National Security Inspectorate
Sentinel House, 5 Reform Road, Maidenhead, SL6 8BY
E: nsi@nsi.org.uk | W: nsi.org.uk

Date: 29 July 2020

To: All NACOSS Gold and Systems Silver approved companies and applicants

TECHNICAL BULLETIN No: 0054

Publication of BS EN 50131-1:2006-A3:2020 – Alarm systems. Intrusion and hold-up systems. System requirements

BS EN 50131 amendment 3 was published in June 2020 and is available from the BSI or NSI as an individual purchase or via the NSI approved company Standards on Subscription service.

Implementation timescale for approved and applicant companies

At the time of writing this technical bulletin, amendment 3 of BS EN 50131-1:2006 was not called up in the current edition of PD 6662. The need for compliance with amendment 3 will coincide with the adoption of a future edition of PD 6662.

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

Where wording of the Standard has been added, this is reproduced in Green.

Where wording of the Standard has been changed, this is reproduced in Blue.

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

Please note this is not a definitive list of all the changes introduced through the publication of the 2020 amendment 3 of BS EN 50131-1. Only significant changes are detailed within this document.

There are a few minor changes to BS EN 50131-1:2006-A3:2020. These relate to changes in associated product standards, the introduction of remote access, and the 'coercive principal' that is required by one or more European country.

1 Scope

This European Standard specifies the requirements for Intrusion and Hold-up Alarm Systems installed in buildings using specific or non-specific wired interconnections or wire-free interconnections. These requirements also apply to the components of an I&HAS installed in a building which are normally mounted on the external structure of a building e.g. ancillary control equipment or warning devices. The standard does not include requirements for exterior I&HAS.

2 Normative references

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

EN 50130-5 - Alarm systems – Part 5: Environmental test methods

EN 50131-6 - Alarm systems – Intrusion and hold-up systems – Part 6: Power supplies

CLC/TS 50131-12 2016 — Intrusion and hold-up systems — Part 12: Methods and requirements for setting and unsetting of Intruder Alarm Systems (IAS)

CLC/TS 50131-12 2016 is a new addition.

BS EN 60073 is no longer applicable.

3.1.13 alternative power source

power source capable of powering the I&HAS for a predetermined time when a prime power source is unavailable

Note 1 to entry: The alternative power source is typically a battery.

Note 1 is a new addition.

3.1.16 authorisation

permission for a user to gain access to the various control functions of an I&HAS

This clause has been changed to clarify that 'authorisation' relates to user access.

3.1.55 prime power source

power source used to support an I&HAS under normal operating conditions

Note 1 to entry: For types A and B PS, the prime power source is equivalent to an external power source (EPS) as defined in EN 50131-6:2017, 3.1.5; also see EN 50131-6:2017 Figure 2.

Note 2 to entry: For Type C PS the prime power source is derived from the PS storage device.

This clause has been changed to specify 'operating conditions'' instead of 'working conditions'.

Note 1 and Note 2 have been reworded.

3.1.56 principal prime power source

energy source capable of supporting the I&HAS for extended periods

Note 1 to entry: The principal prime power source may be derived from, e.g. the public electricity (mains) supply or an electricity supply independent of the public electricity supply.

This clause is a new addition.

3.1.61 signal

variable parameters by which information is conveyed

The 'significant reduction in range' definition has been removed as the need for grade 4 detectors to detect a significant reduction in range is no longer a requirement of this standard.

3.1.67 supplementary prime power source

energy source, independent of the PPPS, capable of supporting an I&HAS for extended periods, without affecting the standby period of the alternate power source

This clause has been changed to state principal prime power source (PPPS) instead of prime power source.

3.2 Abbreviations

For the purposes of this document, the following abbreviations are used:

ARC - alarm receiving centre

ACE - ancillary control equipment

AE - annunciation equipment

ATP - alarm transmission path

ATS - alarm transmission system

CIE - control and indicating equipment

HAS - hold-up alarm system(s)

IAS - intruder alarm system(s)

I&HAS - intrusion and hold-up alarm system(s)

WD - warning device

PS - power supply

PPPS - principle prime power source

RCT - receiving centre transceiver

SPT - supervised premises transceiver

Abbreviation PPPS is a new addition.

8.3 Operation

The requirements of this clause apply irrespective of whether access to an I&HAS is performed directly at the CIE/ACE or remotely.

This paragraph has been added to indicate that access may be performed directly or remotely. This clause now applies regardless as to whether access is gained locally or remotely, e.g. via a smart phone.

8.3.1 Access levels

Level 4 User access e.g. by the manufacturer of the equipment
Access to components to change equipment design.
Access to functions required to be accessible at level 4 shall be restricted by means of a key or code operated switch or lock or other equivalent means.

NOTE 1 Access level 4 applies when changing the operating programme software without having activated a tamper device on the CIE or ACE for example to provide cyber-security patches.

NOTE 1 has been changed to include cyber-security patches as an example.

NOTE 2 This standard does not give requirements for the duration for which the permission to access the system at access level 3 or 4 remains valid. Permitting remote access, particularly for extended periods, could result in contractual liabilities.

NOTE 2 is a new addition to bring attention to contractual liabilities that may be impacted by allowing extended periods of valid access for remote access.

Communication systems used to support access for remote users shall comply with the requirements of Annex B.

NOTE 2 is a new addition.

8.3.2 Authorisation

At security grades 2, 3 and 4, repeated invalid authorization attempts shall be detected and/or restricted.

This paragraph is a new addition.

8.3.5 Prevention of setting

Movement detector range reduction has been removed from Table 4.

8.3.6 Overriding prevention of setting

Movement detector range reduction has been removed from Table 5.

8.3.9 Restoring

Movement detector range reduction has been removed from Table 6.

8.4.6 Reduction or range signals or messages

This clause has been removed.

8.5.1 General

All mandatory indications required by this clause shall be located together in at least one CIE or ACE. Duplicate indications may be provided at other locations. When access to the I&HAS is performed remotely all mandatory indications shall be available to the remote user.

This paragraph has been changed to reference remote users.

NOTE 3 and NOTE 4 have been removed.

Movement detector range reduction has been removed from Table 6.

8.6.2 ATS Notification

For PS Types A and B, notification of prime power source faults may be delayed for a maximum of 1 h.

This paragraph has been changed to include both types A and type B power supplies.

8.7.4 Monitoring of substitution – Timing requirements

Substitution of I&HAS components – Maximum time before detection

The wording and format of this requirement in Table 14 has been changed.

8.8.2.2 Monitoring of interconnections (Coerciveness Principle)

This clause is a new addition.

8.8.3 Availability of interconnections

NOTE It is acceptable to determine compliance with Table 15 by the use of periodic messages between I&HAS components.

This note is a new addition.

8.8.4.1 Interconnection integrity – Periodic communication

Maximum permitted intervals between periodic communication signals or messages

The wording and format of this requirement in Table 16 has been changed.

8.8.4.2 Verification during the setting procedure

Maximum time from the receipt of the most recent signal or message

The wording and format of this requirement in Table 17 has been changed.

8.10 Event recording

Dependent upon the Grade of an I&HAS, the events specified in Table 21 shall be recorded. It shall be possible from the event record to determine if an event was recorded as a result of remote access together with the identity of the remote user.

This paragraph has been changed to include remote access.

Rejected attempts to setup remote communication with an I&HAS (see Annex B)

This event is a new addition to Table 21.

9.2 Requirements

For Type A and B power supplies in grades 3 & 4 I&HAS, when a prime power source fault is notified to an alarm receiving centre or other remote centre, the duration of the alternative power supply may be halved.

This statement is a new addiction to Table 22.

The format of Table 22 has been changed.

The note in Table 22 has been removed.

For Type A and B power supplies when a supplementary prime power source, with automatic change over between the principal prime power source and the supplementary prime power

source is provided, the period the alternative power source is required to power the I&HAS may be reduced to 4 h.

This paragraph has been changed to reference the principle prime power source.

In I&HAS including a type A power supply, the alternative power source shall be recharged to provide 80 % of the capacity required to meet the requirements specified in Table 22 within the periods specified in Table 23.

This paragraph has been changed to provide clarification.

15 Marking/Identification

All I&HAS components shall be marked with the following:

– name of manufacturer or supplier or its registered trademark;

– date of manufacture or batch number or serial number;

– security grade;

– environmental class.

This clause has been changed to reflect that component marking and identification has been modified to allow either a trade mark or the suppliers name as the form of supplier identification.

Annex B

Annex B is a new addition which details requirements applicable when an I&HAS is remotely accessed.

Annex C

Annex C is a new addition which lists some commonly known cyber security threats.