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

BSI STANDARDS

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

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	Text affected

Contents

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

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:

a) 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

b) 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.

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.*

Code of practice

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 page 18. 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 : Part 4 and should be designed, installed and serviced in accordance with the recommendations of BS 5839 : Part 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.

5.3.5 *Variations*

Any changes made to the system design during the negotiation, execution and commissioning stages of the contract should be agreed with interested parties to ensure that the original, or agreed modified, design parameters remain applicable. Any such changes should be documented in the manner agreed in the contract.

5.3.6 *Access to equipment*

The system should be so designed that in situations where the siting, access and vulnerability of the sub-systems are in conflict, this does not affect the operation, control, monitoring and maintenance of the individual sub-systems. To achieve this, it may ultimately be necessary to segregate elements of systems. Guidance on particular requirements is included in the relevant standards for individual sub-systems (see annex B).

For example, the requirements for the location of fire and intruder alarm panels may be different. Fire panels should be clearly visible so that the location of a fire can be quickly established, whereas intruder alarm indicators may need to be kept away from public view. In such cases, where both displays are to be given on the same panel, it is advisable to give fire indications on a separate display with appropriate controls, while the main panel is located in a secure area.

Where integrated systems include controls and indicators for a number of different sub-systems, it is important that the need to provide or prevent easy access to the various indicators and controls is recognized and that appropriate measures are taken at the design stage.

Critical parts of the system should be protected from unauthorized interference, by methods specified in the appropriate standards (see annex B).

5.4 Power supplies

Each sub-system within an integrated system can either be powered separately or from a common source. Sub-systems are likely to have different power supply requirements. Some sub-systems may operate acceptably with only one source of power (e.g. the mains electricity supply), while others may require a stand-by power supply to increase their resilience to failure of one of the power supplies. It is therefore important that the integrity of the different sub-systems is not jeopardized by the failure or degradation of the power supplies associated with other sub-systems.

In an integrated system, the power supply (or supplies) affecting the operation of the security sub-systems should at least conform to the relevant standards (see annex B). In particular, this power supply (supplies) should meet the following conditions.

a) There should be a normal and a stand-by power supply.

b) The security sub-system(s) should continue to operate on stand-by power for at least the minimum period(s) specified in the relevant standards (see annex B). Any additional power requirements from other functions of the integrated system should not reduce the stand-by period below the specified minimum.

c) Where common or interconnected power supplies are used, isolating devices should be included within the integrated system to prevent, as far as possible, short or open circuits, overloads or failure within any sub-system affecting the performance of a security sub-system.

d) Parts of the power supply affecting the operation of the security sub-system(s) should be continuously monitored.

e) Appropriate warning notices should be placed adjacent to fuses, batteries and other easily disconnectable elements of the power supply (supplies) to indicate which security functions are affected by their disconnection.

5.5 Information presentation

5.5.1 *General*

Both visual and audible indication of status and alarms are generated by an integrated system and communicated to system users. The type of information given in an integrated system, together with its formal presentation, is dependent upon the needs of the system's users (e.g. security guards, engineers or firefighters). Specific requirements for the various functions are given in the relevant standards (see **5.3.1** and annex B).

5.5.2 *Reliability*

Information display systems should have a reliability which is commensurate with their importance in terms of displaying safety-critical information in locations where actions will result from its display. Where the display of information is important in terms of the safety of the building or its occupants, display devices should be duplicated or a downgraded back-up display giving the essential information should be provided.

Display devices such as a visual display unit, which would normally be operated directly from the mains electricity supply of a building, and which display safety-critical information, should be provided with an appropriate back-up power supply system to permit their continued operation on failure of the mains electricity supply.

NOTE. A back-up power supply for this purpose may be unnecessary if a downgraded back-up display which is powered from a separate power supply is used.

5.5.3 *Information for users*

In many cases it is desirable that the date and time of all events be recorded.

The amount and type of information present should meet the requirements of the users. For example, a security guard would require the status and alarm information of the security systems, whereas an engineer may require the performance data of sensors.

External users of the system (e.g. police or fire-service personnel) are likely to be unfamiliar with the equipment, and a simple clear presentation of essential information will assist its rapid comprehension. The information should be clearly displayed to ensure that it is unambiguous and that any necessary actions are obvious. In some circumstances this can be achieved by the use of graphic displays.

5.5.4 *Priority of information*

If an integrated system can be operated in a mode where many actions and events occur at the same time (e.g. during a fire), the amount of information displayed should be restricted to prevent the users becoming confused by its volume. When such restrictions are implemented, the displayed information should at least include that of the highest priority (see **5.3.1**). Supplementary information should still be accessible on demand or should be displayed separately in a manner that avoids operator confusion, taking into account priority levels.

5.5.5 *Colour*

The colour of the information displays and their visibility should be such that the most critical information is visible under all anticipated levels of background illumination. Where relevant standards specify display colours for different types of information, these should be adhered to as far as possible, provided that there is no significant conflict and that the information is unambiguous.

5.6 System control

5.6.1 *General*

Suitable facilities should be provided to allow the functional requirements for control of each sub-system to be met. The nature of the controls and their ease of use are dependent upon the needs of the users (e.g. security guards, engineers, fire officers). Specific requirements for the various functions are given in the relevant standards. It should be possible to distinguish readily the controls which relate to each function, particularly where sub-systems have different priorities.

5.6.2 *Ease of use*

Careful consideration should be given to shared control facilities associated with common display systems. For example, for certain users the availability of non-emergency function controls, e.g. those associated with maintenance and fault diagnostics, could cause confusion. Thus, for some users, normal common control facilities such as QWERTY keyboards or other interactive devices (e.g. light pen, mouse and touch screen) should be supplemented by discrete manual controls for emergency functions. These manual controls should be robust and positive in action, e.g. push buttons or keyswitches.

5.6.3 *Reliability*

If discrete controls are not provided for each sub-system, the relevant controls within the integrated system should have at least the same level of reliability as that required by the most onerous specification. This can be achieved by duplication of controls.

5.7 Software and data storage, processing and transmission

NOTE. Attention is drawn to requirements in the standards for individual systems (see annex B) which relate to other aspects of software and data. The recommendations given in **5.7** apply in the absence of requirements in those standards.

5.7.1 *Identification and protection*

A processor-based integrated system may include fixed operating program(s) to which may be added modifiable site-specific data. The identification of any operating program(s), including version number and issue date, should be visibly marked on the hardware.

In addition, records comprising the following should be available on site:

a) site-specific configuration data;

b) the version numbers of the operating programs;

c) system changes; and

d) system manuals.

All records of this nature should be treated as confidential and held in a manner to prevent unauthorized access.

If the integrated system employs distributed processing, the identification of all of the operating programs that make up the system should be available on site.

Security sub-systems should be organized to ensure that data necessary to preserve their operational and functional integrity is protected so that it cannot be overwritten or otherwise masked or lost. No data relating to security sub-systems should be overwritten as a result of activity or faults within non-security sub-systems. Care is needed in the design of the integrated system to achieve this, as the complexity of design often precludes the ability to test under all circumstances.

5.7.2 *Program monitoring*

The correct execution of the security sub-system software by any microprocessor should be monitored by internal self-checking procedures and by an appropriate monitoring circuit, e.g. a watchdog circuit, which conforms to the most onerous integrity requirements of relevant equipment standards (see annex B), or in the absence of such standards, to the following recommendations.

a) The monitoring circuit and its associated indication and signalling circuits should not be prevented from determining and signalling a fault condition by the failure of any monitored microprocessor or associated clock circuits.

b) The monitoring circuit should monitor the operation of routines associated with the main functions of the program-controlled elements (i.e. it should not be solely associated with 'waiting' or other 'housekeeping' routines).

If a microprocessor fails to correctly execute its software, the monitoring circuit should (in addition to initiating an audible and visual fault warning) perform as follows:

1) reinitialize the microprocessor, verifying that the contents of memory, both program and data, are not corrupted;

2) attempt to restart the program at a suitable point within 10 s of the occurrence of the failure;

3) either:

i) record that a failure has occurred, using a system capable of recording a minimum of 99 failures and resettable only by an operation restricted to authorized service personnel; or

ii) automatically reset the equipment and give both a visual and audible warning that an automatic reset has occurred.

5.7.3 ***Storage of software***

5.7.3.1 *General*

All software necessary for the functions required by priority 1 and priority 2 security systems (see **5.3.1**) should be held in solid-state memories. Software should not be held on storage media requiring mechanical moving parts, such as magnetic tape or disks.

Except as stated in **5.7.3.2** and **5.7.3.3**, all the software used by the control and indicating equipment should be held in non-volatile read-only memories.

Each non-volatile read-only memory device should be marked with a designation that can be uniquely cross-referenced with documentation indicating the precise contents of the memory (e.g. program version, data details).

Provision should be made for the regular checking of memory contents (other than configuration data stored in alterable memory (see **5.7.3.2**a) and running data (see **5.7.3.3**)). The checks should be made at intervals not exceeding 7 days.

5.7.3.2 *Configuration data*

The following recommendations apply to configuration data held in memory other than non-volatile read-only memory.

a) The contents of the memory should be automatically monitored (e.g. by a check-sum procedure) at regular intervals not exceeding 24 h.

b) It should be possible to make a clear and unambiguous check of the data held in memory against the documentation to reveal any unauthorized or undocumented changes.

c) Configuration data stored in alterable memory should be modified only by authorized service personnel.

d) Alterable memory should normally be held in the write-disabled state so that no action elsewhere in the processor can cause corruption of the memory. A manual operation should be required before the memory contents can be changed.

e) Volatile memory should be provided with a back-up energy source permanently attached to the same circuit assembly as the memory so that they cannot be easily disassociated. The energy source should have an expected life of at least 10 years and should be capable of retaining the contents of the memory for at least 6 months.

f) A fault indication should be given in the event of a loss of the memory contents, and the equipment should still be capable of signalling a security alarm.

5.7.3.3 *Running data*

If data generated internally by the system during its operation, or data entered from manual controls to initiate test or disablement functions, is stored in alterable memory (which may be volatile memory without a back-up energy source), the equipment should restart in a safe condition (i.e. without any test mode selected or any parts of the system disabled) after a failure of the power supply to the memory.

Any memory contents associated with the selection of test modes or the disablement of parts of the system should be monitored to ensure that the correct indications are given by the control and indicating equipment.

5.7.4 ***Software design and documentation***

5.7.4.1 The software used in the control equipment should be designed in a modular structure appropriate to its function. Adequate documentation of the software should be available to allow conformity with **5.7.2** and **5.7.3** to be properly assessed.

5.7.4.2 To improve reliability, a methodical and formal approach to software design should be followed, based on the following:

a) stated objectives and a formal specification;

b) structured and well documented programs;

c) use of a computer language suited both to the processor and to the application;

d) definition of test procedures to enable the correct operation of the software to be verified, from individual modules and sub-systems to complete system integration.

5.7.5 ***Transmission within the integrated system***

5.7.5.1 *Controlled transmission of data on common channels*

To ensure that there is no unacceptable delay or loss in the transmission of essential data over common channels, transmission buffers should be scanned or controlled in such a way that the highest-priority data is placed at the head of the queue. Protocols that detect and correct transmission errors may be used. No process should be able to permanently hold a channel and hence block transmission of data.

5.7.5.2 *Uncontrolled transmission of data on common lines*

On lines where a number of devices could attempt to communicate simultaneously (e.g. sensor lines), contention detection or avoidance protocols should be used to ensure that essential data cannot be masked or lost.

5.8 Communication with emergency services

5.8.1 Alarms and other messages should be conveyed to emergency services and other parties in the appropriate sequence (see **5.3.1**), i.e. priority 1 alarms signalled first.

5.8.2 The communication system should be appropriate for the degree of criticality of monitored alarms and typically may be one of the following:

a) direct line transmission link;

b) BT red care systems;

c) packet switching radio transmission systems;

d) digital communicator via the public switched telephone network (PSTN);

e) dialling to an ex-directory number;

f) dialling via the '999' network.

5.8.3 If communications are not sent directly to emergency services, they should be sent via central stations conforming to the recommendations of BS 5979.

5.8.4 Where intruder alarm signals are included with, or run along, the same communication cables as other signals, then all communication channels should be afforded at least the degree of protection recommended in BS 4737 : Part 4. This may mean physically protecting communication cables and using tamper monitoring devices both within the building and externally.

5.8.5 Where communications require the interaction of persons, it should be ensured that the sequence of actions will minimize the possibility of mistakes.

6 Installation and wiring

6.1 The installation of the system should be supervised by a person who is (or a team which is) fully conversant with:

a) this British Standard, i.e. BS 7807;

b) electrical installation to BS 7671;

c) data transmission cable installation;

d) project management of multi-discipline ventures;

e) installation practice for each sub-system utilized in the integrated system, and the relevant standards;

f) the Directives 89/336/EEC [1] and 92/31/EEC [2] relating to electromagnetic compatibility (see BS EN 50081-1 and BS EN 50082-1).

6.2 Installation should be by persons who have been adequately trained in the requirements of BS 7671 and the appropriate installation standard for the system.

6.3 The cables used for interconnecting equipment should meet the appropriate specification for such characteristics as current, voltage, data transmission capability and physical and thermal protection.

6.4 The siting, installation and wiring of each part of an integrated system should conform to the standards that apply to that part.

6.5 Where an integrated system uses common wiring, this wiring should be as specified in the standard applicable to the sub-system with the highest integrity requirements.

6.6 All cables to emergency facilities should be wired directly to actuators or to motor control panels and not via an intermediate system such as a BMS computer, unless the intermediate system has been designed with the integrity of the relevant security system.

7 Commissioning

7.1 The commissioning procedure for each part of an integrated system should conform to the relevant standard(s) that apply to that part.

7.2 In addition to **7.1**, the following procedures should be undertaken.

a) The integrated system should be tested to ensure that it operates in accordance with an agreed cause-and-effect schedule.

b) Tests should be undertaken within each sub-system as follows:

1) in its normal operational mode; and

2) with predictable fault conditions such as power-supply failure imposed on the individual sub-system, to establish the effect on other sub-systems.

c) Power-up and power-down procedures should be verified for system integrity and personnel safety. For example, doors or windows held closed may open by accident and cause injury.

d) The procedures used and the results of each test should be recorded, to ensure that all interactions between sub-systems are satisfactory. The record should identify the actual interaction of the various elements of the system during their normal operation.

e) Any tests required by appropriate third parties should be undertaken.

7.3 Certification

The installer should certify that the installation conforms to the recommendations of this British Standard and all other relevant codes of practice, and that components conform to relevant product standards. Alternatively, if deviations have been agreed with the relevant parties, the installer should give a statement of these deviations.

8 Hand-over

8.1 General

The relevant parties (e.g. insurers, local authority officers, fire brigade, police) should be made aware of the state of the installation at the time of hand-over, by the accepted representative of the owner or occupier of the building.

A strict test schedule should be provided by the supplier of the system(s) to enable the user to confirm at regular intervals the correct action and interaction of the installed components and the link between components and sub-systems.

8.2 Total hand-over

When commissioning and certification are complete, the total integrated system should be formally handed over to a person appointed by the owner or occupier of the building to be responsible for the integrated system. The responsible person should ensure that all the necessary documentation has been completed and received before accepting the hand-over.

8.3 Partial hand-over without beneficial use

In some cases a sub-system may be handed over before the remainder of the integrated system is complete. If the sub-system is not to be used immediately, provision should be made for regular stand-by maintenance to minimize damage arising from the activities of other trades.

8.4 Early hand-over with beneficial use

If an integrated system is handed over, in whole or in part, to be used before the building is finished, the agreed maintenance programme should be instituted from the date of hand-over. If the work of other trades is likely to produce environmental conditions more severe than those expected in normal usage, consideration should be given to an increased frequency and extent of maintenance.

If any part of an integrated system is to perform in a life-safety role prior to completion of the building, provision should be made for regular testing.

The system log (see **9.4**) should be kept from the date on which any part of an integrated system is put into operation.

9 User responsibilities

9.1 General

The user should have a high level of training to operate and respond to a multi-functional system.

Fire officers should be invited to inspect and familiarize themselves with the integrated system.

9.2 System supervision

Where the level of integration exceeds that of type 1 systems as classified in annex A, the whole system should be considered as requiring the attention and management necessary for the security sub-system deemed to be the most important.

In cases where the different functions of an integrated system are segregated and a number of people may each be responsible for a particular function, the person responsible for each sub-system should have the level of authority to implement the procedures laid down in the relevant standards for that sub-system.

It is important that all persons responsible for the management, operation and maintenance of the integrated system and/or sub-systems receive formal structured training on the system, from either the manufacturer, the supplier, the contractor or an independent training organization.

The user should take the responsibility for informing the appropriate parties (see **5.2**) of faults likely to leave any part of a security sub-system out of action for long periods.

NOTE. Alternative monitoring arrangements may be needed in these instances.

9.3 System tests

In accordance with the test schedule provided by the supplier (see **8.1**), regular tests should be undertaken and results recorded for later reference by those responsible for maintaining the system. The results should also be available to the regulatory authorities, including the fire brigade and police, during routine visits to the protected premises.

9.4 System log

An operational log should be kept for each sub-system. Performance measurements relating to more than one sub-system, and faults occurring on the integrated system that affect more than one sub-system, should be logged in the integrated system log, and those responsible for dealing with each of the sub-systems should be advised.

NOTE. Details of the operational log which should be kept for some sub-systems are specified in the relevant British Standards (see annex B).

9.5 System maintenance

The owner or occupier of the building should ensure that adequate maintenance of the integrated system is carried out by qualified persons. Where sub-systems interact, the user should ensure that a coordinated approach is taken to the maintenance of these sub-systems.

9.6 System upgrade and modification

Integrated systems are likely to be subject to changes during their operational life. These changes may be more frequent than with non-integrated systems. It is important that the implications of the changes are fully understood and, in particular, that the potential interaction between the various functions of the integrated system is properly tested during recommissioning of any part. The changes should be incorporated into the existing system records.

Before undertaking changes or extensions, consideration should be given to their effect on the performance of the existing system and agreement should be obtained from interested parties.

Suppliers and/or maintenance companies should not make changes to the system without prior instruction from the user.

Where changes to components or sub-systems are made within an integrated system after it has been commissioned, the user should ensure that acceptance tests are undertaken to verify that the changes function in the manner specified.

Where changes affect the performance of more than the sub-system to which they are made, a representative of the person responsible for each affected sub-system should be involved in the acceptance test programme.

10 Maintenance and call-out service

10.1 All persons undertaking maintenance work on the system should be fully conversant with the function and operation of the system on which they are working and its effects upon the other sub-systems. The temptation to carry out maintenance work on an unfamiliar part of the system should be guarded against by training and the administrative control of the work.

10.2 All maintenance carried out on the various component parts of the sub-systems should be in accordance with the recommendations given in the relevant standards for these sub-systems.

10.3 The installer should indicate if any special maintenance procedures are necessary to ensure continued satisfactory operation of the system and sub-systems.

10.4 Records of all preventive and corrective maintenance carried out should be recorded in the system log (see **9.4**).

10.5 Any defects should be reported to the responsible person (see **8.2**) and recorded in the system log. Action taken to correct the defect should also be recorded.

10.6 During maintenance, any changes to the use, layout or partitioning of the premises which affect any part of the integrated system should be noted and the responsible person notified. Examples of such changes include alterations which may affect the fire detection or intruder detection system or the visual coverage of a closed-circuit television (CCTV) system.

Annexes

Annex A (normative)
Classification of integrated systems

A.1 Introduction

Integrated systems can be classified into the following three types, according to their method of incorporation:

a) type 1: integrated systems with segregated function processors;

b) type 2: integrated systems with dedicated line functions;

c) type 3: integrated systems with intermixed line functions.

These types of system are discussed in **A.2, A.3** and **A.4**. The descriptions and drawings are of typical arrangements, but other configurations are possible (for example, the combination of input and output devices on one circuit).

A.2 Type 1: integrated system with segregated function processors

A.2.1 *General*

In this type of integrated system, each function has its own dedicated processing element. These stand-alone systems may be interlinked directly, in order to execute control actions, or via a central processor for display and limited control purposes.

Systems of this type represent the simplest form of integrated system and have been available for a number of years. Figures A.1 and A.2 illustrate the basic system architecture.

The system illustrated in figure A.1 consists of three separate independent processors, each connected to its own input and output devices. Each processor will perform a unique function such as fire alarm, intruder alarm or energy management and should be capable of operating in a stand-alone mode to perform its predetermined role.

Integration of the 'stand-alone' system is achieved by the interconnection of the function processors and is likely to be configured to suit individual sites. An example is the shutting down of a heating, ventilating and air-conditioning system during a fire alarm condition. Interconnection will require very close liaison between those responsible for the specification of each of the functions and those responsible for using the system once it is installed.

In principle, any number of processors may be employed in a system and there is no fundamental constraint upon the number of processors performing a particular function. It may, for example, be appropriate to arrange for separate processors to handle each of the functions in each wing of a large building or in separate buildings of a large site. Such decisions usually relate to the cost-effectiveness of the preferred configuration and also to the overall system reliability that is required.

Figure A.2 illustrates a system similar to that of figure A.1 but with a central processor connected to the individual function processors. This may include facilities such as centralized annunciation and control and monitoring to supplement the stand-alone systems.

In the simplest form of a system incorporating a central processor, data will be transmitted from the function processors to the central processor for the purpose of annunciation. Failure of the central processor should not prevent the function processors from continuing to perform their primary tasks.

When the central processor is capable of providing control signals, it is necessary for data to be transmitted to and from the function processors. A simple example of such control is the initiation of an evacuate alarm signal at the central processor.

With this type of central processor, it may no longer be necessary to directly interconnect each function processor in the manner illustrated in figure A.1. All data may be channelled through the central processor, but this has the disadvantage that a central processor failure may prevent integrated system tasks from being performed.

The illustration in figure A.2 shows one central processor, but more than one can be used. Such arrangements are likely to be advantageous in large installations where much data and many control functions are available at the central processor. For example, engineers may require data on the system service status, whereas the security guards require indications of the fire alarm and intruder alarm systems.

A.2.2 *Advantages*

In addition to the general advantages identified in **5.3.2.1**, the following advantages are provided by systems of this type.

a) With or without a central processor:

1) the individual function processors may operate as 'stand-alone' systems;

2) the individual sub-systems can be managed, operated and maintained by personnel with specific skills in that function.

b) With a central processor:

1) the centralized display of data can be accomplished in a more coordinated manner than in non-integrated systems;

2) the number of personnel necessary to oversee the systems can be reduced by centralized annunciation.

c) With a central processor including control facilities:

1) centralized control may improve the event response;

2) the potential for centralizing the engineering information of larger systems may improve operational efficiency.

A.2.3 ***Limitations***

In addition to the general limitations identified in **5.3.2.2**, the following limitations may be encountered with systems of this type.

a) With or without the central processor:

systems with individual processors for each function are likely to be the most costly configuration of integrated system, although potentially offering the highest reliability.

b) With a central processor:

1) loss of the central processor and the associated annunciation is likely to jeopardize the effective management of events, particularly on large or complex sites;

2) where integrated system-control data to and from individual systems is channelled through the central processor, failure of the central processor is likely to degrade the effectiveness of individual function processors.

c) With a central processor including control facilities:

1) failure of a central processor which includes manual control facilities will result in a lower level of overall system control and is likely to downgrade the potential effectiveness of individual sub-systems;

2) the standard of fault tolerance and protection against deliberate interference, fire or mechanical damage required on communications links to central processors is high. This may necessitate loop wiring, tolerance to a single open or short circuit without loss of communications, tamper protection and physical protection of cables. It may also necessitate duplication of some essential functions by direct hard-wired interlinking. This is likely to increase the cost of the overall installed system.

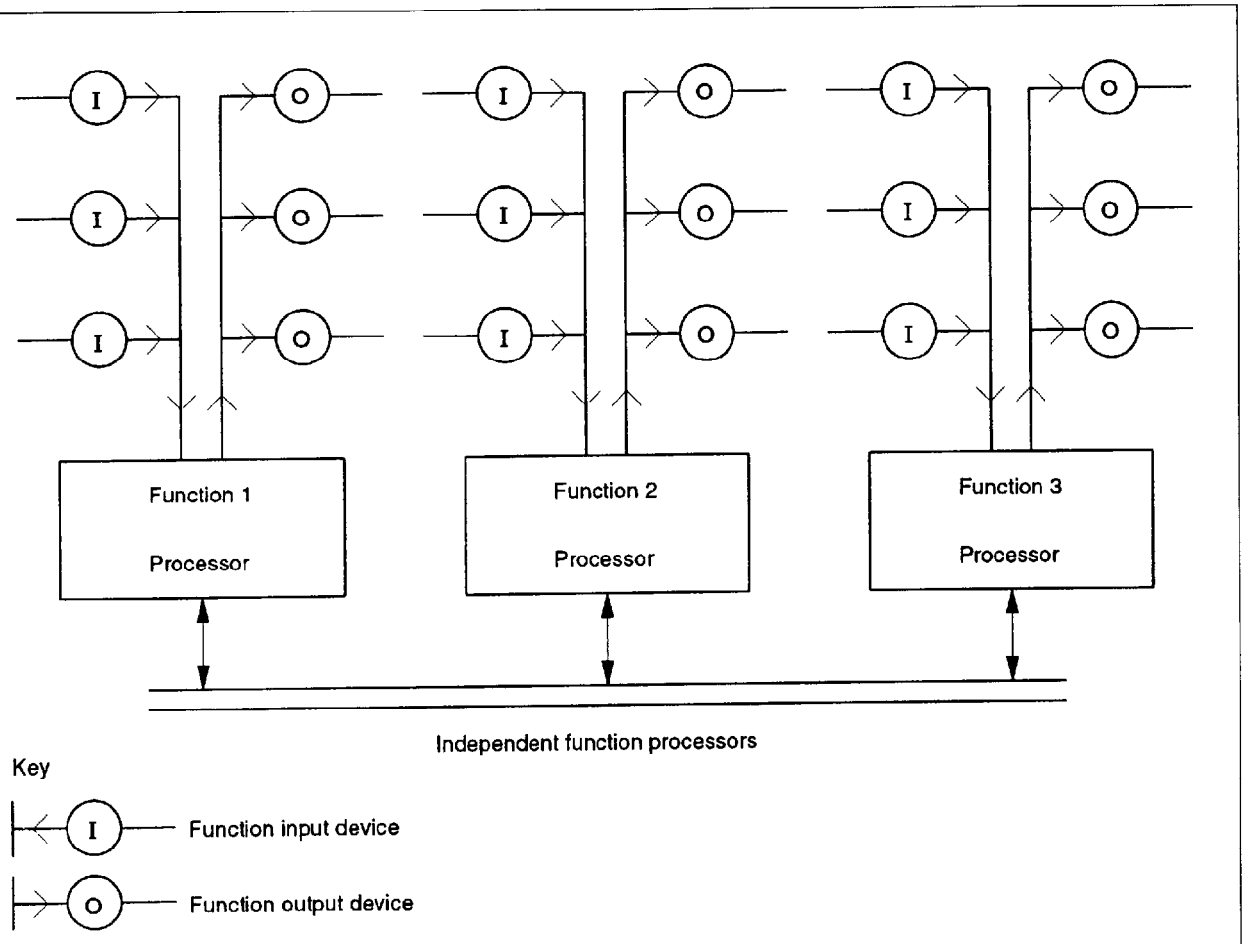


Figure A.1 System type 1: independent function processors

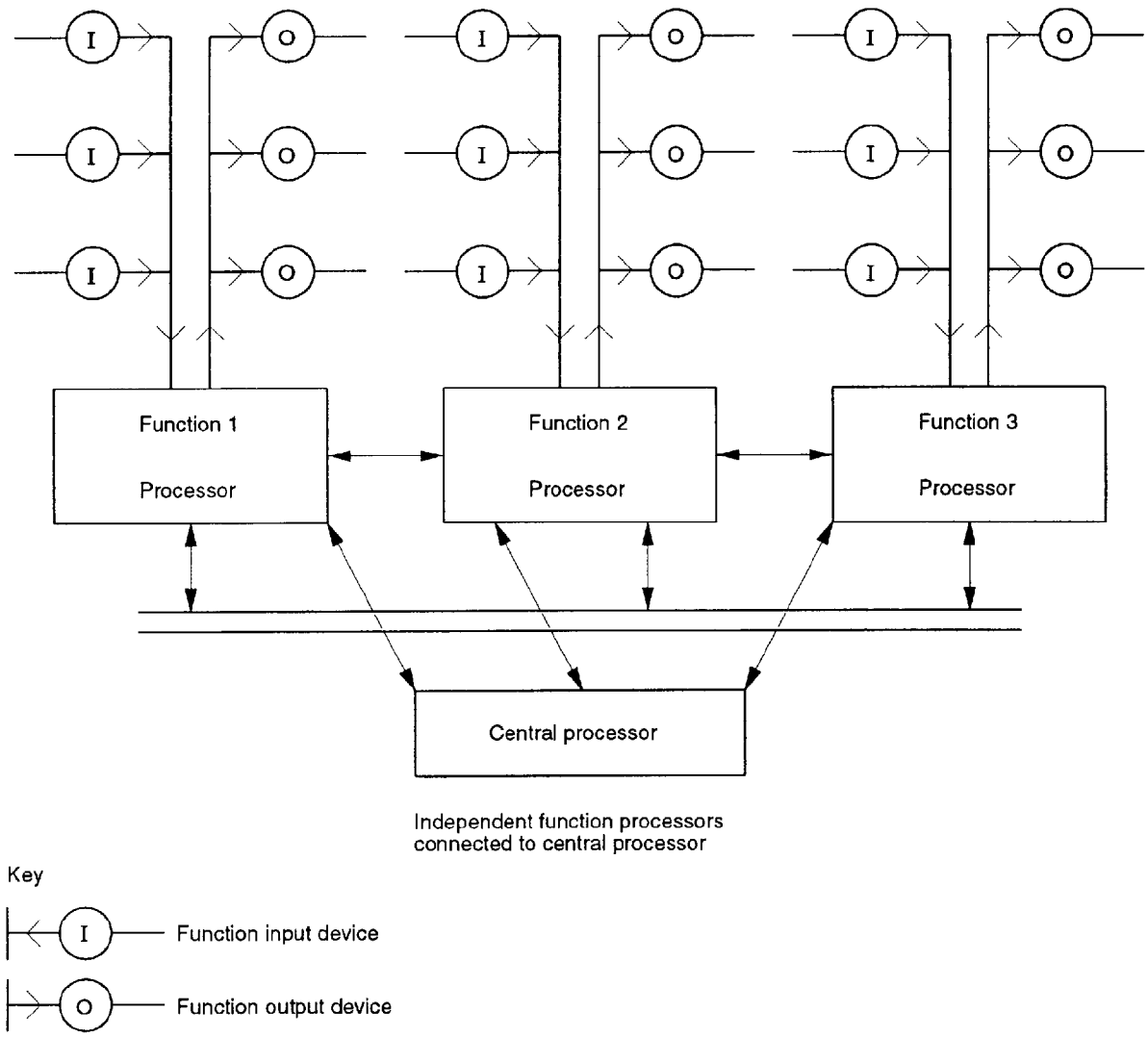


Figure A.2 System type 1: independent function processors connected to a central processor

A.3 Type 2: integrated systems with dedicated line function

A.3.1 *General*

Systems of this type have one common processing element, or group of processing elements, which carry out the processing for some or all of the system functions. Each input/output line circuit of the processing element is dedicated to only one of the functions.

Figure A.3 illustrates a system of this type where, for example, function 1 could be fire alarm, whilst functions 2 and 3 could be intruder alarm and access control. Signals from these functions are input to, and analysed by, the common processor, and generate function-specific outputs. The system may have a common display of data.

It is conceivable that several such integrated functions could be linked into a larger integrated system where site size and geography require distributed local control.

A.3.2 *Advantages*

In addition to the general advantages identified in **5.3.2.1**, the following advantages are provided by systems of this type.

a) As inputs from different functions are received and analysed by the common processor, a more accurate picture of the monitored environment can be derived, allowing better alarm response and coordination of control actions.

b) A reduction in processing and display hardware may increase the mean time between failures of the total system.

c) The combining of the functions into one processor may reduce the interconnections between sub-systems.

d) As each function uses separate and dedicated input/output circuits, the system can be installed without compromising the installation standards required for each specific function, e.g. physical protection of fire-system cables and anti-tamper detection on intruder systems.

e) Because of the separation of line functions, some aspects of system design, installation and commissioning, such as the siting of detectors, can be completed independently of other functions, using personnel with function-specific skills.

A.3.3 ***Limitations***

In addition to the general limitations identified in **5.3.2.2**, the following limitations may be encountered with systems of this type.

a) The implementation of correct interaction between functions, to achieve desired priorities of response and coordination of control actions, requires detailed knowledge of site-dependent parameters. This increases the complexity of the task for both the system designer and the commissioning engineer.

b) As the system monitors several functions, a large number of events can be received at one time. Unless the display information is carefully organized, this may distract from the significance of alarms from security sub-systems.

c) Integration of several functions within one processor may reduce the speed of response to an event on an individual sub-system.

d) Failure of hardware within the common control and display processor can result in the loss of more than one function at a time.

e) A high level of skill and system knowledge is required from an operator who is expected to deal with all the different disciplines in the system. This increases training requirements.

f) Standards previously applied to each individual function may need to be harmonized to cover the interactions between the functions now integrated.

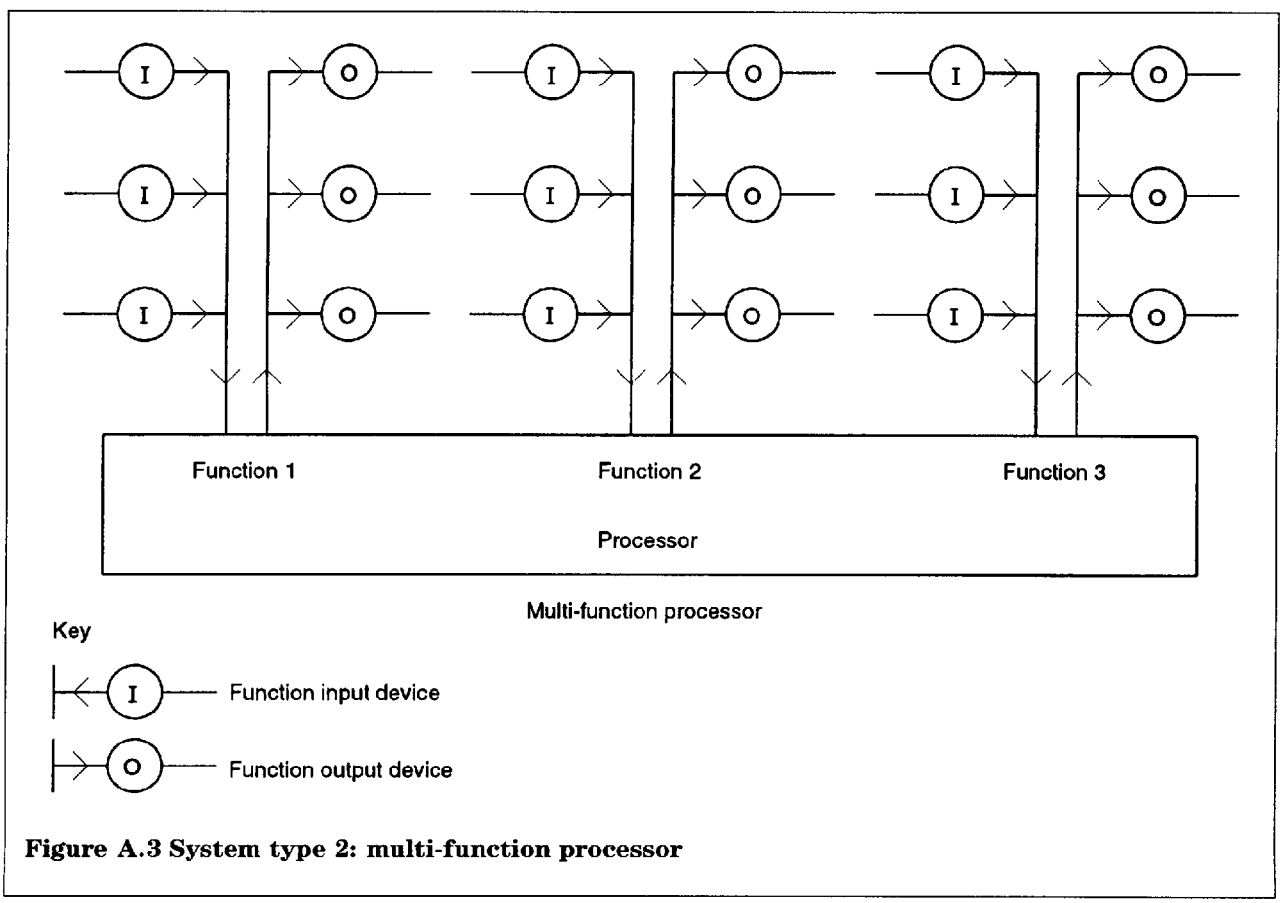


Figure A.3 System type 2: multi-function processor

A.4 Type 3: integrated systems with intermixed line functions

A.4.1 *General*

Systems of this type have one common processing element, or group of processing elements, which carry out the processing for some or all of the system functions. Each input/output line circuit of the processing element is able to handle devices relating to more than one of the system's functions.

This type of system is similar to that described in **A.3.1**, but the function input and output devices share common line circuits. Figure A.4 illustrates this type of system.

A.4.2 *Advantages*

In addition to the general advantages identified in **5.3.2.1**, the following advantages are provided by systems of this type.

a) The wiring of different function devices on the same circuit may reduce system cabling costs.

b) By using input/output devices common to more than one function the system device count is reduced.

c) As inputs from different functions are received and analysed by the common processor, a more accurate picture of the monitored environment can be derived, enabling better alarm response and coordination of control actions.

d) A reduction in processing and display hardware may increase the mean time between failures of the total system.

e) The combining of the functions into one processor removes the interconnections between systems and may increase reliability.

A.4.3 *Limitations*

In addition to the general limitations identified in **5.3.2.2**, the following limitations may be encountered with systems of this type.

a) As the wiring of input and output devices is not limited to one function, it is necessary for installers to possess the appropriate skills to handle the various sub-systems.

b) Failure of any of the input and output line circuits from the processor may cause a failure on some or all of the sub-systems managed by the processor.

c) It may be difficult to meet the requirements of the various individual system standards, e.g. physical protection of the line system cables, differing terminations and junction box requirements, and/or the anti-tamper detection requirements for intruder systems.

d) The implementation of correct interaction between functions, to achieve desired priorities of response and coordination of control actions, requires detailed knowledge of site-dependent parameters. This increases the complexity of the task for both the system designer and the commissioning engineer.

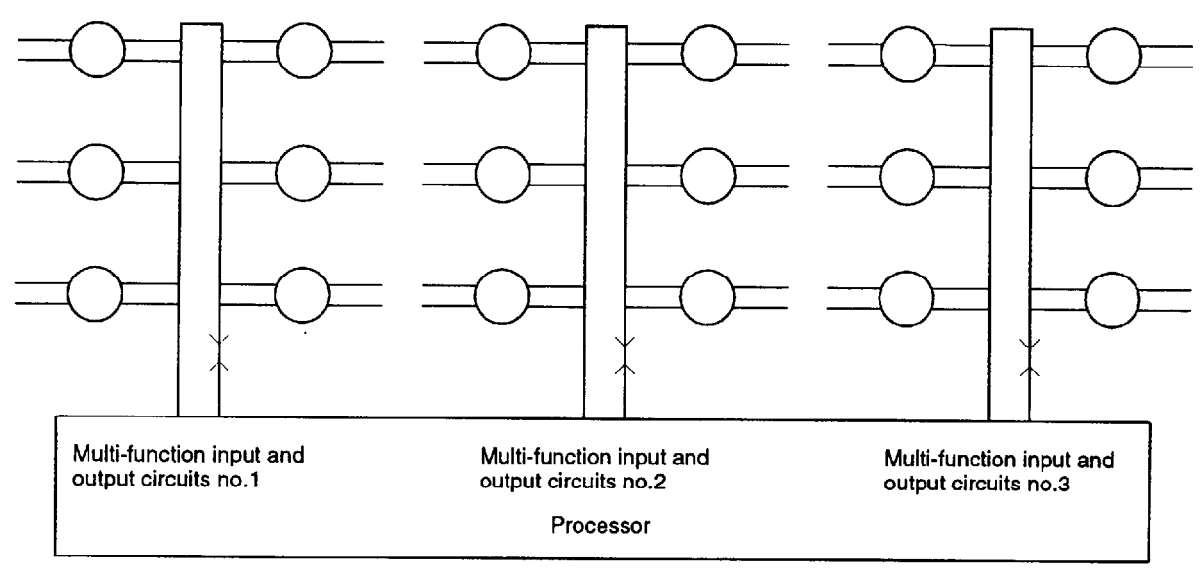
e) As the system monitors several functions, a large number of events can be received at one time. Unless the display information is carefully organized, this may distract from the significance of alarms from security sub-systems.

f) Integration of several functions within one processor may reduce the speed of response to an event on an individual sub-system.

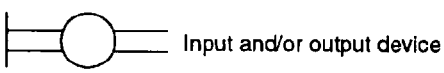
g) Failure of hardware within the common control and display processor can result in the loss of more than one function at a time.

h) A high level of skill and system knowledge is required from an operator who is expected to deal with all the different disciplines in the system. This increases training requirements.

i) Standards previously applied to each individual function may need to be harmonized to cover the interactions between the functions now integrated.



Key



NOTE. These devices may provide input and/or output facilities for more than one function.

Figure A.4 System type 3: multi-function processor with intermixed I/O lines

Annex B (normative)

Applicable standards

This standard should be read in conjunction with the latest editions of the standards relating to each sub-system and with other relevant standards and directives. These include, but are not limited to, those given in table B.1.

Table B.1 Applicable standards

Function	Standard/directive
General	BS 7671 BS 8220 : Parts 2 and 3 BS EN 50081-1 BS EN 50082-1 NACP 11 [3], NACP 20 [4], NACP 30 [5] EEC Directives: 89/336/EEC [1] 92/31/EEC [2]
Fire detection and alarm	BS 5839 : Parts 1 and 4 BS 6266 BS 7273 : Part 1
Emergency lighting	BS 5266 : Part 1
Personal attack	BS 4737 : Part 2
Intruder alarm	BS 4737 : Parts 1 and 4 BS 6799 BS 7042
Fixed fire extinguishing	BS 5306
Central stations	BS 5979
Public address	BS 6259 BS 7443

List of references (see clause 2)

Normative references

BSI publications

BRITISH STANDARDS INSTITUTION, London

BS 4737 :	*Intruder alarm systems*
BS 4737 : Part 1 : 1986	*Specification for installed systems with local audible and/or remote signalling*
BS 4737 : Part 2 : 1986	*Specification for installed systems for deliberate operation*
BS 4737 : Part 4 :	*Codes of practice*
BS 4737 : Section 4.1 : 1987	*Code of practice for planning and installation*
BS 4737 : Section 4.2 : 1986	*Code of practice for maintenance and records*
BS 4737 : Section 4.3 : 1988	*Code of practice for exterior alarm systems*
BS 5266 :	*Emergency lighting*
BS 5266 : Part 1 : 1988	*Code of practice for the emergency lighting of premises other than cinemas and certain other specified premises used for entertainment*
BS 5306	*Fire extinguishing installations and equipment on premises*
BS 5839 :	*Fire detection and alarm systems for buildings*
BS 5839 : Part 1 : 1988	*Code of practice for system design, installation and servicing*
BS 5839 : Part 4 : 1988	*Specification for control and indicating equipment*
BS 5979 : 1993	*Code of practice for remote centres for alarm systems*
BS 6259 : 1982	*Code of practice for planning and installation of sound systems*
BS 6266 : 1992	*Code of practice for fire protection for electronic data processing installations*
BS 6799 : 1986	*Code of practice for wire-free intruder alarm systems*
BS 7042 : 1988	*Specification for high security intruder alarm systems in buildings*
BS 7273 :	*Code of practice for the operation of fire protection measures*
BS 7273 : Part 1 : 1990	*Electrical actuation of gaseous total flooding extinguishing systems*
BS 7443 : 1991	*Specification for sound systems for emergency purposes*
BS 7671 : 1992	*Requirements for electrical installations. IEE Wiring Regulations. Sixteenth edition.*
BS 8220 :	*Guide for security of buildings against crime*
BS 8220 : Part 2 : 1987	*Offices and shops*
BS 8220 : Part 3 : 1990	*Warehouses and distribution units*
BS EN 50081 :	*Electromagnetic compatibility. Generic emission standard*
BS EN 50081-1 : 1992	*Residential, commerical and light industry*
BS EN 50082 :	*Electromagnetic compatibility. Generic immunity standard*
BS EN 50082-1 : 1992	*Residential, commercial and light industry*
BS EN ISO 9000	*Quality systems*

Other references

[1] THE COUNCIL OF THE EUROPEAN COMMUNITIES. Council Directive 89/336/EEC of 3 May 1989 on the approximation of the laws of the Member States relating to electromagnetic compatibility. *Official Journal of the European Communities*, No. L 139, 23.5.89.

[2] THE COUNCIL OF THE EUROPEAN COMMUNITIES. Council Directive 92/31/EEC of 28 April 1992 amending Directive 89/336/EEC on the approximation of the laws of the Member States relating to electromagnetic compatibility. *Official Journal of the European Communities*, No. L 126, 12.5.92.

[3] NATIONAL APPROVAL COUNCIL FOR SECURITY SYSTEMS. NACP 11 *Supplementary code of practice for the planning, installation and maintenance of intruder alarms*, Issue 1, December 1990.[1)]

[4] NATIONAL APPROVAL COUNCIL FOR SECURITY SYSTEMS. NACP 20 *Code of practice for the planning, installation and maintenance of closed-circuit television systems*, Issue 1, December 1990.[1)]

[5] NATIONAL APPROVAL COUNCIL FOR SECURITY SYSTEMS. NACP 30 *Code of practice for the planning, installation and maintenance of access control systems*, Issue 1, December 1990.[1)]

[1)] Available from National Approval Council for Security Systems, Queensgate House, 14 Cookham Road, Maidenhead, Berkshire SL6 8AJ.

BSI — British Standards Institution

BSI is the independent national body responsible for preparing British Standards. It presents the UK view on standards in Europe and at the international level. It is incorporated by Royal Charter.

Contract requirements

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.

Revisions

British Standards are updated by amendment or revision. Users of British Standards should make sure that they possess the latest amendments or editions.

Any person who finds an inaccuracy or ambiguity while using this British Standard should bring it to the attention of the Quality Manager, BSI without delay so that the matter may be investigated swiftly.

BSI offers members an individual updating service called PLUS which ensures that subscribers automatically receive the latest editions of standards.

Buying standards

Orders for all BSI, international and foreign standards publications should be addressed to Customer Services, Sales Department at Chiswick:
Tel: 0181 996 7000; Fax: 0181 996 7001.

In response to orders for international standards, it is BSI policy to supply the BSI implementation of those that have been published as British Standards, unless otherwise requested.

Information on standards

BSI provides a wide range of information on national, European and international standards through its Library, the Standardline Database, the BSI Information Technology Service (BITS) and its Technical Help to Exporters Service. Contact the Information Department at Chiswick:
Tel: 0181 996 7111; Fax: 0181 996 7048.

Subscribing members of BSI are kept up to date with standards developments and receive substantial discounts on the purchase price of standards. For details of these and other benefits contact Customer Services, Membership at Chiswick: Tel: 0181 996 7002; Fax: 0181 996 7001.

Copyright

BSI
389 Chiswick High Road
London
W4 4AL

9507—7—0.6k—RTL

ISBN 0 580 24600 0 Product code 00556594 FSM/12