation equipment, the ARC's communication and network equipment, as well as all voice communication lines shall be monitored for correct functioning.

— Monthly

All components of the electrical power supply system as defined in 7.1 and 7.2, and the ARC's own alarm systems shall be monitored and tested for correct functioning.

— Yearly

All components of the electrical power supply system as defined in 7.1 and 7.2, and the ARC's own alarm systems shall be monitored and tested by shutdown of the primary power supply.

In addition to Daily monitoring and testing requirements, Monthly and Yearly monitoring and testing is required.

9.1.13 Information management

The procedure shall describe how all data are maintained stored, organized, modified, managed and retrieved. The SOP shall detail how master data are interfaced to all alarm receiving equipment for automatic annunciation of all messages for each alarm system and for retention of records of client related operational events. Additional procedures shall describe how the data are maintained, protected, retained and disposed of (disposal shall be in accordance with EN 15713). Measures shall be established and maintained to prevent loss, destruction, falsification, unauthorized access and unauthorized release of data either through inadvertent or malicious interference. These measures shall take into account applicable legislation and regulations, contractual obligations and business requirements. For client master data, 8.4 shall be taken into account.

Each AS connected to the ARC shall be allocated an individual record, uniquely referenced, in which the details are recorded, together with any related instructions. There shall similarly be allocated an individual history record, which may be part of the record, in which all relevant message activity and operator actions are recorded.

9.1.14 Data back-up

The procedure shall describe how all client and system data are backed-up, and to test the availability and reliability of such back-ups. Where an ARC is operated in conjunction with another ARC in order to comply with 10.5.1, access to client data shall be available at each ARC.

9.1.15 Confidentiality and classification of information

The procedure shall describe how person(s) having access to ARC data ensure confidentiality is maintained. The procedure shall include:

- a clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities;
- information classification and labelling instructions in terms of legal requirements value criticality and sensitivity to unauthorised disclosure or modification.

9.1.16 Relationships with essential suppliers

The procedure shall describe how the ARC and essential supplier(s) interact. For each supplier there shall be an individual written contract for the specific agreed procedures. The ARC shall monitor and review the essential suppliers' performance against the agreed procedures and conduct a review at periods not exceeding one year.

9.1.17 Administrative procedures

The procedure shall describe how the ARC's operational processes link to the administrative processes such as those required for sales, client and supplier contract handling, or invoicing to ensure end to end consistency.

9.1.19 Remote access

The procedure shall describe how remote access to and exit from any system within the ARC and to the receiving data processing equipment (see 5.8) shall be controlled by a log-in / log-out procedure recording time and date, credentials of the person involved and actions performed. Remote access can only be granted by authorization of the ARC. See Annex B for further information related to remote system access.

9.1.20 Operational continuity and emergencies

There shall be a procedure for business continuity and disaster recovery. The contingency plan shall include sufficient detail to describe how monitoring services will be restored. The ARC shall conduct a review of the plan at six monthly intervals.

The staff shall be retrained on operational and emergency procedures to deal with disruptive events:

- a) Emergency response procedures shall be agreed with contractors and emergency services to enable the ARC monitoring function to be maintained whilst the emergency incident is investigated, damage contained or repaired.**
- b) In the event of an ARC being put entirely out of action, there shall be an emergency SOP for dealing with this situation (for example transfer of the services to another ARC, information to clients and partners).**

Procedures for operational continuity and emergencies shall be reviewed every 6 months by the ARC.

There shall be a SOP made available providing a procedure to deal with a situation where the ARC is put out of action.

9.1.21 Emergency evacuation and re-entry

The procedure shall describe how partial and full evacuation is achieved and include actions for re-entry and/or recovery following an evacuation.

9.1.22 Emergency entry

The emergency entry procedure as in 5.7.3 shall be documented.

All staff shall receive instruction and training in the emergency procedures at intervals not exceeding six months, which shall be recorded.

Training on the emergency entry procedure shall be given to all staff at intervals not exceeding 6 months.

9.1.23 Key performance indicators

The procedure shall describe how performance statistics are produced and made available to demonstrate the fulfilment of the contracted services and shall cover the following:

- a) Each service provided according to the client contract.
- b) Alarm message handling performance, see 9.2.
- c) ATP failures.

9.2 Performance criteria – message handling

Alarm management equipment and resources shall provide the following performance.

The time ΔT_{OP} shall comply with the performance criteria contractually agreed with each client, but at least as follows:

- for hold-up, fire, fixed fire fighting systems, people monitoring and for other alarms agreed to be of highest priority level conditions: 30 s for 80 % of alarms received and 60 s for 98,5 % of alarms received;
- all other alarm conditions: 90 s for 80 % of alarms received and 180 s for 98,5 % of alarms received.

Where an alarm handling delay forms part of the alarm handling procedure, the delay period may be excluded from the ΔTOP calculation. The handling procedure shall be in compliance with the client contract.

The performance criteria for social alarms shall be fulfilled in accordance with EN 50134-7.

Conformance to above criteria shall be achieved over a rolling twelve-month period.

10 General Principles, Leadership, Governance, Management, and Staffing

10.1 General

This clause describes management tools that shall be in place in the ARC. These shall be considered for the definition of operational procedures, for the design of the technical infrastructure and for the design of premises.

10.2 Governance and Strategy

The ARC management, for example the person(s) responsible for setting objectives, for preparing and making decisions and for executing decisions in order to achieve objectives in an ARC shall ensure the implementation of a management system. It shall in particular:

- establish the vision, set objectives, provide direction and manage the risks of their organization by defining written strategies which take into consideration the needs and expectations of all relevant stakeholders (such as clients, employees, shareholders, business partners, insurers, responders, and public authorities);
- implement and maintain adequate measures to fulfil the conditions of this standard;
- implement an ongoing monitoring of the business environment as well as of the organizational performance;

- establish an ongoing communication with all stakeholders to maintain a high level of awareness in relation to the safety and security oriented services provided.

NOTE A management system following the principles of EN ISO 9001 is considered suitable to satisfy this requirement.

10.3 Legal and operational set-up

ARC services shall only be offered, sold and executed by legal entities which are registered according to the law at their place of business. If ARC services are offered or sold or produced in different places, this requirement shall apply to each place of business used by the ARC.

ARCs shall keep on file originals of all active contracts with clients, business partners and suppliers.

ARC operators shall have access to the necessary operational procedures. Terminated customer contracts shall be kept on file as specified by local law, however at least as long as specified in 8.4.

10.4 Management System

Within the management system ARC's shall in particular have documented and regularly updated policies and plans for:

- Risk and Contingency Management, covering aspects of resilience, business continuity and disaster recovery with a comprehensive risk analysis for example according to ISO 31000 series.
- It shall include plans for ARC site and ARC procedures and take into account measures to handle disruptive events and associated measures for prevention, early detection and remedy at management and technical level. It shall in particular include:
 - Planning of the ARC site and of the ARC standard operating procedures;
 - ICT security (Information and Communication Technology) of the ARC;

NOTE ISO/IEC 27001 gives requirements for information security management.

- Prioritization for the preservation and/or restoration of activities and services, including contact details to contractors and service providers able to undertake reinstatement, description of the means by which services shall be continued or restored;
- Management of staffing levels during disruptive events;
- Communication to all stakeholders during and after disruption;
- Current risk analysis reports and plans shall be available at any time for management review and for audit.
- Information Management, including IT systems and IT security, including observation of the European Data Protection Directive (95/46/EC) or similar.
- Operational Performance Management, covering the following areas:
 - Listing and measurement methods for KPI's that are essential to demonstrate that the services sold perform to specified performance;

- **Listing and measurement methods for operational KPI's that are essential for the daily management and continuous improvement of the ARC performance.**
- **Complaint Handling from all stakeholders with a view to settle each individual complaint, and to identify systematic failures that additionally need an adjustment of procedures, policies or guidelines.**
- **Management of the Services Portfolio for creation, management and out phasing of services provided, including a list of services currently available for new contracts and a list of services that are additionally provided by the ARC to legacy customers.**
- **Management of Staffing with guidelines for security background screening and vetting of all staff with access to the ARC premises and processes, with job descriptions and qualification profiles for all functions, with training plans and career path profiles for employees, and with rules for terminating information access for employees who leave the ARC.**
- **Client Management ensuring that profile data provided by the customer, contract and transaction information are kept current, and that third party liability is clearly excluded – in particular for installers and telecommunication providers.**
- **Business Partner Management considering the various applicable business cases and contractual / operational relationships with the ARC (for example. installer with wholesale monitoring, owned account monitoring, equipment suppliers, telecommunication services providers, guard services providers).**
- **Compliance Audits to be carried out annually by a body accredited to EN ISO/IEC 17065 by any signatory of the EA MLA (European co-operation for Accreditation) for the EN 50518.**

10.5 Staffing

10.5.1 General

There shall be a minimum of two operators in the ARC at all times, capable of carrying out all operational procedures, unless the ARC operates in conjunction with another ARC of the same or higher category and the operational methods ensure compliance with the performance criteria in 9.2.

In the case of clause 10.5.1 a minimum of 2 operators are required in the ARC, each must be competent in all operational procedures, if this is not in place then the ARC must work in conjunction with another ARC.

As BS EN 50518:2019 includes requirements for two categories of ARC it is important that where services are shared between ARCs, or a second Arc might take over the function of a primary ARC then the secondary ARC must meet or exceed the requirements of the primary ARC.

An ARC approved at the appropriate category of BS 50518:2019 or to the 2013 editions of BS EN 50518 & BS 8591 or to BS 5979:2007 will be acceptable.

10.5.2 Security screening and vetting

All employees in relevant employment shall be security screened and vetted. Other than visitors any person entering the ARC shall be screened. Visitors shall be accompanied by an ARC employee at all times while inside the ARC.

Screening shall be of a minimum of five years up to the commencement of relevant employment with the ARC, or back to the date of ceasing full-time education. A progress record shall be maintained to monitor and record the action taken and the information received during the screening and vetting process. The screening process shall be completed as soon as practicable but at least within 12 weeks unless an extension period is authorized by a director/principal of the ARC. In all instances, screening shall not exceed 16 weeks.

If the individual is employed prior to the completion of the screening or vetting process then the individual shall be notified that employment is subject to satisfactory screening and vetting and should be supervised at all times while working in the ARC.

A procedure shall describe how access rights are terminated.

Other than visitors, any person entering the ARC, including all ARC staff, shall be screened in accordance with BS 7858.

Screening shall be completed within 12 weeks unless an extension is authorised by an ARC director/principal, in all instances screening will not take longer than 16 weeks to complete.

Any individual employed before screening or vetting is complete must be supervised at all times whilst working in the ARC.

10.5.3 Training

The company shall adhere to training procedures for all relevant employees covering theoretical and practical skills to comply with the training requirements as laid down by legislation or by the ARC.

There shall be a period of training, appropriate to ensure the minimum competency to carry out the specific duties, provided to all operators before they are allowed to handle alarms without supervision. Further training shall be given on specific subjects such as new technical equipment or changes in operational procedures.

Employees training shall be documented and reviewed every year.

Training to all relevant staff will comply with requirements defined by legislation or by the ARC. Employee training will be reviewed every year.