

DRAFT FOR DEVELOPMENT

Intruder and hold-up alarm systems – Commissioning, maintenance and remote support – Code of practice

ICS 13.310

This publication is not to be regarded as a British Standard.

It is being issued in the Draft for Development series of publications and is of a provisional nature. It should be applied on this provisional basis, so that information and experience of its practical application can be obtained.

A review of this Draft for Development will be carried out not later than 2 years after its publication.

Notification of the start of the review period, with a request for the submission of comments from users of this Draft for Development, will be made in an announcement in the appropriate issue of *Update Standards*.

According to the replies received, the responsible BSI Committee will judge whether the Draft for Development can be converted into a British Standard or what other action should be taken.

Observations which it is felt should receive attention before the official call for comments will be welcomed.

These should be sent to the Secretary of BSI Technical Committee GW/1 at British Standards House, 389 Chiswick High Road, London W4 4AL.



NO COPYING WITHOUT BSI PERMISSION EXCEPT AS PERMITTED BY COPYRIGHT LAW

Publishing and copyright information

The BSI copyright notice displayed in this document indicates when the document was last issued.

© BSI 2007

ISBN 978 0 580 55787 3

The following BSI references relate to the work on this publication:
Committee reference GW/1

Publication history

First published July 2007

Amendments issued since publication

Amd. no.	Date	Text affected
-----------------	-------------	----------------------

Contents

Foreword *ii*

Introduction *1*

- 1** Scope *1*
- 2** Normative references *1*
- 3** Terms, definitions and abbreviations *2*
- 4** Inspection, functional testing and commissioning *4*
- 5** Maintenance *4*
- 6** Remote system checks *6*
- 7** Remote support *7*
- 8** Security measures *9*
- 9** Responsibilities of the user/client *10*

Annexes

- Annex A (normative) Commissioning of an I&HAS *11*
- Annex B (normative) Preventative maintenance *14*
- Annex C (informative) Verification of health of alternative power source *16*
- Annex D (normative) Remote initiation of commands *17*

Bibliography *18*

List of tables

- Table 1 – Minimum frequency of preventative maintenance *5*
- Table 2 – Data security measures *8*
- Table A.1 – Commissioning recommendations *11*
- Table B.1 – Preventative maintenance recommendations *14*
- Table C.1 – Minimum load times for common storage devices *16*
- Table D.1 – Remote initiation of commands *17*

Summary of pages

This document comprises a front cover, an inside front cover, pages i and ii, pages 1 to 18, an inside back cover and a back cover.

Foreword

Publishing information

This Draft for Development was published by BSI on 31 July 2007. It was prepared by Subcommittee GW/1/2, *Installed alarm systems*, under the authority of Technical Committee GW/1, *Electronic security systems*. A list of organizations represented on this committee can be obtained on request to its secretary.

Relationship with other publications

This Draft for Development incorporates maintenance recommendations formerly included in BS 4737, *Intruder alarm systems in buildings*, and is intended to be used in conjunction with PD 6662, *Scheme for the application of European Standards for intruder and hold-up alarm systems*.

Use of this document

As a code of practice, this Draft for Development takes the form of guidance and recommendations. It should not be quoted as if it were a specification and particular care should be taken to ensure that claims of compliance are not misleading.

Any user claiming compliance with this Draft for Development is expected to be able to justify any course of action that deviates from its recommendations.

Presentational conventions

The provisions in this Draft for Development are presented in roman (i.e. upright) type. Its recommendations are expressed in sentences in which the principal auxiliary verb is “should”.

Commentary, explanation and general informative material is presented in smaller italic type, and does not constitute a normative element.

The word “should” is used to express recommendations of this Draft for Development. The word “may” is used in the text to express permissibility, e.g. as an alternative to the primary recommendation of the clause. The word “can” is used to express possibility, e.g. a consequence of an action or an event.

Notes and commentaries are provided throughout the text of this Draft for Development. Notes give references and additional information that are important but do not form part of the recommendations. Commentaries give background information.

Contractual and legal considerations

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

Compliance with a Draft for Development cannot confer immunity from legal obligations.

Introduction

Commissioning of any intruder and hold-up alarm system is vital to ensure the system is fully functional. At the commissioning stage, the status of all parts of the system ought to be recorded to be used as the basis against which any future maintenance is measured.

Maintenance of an intruder and hold-up alarm system is required to ensure that the system's integrity is maintained and that it is fully functional. Such maintenance prevents minor problems becoming major problems, enables alarm company personnel to correct physical, electrical and electronic faults and allows software updates to take place.

Remote support of intruder and hold-up alarm systems permits a range of tasks to be carried out from simple capture of system event records or other parameters through to full maintenance checks, under manual or automatic control, using the self-diagnostic capabilities of the system. Hence an analysis of the system to a level similar to that by alarm company personnel on site might be possible remotely.

Remote system checks can therefore be used to check the electronic integrity of a system, but not the physical condition of the system. A combined approach of both physical visits to the site and remote system checks offers greater confidence to the client.

1 Scope

This Draft for Development gives recommendations for the commissioning, on site corrective and preventative maintenance, remote system checks and remote support of intruder and hold-up alarm systems. They are intended to ensure that a common policy is used for all systems.

NOTE This is intended to encompass all systems under maintenance, including those installed in accordance with previous standards these being BS 4737, BS 6799 and BS 7042.

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.

BS 4737 (all parts), *Intruder alarm systems in buildings*

BS 7671, *Requirements for electrical installations – IEE Wiring Regulations*

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

DD CLC/TS 50131-7:2003, *Alarm systems – Intrusion systems – Part 7: Application guidelines*

3 Terms, definitions and abbreviations

3.1 Terms and definitions

For the purposes of this Draft for Development, the following terms and definitions apply.

3.1.1 alternative power source

power source (e.g. a battery) capable of powering the system for a predetermined period of time when the prime power source is unavailable

3.1.2 authentication

secure validation process where both the I&HAS, at the supervised premises, and the computer, at the remote location, exchange a code or codes to authenticate the identity of both the originator and respondent before proceeding with a remote support operation

3.1.3 authority

person giving the instruction to initiate a dialogue

NOTE This procedure may be automated.

3.1.4 client

individual or corporate body responsible for acquiring the I&HAS

3.1.5 data encryption

coding, translation or other modification of information whereby the manner in which it is modified varies with time in a pseudo-random manner

3.1.6 dialogue

electronic communication between the I&HAS and the authorized remote computer resulting in an exchange of data

3.1.7 event record

record of events arising from the operation of the I&HAS, e.g. for analysis

3.1.8 frequently used detector

detector that is expected to operate during the normal occupation of the supervised premises

3.1.9 on-line restore

restore of an I&HAS performed remotely, after confirming system integrity

3.1.10 parallel connected ATE

ATE using parallel communication from I&HAS CIE, i.e. an individual connection per output channel

3.1.11 prime power source

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

NOTE This term is progressively being replaced in European standards with the term "External power source (EPS)"

- 3.1.12 remote location**
secure premises of an alarm company, an ARC or its contracted agent, from where it is possible to initiate and/or process remote system checks
- 3.1.13 remote support**
ability to exchange data between an I&HAS at supervised premises and a secure computer
- 3.1.14 remote system check**
electronic check of the status of an I&HAS from a remote location
- 3.1.15 ringback**
additional security procedure where the remote location initiates a dialogue via a communications medium and the I&HAS acknowledges after authentication by clearing the initial connection and itself establishing dialogue before permitting data (other than authentication data) to be exchanged
- 3.1.16 secure computer**
computer which is not left unattended with at least one level of pass code protection, so that unauthorized persons cannot gain access to data by normal means
- 3.1.17 serial connected ATE**
ATE using serial communication from CIE, i.e. information for multiple signals conveyed by the same serial link
- 3.1.18 service technician**
personnel at remote location operating the computer controlling a dialogue
NOTE This operation may be automated.
- 3.1.19 site visit**
physical attendance at the supervised premises
- 3.1.20 soak test**
status of a part of an I&HAS from which an alarm condition is intentionally prevented from being notified, but such conditions are recorded in the event record
NOTE See also DD CLC/TS 50131-3.
- 3.1.21 system configuration**
site specific electronic data which is required for correct operation of the I&HAS
- 3.1.22 user**
person authorized to operate an I&HAS

3.2 Abbreviations

For the purposes of this Draft for Development, the following abbreviations apply.

ARC	Alarm Receiving Centre
ACE	Ancillary Control Equipment
APS	Alternative Power Source
ATE	Alarm Transmission Equipment
ATS	Alarm Transmission System
CIE	Control and Indicating Equipment
IAS	Intruder Alarm System
I&HAS	Intruder and Hold-Up Alarm System
PPS	Prime Power Source
SD	Storage Device
WD	Warning Device

4 Inspection, functional testing and commissioning

The inspection, functional testing and commissioning of any I&HAS should be carried out in accordance with DD CLC/TS 50131-7:2003, Clause 10.

The process of commissioning involves thorough testing of the installed system to ensure that it operates correctly in accordance with this Draft for Development and with the system design proposal (and the Installation Plan where applicable) including any agreed changes.

Commissioning of the I&HAS should be in accordance with Annex A.

5 Maintenance

5.1 Preventative maintenance

5.1.1 General

As a minimum, preventative maintenance should be in accordance with Annex B.

The system maintainer should make all reasonable effort to ensure that all parts of the I&HAS are fully tested. Those parts of the system which could not be fully tested should be recorded on the maintenance record, together with the reasons for their omission, and the signature of the client or his representative should be obtained.

There should be a written agreement with the client detailing that remote system checks are to be carried out if applicable.

A record of the checks and work carried out either remotely or on site, should either be left with the customer or dispatched to the customer within 10 days.

NOTE This record may be in electronic form if it is acceptable to the customer.