A user guide to intruder and hold-up alarm systems

incorporating sub–systems

bsia

british security industry association

Contents

Introduction

I&HAS which incorporate "sub-systems" are increasingly being installed. Such "sub-systems" are also known as "split" systems, "partitions," "areas," "wards," "groups" etc.

Their use can, however, create problems, which could lead to an increase in false activations and/or incorrect I&HAS programming. This document has been drawn up to recommend acceptable design parameters to minimise both of the above problems that are inherent with more complex systems.

1. Scope

These recommendations apply to sub-systems within I&HAS installed to PD 6662. They cover design and installation aspects not included within DD CLC/TS 50131-7.

Systems including multiple sub-systems that are installed on a large single site where initial reporting/notification is contained within the site (e.g. a local, manned control room) are not covered by these recommendations.

2. Normative references

The following references are essential for the application of this document. For dated references, only the edition cited applies. For undated references, the version of the publication (including any amendment(s) specified applies.

PD 6662 Scheme for the application of European Standards for intruder and hold-up alarm systems.
DD CLC/TS 50131-7 Alarm systems - Intrusion and hold-up systems - Part 7: Application guidelines
BS EN 50131-1 Alarm systems - Intrusion and hold-up systems. Part 1: System requirements
BS 8243 (DD 243) Installation and configuration of intruder and hold-up alarm systems designed to generate confirmed alarm conditions - Code of practice

3. Definitions and abbreviations

For the purposes of these guidelines, the following definitions apply:

3.1. Definitions

3.1.1. Sub-system
Part of an I&HAS located in a clearly defined area of the supervised premises capable of functioning independently of other parts of the I&HAS.

Note: This is as defined in BS EN 50131-1 which (in clause 6) permits different sub-systems to be installed to different security grades.

3.1.2. Single-occupancy systems
Where the entire I&HAS supervises premises under common occupancy.

Example: one company, with different departments using the various sub-systems.

3.1.3. Multi-occupancy systems
Where different sub-systems supervise different parts of the premises, which are under separate occupancy.

Example: separate companies using the various sub-systems.

3.1.4. System Core
Part of an I&HAS that includes components of the SPT and CIE with functionality, including tamper detection, that cannot be identified as being restricted to a single sub-system and processed as such.

> **Note:** CIE may include the ability to configure peripheral components so that their responses are associated with one or more sub-systems. In the absence of such configuration the CIE component should be considered part of the system core.

> **3.1.5. Key holder**
> Person or agency holding keys to the supervised premises and responsible for attending the premises in the event of an alarm condition.

3.2. Abbreviations

ACE Ancillary control equipment
ARC Alarm receiving centre
CIE Control and indicating equipment
HAS Hold-up alarm systems
IAS Intruder alarm system
I&HAS Intruder and hold-up alarm systems
SPT Supervised premises transceiver

4. Design and operation of I&HAS

4.1. General

The recommendations listed below have been drawn up to enable designers of I&HAS incorporating subsystems to minimise the problems and permit alarm companies to ensure that the sub-systems will provide an effective method of managing the I&HAS, whilst providing customers with the assurance that any additional risk of false alarms from the system has been minimised.

Sub-systems of IAS and sub-systems of HAS need not cover the same locations.

4.2. Overall responsibility for all sub-systems

I&HAS incorporating sub-systems should only be permitted when a clearly defined overall responsibility exists such that:

a. Single-occupancy systems: all sub-systems are under common management so that all key holders have access to all sub-systems.

b. Multi-occupancy systems: there is a clearly defined overall responsibility for the I&HAS, and arrangements made to ensure that a key holder with access to the entire system can be made available as necessary and that an alarm technician can access any part of the I&HAS at any appropriate time. This is essential in order to have effective fault-finding access for alarm technicians, to reduce the possibility of an alarm technician activating a set sub-system, and to provide rapid identification to the police of the area of activation.

4.3. Hold up alarms

Care should be taken when designing HAS where sub-systems are incorporated in the overall system design. The following should be considered:

a. The system design proposal should identify sub-systems where one or more HDs contribute to a confirmed alarm.

b. In a building with multi-occupancy, hold-up confirmation should be restricted to the sub-system level and the notification to the ARC should identify that sub-system.

*Note: Refer also to **4.1** Para 2*

c. In a building with single-occupancy the confirmation may work across all sub-systems.

4.4. Police response

If police response is required for sub-systems when the entire system is not set, the following should apply:

a. All signals to the ARC required by EN 50131 and DD 243/BS 8243 should be sent for each subsystem individually.

Note: This may require the use of extended format signalling. If so, care should be exercised in assessing the consequent risk of information being misinterpreted, especially in respect of hold-up signals.

b. Intruder/tamper and confirmed alarm signals received from set sub-systems may be forwarded to the police in the event that other sub-systems are known to be unset. Alarm signals should not be generated from sub-systems that are unset.

c. In a multi-occupancy system, an unconfirmed alarm from one sub-system should not be confirmed by an unconfirmed alarm from any other sub-system but may cause confirmation of, or be confirmed by, an alarm or tamper attributed to the system core.

The issue of URNs to subsystems in a multi-occupancy I&HAS may be dependent on the response authority. Liaison with that authority is needed to determine the most appropriate notification arrangements.

Note: The use of multiple URNs, where permitted, reduces the risk of information being misinterpreted.

See also clause 4.5.

4.5. Means of completion of unsetting for each sub-system

a. Where police response is required for an individual sub-system, the means of completion of unsetting for each sub-system should comply with the requirements of DD 243/BS 8243.

b. Where required, master keycodes (or equivalent means) may set/unset more than one sub-system from a single ACE.

4.6. Management of user access

a. Single-occupancy systems:
A user may silence an alarm in a sub-system that he does not normally have access to, but he should not be able to unset or reset an alarm in that sub-system.

b. Multi-occupancy systems:
A user is not permitted to silence an alarm in a sub-system under different occupancy. An individual responsible for the management of user codes within a sub-system should not be able to authorize access to a different sub-system.

4.7. Security of CIE & SPT
For all grades, setting any IAS sub-system should also set the sub-system supervising the area in which the system core is located. The system core should be located in the sub-system with the highest grade. If any IAS sub-system is set, events (i.e. alarms, faults, and tampers) attributed to the system core should be processed according to the requirements for a set IAS.

Note: DD CLC/ TS 50131-7 states that this is optional for systems installed to grade 1 or 2.

Where it is not possible for the I&HAS to determine which sub-system an event should be attributed to (e.g. fault or tamper detection of a system core component or interconnection) the I&HAS should process the event as if it had occurred in the system core.

4.8. Audible warning devices
a. The warning device requirements of EN 50131-1 Table 10 should apply to each sub-system of the multi-occupancy system.

b. For a single-occupancy system, the requirements of Table 10 apply overall.

For both (a) and (b), each audible warning device should be accompanied by the relevant delay/cut-off timers. No individual audible warning device should sound for longer than the maximum time permitted by EN 50131-1 or local regulations.

5. Engineering considerations

a. An alarm technician should place the I&HAS on test with the ARC before commencing work at site or remotely. Where this is not practicable, and certain sub-sections must remain live, this should be clarified with the ARC, and steps taken to minimise the risk of the alarm technician triggering the live sub-systems. If this restricts the client's security – e.g. by temporary removal of hold-up facility – the client should be advised in time for all system users to be made aware of the situation.

b. In the event of a material change being made to the system configuration, the new configuration should be thoroughly tested. If this is not practicable due to the nature of the site, it should be checked by someone other than the person who carried out the programming.

Note: *This may be carried out by simulation.*

c. If a change is made to one sub-system in a multi-occupancy site, the occupants of the other sub-systems should be made aware if that change could impact their system.

6. Selection of equipment

The CIE and ACE used to control the system must be designed for this purpose. In particular, the operation of any sub-system should not unintentionally affect or prevent operation of another sub-system.

Annex A

Additional considerations for an I&HAS incorporating sub-systems.

Consideration should be given to the following aspects of system design, installation, and operation to minimize the risk of false activations:
- Entry routes for individual sub-systems
- Correct system configuration
- Correct configuration at ARC
- Training of users

About the **BSIA**

The British Security Industry Association (BSIA) is the trade association for the professional security industry in the UK.

Our members are responsible for more than 70% of privately provided UK security products and services (by turnover) including the manufacture, distribution and installation of electronic and physical security equipment and the provision of security guarding and consultancy services.

Our members are industry professionals ranging in size from global companies to small and medium enterprises, offering quality products and services to a vast spectrum of end-users.

THE VOICE OF THE **PROFESSIONAL SECURITY INDUSTRY**

bsia
british security industry association