BS EN 50136-3:2013

BSI Standards Publication

Alarm systems — Alarm transmission systems and equipment -

Part 3: Requirements for Receiving Centre Transceiver (RCT)

bsi.

...making excellence a habit.™

National foreword

This British Standard is the UK implementation of EN 50136-3:2013.

The UK participation in its preparation was entrusted to Technical Committee GW/1/5, Transmission equipment and networks.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

ISBN 978 0 580 65888 4

ICS 13.320

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 September 2013.

Amendments issued since publication

Date	Text affected

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 50136-3

August 2013

ICS 13.320

English version

Alarm systems - Alarm transmission systems and equipment - Part 3: Requirements for Receiving Centre Transceiver (RCT)

Systèmes d'alarme - Systèmes et équipements de transmission d'alarme - Partie 3: Exigences pour les transmetteurs du centre de réception (RCT)

Alarmanlagen - Alarmübertragungsanlagen und -einrichtungen - Teil 3: Anforderungen an Übertragungszentralen (ÜZ)

CENELEC

European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

CEN-CENELEC Management Centre: Avenue Marnix 17, B - 1000 Brussels

Ref. No. EN 50136-3:2013 E

Contents

Tables

Foreword

This document (EN 50136-3:2013) has been prepared by CLC/TC 79 "Alarm systems".

The following dates are proposed:

• latest date by which this document has to be implemented at national level by publication of an identical national standard or by endorsement	(dop)	2014-08-12
• latest date by which the national standards conflicting with this document have to be withdrawn	(dow)	2016-08-12

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CENELEC [and/or CEN] shall not be held responsible for identifying any or all such patent rights.

EN 50136 consists of the following parts, under the general title, *Alarm systems — Alarm transmission systems and equipment*:

- *Part 1: General requirements for alarm transmission systems*;
- *Part 2: Requirements for Supervised Premises Transceiver (SPT)*;
- *Part 3: Requirements for Receiving Centre Transceiver (RCT)*;
- *Part 4: Annunciation equipment used in alarm receiving centres* (Technical Specification);
- *Part 7: Application guidelines* (Technical Specification);
- *Part 9: Requirements for common protocol for alarm transmission using the Internet protocol* (Technical Specification).

1 Scope

This European Standard specifies the minimum equipment requirements for the performance, reliability, resilience, security and safety characteristics of the receiving centre transceiver (RCT) installed in ARC and used in alarm transmission systems.

The alarm transmission system requirements and classifications are defined within EN 50136-1. Different types of alarm systems may in addition to alarm messages also send other types of messages, e.g. fault messages and status messages. These messages are also considered to be alarm messages. The term alarm message is used in this broad sense throughout the document.

Where application specific standards exist, the RCT should comply with relevant standards called up by that application.

The RCT can be either an integrated element of any receiving/annunciation equipment, or a stand-alone device. In either case, the requirements of this European Standard should apply.

The function of the RCT is to monitor the ATPs, receive alarm messages, forward alarm messages to one or more AEs and send acknowledgements to the SPTs.

Management of the transmission network is not in the scope of this European Standard.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

EN 50130-4, *Alarm systems — Part 4: Electromagnetic compatibility — Product family standard: Immunity requirements for components of fire, intruder, hold up, CCTV, access control and social alarm systems*

EN 50130-5, *Alarm systems — Part 5: Environmental test methods*

EN 50136-1:2012, *Alarm systems — Alarm transmission systems and equipment — Part 1: General requirements for alarm transmission systems*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in EN 50136-1:2012 and the following apply.

3.1
remote access
access to the equipment from any location that is outside the protected premises in which the equipment is located

4 Object

This European Standard specifies the minimum equipment requirements for the performance, reliability, resilience, security and safety characteristics of the Receiving Centre Transceiver (RCT) installed in alarm receiving centres and to define parameters that shall be tested to ensure its compatibility with ATS categories.

5 General

5.1 Introduction

Where appropriate, equipment shall comply with local, national and European requirements and regulations for connection and transmission via public or private networks.

Requirements in this European Standard shall be considered as a minimum. As the RCT is used together with or integrated receiving/annunciation equipment, the requirements of the specific applications or related standards shall apply.

5.2 RCT classification

This European Standard defines RCT requirements. For the purpose of RCT classification reference is made to the ATS categories in EN 50136-1. The RCT documentation shall describe for which ATS categories the RCT complies with the requirements.

6 Functional requirements

6.1 General

The RCT shall provide communication between one or more AEs and one or more SPTs and monitor the interface(s) to one or more AEs.

The RCT shall monitor the ATSs.

6.2 Access levels

This European Standard specifies four levels of access that categorise the ability of users to access the RCT functions.

Access levels are defined as following:

- Level 1 Access to indications;

- Level 2 Access to the operational status and commissioning functions;

- Level 3 Maintenance functions, access to affect the RCT configuration including site-specific data and other operations that directly, or indirectly, may adversely influence the functions of the RCT;

- Level 4 Access to software updates and read-only parameters.

These access levels apply only for logical access (i.e. not physical access). Access to all functions shall require authorisation with a key.

Access levels 2, 3 and 4 shall use personalised accounts to achieve traceability.

A level 4 user shall be authorised by a user with level 3 access. This authorisation may be permanent or time limited.

Access at all levels shall require authorisation with a key. The key mechanism shall be able to provide at least 1 000 000 different keys.

Where it is possible to attempt to gain access more than 3 times in a 60-second period the RCT shall have the ability to delay repeated attempts. After the third attempt, each further attempt shall be prevented for a minimum of 90 s.

Where factory default keys are provided, it shall not be possible to complete the RCT commissioning without first, changing these keys during installation.

Remote access shall require a secure connection and meet the data security requirements of EN 50136-1.

Automatic logout of remote access sessions shall be activated after a period of inactivity. The inactivity period shall be configurable.

Table 1 — Access levels – Logical access to functions

Access Level	**Level 1**	**Level 2**	**Level 3**	**Level 4**
View RCT indications	P	P	P	P
Change RCT configuration	NP	NP	P	NP
View RCT configuration	NP	P	P	P
Commission/De-Commission SPT	NP	P	P	NP
View RCT Event/Alarm Log	NP	P	P	P
Change RCT Software	NP	NP	NP	P
Change users and/or user rights	NP	NP	P	NP
Change and/or delete entries in the event log	NP	NP	NP	NP

Key

P = Permitted
NP = Not Permitted

NOTE The requirement to restrict or permit access to a certain function does not imply that implementation of the function is required.

6.3 Uploading and downloading of software

The upload and download of software in/out of an RCT is only allowed at appropriate access level as defined in 6.3.

6.4 Storage of parameters and data

Power cycle or a software restart shall not result in the loss of any configuration, log and secured alarm messages. The RCT shall return to normal operation automatically after such power cycle or software restart.

6.5 Monitoring and notification of failure of the ATP and ATS

For compliance to the relevant standards of the application, the RCT shall monitor ATP and ATS and report failures to the AE as defined in EN 50136-1:2012, 6.6, Table 4.

The documentation supplied by the manufacturer shall describe the notification signal.

6.6 Interface(s) to the AE(s)

The interface(s) to the AE(s) shall be monitored in accordance with EN 50136-1. The reporting time of the connection failure shall be less or equal to the reporting time of the ATS with the highest category or 60 s whichever is shorter. In the event of an interface failure, a fault signal shall be generated, and an event logged.

The manufacturer shall state in their product documentation the specifications of the interface(s) to the AE and how the fault signal is presented and logged.

An alternative AE interface may be provided.

6.7 Fault signalling

The RCT shall have a means to signal faults when any of the following faults occur:

- AE interface failure;
- transmission network interface failure;
- RCT system failure.

The manufacturer shall specify in the RCT documentation how these faults are signalled.

6.8 Event recording

For an RCT supporting and meeting any category of EN 50136-1:2012 other than SP1, SP2 and DP1 a logging function shall be provided for the purposes of providing an audit trail and problem resolution.

The events specified in Table 2 shall be recorded.

The event log may be stored outside of the RCT.

The means of recording events shall be non-volatile. The log entries shall be kept for no less than 3 years. The manufacturer shall specify in their documentation how this is achieved.

Events older than 3 years may be deleted.

The log shall record, in addition to the event, the time and date at which the event occurred. The timing resolution shall be a minimum of 1 s and it shall be accurate to the coordinated universal time within $\pm$ 5 s.

The RCT shall provide a means to synchronise the UTC date and time. The manufacturer shall specify in their documentation how time synchronisation with UTC is achieved.

The RCT may use local time-zones.

To optimise storage of events, where identical sequentially repeated events occur within any 12-h period, then only the first and last event need to be recorded. Where this is done then the number of identical events shall be recorded.

When required by the requirements of Table 2, the logging of access to the RCT shall include user identification.

Table 2 — Event recording classification – Events to be recorded

	Events to be recorded	
	Event	**User identification**
1	Alarm messages from ATS	n/a
2	AE interface(s) failure and restore	n/a
3	Transmission network Interface(s) failure and restore	n/a
4	Changes to the configuration of the RCT	M
5	Power-up or reset	M
6	Any change to software	M
7	Changes to the date and time	M
8	Access to the RCT	M
9	Changes to users and/of user rights	M
Key n/a = Not applicable M = Mandatory NOTE Recording the user identification is only mandatory if the event is triggered by user intervention.		

6.9 Mode of operation (store-and-forward or pass-through)

6.9.1 General

Two modes of operation are permitted:

a) store-and-forward;

b) pass-through.

The manufacturer shall declare in the product documentation which modes are supported.

6.9.2 Store-and-forward operation requirements

When an alarm is received from the SPT, the RCT shall secure the alarm and provide acknowledgement of the correct receipt of the alarm to the SPT.

If the store-and-forward operation is used, all alarm messages shall include the date and time stamp when the alarm was received by the SPT.

The RCT may also log the date and time stamp when the alarm was forwarded to the AE and/or when the acknowledgement was received from the AE.

Securing the alarm shall be achieved by storing the alarm in the RCT's non-volatile memory (data base), this is to secure acknowledged alarms whilst there is an AE interface failure or during a power failure. Stored alarms shall be transmitted when the fault condition clears.

The secured alarm shall be transmitted from the RCT to the AE(s).

The reception of an acknowledgement from the AE(s) shall not be forwarded to the SPT, since the SPT has already received an acknowledgement from the RCT.

NOTE The loss of an alarm message is regarded as a worse situation than sending a delayed message.

6.9.3 Pass-through operation requirements

When an alarm is received from the SPT the RCT shall forward the alarm to the AE(s).

The RCT shall not acknowledge the alarm to the SPT before receiving an acknowledgement from at least one AE. When the RCT receives an acknowledgement from the AE(s) the acknowledgement shall be forwarded to the SPT.

6.10 Denial of service

The manufacturer of the RCT shall declare in their documentation how compliance with the requirements of EN 50136-1:2012, 6.2.5 is achieved.

6.11 Information security

The manufacturer shall provide their stated methodology used to achieve compliance with EN 50136-1:2012, 6.8.3 (Information security) for both SPT communication and remote access.

6.12 Substitution security

The manufacturer shall provide their stated methodology used to achieve compliance with EN 50136-1:2012, 6.8.2 (Substitution security).

6.13 RCT redundancy

If the RCT supports Dual Path category ATS (DP1 – DP4) the RCT shall comply with the redundancy requirements of EN 50136-1:2012, Table 1. The manufacturer shall specify and demonstrate how compliance is achieved.

6.14 Documentation

Documentation relating to an RCT shall be concise, complete and unambiguous. Information shall be provided sufficient to install, put into operation, operate and maintain an RCT.

Instructions relating to the operation of an RCT shall be designed to minimise the possibility of incorrect operation and be structured to reflect the access level of the user.

Where there are user serviceable parts (e.g. fuses) their type and values shall be given.

The documentation shall include:

- name of manufacturer or supplier,
- description of equipment,
- standard to which component claims compliance,
- name or mark of the certification body,
- the maximum number of SPTs that can be connected for each category,
- the maximum number of AEs that can be connected,
- the maximum number of transmission network interfaces,
- the maximum number of alarms that can be processed per second,
- a list of supported ATS categories,

- power requirements.

6.15 Marking/identification

The RCT shall be marked with the following:

- name of manufacturer;
- ATS categories for which the RCT is suitable.

The marking shall be legible, durable and unambiguous. If the RCT does not use dedicated hardware (i.e. the RCT is a software solution), the software shall be able to display the required markings/identifications.

7 Tests

7.1 General

Specific applications may require additional testing of the RCT. If such characteristics are provided and are submitted for testing, they shall be specified by the manufacturer at the time of testing.

7.2 Test conditions

7.2.1 Laboratory conditions and tolerance

Testing conditions shall be in accordance with EN 50130-4 and EN 50130-5, as follows:

1) temperature: 15 °C to 35 °C;

2) relative humidity: 25 % to 75 %;

3) air pressure: 86 kPa to 106 kPa.

7.2.2 Mounting

The RCT shall be mounted in accordance with the manufacturer's installation instructions. Any additional equipment necessary to carry out the tests (EXAMPLE: simulation of the ATS and SPT) shall be supplied by the manufacturer in agreement with the test house.

7.2.3 Documentation

The product documentation (as required in 6.14) shall be provided with the RCT.

7.2.4 Power supply

Unless otherwise required, the RCT shall be powered by a power supply that meets the performance as specified by the manufacturer.

7.3 Functional tests

7.3.1 General

The purpose of the functional tests is to demonstrate that RCT performs its required functions. The manufacturer shall provide a fully functional test setup. Other ATS components such as AS, SPT, and network may be provided as simulating equipment and/or network(s).

If more than one single and/or dual path category is supported for testing only the most demanding supported single and/or dual path categories shall be tested. The maximum reporting time requirement shall be tested for each individual supported category.

All network interfaces shall be tested.

All AE interfaces shall be tested.

Table 3 — Summary of functional tests *(1 of 2)*

Section reference	Requirement to test	Test/validation objective	Validate or test
6.1	Processing of alarm signals	Demonstrate the ability of the RCT to receive, process and forward a signal or message from the ATS.	Test (7.3.9)
6.2	Access levels	Demonstrate that all access levels exist.	Test (7.3.2)
6.3	Upload and download of software	Demonstrate that the RCT will recover after an unsuccessful software upload/download.	Test (7.3.3)
6.4	Storage of parameters and customer specific data	Demonstrate that the RCT will not lose any parameters or customer specific data after a reset or power cycle.	Test (7.3.4)
6.5	Notification of an ATS failure for a single path ATS	Demonstrate that the RCT signals an ATS failure to the AE as defined in EN 50136-1:2012, Table 4.	Test (7.3.5)
6.5	Notification of an ATS failure for a dual path ATS	Demonstrate that the RCT signals an ATS failure to the AE as defined in EN 50136-1:2012, Table 4.	Test (7.3.6)
6.6	Interface(s) to the AE(s)	Demonstrate that the interface(s) to the AE(s) are monitored.	Test (7.3.7)
6.7	Fault signalling	Demonstrate that faults are signalled according to the manufacturer RCT documentation.	Test (7.3.8)
6.8	Event recording	Demonstrate that all mandatory events are recorded as required in Table 2.	Test (7.3.10)
6.8	Clock resolution and synchronisation	Demonstrate that the accuracy of the timestamps as attached to events in the log complies with the requirements of 6.9.	Test (7.3.11)
6.8	Endurance of the log	Verify that the manufacturer documentation specifies how 3-year endurance of log entries is achieved.	Validate (7.3.12)
6.8	Optimising methods of storage of events	(only if implemented) Demonstrate that event storage by grouping them as described in 6.9 is implemented and compliant with the requirements.	Test (7.3.13)
6.8	User identification of log entries	Demonstrate that user identification for log entries is logged according to the requirements of Table 2.	Test (7.3.14)
6.9	Mode of operation	Demonstrate that the implemented modes of operation comply with the requirements of 6.10.	Test (7.3.15)
6.10	Denial of service	Verify the manufacturer RCT documentation.	Validate (7.3.16)

Table 3 *(2 of 2)*

Section reference	Requirement to test	Test/validation objective	Validate or test
6.11	Information security	Verify the manufacturer declaration how information security is implemented and complies with the requirements of this section.	Validate (7.3.17)
6.12	Substitution security	Verify the manufacturer declaration how substitution security is implemented and complies with the requirements of this section.	Validate (7.3.17)
6.13	RCT Redundancy	Verify where a RCT can be used in a Dual Path ATS configuration a failure of one RCT shall not compromise the ATS according to EN 50136-1:2012, Table 1.	Test (7.3.18)
6.14	Documentation	Verify the manufacturer documentation against the requirements of 6.14.	Validate (7.3.19)
6.15	Marking/identification	Verify the marking and identification against the requirements of 6.15.	Validate

7.3.2 Access levels

a) Object of the test:

To demonstrate the ability of the RCT to comply with 6.2 to provide up to 4 levels of access and verify the relevant access to the functions and controls.

b) Principle:

The test consists of attempting to use the functions and the controls required by 6.2, operating the RCT at each access level and verifying that access is granted for permitted functions and is denied for non-permitted functions.

Table 4 — Test of access levels

Step	Test condition (c)	Test procedure (d)	Measurement (e)	Pass criteria (f)
1	The RCT and any necessary equipment to allow the RCT to perform as required shall be installed and in a functional state	At access level 1 attempt to operate all the functions and controls for access level 1.	Record whether access is permitted.	Access is in accordance with 6.3.
2	As above	Repeat as step 1 for access level 2.	As above	As above
3	As above	Repeat as step 1 for access level 3.	As above	As above
4	As above	Repeat as step 1 for access level 4.	Record if level 4 access is only possible if granted by a level 3 user.	As above
5	As above	Try to get access by using three times a wrong key.	Record whether access is denied.	No access is granted.
6	State after test nr.5.	Wait less than 300 s and retry with a valid key to get access.	Record whether access is denied.	No access is granted.
7	State after test nr.5.	Wait longer than the time specified by the manufacturer and retry with a valid key to get access.	Record whether access is granted.	Access is granted.
8	As above	Try to let the factory default key unchanged.	Record if there is no ability to complete commissioning with the factory key unchanged.	Key shall be changed otherwise commissioning could not be finished.
8	See manufacturers proof of quality of the algorithm used to achieve remote access with a key of at least 1000 000 differs.	Review document.	-	The documentation states that the key algorithm can distinguish between at least 1 000 000 key differs.

7.3.3 Upload and download of software

a) Object of the test

The principle of this test is to prove that upload and download of software of the RCT, if implemented, complies with the requirements of 6.3.

b) Principle

The test consists of attempting to update software of the RCT, operating the RCT at the appropriate access level and following the instructions in the RCT manual.

Table 5 — Test of upload and download of software

STEP	Test condition (c)	Test procedure (d)	Measurement (e)	Pass criteria (f)
1	The RCT and any necessary equipment to allow the RCT to perform as required shall be installed and in a functional state.	At access level 1 attempt to apply a software update.	Record whether a software update is permitted.	A software update shall not be permitted.
2	As above	Repeat as above for access level 2.	As above	As above
3	As above	Repeat as above for access level 3.	As above	As above
4	As above	Repeat as above for access level 4.	As above	A software update shall be permitted.
5	As above	Repeat as above for access level 4. Disconnect the network cable during the software update procedure.	Record whether the RCT fails to operate or restores normal operation.	The RCT shall operate normally after the attempt to download software.

7.3.4 Parameter storage

a) Object of the test:

To demonstrate the ability of the RCT to comply with 6.4 to provide immunity of the storage of parameters against power failure or boot up sequence.

b) Principle:

The test consists of changing at least 2 site-specific parameters and read back these parameters after a power cycle (power loss / power recovery) or boot up sequence.

Table 6 — Test of parameter storage

Step	Test condition (c)	Test procedure (d)	Measurement (e)	Pass criteria (f)
1	The RCT and any necessary equipment to allow the RCT to perform as required shall be installed and in a functional state.	Change and save at least 2 site-specific data according to the procedure in the manual.	Record whether the changes are stored.	--
2	As above	power off the RCT	-	-
3	RCT in power off state	Wait at least 10 s and power on the RCT again.	Record whether the RCT is in operational state.	RCT shall be in a functional state as before the power cycle.
4	Same as Step 1	Read the changed parameters according to the procedure in the manual.	Record the parameter values.	The parameter values shall be the same as before the power cycle.
5	As above	Power cycle the RCT according to the reset procedure in the manual.	Record the parameter values.	The parameter values shall be the same as before the reset procedure.

7.3.5 Monitoring and notification of an ATS failure for a single path ATS

a) Object of the test:

Demonstrate that the RCT signals an ATS failure to the AE as defined in EN 50136-1:2012, Table 4.

b) Principle:

The tests consists of configuring a SPT for the reporting time of every single path category supported by the RCT. Connecting the SPT to the RCT via a transmission network. Disabling the SPT and recording that the ATS failure is reported to the AE within the maximum reporting time for each single path category.

c) Test conditions:

Fully operational SPT connected via a network to the RCT.

d) Test procedure:

Disable the SPT by powering off the SPT.

e) Measurement:

Record the ATS failure transmitted to the AE.

f) Pass criteria:

An ATS failure shall be transmitted to the AE within the maximum ATS reporting time. Optionally an ATP failure may be transmitted to the AE.

7.3.6 Monitoring and notification of an ATS failure for a dual path ATS

a) Object of the test:

Demonstrate that the RCT signals an ATS failure to the AE as defined in EN 50136-1:2012, Table 4.

b) Principle:

The test consists of configuring a SPT for the reporting time of every dual path category supported by the RCT. Connecting the SPT to the RCT via two diverse technology transmission networks. Disabling the SPT and recording that the ATS failure is reported to the AE within the maximum ATS reporting time for each dual path category.

c) Test conditions:

Fully operational SPT connected via two diverse technology networks to the network interfaces of the RCT.

d) Test procedure:

Disable the SPT by powering off the SPT.

e) Measurement:

Record the ATS failure transmitted to the AE.

f) Pass criteria:

An ATS failure shall be transmitted to the AE within the maximum ATS reporting time. Optionally ATP failures may be transmitted to the AE.

7.3.7 Interface(s) to the AE(s)

a) Object of the test:

The principle of this test is to prove that the interface to the AE complies with the requirements of 6.6.

b) Principle:

The test consists of commissioning the RCT and connecting it to the AE according to the user manual provided by the manufacturer.

Table 7 — Test of interface(s) to the AE(s)

STEP	Test condition (c)	Test procedure (d)	Measurement (e)	Pass criteria (f)
1	The RCT and any necessary equipment to allow the RCT to perform as required shall be installed and in a functional state.	Connect RCT to AE as specified in the product documentation.	Record whether interconnecting RCT with AE is in line with documentation.	The interface between AE and RCT is operational (i.e. communication established).
2	As above	Disconnect AE interface.	Record the time till an AE failure is indicated at the RCT.	The time shall be according to the requirements in 6.6.

7.3.8 Fault signalling

a) Object of the test:

The object of this test is to prove that the fault signalling complies with the requirements of 6.7.

b) Principle:

The test consists of triggering various faults and monitoring if the faults are signalled from the RCT to the AE.

Table 8 — Fault signalling

STEP	Test condition (c)	Test procedure (d)	Measurement (e)	Pass criteria (f)
1	General condition: The RCT is connected to the AE. The ATS is fully operational and configured for any ATS category.	Trigger an ATS fault.	Monitor if an ATS failure is reported to the AE.	An ATS failure shall be reported to the AE.
2	As above Test only if ATP fault reporting is implemented.	Trigger an ATP fault.	Monitor if an ATP failure is reported to the AE.	An ATP failure shall be reported to the AE.
3	As above	Trigger an AE interface failure.	Monitor if an AE failure is logged.	An AE failure shall be signalled according to the manufacturer documentation.
4	As above	Trigger a transmission network interface failure.	Monitor if a transmission network interface failure is reported to the AE.	A transmission network interface failure shall be signalled according to the manufacturer documentation. If failing the transmission network interface leads to an ATS fault, an ATS fault shall be signalled to the AE.

7.3.9 Processing of alarm signals

a) Object of the test:

To demonstrate the ability of the RCT to receive, process and forward a signal or message from the ATS.

b) Principle:

The test consists of verifying that an alarm signal or message applied to the transmission network interface of the RCT is recognised and processed correctly and transmitted to the associated AE.

c) Test conditions:

The RCT shall be mounted and installed as specified by the manufacturer in the installation instruction. If multiple transmission network interfaces to the ATS are provided the test shall be performed for every interface.

d) Test procedure:

An alarm signal or message shall be generated at the transmission network interface of the RCT.

e) Measurement:

Record the reception of the alarm signal or message.

f) Pass criteria:

The alarm signal or message is received and presented at the AE.

7.3.10 Event recording

a) Object of the test:

The principle of this test is to demonstrate that for all implemented functions, all events are recorded and secured at the RCT as required in Table 2 according to 6.8.

b) Principle:

The test consists of triggering all implemented functions and generating all events that are required in Table 2, then reviewing that they are recorded in the RCT event log and secured against power failure.

Table 9 — Test of event recording

STEP	Test condition (c)	Test procedure (d)	Measurement (e)	Pass criteria (f)
1	The RCT and any necessary equipment (ATS) to allow the RCT to perform as required shall be installed and in a functional state.	Create all events according to Table 2 at least once.	Check that every event is logged as per the product documentation.	All event records logged correctly with date and time stamp
2	As above	Remove power from the RCT. Restore power to the RCT.	Check that no events are affected.	All events still remain logged correctly.

7.3.11 Clock resolution and synchronisation

a) Object of the test:

The object of this test is to prove that the accuracy of the timestamps as attached to events in the log complies with the requirements of 6.8.

b) Principle:

The test consists of creating events, while verifying the timestamps against a reference time source.

The tests shall be done against a well-defined time reference. For this purpose, an NTP server on Stratum 2 level (generally available on the Internet) provides the required accuracy.

Table 10 — Test of clock resolution and synchronisation

STEP	Test condition (c)	Test procedure (d)	Measurement (e)	Pass criteria (f)
1	Normal commissioned condition	Synchronise the clock according to the manufacturer specification.	Record if the time is synchronised with UTC time.	The time is synchronised with UTC time
2	Normal commissioned condition	Create an event.	Record timestamp of event creation.	There shall be a log entry, with a minimum of one second resolution and a deviation in relation to the reference time of less than 5 s.
3	As after test nr. 2	Wait for at least 72 h. Create a second event.	Record timestamps of event creation (log against reference time source).	As above

7.3.12 Endurance of the log

Verify that the manufacturer documentation specifies how 3-year endurance of log entries is achieved.

7.3.13 Optimising methods of storage of events

a) Object of the test:

If optimising of event storage by grouping them as described in 6.8 is implemented, the grouping and time stamping shall be checked.

b) Principle:

The test consists of generating identical sequentially repeated events then reviewing that they are recorded in the RCT according to 6.9.

Table 11 — Test of log optimisation

STEP	Test condition (c)	Test procedure (d)	Measurement (e)	Pass criteria (f)
1	The RCT and any necessary equipment (ATS) to allow the RCT to perform as required shall be installed and in a functional state.	Generate identical sequentially repeated events.	Check that events are logged according to 6.9.	All events records logged correctly with date and time stamp and that the number of identical events is correct.

7.3.14 User identification for log entries

a) Object of the test:

Verify that user identification for log entries: changes to configuration, changes to users and/or user rights, manual change to date and time, changes to software and access to the RCT, is logged.

b) Principle:

The test consists of generating the following logs: changes to configuration, changes to users and/or user rights, manual change to date and time, changes to software and access to the RCT and verifying that they are logged with user identification.

Table 12 — Test of user identification logging

STEP	Test condition (c)	Test procedure (d)	Measurement (e)	Pass criteria (f)
1	The RCT and any necessary equipment (ATS) to allow the RCT to perform as required shall be installed and in a functional state	Generate at least one log entry of the following type: changes to configuration, changes to users and/or user rights, manual change to date and time, changes to software and access to the RCT.	Check that events are logged according to 6.9.	All event records logged with user identification.

7.3.15 Mode of operation

7.3.15.1 General

The manufacturer documentation shall contain information about what mode(s) of operation are supported.

a) Object of the test;

The object of this test is to prove that all the supported modes of operation comply with the requirements of 6.9.

b) Principle;

The test consists of triggering an alarm from the AS and/or SPT to the RCT(s) and monitoring if an acknowledgement is transmitted from the RCT(s) to the SPT under various AE(s) interface conditions.

Table 13 — Test of mode of operation

STEP	Test condition (c)	Test procedure (d)	Measurement (e)	Pass/fail criteria (f)
1	*General condition:* *The RCT is connected to the AE.* The ATS is fully operational and configured for any ATS category.	Trigger an alarm transmission from AS/SPT to RCT(s).	Monitor if the alarm is displayed at the AE(s) within the requirements of the appropriate ATS category.	The alarm shall be displayed by the AE(s).
2	General condition, and: No AE(s) are connected; i.e. to make sure that no alarm transmission between RCT(s) and AE(s) is possible.	Trigger an alarm transmission from AS/SPT to the RCT(s).	Monitor if an alarm is displayed at the AE(s).	No alarm shall be displayed by the AE(s).
3	As after step 2 Wait at least the transmission time of the requirements of the appropriate ATS category.	Restore the AE interface (i.e. reconnect the RCT(s) to the AE(s)).	Monitor if the alarm that was triggered in step 2 is displayed by the AE(s).	The alarm shall be displayed by the AE(s).

7.3.16 Denial of service

a) Object of the test:

The object of this test is to determine that the equipment documentation states that DoS attack on one transmission network interface does not adversely affect the operation of the RCT or the operation of any other RCT transmission network interface.

b) Principle:

The test consists of inspection of the manufacturer's documentation relating to the RCT.

c) Test procedure:

Inspect the manufacturer's documentation relating to the RCT.

d) Measurement:

Check that a DoS Attack section states that a DoS attack on one transmission network interface does not adversely affect the operation of the RCT or the operation of any other RCT transmission network interface.

e) Pass criteria:

The measurement is confirmed.

7.3.17 Information and substitution security

The manufacturer shall describe in the RCT documentation the methods used for the protection against substitution of the SPT with identical equipment or simulation equipment to the requirements outlined in 6.12.

The manufacturer shall describe in the RCT documentation the methods used for the protection of the information transmitted by the ATS to prevent unauthorised reading and to unauthorised modification of the information transmitted to the requirements described in 6.11.

7.3.18 RCT redundancy

This test only applies to RCTs that support Dual Path ATS.

Table 14 — Test of RCT redundancy

STEP	Test condition (c)	Test procedure (d)	Measurement (e)	Pass criteria (f)
1	General condition: The ATS is fully operational and configured for any Dual Path ATS category. Both RCTs are connected to the AE.	Trigger an alarm transmission from SPT to RCT.	Monitor if the alarm is received at the AE.	The alarm shall be received by the AE.
2	General condition, and: Disable RCT1 (RCT2 remains operational).	As above	Monitor if the alarm is received at the AE.	The alarm shall be received by the AE.
2	General condition, and: Disable RCT2 (RCT1 remains operational).	As above	Monitor if the alarm is received at the AE.	The alarm shall be received by the AE.
3	General condition, and: Fail all transmission network interfaces for both RCTs.	As above	Monitor if the ATS fault is received at the AE.	The ATS fault shall be received by the AE.

7.3.19 Documentation

To verify that all required documentation is provided, complete and correct.

Bibliography

[1] EN 50136-2, *Alarm systems — Alarm transmission systems and equipment — Part 2: Requirements for Supervised Premises Transceiver (SPT)*

This page deliberately left blank

This page deliberately left blank

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email bsmusales@bsigroup.com.

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Copyright

Useful Contacts:

Customer Services
Tel: +44 845 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 845 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

bsi.

...making excellence a habit.™