PD CLC/TS 50131-9:2014

BSI Standards Publication

Alarm systems — Intrusion and hold-up systems

Part 9: Alarm verification — Methods and principles

bsi.

...making excellence a habit.™

National foreword

This Published Document is the UK implementation of CLC/TS 50131-9:2014.

The UK participation in its preparation was entrusted by Technical Committee GW/1, Electronic security systems, to Subcommittee GW/1/2, Installed alarm systems.

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.

Published by BSI Standards Limited 2014

ISBN 978 0 580 71373 6
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 31 July 2014.

Amendments/corrigenda issued since publication

Date	Text affected

TECHNICAL SPECIFICATION

SPÉCIFICATION TECHNIQUE

TECHNISCHE SPEZIFIKATION

CLC/TS 50131-9

June 2014

ICS 13.320

English Version

Alarm systems - Intrusion and hold-up systems - Part 9: Alarm verification - Methods and principles

Systèmes d'alarme - Systèmes d'alarme contre l'intrusion et les hold-up - Partie 9: Vérification d'alarme - Méthodes et principes

Alarmanlagen - Einbruch- und Überfallmeldeanlagen - Teil 9: Alarmvorprüfung - Verfahren und Grundsätze

This Technical Specification was approved by CENELEC on 2014-04-11.

CENELEC members are required to announce the existence of this TS in the same way as for an EN and to make the TS available promptly at national level in an appropriate form. It is permissible to keep conflicting national standards in force.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

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

Contents

page

Figures and Tables

Foreword

This document (CLC/TS 50131-9:2014) has been prepared by CLC/TC 79 "*Alarm systems*".

EN 50131 (all parts) will consist of the following parts, under the general title *Alarm systems – Intrusion and hold-up systems*:

Part 1	System requirements
Part 2-2	Intrusion detectors – Passive infrared detectors
Part 2-3	Requirements for microwave detectors
Part 2-4	Requirements for combined passive infrared and microwave detectors
Part 2-5	Requirements for combined passive infrared and ultrasonic detectors
Part 2-6	Opening contacts (magnetic)
Part 2-7-1	Intrusion detectors – Glass break detectors (acoustics)
Part 2-7-2	Intrusion detectors – Glass break detectors (passive)
Part 2-7-3	Intrusion detectors – Glass break detectors (active)
Part 2-8	Intrusion detectors – Shock detectors
Part 2-9 [1)]	Intrusion detectors – Active infrared detectors
Part 3	Control and indicating equipment
Part 4	Warning devices
Part 5-1 [1)]	Requirements for wired interconnection for I&HAS equipments located in supervised premises
Part 5-3	Requirements for interconnections equipment using radio frequency techniques
Part 5-4	System compatibility testing for I&HAS equipments located in supervised premises
Part 6	Power supplies
Part 7	Application guidelines
Part 8	Security fog device/systems
Part 9	Alarm verification – Methods and principles
Part 10	Application specific requirements for Supervised Premises Transceiver (SPT)

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.

[1)] At draft stage.

Introduction

Unwanted alarms have been a significant problem for response authorities throughout Europe. Alarm verification (also known as “Confirmation”) is one means developed to reduce this problem.

Development of alarm verification technologies has been carried out nationally on an “as needed” basis, resulting in different methods and practices being used – thus negating the benefits of having common European Standards for Intrusion and Hold-up Alarm Systems (I&HAS) and associated components.

This specification provides a basis for use of the technology that could be applied to verification of intruder and hold-up alarms such that countries that wish to do so could introduce alarm verification measures in a way that will permit later standardisation across Europe.

It provides a framework with limited options for the design, manufacture and testing of equipment (especially CIE) whilst enabling a multiplicity of implementations, thus removing the restrictions to trade imposed by the use of conflicting national recommendations.

The framework includes all methods in current use. Newly developed methods could be added to this specification, or its principles used to derive guidance for the implementation of such methods.

Alarm verification technology does not supersede the need for best practice in the design and installation of such systems, but supplements the requirements of EN 50131-1 in order to increase the probability that an alarm notified to an ARC by an Intrusion and Hold-up Alarm System may be considered to be genuine.

This European Technical Specification contains recommendations affecting a number of standards and application guidelines for both systems and products. There are a number of reasons for this:

- to group all relevant recommendations in a single document to simplify reference by those wishing to introduce an implementation of alarm verification;
- to allow alarm verification to be tested before review and eventual incorporation into European Standards;
- to recommend the additional product requirements necessary to provide the additional functionality for an installed I&HAS to meet these recommendations (see Annex A), pending incorporation of these recommendations into EN 50131 (or other) product standards;
- it should also be noted that some aspects of alarm verification do not have a related standard (e.g. audible and visual methods and related equipment).

Methods of reducing unwanted alarms specific to entry and exit procedures will be detailed in a future standard.

1 Scope

This European Technical Specification is available for use where alarm verification methods are considered necessary. It provides recommendations for the addition and use of alarm verification technology in Intrusion and Hold-up Alarm Systems (I&HAS) installed to comply with EN 50131-1.

These recommendations should be incorporated into the respective standards in the EN 5013x series.

This Technical Specification does not detail methods of alarm verification relying solely on Alarm Receiving Centre (ARC) procedures, but does not preclude their use.

This Technical Specification describes alarm verification methods that could be applied and details applicable to system and equipment design. The framework limits the range of options in order to provide for local regulations and circumstances, whilst permitting a standardised approach to equipment design.

This Technical Specification also provides (in Annex A) recommendations for equipment in order to permit the manufacture of standardised equipment to provide the functionality needed by an I&HAS incorporating alarm verification technology.

The associated guidelines for use in ARCs to monitor notification from such I&HAS can be found in EN 50518-3.

NOTE Alarm verification may also be referred to as “alarm confirmation”.

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 50131-1:2006, *Alarm systems — Intrusion and hold-up systems — Part 1: System requirements*

CLC/TS 50131-7:2010, *Alarm systems — Intrusion and hold-up systems — Part 7: Application guidelines*

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

EN 50518-3:2013 , *Monitoring and alarm receiving centre — Part 3: Procedures and requirements for operation*

3 Terms, definitions and abbreviations

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in EN 50131-1:2006 and the following apply.

3.1.1
abort signal or message
signal or message from an I&HAS identifiable at with the ARC to indicate that an authorised user has performed an action on the I&HAS to report that the previously notified alarm should be cancelled

3.1.2
alarm verification
process to provide information additional to a notified alarm, which increases the probability that the alarm should be considered genuine

[SOURCE: EN 50518-3:2013]

3.1.3
audible alarm verification
verification of an intruder or hold-up alarm by sound received from the supervised premises

3.1.4
audio listening device
device converting sound waves into electrical energy suitable for transmission from the supervised premises

EXAMPLE Microphone

Note 1 to entry: This device may be integrated into its associated detector.

3.1.5
audio monitoring device
device activated by sounds above a specified threshold and which, after activation, carries out the functionality of an audio listening device (See Annex A)

3.1.6
automatic reinstatement
process of I&HAS terminating an alarm verification time sequence if no sequentially verified alarm has occurred, in readiness for the possibility of a new unverified alarm

3.1.7
digital key
portable device containing digitally coded information used by an authorized user to gain access to restricted functions or parts of a CIE

EXAMPLE Magnetic card, electronic token or similar

[SOURCE: EN 50131-3:2009]

3.1.8
imaging device
device that converts an optical image into an electrical signal

EXAMPLE Camera

Note 1 to entry: This device may be integrated into its associated detector.

[SOURCE: EN 50132-7:2012, 3.1.21]

3.1.9
multi-action hold-up device
device consisting of two (or more) different operating mechanisms whose processed outputs are independently communicated to the CIE for use in sequentially verified HAS

3.1.10
multi-output combined detector
detector consisting of two (or more) separate sensors whose processed outputs are configured to communicate independently to the CIE for use in sequentially verified IAS

Note 1 to entry: The multiple sensors may be of the same technology (see A.3).

Note 2 to entry: For the purposes of this document, if a multi-output combined detector includes one or more single-output combined detectors, such single-output combined detectors should each be considered equivalent to a single sensor.

3.1.11
notified alarm
alarm that has been notified to the ARC in accordance with EN 50131-1

3.1.12
sequential alarm verification
verification of an intruder or hold-up alarm by using sequence of alarms originating from different detectors or hold-up devices to lead to designation of an alarm as verified

Note 1 to entry: Permitted detection combinations are recommended in 7.2.2 (intruder) and.8.1.2 (hold-up).

Note 2 to entry: Time lines illustrating the operation of a sequentially verified intruder alarm are included in Clause 7.

Note 3 to entry: Multi-output detection devices may be used instead of separate detectors (see 7.3.2).

3.1.13
single-output combined detector
detection device consisting of two (or more) separate intrusion detection sensors whose outputs are configured to be processed and communicated to the CIE as one signal or message

3.1.14
unverified alarm
intruder or hold-up alarm that has not yet been sequentially, visually or audibly verified

3.1.15
alarm verification time
pre-determined time following an unverified alarm, during which a sequentially verified alarm may be generated

Note 1 to entry: If no sequentially verified alarm has been generated during this time, automatic reinstatement takes place.

3.1.16
verified alarm
alarm considered genuine as a result of the use of alarm verification

Note 1 to entry: According to the method in use, the designation as verified may be carried out by the CIE or by the ARC operator.

3.1.17
video monitoring device
device detecting variations within a video signal, interpreting those above a specified threshold as evidence of movement

EXAMPLE Processing integrated into an imaging device

Note 1 to entry: See Annex A.

3.1.18
visual alarm verification
verification of an intruder alarm by images received from the supervised premises

3.2 Abbreviations

For the purposes of this document, the abbreviations given in EN 50131-1:2006 and the following apply.

- ALD Audio Listening Device
- AMD Audio Monitoring Device
- HUA Hold-Up Alarm
- VMD Video Monitoring Device

The following abbreviations are extracted from EN 50131-1:

- ACE Ancillary Control Equipment
- ARC Alarm Receiving Centre
- ATS Alarm Transmission System
- CIE Control and Indicating Equipment
- CLC CENELEC
- HAS Hold-up Alarm System
- IAS Intruder Alarm System
- I&HAS Intrusion and Hold-up Alarm System
- SPT Supervised Premises Transceiver
- WD Warning Device

4 Overview

It is not necessary that the entire supervised premises include means of alarm verification where this is not appropriate.

Where appropriate, different methods of alarm verification may be used for different parts of the same I&HAS.

The alarm verification principles and methods described in this document are as follows:

- General recommendations — See Clause 6
- Sequential verification of intruder alarms — See Clause 7
- Sequential verification of hold-up alarms — See Clause 8
- Audible alarm verification — See Clause 9
- Visual alarm verification — See Clause 10
- ATS faults — See Clause 11
- Equipment specifications — See Annex A
- Equipment Test Procedures — See Annex B

Any specification based on this document should specify which methods of alarm verification are permitted and which options and parameter limits are to be implemented

If other methods of alarm verification are to be used, relevant principles should be drawn from this specification.

Consideration should be given to the recommendations that sequential alarm verification be operational when audible or visual alarm verification is in use in IAS and that a telephone call-back procedure from the ARC be available when audible or visual alarm verification is used for HAS.

5 Parameter variation

This specification includes requirements offering a range of values for certain parameters to suit the needs of different sites or countries, which should be applied within the limits stated within each requirement.

6 General recommendations for I&HAS incorporating alarm verification

6.1 General

The following recommendations are additional to EN 50131-1 and related product standards and should be considered for all I&HAS using alarm verification, at all security grades (except where stated).

6.2 Setting and unsetting

There should be provision to warn a user of failure to complete the setting procedure (Refer to EN 50131-3:2009, 8.3.3.3).

Consideration should be given to the methods of entry and exit employed, to further minimize unwanted alarms.

6.3 Indications

The indication requirements of EN 50131-1:2006, 8.5, should be met by an I&HAS using alarm verification.

NOTE 1 If setting is carried out external to the supervised premises using a digital key, the provisions of EN 50131-3:2009, 8.3.2.2.2, are applicable.

The following indications, additional to those shown in EN 50131-1:2006, Table 8 and EN 50131-3:2009, Table 6, should be provided by I&HAS using sequential alarm verification:

- unverified alarm;
- sequentially verified alarm;
- automatic reinstatement;
- detector inhibited at automatic reinstatement (including, at grades 3 and 4, identification of detector).

If the unverified alarm or sequentially verified alarm is generated by a tamper condition, this should be separately identified, as required by EN 50131-1, for I&HAS grades 3 and 4.

NOTE 2 The requirement of EN 50131-1 (Table 8) for an “intruder alarm” indication is met by the “unverified alarm.”

6.4 Processing and Notification

The processing requirements and timing performance specified in EN 50131-1:2006, 8.4 and 8.9, should apply to each alarm condition individually.

The use of a dual path alarm transmission system should be considered in order to maximize the ability to transmit a second signal to the ARC. (See also Clause 11.)

The generation of a verified intruder alarm should not be permitted whilst the IAS is unset.

All IAS including alarm verification techniques should either

- notify all set / unset events to the ARC,
- or
- notify “abort” to the ARC to indicate to that an authorised user has performed an action to report that the previously notified alarm should be cancelled.

The generation of a verified hold-up alarm should not be permitted whilst the HAS (or HAS portion of an I&HAS) is unset.

Consideration should be given to the use of an alarm reporting format capable of providing detailed information about alarms to the ARC (EXAMPLE: identification of detector(s)).

The following additional signals or messages, additional to EN 50131-1:2006, Table 8, should be processed and notified to an ARC by I&HAS using sequential alarm verification:

- unverified alarm;
- sequentially verified alarm;
- automatic reinstatement;
- automatic reinstatement with detector inhibited.

If the unverified or sequentially verified alarm is generated by a tamper condition, the tamper condition should be separately notified, as required by EN 50131-1:2006, Table 8, for I&HAS grades 3 and 4.

NOTE 1 The requirement of EN 50131-1:2006, Table 8, for an “intruder alarm” signal or message is met by the “unverified alarm.”

NOTE 2 “Automatic reinstatement” may be notified by restore of the unverified alarm notification signal or message.

6.5 Event recording

The event recording requirements of EN 50131-1:2006, 8.10 should be met by an I&HAS using alarm verification.

The following events, additional to those shown in EN 50131-1:2006, Table 22 and EN 50131-3:2009 Table 11, should be recorded by I&HAS using sequential alarm verification:

- unverified alarm;
- sequentially verified alarm;
- automatic reinstatement;
- detector inhibited at automatic reinstatement (including, at grades 3 and 4, identification of detector).

NOTE 1 The recording of events is optional at grade 1

NOTE 2 The requirement of EN 50131-1:2006, Table 22, for an “intruder alarm” event is met by the “unverified alarm.”

If an unverified alarm or sequentially verified alarm is generated by a tamper condition, this should be identified accordingly, as required by EN 50131-1:2006, Table 22.

NOTE 3 For a sequentially verified I&HAS, the final paragraph of EN 50131-1:2006, 8.10 may be read as applicable to each alarm verification period; the number of events recorded could therefore exceed ten during a single set period.

6.6 Restore

Reference EN 50131-1:2006, Table 6, the permitted access level to restore an unverified alarm should be as specified for “hold-up,” “intruder” or “tamper” as applicable.

Restoration of an I&HAS following a sequentially verified alarm should be by access level 2 or 3 user, or may be restricted to access level 3.

NOTE If one or both of the alarms resulting in a verified alarm is a tamper, the minimum access level specified in EN 50131-1:2006, Table 6 applies.

6.7 Documentation

Documentation for I&HAS including alarm verification should comply with CLC/TS 50131-7:2010, Annex G with the following additional information

- details of alarm verification method(s) used including, where applicable, details of parts of the supervised premises in which verification is applied, itemising each method of alarm verification separately where applicable;
- cautions for the client with regard to response limitations imposed by the system design choices made;
- the location of each HUA device, which information should be available to the ARC (see 8.1.1).

6.8 Hold-up alarms

Verification of hold-up alarms should be applied only where considered necessary or is specified (EXAMPLE: by response authority)

It is recommended that a telephone call-back procedure should be available for the ARC to follow if the results of any method of alarm verification are inconclusive. Where this method is used, only correct use of an identity code or password should be acceptable to cancel response to a hold-up alarm.

NOTE A single identification code / password may be shared by all users at the supervised premises.

7 Sequential verification of intruder alarms

7.1 General

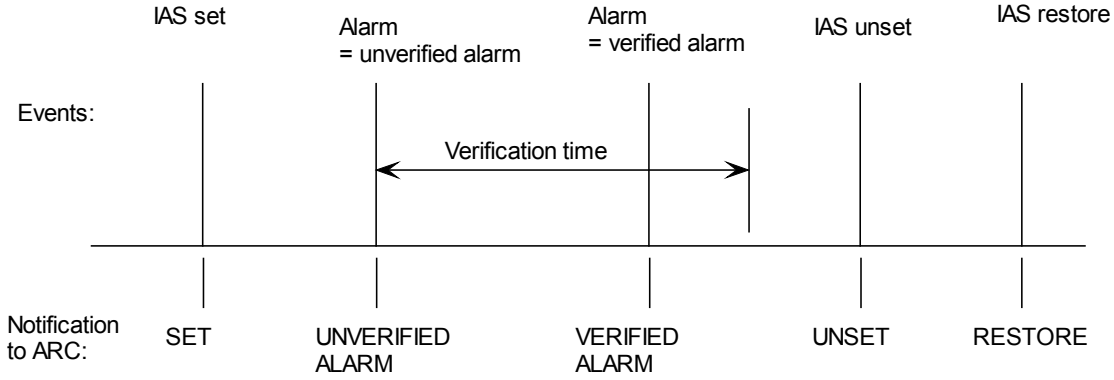

Figure 1 – Time line of completed sequentially verified alarm sequence

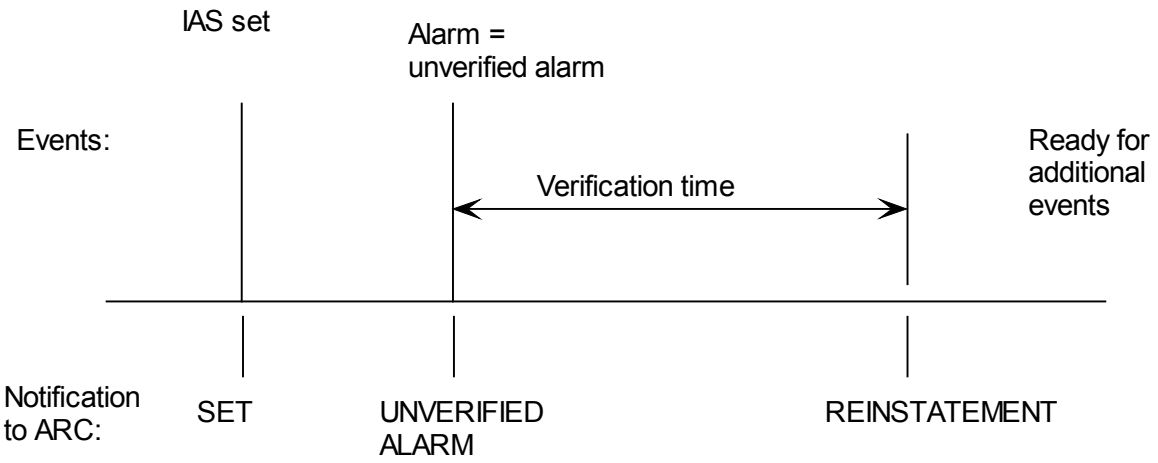

Figure 2 – Time line of unverified alarm sequence

7.2 Recommendations for system requirements

7.2.1 General

These recommendations are additional to the requirements of EN 50131-1.

The following recommendations are applicable to all IAS using sequential alarm verification, at all security grades (except where stated).

7.2.2 Types of alarm

An alarm should be designated as sequentially verified when a minimum of two of the conditions identified in Table 1 are present in any combination.

Table 1 – Types of alarm permitted to contribute to a sequentially verified intruder alarm

	Type of alarm	Notes
a	Intruder	Meeting the recommendations of 7.3.2
b	Intruder during entry time (detector not part of entry route)	Subject to special conditions of EN 50131-1:2006, 8.3.8.2
c	Expiry of entry time	
d	Tamper	
	Tamper identifiable as applicable to a single device or failure of interconnection to a single device	It is optionally permitted for a single tamper alarm to be designated as a verified alarm.
	Tamper applicable to interconnection carrying signals or messages relevant to multiple devices	Designated as sequentially verified immediately (unverified plus verified alarm notifications).
e	ATS path fault	Designation made at ARC (see Clause 11)

The combination of a tamper alarm or ATS path fault with a hold-up alarm should be interpreted as a verified hold-up alarm (see 8.1.2).

7.2.3 Alarm verification time

To be designated as a sequentially verified alarm, the sequential alarm should be generated within a maximum of 60 min after the unverified alarm.

In the event that a sequentially verified alarm does not take place within this time, automatic reinstatement of the IAS should take place (see 7.2.4).

NOTE The time intervals when an ATS path fault is valid as one of the alarm verification conditions (see Table 1) are specified in Clause 11.

7.2.4 Automatic reinstatement

If a sequentially verified alarm has not been notified before the expiry of alarm verification time, the I&HAS should remain in the set state, but be able to respond to detection of a new unverified alarm.

In the event that the detector initiating an unverified alarm remains in alarm at the time of automatic reinstatement, the detector should be automatically inhibited and should remain inhibited until the I&HAS is manually restored (see 6.6).

Automatic reinstatement should be notified to the ARC, including, if applicable, warning that a detector has been inhibited (see 6.4)

If a detector that would normally start a timed entry procedure is inhibited, there should be an alternative means of starting the procedure.

NOTE This may be performed by design of the I&HAS or by the CIE automatically changing the operation of other detectors forming part of the entry/exit route.

7.3 Installation guidelines

7.3.1 General

These recommendations are additional to those in CLC/TS 50131-7.

Design of the I&HAS should ensure that alarm verification capability is commensurate with the risk.

7.3.2 Selection and siting of detectors

The risk assessment should ensure that detectors are sited such that triggering of two detectors provides a high probability of a genuine intrusion, in particular:

a) siting of detectors using the same technology should be restricted, in order that their coverage does not overlap,.

b) detectors of the same technology should be sited such that a single environmental effect would not result in activation of both detectors (see also CLC/TS 50131-7:2010, Annex C),

c) an alarm generated by a single “single-output combined detector” should not constitute a sequentially verified alarm,

d) if “multi-combined detectors” (See A.3) are used to generate a sequentially verified alarm, care should be taken so that a single environmental stimulus could not result in a verified alarm,

e) configuration of a single detector to require two or more activations in a nominated period (or a single activation lasting for a nominated period) before an alarm is presented to the IAS should not permit an alarm to be considered as verified,

f) a second activation of the SAME detector should not be notified as a sequentially verified alarm unless the activations are an intrusion event and a tamper event, in either order.

7.3.3 Indication of verified alarm to a user

Consideration should be given to providing means for a user responding to an unverified alarm to be made aware of the fact that an alarm has subsequently become verified, before entering the premises. (EXAMPLE: indication at point of entry, strobe fixed to WD activated by verified alarm, etc.).

7.3.4 Contribution of ATS path fault to intrusion alarm

See Clause 11.

7.4 ARC responses

ARC responses are specified in EN 50518-3.

8 Sequential verification of hold-up alarms

8.1 Recommendations for system requirements

8.1.1 General

These recommendations are additional to the requirements of EN 50131-1.

If sequential verification of hold-up alarms is used, the ATS should permit transmission of separate signals or messages from different hold-up alarm devices or the different outputs of a multi-action hold-up device.

Zoning of hold-up devices should be optimized for the most timely and effective response in accordance with EN 50131-1:2006, Table 7, Note b. Thus zoning information should be passed to the ARC.

8.1.2 Types of alarm

The sequential alarm sequence of a hold-up alarm combined with a second hold-up alarm, an ATS path fault, an intrusion alarm or a tamper alarm should be interpreted as a verified hold-up alarm.

Two hold-up alarms being designated as a verified hold-up alarm may originate from two separate devices, or from a single multi-action hold-up device.

8.1.3 Alarm verification time

The alarm verification time for hold-up alarms should be within a maximum of 24 h of the unverified alarm.

In the event that a sequentially verified hold-up alarm does not take place within this time, automatic reinstatement of the HAS should take place.

NOTE The time intervals when an ATS path fault is valid as one of the alarm verification conditions (see Table 1) are specified in Clause 11.

8.2 Installation guidelines

8.2.1 General

These recommendations are additional to those in CLC/TS 50131-7.

Design of the I&HAS should ensure that alarm verification capability is commensurate with the risk, and that the most appropriate type of hold-up device (or multi-action hold-up device) is used.

8.2.2 Contribution of ATS path fault to verified alarm

See Clause 11.

8.3 ARC responses

ARC responses are specified in EN 50518-3.

9 Audible alarm verification

9.1 System design factors

9.1.1 General

These recommendations are additional to the requirements of EN 50131-1.

Precautions should be taken to prevent breaches of privacy legislation.

Consideration should be given to supplementing audible alarm verification by sequential alarm verification (see also Clause 4).

9.1.2 Audio information at supervised premises

In order to provide means of audible alarm verification there should be means to:

a) store at least 10 s of audio immediately prior to an alarm, ready for transmission to ARC on demand,

Where detection is by AMD, this may be reduced to 1 s.

b) store audio following an alarm at least until the audio link is established with the ARC,

c) transmit live audio to the ARC on demand.

Where the I&HAS is divided into sub-systems, it should be possible to transmit audio information relevant only to a sub-system of the I&HAS that is set at the time of the activation.

It should be possible to transmit audio information only following an alarm or as part of maintenance or other procedures with the agreement of the client.

9.1.3 Warning devices

In order to prevent interference with audio information being transmitted to the ARC, notification to warning devices should be delayed until an alarm is designated as verified by the ARC or inhibited, as permitted by EN 50131-1:2006, 8.6.

NOTE Audible alarm verification of the entry route may not be appropriate.

9.2 Installation guidelines

9.2.1 General

These recommendations are additional to those in CLC/TS 50131-7.

9.2.2 Selection and Siting of equipment

All detectors and hold-up devices for which alarm verification is required, as well as CIE and SPT, should be located within the area of coverage of an ALD.

ALDs should be sited to avoid noise sources that could interfere with the ARC operator’s ability to listen to audio information transmitted from site.

9.2.3 Coverage of audio listening devices

The area of coverage of an ALD should be greater than the area of coverage of the associated detector(s).

In the case of audible verification of hold-up alarms, the area of coverage of an ALD should be tailored to the threat which may be present. The area of coverage may thus differ from the location of the HUA device.

Where the I&HAS is divided into sub-systems, care should be taken to ensure that audio information from devices within a sub-system that is set cannot transmit audio from another sub-system that is not set.

9.3 ARC responses

ARC responses are specified in EN 50518-3.

10 Visual alarm verification

10.1 System design factors

10.1.1 General

These recommendations are additional to the requirements of EN 50131-1 and EN 50132-1.

Precautions should be taken to prevent breaches of privacy legislation.

Consideration should be given to supplementing visual alarm verification by sequential alarm verification (see Clause 4).

10.1.2 Video information at supervised premises

In order to provide means of visual alarm verification there should be means to transmit at least 4 images to the ARC – one originating within one second prior to the activation, one at the time of the alarm activation (or the activation of the VMD), plus two additional images within 5 s of the activation.

Where the I&HAS is divided into sub-systems, it should be possible to transmit visual information relevant only to a sub-system of the I&HAS that is set at the time of the activation.

It should be possible to transmit visual information only following an alarm or as part of maintenance or other procedures with the agreement of the client.

10.2 Installation guidelines

10.2.1 General

These recommendations are additional to those in CLC/TS 50131-7.

10.2.2 Selection and siting of equipment

All relevant detectors and hold-up devices for which alarm verification is required, as well as CIE and SPT, should be located within the area of coverage of an imaging device.

The illumination of the area of coverage of an imaging device should be adequate to meet the selected requirement of EN 50132-7:2012, 6.7 such that visual verification of an alarm event is possible.

Imaging devices should be sited to avoid light sources that could interfere with the ARC operator's ability to view information transmitted from site. In particular, strobing devices attached to WDs should be sited so as to avoid interfering with visual information or be inhibited until the ARC has designated an alarm as verified.

10.2.3 Coverage of imaging devices

The area of coverage of an imaging device should be greater than the area of coverage of the associated detector.

In the case of visual verification of hold-up alarms, the area of coverage of an imaging device should be tailored to the threat which may be present.

NOTE The area of coverage may thus differ from the location of the HUA device.

Where the I&HAS is divided into sub-systems, care should be taken to ensure that visual information from devices within a sub-system that is set cannot transmit images including part of another sub-system that is not set.

10.3 ARC responses

ARC responses are specified in EN 50518-3.

11 ATS faults

11.1 System design factors

11.1.1 General

These recommendations are additional to those included in EN 50131-1 and EN 50136-1.

11.1.2 Contribution of ATS path faults to a verified alarm

ATS path faults may contribute to a verified alarm as follows:

a) an ATS path fault followed by an intrusion, tamper or hold-up alarm within the same set period;

b) an intrusion, tamper or hold-up alarm signal or message followed by an ATS path fault during the same set period;

c) two ATS path faults, relevant to different paths, during the same set period. The two paths should be of different technologies (see EN 50518-3:2013, 5.7); typically land-line and wireless.

The time permitted during the set period may be varied independently for intrusion and hold-up alarms.

The sequential alarm sequence of a hold-up alarm combined with an ATS path fault should be interpreted as a verified hold-up alarm (see 8.1.2).

11.2 Installation guidelines

These recommendations are additional to those included in CLC/TS 50131-7 and the requirements of EN 50136-1.

NOTE 1 The provision of a dual-path ATS does not, of itself, constitute a method of alarm verification.

NOTE 2 Consideration should be given to the use of dual-path ATS to prevent notification of alarm verification being disabled by a single path fault.

11.3 ARC responses

ARC responses are specified in EN 50518-3.

Annex A
(informative)

Equipment specifications

A.1 General

The recommendations of this annex should be applied when components are intended to permit I&HAS to perform alarm verification.

Equipment need not be designed to meet ALL recommendations of this annex, but the manufacturer's documentation should identify all recommendations implemented, along with details of the optional parameters provided.

A.2 Control and indicating equipment

A.2.1 General

These recommendations are additional to the requirements of EN 50131-3.

A.2.2 Alarm types

The CIE should recognise the combinations of alarm types identified in 7.2.2 as valid for generation of a sequentially verified intruder alarm, and those identified in 8.1.2 as valid for a sequentially verified hold-up alarm.

A.2.3 Alarm verification time

The CIE should have the facility to programme the alarm verification time between the limits defined at 7.2.3 for intruder alarms and at 8.1.3 for hold-up alarms.

A.2.4 Automatic reinstatement

The CIE should have the facility to terminate an unverified alarm at the end of alarm verification time and be prepared for further alarm events, as defined at 7.2.4.

A.2.5 Restore

The CIE should have means to be restored at the access level specified for the I&HAS in 6.6.

A.2.6 Processing and notification

The CIE should have the means to provide the notification signals or messages defined in 6.4.

The CIE should have means to delay the notification to a warning device, either for a fixed period or until an alarm is designated as verified.

NOTE This designation may be the generation of a sequentially verified alarm by the CIE, or by a signal or message received from the ARC, whether direct or via audio or visual control equipment.

A.2.7 Indication

The CIE should have the means to provide the indications defined in 6.3.

A.2.8 Event recording

The CIE should have the means to record the events defined in 6.5.

A.2.9 Interface to audible alarm verification equipment

The CIE should provide the means to interface with audio alarm verification equipment in order to

a) convey status of the I&HAS to enable transmission of audio information associated with the triggered detector,

b) control the inhibit of warning device(s).

A.2.10 Interface to visual alarm verification equipment

The CIE should provide the means to interface with video alarm verification equipment in order to convey the status of the I&HAS to enable transmission of visual information associated with the triggered detector.

A.2.11 Documentation

The manufacturer's documentation should include

a) details of options specified in this annex that are provided in the product

b) limits of programming of relevant options,

c) details of interfaces to audible and visual alarm verification equipment (A.2.9 and A.2.10) including identification of signal or message protocol used,

A.3 Multi-output combined detectors

A.3.1 General

These recommendations are additional to the requirements of EN 50131-2 (all parts).

NOTE a detector may be capable of being configured internally as either a "single-output combined detector" or a "multi-output combined detector".

A.3.2 Recommendations

Where a multi-output combined detection device is designed with two (or more) sensors in the same housing in order to fulfil the recommendations of 7.3.2, the following should apply:

a) the sensors should be of different technologies or have non-overlapping monitoring coverage;

b) the processed intrusion outputs from the sensors should be communicated independently to the CIE;

c) the processing of the status of any sensor should not influence, or be influenced by, the processing of the status of any other sensor;

NOTE This does NOT require that the device use separate means of processing (EXAMPLE: separate microprocessors) to deal with the outputs from each sensor.

d) masking and fault signals may be processed individually for each sensor, or as single masking and fault signals or messages (where relevant) for the overall device.

A.3.3 Documentation

The manufacturer's documentation should include

a) details of monitored coverage area of the independent sensors, including any gaps between,

b) identification of outputs to CIE relative to the independent sensors.

A.4 Multi-action hold-up device

A.4.1 General

These recommendations are additional to the requirements of CLC/TS 50131-11.

A.4.2 Recommendations

Where a multi-action Hold-Up Device is designed with two (or more) actions in order to fulfil the recommendations of 8.1.2, the following should apply:

a) the actions should be of different methods or an intended order of the same or different methods;

b) the processed hold-up output(s) from the hold-up device should be communicated independently to the CIE in the order they are generated;

c) the processing of the output of any action should not influence, or be influenced by the processing of the output of any other action;

NOTE This does NOT require that the device use separate means of processing (EXAMPLE: separate microprocessors) to deal with the output(s) from each action or operating part.

d) masking and fault signals may be processed individually for each output, or as single masking and fault signals or messages (where relevant) for the overall device.

A.4.3 Documentation

The manufacturer's documentation should include

a) details of the operating method(s) and action(s)

b) identification of output(s) to CIE relative to the independent operating method(s), if required

A.5 Audible alarm verification equipment

A.5.1 Recommendations

A.5.1.1 Audible alarm verification control equipment

Equipment used to control the means of audible alarm verification should have means to receive signals or messages from the I&HAS to identify alarm information.

This information should be processed to receive sound from the ALD associated with the alarm event. This sound should be recorded and transmitted to the ARC in accordance with the recommendations of 9.1.2 and 9.1.3.

The equipment should also have means to interface with CIE as required by A.2.9.

NOTE 1 Part or all of this functionality may be integrated into the CIE or SPT, or into ALD(s) or AMD(s).).

NOTE 2 Provision may additionally be made for the transmission of live audio messages to the site, or for the playback of pre-recorded messages.

A.5.1.2 Audio listening device

Audio listening devices used should be activated by the audio alarm verification control equipment and then pass audio information to the audible alarm verification control equipment in real time

A.5.1.3 Audio monitoring device

The audio monitoring device should detect sounds above a preset threshold and present this output to the I&HAS to generate an alarm.

The audio monitoring device should then perform the functionality of an audio listening device (see 3.1.4), presenting its output to the audio alarm verification control equipment to enable sounds at the supervised premises to be monitored to permit the alarm to be designated as verified when appropriate.

A.5.2 Tamper protection and detection recommendations

Audible alarm verification equipment should meet the tamper protection and detection requirements of EN 50131-1, according to the nature of the equivalent component, as specified in Table A.1, at the system grade specified for the equipment.

A.5.3 Environmental recommendations

Audible alarm verification equipment should meet the environmental requirements of the equivalent device, as identified in Table A.1.

Table A.1 – Tamper protection, tamper detection and environmental recommendations for audible alarm verification equipment

Type of component	Equivalent component
Audio listening device	Acoustic break-glass detector (CLC/TS 50131-2-7-1)
Audio monitoring device	Acoustic break-glass detector (CLCTS 50131-2-7-1)
Audio control equipment	CIE (EN 50131-3)
ALD / AMD expansion equipment	CIE (EN 50131-3)
Audio transmission device	SPT (EN 50131-10)

A.5.4 Documentation

The manufacturer's documentation should include

a) installation instructions,

b) (for control equipment) details of interface to I&HAS CIE (A.2.9) including identification of signal or message protocol used,

c) (for audio monitoring devices) sound level threshold adjustment,

d) any special settings required on audio alarm verification control equipment or on I&HAS CIE to comply with the recommendations of this document.

A.6 Visual alarm verification equipment

A.6.1 Visual alarm verification control equipment

Equipment used to control the means of visual alarm verification should have means to receive signals or messages from the I&HAS to identify alarm information.

This information should be processed to receive images from the imaging device associated with the alarm event. These images should be recorded and transmitted to the ARC in accordance with the recommendations of 10.1.2.

This equipment should also have the means to interface with CIE as required by A.2.10.

NOTE Part or all of this functionality may be integrated into the CIE or SPT, or into imaging devices or VMD(s).

A.6.2 Other visual alarm verification equipment

Visual surveillance (or CCTV) equipment used in visual alarm verification systems should comply with the recommendations of this clause, in addition to those of the standard relevant to the equipment.

A.6.3 Tamper protection and detection recommendations

Equipment used in visual alarm verification systems should meet the tamper protection and detection requirements of equivalent standards identified in Table A.2 at the system grade specified for the equipment.

A.6.4 Environmental recommendations

Equipment used in visual alarm verification systems should meet the environmental requirements of EN 50132-1:2010, Clause 7. For test purposes, the specific requirements for the equivalent device, as identified in Table A.2 should be used:

Table A.2 – Tamper protection, tamper detection and environmental recommendations for visual alarm verification equipment

Type of component	Equivalent component
Imaging device	Camera (EN 50132-1:2010, 6.3.2.3, Table 5)
Video monitoring device	Camera (EN 50132-1:2010, 6.3.2.3, Table 5)
Visual alarm verification control equipment	CIE (EN 50131-3)
Imaging device expansion equipment	CIE (EN 50131-3)
Video transmission device	Video Transmission devices (EN 50132-1)

A.6.5 Documentation

The manufacturer's documentation for visual alarm verification control equipment should include:

a) details of interface to I&HAS CIE (A.2.10) including identification of signal or message protocol used,

b) any special settings required on visual equipment or on I&HAS CIE to comply with the recommendations of this document.

Annex B
(informative)

Equipment test procedures

B.1 CIE

The following tests are additional to EN 50131-3 and apply to all CIE providing relevant options intended to meet the recommendations of this specification:

Table B.1 – CIE tests for alarm verification functions *(1 of 3)*

Step	Test condition (c)	Action (d)	Measurement (e)	Pass/fail criteria (in addition to requirements of EN 50131-3) (f)
Alarm types (A.2.2), Restore (A.2.5), Processing and notification (A.2.6), Indication (A.2.7) and Event recording (A.2.8).				
1a	IAS portion of alarm system set, Absence of "intruder, tamper, fault signals and messages" No indication active	Generate an intruder alarm	Check indications, notification and event recording	Indication, notification, and event recording should comply with 6.3, 6.4 & 6.5
1b		Generate a second intruder alarm	Check indications, notification and event recording	Indication, notification and event recording should comply with 6.3, 6.4 & 6.5
1c	Restore IAS			Restore should only be possible at the access level defined in EN 50131-1 for the type of alarm
1d	Repeat Steps 1a to 1c using combinations of alarm signals or messages as defined in Table 1 (7.2.2), except ATS path faults See Steps 1e – 1f		Check indications, notification and event recording	Indication, notification and event recording should comply with 6.3, 6.4 & 6.5 Restore should only be possible at the access level defined in EN 50131-1 for the type of alarm
2a	Adjust programming for restore access level to be level 3			
2b	For one suitable combination of Step 1d		Check access level at which restore is possible	Restore should only be possible at access level 3.
3a	HAS portion of CIE set, Absence of "hold-up signals and messages" No indication active	Generate a hold-up alarm	Check indications, notification and event recording	Indication, notification and event recording should comply with 6.3, 6.4 & 6.5
3b		Generate a second hold-up alarm	Check indications, notification and event recording	Indication, notification and event recording should comply with 6.3, 6.4 & 6.5
3c	Cancel alarm and Restore HAS (as described by manufacturer)			Restore should be possible at the access level defined in EN 50131-1 for the type of alarm

Table B.1 *(2 of 3)*

Step	Test condition (c)	Action (d)	Measurement (e)	Pass/fail criteria (in addition to requirements of EN 50131-3) (f)
4	Repeat Steps 3a to 3b using combinations of alarm signals or messages as defined in 8.1.2, except ATS path faults See Steps 5a – 5b		Check indications, notification and event recording	Indication, notification and event recording should comply with 6.3, 6.4 & 6.5 Restore should be possible at the access level defined in EN 50131-1 for the type of alarm
5a	Adjust programming for restore access level to be level 3			
5b	For one suitable combination of Step 4		Check access level at which restore is possible	Restore should only be possible at access level 3.
5c	Repeat Steps 1a and 1b using combinations of alarm signals or messages NOT defined in 7.2.2 or 8.1.2		Check indications, notification and event recording	Indication, notification and event recording should NOT include verified hold-up alarm
Alarm verification time (A.2.3) and Automatic reinstatement (A.2.4)				
6a	IAS portion of alarm system set	Generate an intruder alarm, leaving the trigger signal or message present until Step 6d completed	Check indications, notification and event recording	Indication, notification and event recording should comply with 6.3, 6.4 & 6.5
6b		Allow alarm verification time to expire	Check indications, notification and event recording	Indication, notification and event recording should comply with 6.3, 6.4 & 6.5
6c		Generate a different intruder alarm	Check indications, notification and event recording	Indication, notification and event recording should comply with 6.3, 6.4 & 6.5
6d	Unset IAS		Check indications, notification and event recording	System in normal unset condition
7	Verify range of programming available for alarm verification time		Record range of programming available	Range of times covers limits required by 7.2.3
8a	HAS portion of alarm system set	Generate a hold-up alarm, leaving the signal or message present until Step 8d completed	Check indications, notification and event recording	Indication, notification and event recording should comply with 6.3, 6.4 & 6.5
8b		Allow alarm verification time to expire	Check indications, notification and event recording	Indication, notification and event recording should comply with 6.3, 6.4 & 6.5
8c		Generate a different hold-up alarm	Check indications, notification and event recording	Indication, notification and event recording should comply with 6.3, 6.4 & 6.5
8d	Unset HAS		Check indications, notification and event recording	System in normal unset condition

Table B.1 *(3 of 3)*

Step	Test condition (c)	Action (d)	Measurement (e)	Pass/fail criteria (in addition to requirements of EN 50131-3) (f)
8e	Verify range of programming available for alarm verification time		Record range of programming available	Range of times covers limits required by 8.1.3
Interface to audio control equipment (A.2.9) and Interface to visual control equipment (A.2.10)				
9	The manufacturer should provide sufficient information, and means to verify correct operation of the interface at the CIE for a test laboratory to evaluate compliance with the recommendations of A.2.9 and A.2.10, NOTE It is not mandatory that this is tested with audio / visual control equipment connected, though this is permitted.			The interface should comply with A.2.9 / A.2.10 for at least one of each type of equipment
Manufacturer's documentation (A.2.11)				
10	Check manufacturer's documentation			Documentation should comply with the recommendations of A.2.11

B.2 Multi-output combined detectors

B.2.1 General

The following tests are additional to EN 50131-2 and apply to all multi-output combined detectors intended to meet the recommendations of this specification:

B.2.2 Whilst performing the coverage test

a) If the output response is selectable between single or multiple output, check that this is set to the correct mode.

b) verify that the coverage patterns are non-overlapping, if the sensors are of the same technology;

c) verify that the sensor responses are processed independently and communicated separately to the CIE.

B.2.3 Documentation

The manufacturer's documentation should be checked for compliance with A.3.3.

B.3 Audible alarm verification equipment

B.3.1 General

The following tests apply to all audible alarm verification equipment intended to meet the recommendations of this specification:

B.3.2 Audio alarm Verification control equipment

The manufacturer of audio alarm verification control equipment should provide sufficient information and equipment to verify compliance with A.5.1.1, with specific emphasis on

a) the recommendations for storage and transmission of audio information of 9.1.2,

b) the correct correspondence between ALD and the intrusion detector triggered (See 9.1.2),

c) correct interfacing with I&HAS CIE to control output(s) to warning device(s) (See 9.1.3).

B.3.3 The manufacturer of audio listening devices or audio monitoring devices should provide sufficient information to verify compliance with 5.1.2 or 5.1.3 respectively.

B.3.4 The tamper protection and detection recommendations (A.5.2) should be tested in accordance with the product standard for the equivalent component (as per Table A.1).

B.3.5 The environmental recommendations of A.5.3 should be tested in accordance with the product standard for the equivalent component (as per Table A.1).

B.3.6 The manufacturer's documentation should be checked for compliance with A.5.4.

B.4 Visual alarm verification equipment

B.4.1 Visual alarm verification control equipment

The following tests apply to all visual alarm verification control equipment intended to meet the recommendations of this specification:

The manufacturer should provide sufficient information and equipment to verify compliance with A.6.1 with specific emphasis on:

a) the recommendations for storage and transmission of visual information of 10.1.2;

b) the correct correspondence between imaging device and the intrusion detector triggered (A.6.1).

B.4.2 Other visual alarm verification equipment

Visual surveillance (or CCTV) equipment to be used in visual alarm verification systems should be tested to ensure compliance with the standard relevant to the equipment, or evidence presented of prior compliance testing.

B.4.3 The tamper protection and detection recommendations (A.6.3) should be tested in accordance with the product standard for the equivalent component (as per table A.2).

B.4.4 The environmental recommendations of A.6.4 should be tested in accordance with the product standard for the equivalent component (as per Table A.2).

B.4.5 The manufacturer's documentation should be checked for compliance with A.6.5.

Bibliography

EN 50131-2 (all parts), *Alarm systems — Intrusion and hold-up systems*

CLC/TS 50131-2-7-1, *Alarm systems — Intrusion and hold-up systems — Part 2-7-1: Intrusion detectors - Glass break detectors (acoustic)*

EN 50131-3:2009 [2)], *Alarm systems — Intrusion and hold-up systems — Part 3: Control and indicating equipment*

EN 50131-10:2010, *Alarm systems — Intrusion and hold-up systems — Part 10: Application specific requirements for Supervised Premises Transceiver (SPT)*

CLC/TS 50131-11, *Alarm systems — Intrusion and hold-up systems — Part 11: Hold-up devices*

EN 50132-1:2010, *Alarm systems — CCTV surveillance systems for use in security applications — Part 1: System requirements*

EN 50132-7:2012, *Alarm systems — CCTV surveillance systems for use in security applications — Part 7: Application guidelines*

[2)] A corrigendum is in preparation

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.™