

Code of practice for

Design, installation and servicing of integrated systems incorporating fire detection and alarm systems and/or other security systems for buildings

UDC 699.8:654.924:614.842.4

NO COPYING WITHOUT BSI PERMISSION EXCEPT AS PERMITTED BY COPYRIGHT LAW



Document Sharing Hub

Committees responsible for this British Standard

The preparation of this British Standard was entrusted to Technical Committee FSM/12, Fire detection and alarm systems, upon which the following bodies were represented:

- AEA Technology
- British Cable Makers' Confederation
- British Fire Protection Systems Association Ltd.
- British Fire Services' Association
- British Telecommunications plc
- Chartered Institution of Building Services Engineers
- Chief and Assistant Chief Fire Officers' Association
- Department of Health
- Department of the Environment [Central (DCSS Fire Branch)]
- Department of the Environment (Building Research Establishment)
- Department of the Environment (Property and Buildings Directorate)
- Electrical Contractors' Association
- Home Office
- Institute of Fire Safety
- Institution of Electrical Engineers
- Institution of Fire Engineers
- London Fire and Civil Defence Authority
- Loss Prevention Council
- Marine Safety Agency
- Ministry of Defence
- National Association of Fire Officers
- National Caravan Council Limited
- National Inspection Council for Electrical Installation Contracting
- National Quality Assurance
- Trades Union Congress

The following bodies were also represented in the drafting of the standard, through subcommittees and panels:

- Engineering Industries Association
- Sound and Communications Industries Federation

This British Standard, having been prepared under the direction of the Consumer Products and Services Sector Board, was published under the authority of the Standards Board and comes into effect on 15 July 1995

© BSI 02-1999

The following BSI references relate to the work on this standard:
Committee reference FSM/12
Draft for comment 92/47057 DC

ISBN 0 580 24600 0

Amendments issued since publication

Amd. No.	Date	Comments

Contents

	Page
Committees responsible	Inside front cover
Foreword	ii
1 Scope	1
2 Normative references	1
3 Definitions	1
4 Quality	2
5 Design	2
6 Installation and wiring	8
7 Commissioning	9
8 Hand-over	9
9 User responsibilities	10
10 Maintenance and call-out service	10
Annex A (normative) Classification of integrated systems	12
Annex B (normative) Applicable standards	19
Figure A.1 — System type 1: independent function processors	14
Figure A.2 — System type 1: independent function processors connected to a central processor	15
Figure A.3 — System type 2: multi-function processor	16
Figure A.4 — System type 3: multi-function processor with intermixed I/O lines	18
Table B.1 — Applicable standards	19
List of references	20

Foreword

This British Standard has been prepared by Subcommittee FSM/12/1, Installation and servicing, under the direction of Technical Committee FSM/12, Fire detection and alarm systems. It should be read in conjunction, where appropriate, with the following British Standards:

BS 4737-4	<i>Intruder alarm systems. Codes of practice</i>
BS 5839-1	<i>Fire detection and alarm systems for buildings. Code of practice for system design, installation and servicing</i>
BS 7443	<i>Specification for sound systems for emergency purposes</i>
BS 8220-2	<i>Guide for security of buildings against crime. Offices and shops</i>
BS 8220-3	<i>Guide for security of buildings against crime. Warehouses and distribution units.</i>

In view of the increasing use of integrated systems, it is important that a code of practice be provided for designers, installers, service organizations and users. This code therefore is intended to assist interested parties in acquiring a better understanding of the complexity of such systems and to ensure that the overall integrity is at least as good as the integrity of the individual systems that are replaced.

The code aims to:

- provide a common basis of standards to recognize technical advances in the development of both integrated systems and sub-systems which may not yet be reflected in individual regulations, standards and codes of practice; and
- ensure that the highest standards of security, safety and reliability are achieved where systems have been integrated.

NOTE National, European and international standards, regulations and codes of practice may apply individually to each of the functions included within an integrated system. These standards may cite different requirements which may conflict. It is intended that, after consideration by interested parties, this code of practice may ultimately be used by standards-making bodies to assist in resolving any such conflicts.

As a code of practice, this British Standard 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.

A British Standard does not purport to include all the necessary provisions of a contract. Users of British Standards are responsible for their correct application.

Compliance with a British Standard does not of itself confer immunity from legal obligations. In particular, attention is drawn to BS 7671 *Requirements for electrical installations. IEE Wiring Regulations*.

Summary of pages

This document comprises a front cover, an inside front cover, pages i and ii, pages 1 to 20, an inside back cover and a back cover.

This standard has been updated (see copyright date) and may have had amendments incorporated. This will be indicated in the amendment table on the inside front cover.

1 Scope

This British Standard provides recommendations for the integration of a security system (see 3.1) with other security systems or with non-security systems (see 3.2) for use in and around buildings other than dwellings. The recommendations relate to the specification, design, installation, commissioning, hand-over and maintenance of such integrated systems, and to the user's responsibilities for operating and testing them.

NOTE Various configurations of integrated system are classified, with conceptual examples, in Annex A.

2 Normative references

This British Standard incorporates, by dated or undated reference, provisions from other publications. These normative references are made at the appropriate places in the text and the cited publications are listed on inside back cover. For dated references, only the edition cited applies; any subsequent amendments to or revisions of the cited publication apply to this British Standard only when incorporated in the reference by amendment or revision. For undated references, the latest edition of the cited publication applies, together with any amendments.

3 Definitions

3.1

security system

a fire alarm system, an intruder alarm system, a hazard warning system or any other system intended for the protection of life and/or property

3.2

non-security system

a system intended to provide environmental or management control and not intended primarily for the protection of life or property

NOTE Energy management is an example of a non-security system.

3.3

dwelling

a building or part of a building occupied or intended to be occupied as a separate unit of housing, usually by a single family, together with any garage, outhouse or other extension belonging to or usually enjoyed with that building or part

3.4

designer/specifying organization

the person or organization responsible for all aspects of system design and specification (see 5.3.3)

3.5

manufacturer

the person or organization responsible for the manufacture of all or some of the components of the integrated system

3.6

supplier/contractor

the person or organization with whom the contract is made and who is responsible for the quality of the system and its installation

3.7

installer

the person or organization carrying out the installation of the integrated system and its subsequent commissioning and hand-over

3.8

integrated system

a system comprising any combination of the following, which may share common facilities (such as hardware, software or transmission medium), but with at least one security system included:

- a) fire detection and alarm;
- b) personal attack alarm;
- c) intruder alarm;
- d) hazard warning;
- e) fixed fire extinguishing;
- f) public address;
- g) access control;
- h) closed circuit television;
- i) building management system (BMS);
- j) heating and ventilating;
- k) energy management.

NOTE This list of systems may not be comprehensive.

3.9

sub-system

that part of an integrated system which performs an individual function such as fire alarm, intruder alarm, building management

3.10

access level

the degree of access permitted to controls and indicators, subclassified as follows:

- a) access level 1: no restrictions;
- b) access level 2: restricted to authorized operators and service personnel;
- c) access level 3: restricted to authorized service personnel.

3.11 maintenance

the work of inspection, servicing and repair necessary for the continuing efficient operation of the installed system

3.12 expert system

a system of hardware and software using a database of human expertise for problem solving

3.13 user

a person authorized to operate the system

4 Quality

4.1 All phases of the establishment of the integrated system should be undertaken within a quality management system commensurate with the significance of the relevant sub-system. Particular attention should be paid to those elements of the integrated system which directly affect the functionality and reliability of security sub-systems.

4.2 The major phases for consideration are:

- a) system specification;
- b) system and product design;
- c) manufacturing;
- d) installation;
- e) commissioning;
- f) hand-over;
- g) maintenance.

4.3 Quality management systems should at least conform to relevant standards of the BS EN ISO 9000 series.

NOTE Individual sub-systems may have particular quality requirements specified within relevant standards for product and system approvals or certification.

4.4 In considering potential installers, consideration should be given to the status of the installing company, and in particular to whether its work is subject to technical inspections by a third party.

5 Design

5.1 General

A design controller should be appointed, having responsibility for the design of the complete system.

5.2 Design concepts

It is likely that a number of organizations will be involved in the design, installation and servicing of integrated systems. The organization responsible for the building may appoint persons with specific responsibilities for security systems and others with responsibilities, for example, for building management systems. The responsibilities, terms and requirements of each of the organizations should be clarified, documented and fully considered before system design and installation is undertaken.

All references in this standard to the requirements of the system refer to minimum requirements and the designers of such systems should take into account the nature of the premises, the value of its contents, the degree of risk and any other factors which may influence the choice and content of the system.

Consideration should be given to the means of communicating with people and organizations, both on and off site, who are involved in responding to emergencies. The security and integrity of the method of communication should be commensurate with the type of risk.

The alarm organization plan should be suitably detailed to cover all foreseeable eventualities.

Aspects to be considered should include:

- a) the level of risk and any risk classification (if appropriate);
- b) the number and location of in-house personnel to be summoned in the event of an alarm condition;
- c) the methods of communication employed: for example, pocket pagers and voice messages;
- d) the appropriate in-house response at various times of the day and night;
- e) who is responsible for ensuring that correct actions are taken at various times of the day and night;
- f) who is responsible for ensuring that faults or failures in any part of the system are rectified.

Any form of automatic transmission of signals should clearly discriminate as to the nature of the event being signalled (see 5.8).

Appropriate third parties should be consulted (for example, the insurer, police, fire service, local authorities, architects and suppliers of utilities to the building).

System design should take into account the requirements of all applicable standards (see Annex B).

5.3 Design considerations

5.3.1 Priorities

The design of the system, the method of information display and the extent of control facilities should be tailored both to the operational procedures that apply in the event of an alarm fault or status signal and the nature of the personnel who use the system.

Controls and indications forming part of the integrated system should meet the relevant requirements of applicable British Standards. For example, systems monitoring for fire should conform at least to BS 5839-4 and should be designed, installed and serviced in accordance with the recommendations of BS 5839-1.

The correct allocation of priorities of information presented by the integrated system in an alarm situation is crucial in ensuring that the most appropriate sequence of actions is taken at the earliest possible time. In view of this, it is important that early consultation be undertaken with all interested parties (see 5.2), in order to determine the most appropriate priority for each of the functions.

Similarly, it may be necessary to prioritize the fault indications or other warnings to ensure that their effects on the functionality of the system are minimized.

Information should be prioritized and displayed in a planned, clear and unambiguous manner, to minimize the possibility of information being misread or misinterpreted.

All possible scenarios, and their likely consequences, should be considered in determining the output priorities. Interactions between the functions may result in enhanced overall performance and thus should also be considered, together with additional factors such as those identified in 1) to 8) below.

In general, the following priorities should be used:

- a) priority 1: life safety (e.g. fire alarm for life safety, personal attack alarm);
- b) priority 2: property protection (e.g. fire alarm for property protection, intruder alarm);
- c) priority 3: non-security systems (e.g. environmental control alarm).

However, the objectives behind the setting of priorities should always be evaluated as, in some cases, the above order may be inappropriate. Factors to be considered should include the following.

- 1) Security systems with the function of protecting life should take priority over security systems that protect property.
- 2) In the event of a conflict of life protection systems, the system that protects against risks with the more immediate consequence should take priority.
- 3) Sub-priorities may be necessary within the priority system to enable the significance of particular events at any priority level to be recognized.
- 4) A compounding series of events could result in temporary loss of detailed indication of relevant and important information that may normally be regarded as being of lower priority.
- 5) Seemingly “non-security system” type of information may warrant a higher priority when its consequences are seen as part of the global protection plan.
- 6) The series of actions taken as a consequence of the order of priorities given, may not be the optimum sequence for the best method of loss and disaster reduction.
- 7) Fault warnings in some functions may be more critical and therefore should take precedence over alarms in other functions.
- 8) When expert systems are included to aid with complex scenarios, base information may need to be given, as well as decisions which are made by the system.

For example, in view of the above factors, a high-pressure alarm in a boiler system may be considered to require a more prompt response than some security-system alarms, and therefore may be given priority 1.

5.3.2 Integration

5.3.2.1 Advantages of integration

Regardless of the actual construction or physical arrangement, integrated systems have the following general advantages.

- a) Better coordination of monitoring and control. By incorporating all the monitoring and control into one single system, it may be more easily rationalized and coordinated. Effective prioritization of the alarms and controls, along with the adjustment of the system parameters, may also be more readily implemented.

- b) Centralized presentation of information. A rational and coherent format for the presentation of information may be adopted by using one central annunciator or group of annunciators.
- c) Improved administration. Having only one system for several functions provides the opportunity for more efficient administration by the user.
- d) Ease of installation, alteration and extension. Reduced cabling in the form of a common network bus enables the system configuration to be readily modified or expanded without additional wiring and may lead to significant cost reductions.

5.3.2.2 Limitations of integration

Regardless of the actual construction or physical arrangements, integrated systems have the following general limitations. It is the purpose of this code to give guidance to minimize the effect of these limitations.

- a) Site-dependent alarms coordination. Although priorities for the various alarms and other annunciations can be readily coordinated and allocated, each installation can have different requirements. This necessitates the careful preparation of the site-specific operational configuration. The specification and design of each sub-system therefore require great knowledge, skill and care.
- b) Alarm priorities. Unless the alarm annunciations are effectively prioritized, it is possible for critical alarms (e.g. fire) to be missed by an operator occupied by other alarm signals.
- c) Software complexity. Integrated systems are dependent on their software, which tends to be complex. A high degree of skill and care is therefore needed during the design and subsequent testing phases.
- d) Adverse interactions. The system response to a functional input may produce an undesired effect on one or more of the other functions. Any such interactions should be resolved during the design and commissioning of the system.
- e) System vulnerability. Integrated systems may be dependent on a single piece of equipment or wiring common to several functions, which could be vulnerable under certain conditions.
- f) Engineer skills. Some parts of the overall system may have an effect on more than one of its functions. Engineers involved in the installation, maintenance, expansion or modification of the system should have a high level of training and skill. An appreciation of the interactions between the system functions is also needed.

5.3.3 Expertise

To ensure that an integrated system functions correctly as a whole, persons involved with the system at all stages from specification through to the service stage should have a level of knowledge and experience commensurate with the requirements of their involvement. There may be more than one organization involved in work on the integrated system. In this case, one principal organization should be given overall responsibility and this should be documented.

The specifying organization should be conversant with the general requirements of the users and of standards relevant to the sub-systems. They should also be conversant with the qualities and features of the equipment that will be used in the construction of the integrated system. The specifying organization should possess the appropriate expertise to define adequately the interfaces between the individual sub-systems.

Design personnel should be fully aware of how the sub-system(s) with which they are involved interact with the other parts of the integrated system. Potential interactions between different parts of the integrated system should be recognized and accommodated within the system design.

5.3.4 System integrity

Each sub-system within an integrated system should have the integrity required by the standards relating to that sub-system (see Table B.1). Sub-systems may share facilities and components within the integrated system and these shared facilities and components should meet the most onerous integrity requirements of the relevant sub-systems.

The integrated system should be so designed and installed that a failure or fault in one sub-system does not adversely affect the performance of any other sub-system unless the failure is in a part of the system which is shared between the sub-systems. However, in order to minimize any adverse effects, careful consideration should be given to which parts of the integrated system may be common to several sub-systems and which parts of the sub-systems should be clearly segregated, for example using discrete wiring or processing.

All physical parts of an integrated system should be designed to perform correctly within the environment in which they are installed. In addition, those parts affecting the performance of a security system should meet the environmental requirements specified in the relevant standards listed in Annex B.