

# COMITÉ EUROPÉEN DES ASSURANCES

SECRETARIAT GENERAL  
3bis, rue de la Chaussée d'Antin F 75009 Paris  
Tél. : +33 1 44 83 11 73 Fax : +33 1 44 83 11 85  
Web : cea.assur.org



DELEGATION A BRUXELLES  
Square de Meeûs, 29 B 1000 Bruxelles  
Tél. : +32 2 547 58 11 Fax : +32 2 547 58 19  
Web : cea.assur.org

## PROPERTY INSURANCE COMMITTEE Prevention Specifications

### **Recommendations For Remote Monitoring Centres (RMC)**

**(Alarm receiving centre and satellite centre)**

**"Requirements for construction, technical equipment,  
personnel and operation"**

*CEA 4036: January 2002 (en)*

*Copyright by CEA – 3 bis, rue de la Chaussée d'Antin – 75009 PARIS*

## TABLE OF CONTENTS

1. Foreword
2. Scope
3. Normative references
4. Definitions
5. Requirements for an alarm receiving centre
  - 5.1 Planning and location
  - 5.2 Construction
    - 5.2.1 Boundary
    - 5.2.2 Doors and locks
    - 5.2.3 Glazed area
    - 5.2.4 Walls
    - 5.2.5 Ventilation
    - 5.2.6 Staff facilities
    - 5.2.7 Protection against lightning strike
    - 5.2.8 Overvoltage protection
    - 5.2.9 Emergency light
    - 5.2.10 Water pipes
  - 5.3 Fire protection
  - 5.4 Security protection
6. Technical requirements for equipment
  - 6.1 General
  - 6.2 Tranceiver equipment
  - 6.3 Annunciation equipment
  - 6.4 Operator work stations
  - 6.5 Operating system
  - 6.6 Alarm confirmation equipment
  - 6.7 Power supply for alarm receiving centre
    - 6.7.1 General requirements
    - 6.7.2 Standby power
  - 6.8 Recording equipment
    - 6.8.1 General requirements
    - 6.8.2 Scope of record
    - 6.8.3 Capacity of data base
    - 6.8.4 Method of recording
    - 6.8.5 Integrity of records
    - 6.8.6 Data and time
    - 6.8.7 Loss of energy
    - 6.8.8 Records of event
    - 6.8.9 Electronic records
  - 6.9 Communication equipment
  - 6.10 Back-up procedure and standby equipment

- 6.10.1 Failure of an item of equipment
- 6.10.2 Total failure of part of an alarm receiving centre

7. Personnel

8. Operation

9. Internal auditing

10. Requirements for a satellite

- 10.1 Location

- 10.2 Equipment protection

- 10.3 Fire alarm

- 10.4 Transmission path

- 10.5 Power supply

Appendix 1

Appendix 2

## 1. Foreword

*These specifications prepared by the Comité Européen des Assurances (CEA) in the framework of the traditional loss prevention work by European insurers and in line with the EC Commission's group exemption regulation (regulation No. 3932/92 dated 21 December 1992) are aimed at providing the conditions for an Europe-wide uniform high level of personal and property protection.*

*With the explicit endorsement of the European Fire and Security Advisory Council (EFSAC) it is confirmed that these specifications have the support of all relevant European organizations and document the state of European loss prevention practice.*

*This document defines the specifications for construction technical equipment, personnel and operation of remote monitoring centres which should be attained to ensure systems which are reliable and effective.*

*It is recommended that the CEA document shall not contradict the CEN and CENELEC standard.*

*It is recommended also that compliance with these specifications is shown through certification given by a certification body recognized by the relevant national insurers' association. The certification body shall be accredited to the relevant standard of the EN 45000 series.*

*The conditions in this document are not intended to override national statutory requirements or regulations issued by local Fire Brigades or Police.*

## 2. Scope

This document specifies recommendations for the means of passing information to emergency services (e.g. fire brigade, police) and/or contractually designated organisations or persons.

This document also specifies recommendations for the structure and operation of remote monitoring centres which handle alarm and/or fault signals transmitted by fire safety installations (1) and intruder alarm systems and hold-up alarm systems.

The specifications for the operation of remote monitoring centres includes specifications for equipment and for the procedures which should be followed by personnel.

*(1) Fire safety installations include automatic fire alarm systems and automatic water or gas fire extinguishing systems.*

### 3. Normative references

EN 50131-1	Alarm systems - Intrusion systems: systems requirements
EN 50131-6	Alarm systems - Intrusion systems: power supplies
EN 50132-2-1	Alarm systems - CCTV surveillance systems for use in security applications: black and white cameras
prEN 50132-4-1	Alarm systems - CCTV surveillance systems for use in security applications: black and white monitors
EN 50132-7	Alarm systems - CCTV surveillance systems for use in security applications: application guidelines
EN 50136-1-1	Alarm systems - Alarm transmission systems: system general requirements
EN 50136-1-2	Alarm systems - Alarm transmission systems: requirements for systems using dedicated alarm paths
EN 50136-1-3	Alarm systems - Alarm transmission systems: requirements for systems with digital communicators using the public switched telephone network
EN 50136-1-4	Alarm systems - Alarm transmission systems: requirements for systems with voice communicators using the public switched telephone network
EN 50136-2-1	Alarm transmission equipment: general requirements
EN 50136-2-2	Alarm transmission equipment: requirements for equipment used in systems using dedicated alarm paths
EN 50136-2-3	Alarm transmission equipment: requirements for digital communicators
EN 50136-2-4	Alarm transmission equipment: requirements for voice communicators
EN 50136-7	Alarm transmission systems and equipment. Annunciation equipment to be used in alarm receiving centres - Application guidelines
EN 60950	Apparatus for information technology and office electrical machines - Safety
IEC 664	Insulation coordination for equipment within low voltage systems
CEA (Draft 15.10.00)	Aim-oriented requirements for Alarm Transmission Systems(ATS).
CEA (Draft 03.07.01)	Requirements, classification and test methods for burglary resistant lock set.
EN 1063	Glass in builds, security glazing testing and classification of resistance against bullet attack
EN 356	Glass in builds, security glazing testing and classification of resistance against manual attack

### 4. Definitions

#### 4.1 Alarm

A warning of the presence of a hazard to life, property or the environment.

#### 4.2 Alarm Company

An organisation which provides services for alarm systems.

#### 4.3 Alarm Condition

A condition of an alarm system, or part thereof, which results from the response of the system to the presence of a hazard.

#### 4.4 Alarm Confirmation

A procedure whereby additional information (e.g. audio information, image transmission, sequential alarm signals) concerning an alarm from the supervised premises is received and processed thereby indicating that the alarm is likely to be genuine.

#### 4.5 Alarm Notification

The passing of an alarm condition to warning devices and/or alarm transmission systems.

#### 4.6 Alarm Receiving Centre (ARC)

A continuously manned remote monitoring centre in which the information concerning the state of alarm systems is displayed, managed and/or recorded.

#### 4.7 Alarm System

An electrical installation which responds to the manual or automatic detection of the presence of a hazard.

#### 4.8 Alarm Transmission Equipment

Equipment which is used primarily for the transmission of alarm messages from the supervised premises trceiver interface to the alarm system interface at the supervised premises to the alarm receiving centre trceiver interface to the annunciation equipment at the alarm receiving centre. It may also transmit information or commands from the alarm receiving centre to one or more alarm systems.

Note: This does not include equipment provided by a public telephone network operator or other common carrier as part of a general purpose, public transmission system, but does include general telecommunications equipment (e.g. modems) where these are used primarily for alarm transmission.

#### 4.9 Alarm Transmission System

Equipment and network which is used to transfer information concerned with the state of one or more alarm systems to one or more remote monitoring centres.

Note: Transmission systems exclude local direct connections, i. e. interconnections between parts of an alarm system which do not require an interface to transform the alarm system information into a form suitable for transmission.

#### 4.10. Annunciation Equipment

Equipment located in a remote monitoring centre which processes and/or presents directly or after processing, information contained in messages.

#### 4.11 Authentication for Alarm Transmission

The exchange of codes to uniquely identify an Alarm Transmission Equipment at the supervised premises in order to avoid substitution by identical equipment.

#### 4.12 Boundary

All surfaces which define the volume of a remote monitoring centre, i.e. walls, floors, ceilings and any openings therein, including security lobby.

#### 4.13 Control

A check of the functional continuity of an alarm transmission system.

Note : This is carried out either by the network operator or the remote monitoring centre.

#### 4.14 Digital Communicator System

An alarm transmission system which transfers information by digital encoded signals over a transmission path established by automatic dialling via the Public Switched Telephone Network (PSTN) to a remote monitoring centre.

#### 4.15 Encryption

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

#### 4.16 Fault Condition

Condition of the equipment which is not working correctly.

#### 4.17 Logging Unit

A facility which stores chronologically the incoming and outgoing information.

#### 4.18 Main Power Supply

Normal power supply used for ensuring the operation of the remote monitoring centre.

#### 4.19 Monitoring

A check of communication via an alarm transmission system.

*Note : This is carried out either by the network operator or the remote monitoring centre.*

#### 4.20 Operator

Person responsible for the handling of messages presented at the annunciation equipment.

#### 4.21 Receiving Centre Tranceiver

The alarm transmission equipment which is located at the remote monitoring centre.

#### 4.22 Remote Monitoring Centre (RMC)

Location remote from the protected premises in which the informations concerned with the state of one or more alarm systems is collected either for reporting (e.g. an ARC) or for onward transmission.

#### 4.23 Remote Monitoring

The monitoring of signals notified by alarm systems (e.g. fire or intruder alarm systems) to an alarm receiving centre.

#### 4.24 Satellite Centre

A remote monitoring centre, normally unmanned, in which the information concerning the state of alarm systems is collected and processed for onward transmission either direct, or via a further satellite, to an alarm receiving centre.

#### 4.25 Standby Power Supply

Power supply for operating remote monitoring centre equipment in the absence of the main power supply.

#### 4.26 Supervised Premises

That part of a building and/or area in which a hazard may be detected by an alarm system.

#### 4.27 Supervised Premises Tranceiver

Equipment at the supervised premises including the interface to the alarm system and the interface to the alarm transmission system.

#### 4.28 Tamper Detection

The detection of deliberate interference with an alarm system or part thereof.

## 4.29 Tamper Protection

Methods or means used to protect an alarm system or part thereof against deliberate interference.

# 5. Requirements for an alarm receiving centre

## 5.1 Planning and location

The alarm receiving centre should be located on a site affording low risks of fire, explosion, flooding, vandalism and exposure hazards from other sites.

Where the alarm receiving centre does not occupy all the building in which it is located, it should be separated from the rest of the building by a physical boundary consisting of walls, floors, ceilings and essential openings (see 5.2.1).

The possibility of gas seepage around cables or pipes below ground level into the alarm receiving centre should be considered and, if the possibility exists, prevented.

*Note: Appropriate consultation should be undertaken with other interested organisations such as those involved in telecommunications, health and safety, environmental health, insurance and emergency service.*

## 5.2 Construction

An alarm receiving centre should, as a minimum, accommodate all of the following :

- a security lobby
- an operations area
- equipment and UPS/battery area(s)
- staff facilities: toilet and washing, preparation of food and drink etc.

(see Appendix 1)

Plan of an alarm receiving centre

### 5.2.1 Boundary

The boundary of an alarm receiving centre should consist of walls, floors and ceilings, and essential openings such as entry and exit doors, ventilation inlets and outlets, and entry points for service cables and pipes. An alarm receiving centre may, in addition, have a key transfer hatch in the boundary.

### 5.2.2 Doors and locks

All entry door should be of attack resistant construction.

Hinges, frames, fixings and locking devices for doors should be of substantial construction with a similar resistance to attack of walls, floors and ceilings.

The interior of the operations area and equipment and UPS/Battery room(s) should not at any time be directly visible from outside the alarm receiving centre.

Normal entry to an alarm receiving centre should be via a security lobby. The doors should be controlled from within the operations area by separate physical actions. Other means of normal entry offering at least the same level of security can be provided.

Emergency exits should be resistant to physical attack and should not be capable of being opened from the outside.

### 5.2.3 Glazed area



Any glazed area together with its frame and fixing should have substantial resistance to physical attack. As a minimum this should be achieved by the use of bullet resistant glass.

#### **5.2.4 Walls**

The walls and all supporting structures should be constructed to be resistant to physical attack (i.e. solid brick minimum thickness 215 mm or reinforced concrete block minimum thickness 200 mm, or 150 mm reinforced concrete cast).

#### **5.2.5 Ventilation**

The ventilation system should be controlled manually or automatically from inside the alarm receiving centre to allow it to be turned off, if gas or smoke or fire is being drawn into the alarm receiving centre. The ducting should be constructed from incombustible material. All ventilation inlets and outlets in the boundary should be protected with an air-tight flap which can readily be closed from inside the alarm receiving centre.

Ventilation inlets and outlets larger than 20.000 mm<sup>2</sup> cross sectional area should be protected against attempts at entry by expanded steel mesh or solid low carbon steel bars and should be supervised internally by a detection device connected to the intruder alarm system of the alarm receiving centre.

#### **5.2.6 Staff facilities**

Toilet and washing facilities should be provided within the ARC. Facilities for the preparation of food and drink should be provided and should be located within ARC. Where a cooking appliance is provided, it should be separated from the operational area.

#### **5.2.7 Protection against lightning strike**

The building housing an ARC should be protected against the effects of lightning strike.

*Note: in the case of an alarm receiving centre commissioned prior to 1<sup>st</sup> January 2002, if the alarm receiving centre is located in a multiple occupancy building and agreement cannot be obtained for the installation of lightning protection in areas of the building outside the control of the alarm receiving centre operator, the lightning protection for the building should be installed as far as it is reasonably possible to do so.*

#### **5.2.8 Overvoltage protection**

A comprehensive safeguard against damage caused by lightning and overvoltage is achieved by measures providing for an external and internal protection:

- installation of the external lightning protection system;
- provision of the equipotential bonding as protection against lightning;
- safety distances(exposure);
- installation of screening (buildings, rooms, ducts, pipework) and connection of cable and line screens to the equipotential bonding system protecting against lightning;
- use of optical fibre cables;
- use of lightning stroke current conductors (arresters);
- use of overvoltage conductors (arresters).

#### **5.2.9 Emergency light**

The alarm receiving centre should be equipped with emergency lighting to enable monitoring to continue if there is a failure of a main power supply.

#### **5.2.10 Water pipes**

Only pipes carrying fluids indispensable for the functioning of the alarm receiving centre should be permitted to run inside the alarm receiving centre. Pipes carrying water should not run through the operations area.

### **5.3 Fire protection**

The boundary of an alarm receiving centre and all supporting structures should have a fire resistance of not less than 60 minutes as determined from the exterior towards the interior of the centre.

Any holes made in the boundary of an alarm receiving centre should be filled with material of equivalent specification to that of the boundary.

The outer door of the security lobby should have a fire resistance of not less than 60 minutes as determined from the exterior towards the interior of the centre.

The inside of an alarm receiving centre should be equipped with an automatic fire detection system.

An alarm receiving centre should be equipped with portable fire extinguishers which meet national legal requirements and/or EN 3 series standard. The choice and location of portable extinguishers should be appropriate for the area and the type(s) of fires. At least two portable fire extinguishers suitable for fires involving electrical equipment should be installed in the operations area.

### **5.4 Security protection**

An alarm condition should be signalled if both lobby doors are open at the same time or if an emergency exit is open.

Any unauthorized opening of doors should be detected.

The immediate area surrounding the alarm receiving centre should be permanently monitored using surveillance facilities. It should be possible for alarm receiving centre staff to view the outside of the alarm receiving centre boundary from inside the centre.

Surveillance facilities should be provided to enable alarm receiving centre staff to identify visitors before permitting them to enter the security lobby and to view activity within the lobby. Surveillance facilities should be provided to enable alarm receiving centre staff to identify personnel using any key transfer hatch.

The intruder alarm system should incorporate detectors which will respond to physical attack upon the boundary, doors, ventilation openings and key transfer hatches.

The intruder alarm system should include deliberately-operated devices (Hold-up triggering devices) installed at normal operating positions, key transfer hatches, entrance(s) and emergency exit(s) for summoning assistance from emergency services.

Where practicable, the availability and continuity of alarm transmission systems associated with counter measures should preferably be permanently monitored.

When there is only one operator working alone, the operator has to confirm his/her presence at least every 10 minutes.

Should the operator fail to provide confirmation (e.g. on account of any physical deficiency), an alarm signal should be automatically transmitted to a permanently manned centre from where emergency assistance can be organized.

Emergency procedures should be specified in a company confidential manual and should include details of the procedure for emergency access to an alarm receiving centre. Such procedures should include provision for the rescue of the operators.

## **6. Technical requirements for equipment**

### **6.1 General**

The technical requirements of the alarm transmission systems and equipment used for an Alarm Receiving Centre

(ARC) are specified, as follows, taking account of the characteristics of each transmission system and each apparatus making up the configuration of an ARC (see Appendix 2).

An Alarm Receiving Centre to manage security information is fundamentally constituted by the following parts:

- alarm receiving centre transceiver equipment;
- annunciation equipment;
- power supply;
- recording equipment;
- communication equipment;
- standby equipment;
- alarm confirmation equipment (optional part).

## 6.2 Transceiver equipment

Alarm receiving centre transceiver equipment should have sufficient capacity to receive all signals from supervised premises relating to monitored events.

All signals received at an alarm receiving centre should be recorded by the receiving centre transceiver or by the annunciation equipment.

All signal received by receiving centre transceiver should be transmitted to annunciation equipment without delay.

## 6.3 Annunciation equipment

Alarm receiving centre annunciation equipment should have sufficient capacity to receive and display all signals from supervised premises relating to monitored events.

The display of information can be made by a visual display terminal, with clear or simply coded messages. Priority codes should be supplied so that alarm signals are immediately shown.

Priority coded alarm informations should be displayed continuously until alarm handling has been completed. The presentation of records for a particular alarm system should not obscure the priority coded alarm information.

The annunciation equipment should have the means to enable the operator to manage the alarm.

Note: It is necessary to identify the operator working in an ARC with a password.

Annunciation equipment should execute primarily the following functions:

- a. transcoding of the data concerning the information received from the transceiver equipment;
- b. automatic presentation of the received information to the operator,
- c. automatic recording of the received information unless recording has been carrying out by the transceiver equipment.

The received signal should be presented to the operators in a maximum time of 5 s, starting from its reception by transceiver equipment in an ARC.

There should be backup procedures for all electronically stored data.

There should be at least three different access levels to electronic systems covering entry to operating systems, software programs and records respectively. There should be a different security code number for each access level. Entry to each level should, in addition, require the use of a password which is unique to each authorised person using the system (e.g. software programmer, operator). All access level entries should be logged and it should not be possible for the manager or an operator to amend the log of entries.

## 6.4 Operator work stations

An operator's work station should be equipped with equipment suitable to manage all relevant information from supervised premises. This may include voice communication associated with alarms.

The operator's work station should guarantee:

- a. interaction between the annunciation equipment and the operator, related to the type of the managed event, to the kind of the supplied service and/or to the installation from supervised premises;
- b. activation of the visual and audible local indication devices, depending on the system condition (e.g. incoming signals distributed to the operator's work station not taken in charge, etc.); in any case, the information should be recorded and managed.

## **6.5 Operating system**

The operating system manages over the execution of all the necessary operating functions.

The primary functions that the operating system should execute are the following:

- a. possibility to define multilevel access to the different kinds of management functions (e.g. access to the data and/or tables, etc.);
- b. possibility to automatically present, related to the monitored event, the received signals to another work station or to a satellite centre;
- c. presentation and management of the incoming signals queue not yet taken in charge;
- d. presentation and management of the incoming signals queue taken in charge, but with dispatch of the required management not completed;
- e. management of the on-line "voice-communication function", if available to the services;
- f. management of the on-line "CCTV images acquisition function", if available to the services;
- g. possibility of the automatic control of critical procedures aimed to the security of persons at protected premises;
- h. management of multimedia data bases concerning information related to the protection of installations connected to the ARC;
- i. management of a multimedia data base concerning information about the customers of the ARC;
- j. management of data bases concerning information about the organizations responsible for the intervention, in case of alarm (e.g. police, private guards, fire brigade, etc.);
- l. automatic opening of the alarm handling predetermined procedures, just when the incoming event is taken in charge by the operator. Management of operating information with an automatic audit control on the various management steps and chronological recording, within appropriate logs, of all the actions executed, together with the code and the name of the operator;
- m. possibility to recall operating information and logs about specific events;
- n. recording of all the data concerning alarm signals and operating response on a data base of the ARC, in order to create appropriate check-reports of the system or operating management (reaction-time, length of response, etc.), in case of a request of the customer or of other involved organizations;
- o. possibility to execute the "dead-man" function;
- p. automatic polling, per groups and/or zones, of the installations connected to the ARC;
- q. unloading of the data for sending to the back-up monitoring centre or satellite centre, if necessary.

## **6.6 Alarm confirmation equipment**

The function of the confirmation equipment (i.e. CCTV system, audio system) could be available or not, related to the supplied application and/or service.

The primary functions of the confirmation equipment if present, are the following:

- **CCTV systems**

- possibility to acquire on-line CCTV images of the premises protected by the intruder alarm systems;
- possibility to acquire, by manual action, single or contemporary CCTV images from different remote cameras, connected to alarm events.

- **Audio systems**

- possibility to acquire on-line audio information of the premises protected by the intruder alarm system;
- possibility to acquire, by manual action, audio information connected to alarm events.

## **6.7 Power supply for alarm receiving centre**

### **6.7.1 General requirements**

The public mains supply should normally be used as the main power supply, although reliable alternatives may be used, and a standby power supply should be provided as a backup.

The main power source should be such that it is capable of providing sufficient power for the normal load of the alarm receiving centre and for simultaneously recharging the standby batteries to 80% of the capacity within 24 hours.

Changeover to, or from, a standby power supply should not cause a malfunction of equipment.

There should always be an indication in the operations area of the current source of power.

Any failure in the main power supply should be indicated by a visual and audible alarm in the operations area.

Power cables external to the alarm receiving centre should be protected against physical and fire damage.

### **6.7.2 Standby power**

A standby power supply should be provided, located within the alarm receiving centre. This should be of sufficient capacity for uninterrupted operation of all communication, signalling, monitoring, recording, essential ventilation and essential lighting equipment, including that required for the necessary surveillance, for a period of 24 h based on a demand of 1,5 times the average requirement.

The standby power source should be either:

- a) standby batteries with associated charging equipment; or
- b) a standby generator or generators supported by a standby battery and associated charging equipment.

The standby batteries should be brought into use automatically immediately the mains voltage falls below the level required to operate the alarm receiving centre equipment. The centre should return to mains power operation and the standby batteries should recharge automatically when the mains voltage is restored.

Where one stand by generator is provided, the capacity of the standby batteries should be sufficient to power the alarm receiving centre equipment for at least 4 h based on a demand of 1,5 times the average requirement.

Where two standby generators are provided, the capacity of the standby batteries should be sufficient to power the alarm receiving centre equipment for at least 30 min based on a demand of 1,5 times the average requirement.

Standby batteries should be electrically supervised by fuses or circuit breakers. Wet cells should be located in a separate battery room with its own ventilation.

All standby generators should be provided with a fuel supply on site sufficient to operate them for at least 24 h.

Note: Attention is drawn to National regulations concerning fuel storage and safety.

All standby generators should have an independent means for starting which should be automatic or controlled from within the alarm receiving centre when the normal power supply fails. Batteries required for starting a standby generator should be charged by a means which is independent of the operation of the generator.

Any generator situated inside an alarm receiving centre should be separated from the operation area by sound resistant and fire resistant walls / partitions with construction of at least 1 h fire resistance.

Any standby power generator not installed within the alarm receiving centre should be in a restricted area.

Area(s) housing generators should be protected by automatic fire detection system and intruder alarm system.

## 6.8 Recording equipment

### 6.8.1 General requirements

The recording equipment should be able to record automatically all the signals received by the ARC and signals sent from the ARC to the alarm systems at the supervised premises.

### 6.8.2 Scope of record

The following signals and functions should be recorded with date and time and the unique reference:

- signals coming in and going out from the alarm receiving centre transceiver interface to the transmission network and annunciation equipment;
- missing test signals from alarm systems;
- orders to the alarm systems which are operated by the alarm receiving centre;
- automatically operated processes;
- malfunction of the annunciation equipment and the transceiver equipment;
- setting of time and date of the recording equipment;
- identification of the operator in the ARC.

All the signals and operations should be recorded in such a way as to indicate the source, time, date and name or number of the operator, as well as the type of action to be taken. Any technical fault should not cause a loss of information

### 6.8.3 Capacity of database

The database should be able to record all the signals indicated in the scope of record (see 7.9.2). If the capacity of the database is full (90% of the capacity), the receiving and handling of alarm signals should not be affected.

### 6.8.4 Method of recording

All the signals should be recorded automatically and permanently saved. The recording equipment should not allow the changing and deleting of records. Notes can be added by operator.

The access to the records and their use should be in accordance with national privacy laws.

The printing of electronic records should be available at all times.

### 6.8.5 Integrity of records

The records should be numbered consecutively with a numerical order of at least six figures.

### 6.8.6 Data and Time

The time should not deviate more than 2 minutes from the official local time in a period of 30 days. In any case, the record time should be coincident with the official time indicated on the ARC clock. Only an authorized person may set the time and date of the system, the setting should be recorded.

### 6.8.7 Loss of energy

During malfunction of the recording equipment or a total loss of energy, the records should be stored for a period of 30 days.

#### **6.8.8 Records of event**

Records for alarm systems connected to the alarm receiving centre should be readily available to operators. Records may be written or they may be stored electronically, in which case they should be available for printing on demand. These records should contain all information relevant to clients and all details of alarm handling requirements.

All changes to client information should be logged against the person using the system (i.e. audit trail) according to the date and time of the change. It should not be possible for the manager or operators to amend the log.

Records of all alarms and other monitored events should be kept for not less than 3 years after the alarm or event to which they refer.

A log should be maintained of all routine testing, maintenance and emergency servicing to alarm receiving centre equipment.

All telephone communications to and from an alarm receiving centre should be recorded with their time and date. These communications should be kept for at least 3 months, or in accordance with national regulations, and be capable of being replayed.

All data communications to and from an alarm receiving centre relating to alarms and all other monitored events should be recorded with their time and date. These communications should be kept for at least 3 months, or in accordance with national regulations, and be capable of being printed and / or displayed.

All records should be stored securely. Records essential to the maintenance of services to clients should be duplicated and stored in fire-resistant cabinets or in secure areas either on or off site. Disposal of all records of a confidential nature should be carried out in secure manner.

#### **6.8.9 Electronic Records**

All alarms and all other monitored events should be logged according to the date and time received at the alarm receiving centre. It should not be possible for the manager or an operator to amend the log of alarms / events.

All changes to client information should be logged against the authorised person using the system according to the date and time of the change. It should not be possible for the manager or an operator to amend the log of changes.

### **6.9 Communication Equipment**

There should be at least two exchange telephone lines for outgoing voice communication, either routed underground or concealed, which should be dedicated to alarm communications and barred to incoming calls.

A radio communication facility (e.g. radio transceiver or cellular mobile telephone) should be installed to permit external communication with a permanently manned control room or another alarm receiving centre. If radio communication is not practical or reliable there should be an additional exchange telephone line barred to incoming calls.

## **6.10 Back-up procedure and standby equipment**

### **6.10.1 Failure of an item of equipment**

Any item of tranceiver equipment, annunciation equipment, power supply equipment, recording and communication equipment, alarm confirmation equipment, should have a standby equipment or procedure which can be brought into use either automatically or manually within 1 hour.

The alarm receiving centre should be provided with adequate spares for all reasonably foreseeable failures of tranceiver, annunciation and display equipment which is common to more than one connected system.

Emergency response procedures should be developed with local contractors and the emergency services to enable the alarm monitoring service to be maintained whilst an emergency incident is investigated and/or the damage contained or repaired.

The layout of the alarm receiving centre tranceiver equipment should be designed in such a way as to facilitate handling of any fault in the components so that information can always normally be received from fire alarm or intruder detection systems (minimum mode operation).

### **6.10.2 Total failure of part of an alarm receiving centre**

In the event of an alarm receiving centre being put out of action there should be a contingency plan for dealing with the consequence.

The plan should provide for any reasonably foreseeable emergency at the alarm receiving centre.

In cases where it is foreseen that an emergency incident could lead to loss of monitoring services, plans should be made to reinstate alarm monitoring operations on site or to transfer to an alternative alarm receiving centre.

Contingency plans should be rehearsed at intervals not exceeding 6 months by simulating a damage incident.

Appropriate measures should be taken to ensure that the continuity and quality of the services defined above are maintained at all times and in all circumstances, within a time limit of 4 hours.

## **7. Personnel**

An alarm receiving centre and its operators should be under the responsibility of a trained manager.

All operators should have appropriate skills and should be trained in the use of the equipment and to take correct action in response to alarm signals received.

All operators should have immediate access to all relevant documented procedures and the manager should ensure that all operators follow the procedures. The procedures should include full details of all routine work and should include details of the actions to be taken in the event of foreseeable emergencies. The documented procedures should not normally be allowed to leave the alarm receiving centre.

Where emergency services (e.g. fire brigade or police) are to be called in response to alarms, operators should initiate calls within the procedures agreed with all relevant parties.

The number of operators in the alarm receiving centre should be sufficient, under all normal circumstances, to meet the agreed alarm handling procedures. At least one operator being at his work station at all times.

Single manning is permissible provided the one operator is able, under normal circumstances, to meet the alarm handling times for the alarms being received and provided the requirements of 5.4 relevant to single manning are met.

Provision should be made for reserve operators to report for duty within 30 minutes in an emergency for single manned alarm receiving centres and 1 hour for others.

There should be one person in the alarm receiving centre at all times who is trained to deal with minor technical



problems. It is permissible for this person also to be an operator if appropriately trained.

Arrangements should exist for a trained engineer to attend an alarm receiving centre within 4 hours of a fault being detected that cannot be rectified by the person trained to deal with minor technical problems.

A written procedures should exist for the control of access (i.e. entry into and exit from) the alarm receiving centre. Routine access to an alarm receiving centre should be restricted to authorised staff (e.g. manager and operators) who have a need to enter on a regular basis. The names and photographs of all authorised staff should be readily available to those persons responsible for controlling access to the alarm receiving centre.

All visitors (i.e. all persons who are not authorised staff), should be authorised in advance of the visit and should always be accompanied by authorised staff.

All entry / exit movements to / from an alarm receiving centre should be logged. As a minimum, an audit of the logs should be conducted monthly to check for unauthorised movements.

## **8. Operation**

The primary function of an alarm receiving centre should be the handling of alarm signals, together with other signals relating to the change of status of the alarm systems, such as set or unset signals or alarm and fault signals relating to alarm transmission systems.

Authentication procedures should be established and operated for the exchange of confidential information between the alarm receiving centre and client. The client should be allocated an agreed authentication code, or code word, to be used when exchanging confidential information concerning the operation of the alarm system, information about the supervised premises or personal details.

Clear guidelines on the actions to be taken on the receipt of alarm signals should be laid down. These actions should be in accordance with the requirements of emergency services, any other nationally agreed regulations, and the requirements of clients.

All data displays should provide clear, unambiguous information and alarm information should be clearly distinguishable from other information.

Alarm indications should have handling priority over other indications (e.g. fault, status information).

Fire alarm indications should be clearly distinguishable from other alarm indications.

The priority of handling alarms should be made clear to clients and should comply with any nationally agreed priorities (e.g. fire alarms usually have priority over other alarms).

## **9. Internal auditing**

There are at least three different reason for carrying out auditing of procedures for the alarm receiving centre:

1. fault condition, breakage, etc.;
2. involuntary mistake, negligence, etc.
3. computer crime.

The manager should ensure that all procedures are carried out correctly and that a documented audit is undertaken at periods not exceeding 6 months for at least 3 years from the date of its performance.

The main power supply, standby power supply, equipment, circuits and accessories, protection installations of the premises etc.should be checked for correct operational weekly.

It will be necessary to verify, e.g. by means of the check-list, if the operators have executed the check of the remote monitoring centre equipments and of the respective technical sheets concerning hardware and software, of the

installations connected with remote monitoring centre (fire detection systems, intruder alarm systems, CCTV systems, etc.). It is also necessary to verify the presence of a maintenance contract of the software packaging used inside the monitoring centre and the availability of the source code.

The auditing procedure will have to take into account the control on the operators' activity, and, in particular, if the operators apply the expected procedures correctly.

The auditing procedure will have to take into account the verification of the customer satisfaction.

## **10. Requirements for a satellite**

### **10.1 Location**

A satellite should be located within a permanent building, or part of a permanent building, to which the alarm receiving centre operating or parent company has exclusive control of access at all times.

### **10.2 Equipment protection**

The equipment in a satellite should be protected against attack or malicious damage (e.g. vandalism). The satellite equipment should be protected as follows:

- the construction of the boundary entrance, exits, glazed openings, inlets and outlets of the satellite and service inlets and outlets should be as recommended for alarm receiving centres; the normal entrance may be a single door and not a lobby with doors;
- an intruder alarm system should be installed conforming to the EN 50131 and/or the local standard, which should signal an alarm condition to the alarm receiving centre by a dedicated alarm transmission path in the event of attack. If the satellite is capable of being manned, the alarm system should include deliberately-operated devices located within the boundary of the satellite. A signal should be transmitted automatically to the alarm receiving centre whenever any access door to the satellite is not closed and locked.

### **10.3 Fire alarm**

An automatic fire alarm system conforming the local standards should be installed throughout the satellite. A fire alarm condition resulting from a fire within the satellite should transmit an alarm automatically to the alarm receiving centre or Fire Brigade.

### **10.4 Transmission path**

A satellite should have one or more dedicated alarm transmission paths to its alarm receiving centre for the transmission of alarm signals, supplemented by alternative communication means and/or provision for manning to enable the processing of alarm signals from connected alarm systems in the event that normal communication to the controlling alarm receiving centre is lost. The choice between these alternatives should be related to the number of alarm system connections as follows:

- a) for less than 16 alarm systems connected, a dedicated alarm transmission path only;
- b) for 16 to 64 alarm systems connected, a dedicated alarm transmission path and either an alternative communication means or provision for manning;
- c) for more than 64 alarm systems connected, a dedicated alarm transmission path and both an alternative communication means and provision for manning.

Where the satellite has provision for manning there should be a telephone with an ex-directory number for voice communication.

## 10.5 Power supply

The public mains supply should be used as the principal source of electrical power although reliable alternatives may be used and a standby power source should be provided as a backup. Changeover to, or from, a standby power supply should not cause a malfunction of equipment. Cables external to the boundary of the alarm receiving centre should be protected against physical and fire damage. There should be an indication in the operations area of the current source of power.

A standby power supply should be provided, located within the satellite and of sufficient capacity for the uninterrupted operation of all communication, signalling, monitoring, recording, essential ventilation and essential lighting equipment, including that required for the necessary surveillance for a period of 24 hours based on a demand of 1,5 times the average requirement.

The standby power source should be either :

- a) a standby battery with associated charging equipment; or
- b) a standby generator or generators supported by a standby battery and associated charging equipment.

The standby batteries should be brought into use automatically immediately the mains voltage falls below the level required to operate the satellite. The satellite should return to mains power operation and the standby batteries recharge automatically when the mains voltage is restored to its minimum value.

The mains power source should be such that it is capable of providing sufficient power for the normal load of the satellite and for simultaneously recharging the batteries to 80% of the required capacity within 24 hours.

Where a standby generator is provided, the standby battery capacity should be sufficient to power the satellite equipment for at least 4 hours.

Where a second standby generator is provided, the standby battery capacity should be sufficient to provide the required power for at least 30 min.

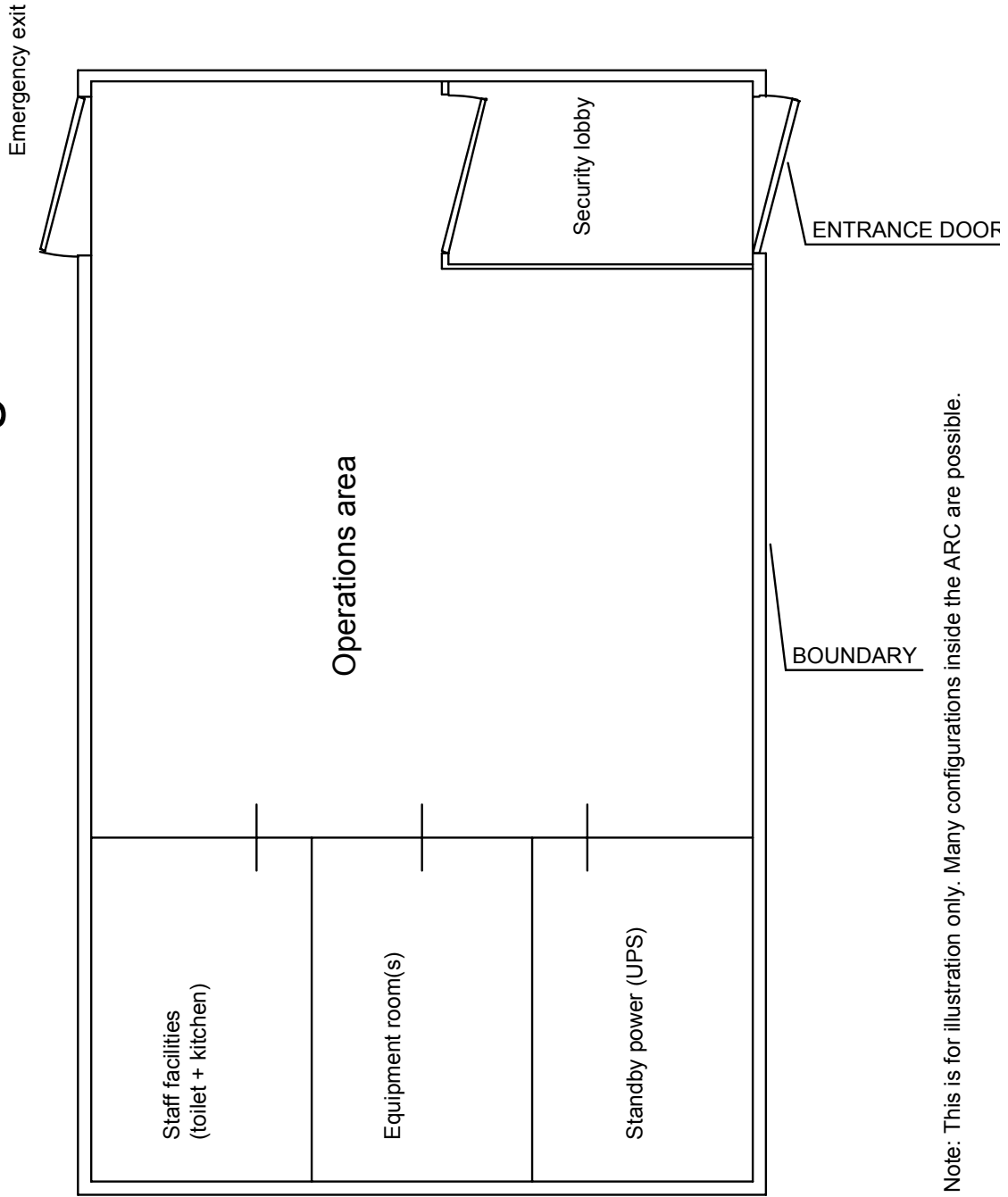
The standby batteries should be electrically supervised by fuses or circuit breakers. Wet cells should be located in a separate battery room with its own ventilation.

All standby generators should be provided with a fuel supply sufficient to operate the generator for at least 24 hours. They should have an independent means of starting which should be automatic or controlled from within satellite when the normal power supply fails. Batteries required for starting a standby generator should be charged by a means which is independent of the operation of the generator.

Any standby power generator not installed within the satellite boundary should be in a restricted access area.

Area housing generators should be supervised by fire detection system and intruder alarm system.

# Plan of an alarm receiving centre



Note: This is for illustration only. Many configurations inside the ARC are possible.

Appendix 2

