National Security Inspectorate

NSI Code of Practice
for the Design, Installation
and Maintenance of
Scaffolding Alarm Systems
NCP 115 (Issue 1)

This Code of Practice is to be read in conjunction with the NSI Regulations relating to approval by NSI, the NACOSS Gold approval criteria and the Systems Silver approval criteria.
No company shall hold out or claim that it adheres to this Code, save by virtue of holding NSI approval, or having obtained the written permission of NSI.

NCP 115 (Issue 1)

January 2013

National Security Inspectorate

Code of Practice for the Design, Installation and Maintenance of Scaffolding Alarm Systems

LIST OF CONTENTS

In this document, material (such as guidelines, information, recommendations, advice) that does not form a mandatory requirement of this Code is shown in italics

FOREWORD

The erection of scaffolding potentially provides intruders with access to premises by means that would not be available normally. Such premises may be occupied or unoccupied depending on the circumstances.

A scaffolding alarm system includes control equipment, intruder detection devices and means for notifying alarm conditions, either locally and/or remotely.

The purpose of a scaffolding alarm system is to detect intruders on the scaffolding. A scaffolding alarm system is not intended to be a substitute for having an intruder alarm system inside the premises where the scaffolding has been erected.

This Code of Practice:

Aims to assist purchasers, specifiers, installers and users in selecting the scaffolding alarm system best suited to a particular task.

Provides requirements for the design and installation and maintenance of scaffolding alarm systems.

Provides minimum specifications for two categories of scaffolding alarm system, basic and enhanced.

The successful operation of a scaffolding alarm system requires the active co-operation of the user in carrying out the necessary procedures carefully and thoroughly. The usefulness of the whole system and its security and social acceptability can be jeopardised by lack of care. This care has to extend to security code numbers and/or digital keys used to operate the system and to information regarding the system, its design, installation and method of operation and to ensure adequate maintenance, to preserve the security of operation.

We draw your attention to:

The Construction (Design and Management) Regulations 2007.

Approved Document B of the Building Regulations, which covers fire safety.

Approved Document M of the Building Regulations, which covers access to and use of buildings.

BS 7671, Requirements for Electrical Installations (also known as the "IET Wiring Regulations").

1 SCOPE

This Code of Practice includes requirements for the design and installation and maintenance of scaffolding alarm systems including commissioning and handover.

This Code of Practice includes a functional specification for two categories of scaffolding alarm system, basic and enhanced.

NSI NACOSS Gold and Systems Silver approved companies designing, installing and/or maintaining scaffolding alarm systems must comply with this Code of Practice (NCP 115).

2 NORMATIVE REFERENCES

BS EN 60529:1992	Specification for degrees of protection provided by enclosures (IP code)
BS 5979:2007	Remote centres receiving signals from fire and security systems – Code of practice.
BS 7858:2012	Security screening of individuals employed in a security environment – Code of practice
EN 60065:2002+A12:2011	Audio, video and similar electronic apparatus – Safety requirements
EN 60950-1:2006+A12:2011	Information technology equipment – Safety – Part 1: General requirements

3 DEFINITIONS AND ABBREVIATIONS

3.1 Definitions

For the purposes of this Code of Practice the following definitions apply:

3.1.1 access level

level of access to particular functions of an SAS

3.1.2 alarm

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

3.1.3 alarm company

organisation that provides services (such as design, installation and maintenance) for SAS

3.1.4 alarm condition

condition of a SAS, or part thereof, which results from the response of the SAS to the presence of a hazard

3.1.5 alarm notification

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

3.1.6 alarm receiving centre (ARC)

continuously manned centre complying with Category II of BS 5979 to which information concerning the status of one or more alarm systems is reported

3.1.7 alarm transmission system (ATS)

equipment and network used to transfer information concerning the status of SAS to an ARC

3.1.8 alternative power source (APS)

power source capable of powering the SAS for a predetermined time when a prime power source is unavailable

3.1.9 ancillary control equipment (ACE)

equipment used for supplementary control purposes

3.1.10 as-fitted document

document in which the details of the SAS actually installed are recorded

3.1.11 authorisation

permission to gain access to the various control functions of an SAS

3.1.12 authorisation codes

mechanical or logical keys which permit access to SAS functions

3.1.13 availability of interconnection

condition when an interconnection is capable of conveying a signal or message

3.1.14 board

wooden plank laid on transoms to enable people to walk across the scaffolding

3.1.15 boarded lift

lift with boards

Boarded lifts typically have 4 or 5 boards laid side by side to provide the required width.

3.1.16 client

individual or corporate body responsible for acquiring a SAS

3.1.17 commissioning

placing a SAS into operational mode following inspection and testing

3.1.18 confirmation of alarm condition

means of confirming the detection of an intruder, for example by requiring the activation of more than one detector or audibly or visibly verifying an alarm condition at an ARC

3.1.19 control equipment (CE)

equipment for receiving, processing, controlling and indicating and initiating the onward transmission of information

3.1.20 corrective maintenance

emergency servicing of a SAS, or part thereof, carried out in response to the development of a fault

3.1.21 cross braces

tubes placed diagonally from ledger to ledger, next to the uprights to which they are fitted

Cross braces provide extra rigidity to the scaffolding.

3.1.22 detector

device designed to generate an intruder alarm condition in response to sensing an abnormal condition indicating the presence of a hazard

3.1.23 documentation

paperwork or other media recording details of the SAS prepared during the design, installation, commissioning and handover of SAS

3.1.24 elevation

side view of premises as viewed from front, back, left or right

A top down plan of the premises may provide details of each elevation.

3.1.25 equipment schedule

list of equipment to be installed or actually installed

3.1.26 end stop

intrusion detection installed at the end of a lift

Example: Use of passive infra-red (PIR) movement detectors.

3.1.27 entry/exit route

route by which authorised entry or exit to the supervised lift or part thereof may be achieved

3.1.28 fault condition

condition of a SAS which prevents the SAS or parts thereof from functioning normally

3.1.29 indication

information (in audible, visual or any other form) provided to assist the user in the operation of a SAS

3.1.30 inhibit

status of a part of a SAS in which an alarm condition cannot be notified, such status remaining until the SAS or part thereof passes from the set to the unset status

3.1.31 interconnection

means by which messages and/or signals are transmitted between SAS components

3.1.32 intruder alarm condition

condition of a SAS, or part thereof, which results from the response of the SAS to the presence of a hazard

3.1.33 isolation

status of a part of a SAS in which an alarm condition cannot be notified, such status remaining until cancelled by a user

3.1.34 ledger

horizontal tube which connects between uprights

3.1.35 lift

scaffolding at a given level

Examples: Base lift is normally at ground level. First lift is normally at first floor level.

3.1.36 local notification

passing of alarm, tamper or fault conditions to local audible warning device(s)

3.1.37 monitoring

process of verifying that interconnections and equipment are functioning correctly

3.1.38 notification

passing of alarm, tamper or fault conditions to audible warning device(s) and/or ARC

3.1.39 operational mode

state of a SAS when it is complete, commissioned and ready for use

3.1.40 operator

authorised individual (a user) using a SAS for its intended purpose

3.1.41 override

intervention, by a user, to permit setting when a SAS is not in a normal condition

3.1.42 part set

status of a SAS in which an intruder alarm condition can be notified but part of the SAS is unset

3.1.43 power supply (PS)

part of an alarm system which provides power for a SAS or any part thereof

3.1.44 preventative maintenance

routine servicing of a SAS, carried out on a scheduled basis

3.1.45 prime power source (PPS)

power source used to support the SAS under normal working conditions

3.1.46 remote notification

passing of alarm, tamper or fault conditions to an ARC or other remote location indicating that a hazard has been detected

3.1.47 response personnel

person or organisation responsible for taking appropriate action agreed with the client following the activation of a SAS

This may be the organisation that supplied the SAS or a third party.

3.1.48 restore

procedure of cancelling an alarm, tamper, fault or other condition and returning a SAS to a previous condition

3.1.49 scaffolding

temporary structure used to support people and materials in the construction or repair of buildings and other large structures

3.1.50 scaffolding alarm system (SAS)

electrical installation installed on scaffolding lift(s) which responds to the automatic detection of the presence of a hazard

3.1.51 self powered device

device incorporating its own power source

3.1.52 set

status of a SAS or part thereof in which an alarm condition can be notified

3.1.53 skeleton scaffolding

scaffolding without boards

3.1.54 specifier

individual or corporate body responsible for stipulating the requirements SAS will be required to meet

3.1.55 supervised lift

part of scaffolding in which an intrusion or hazard may be detected by a SAS

3.1.56 supervised premises transceiver (SPT)

alarm transmission equipment on the scaffolding at the premises including the interface to the SAS and the interface to one or more transmission networks

3.1.57 supplementary prime power source (SPPS)

energy source (independent of the prime power source) capable of supporting the SAS for extended periods, without affecting the standby period of the alternate power source

3.1.58 system components

individual items of equipment which constitute a SAS when configured together

3.1.59 tamper

deliberate interference with a SAS or part thereof

3.1.60 tamper alarm

alarm generated by tamper detection

3.1.61 tamper condition

condition of SAS in which tampering has been detected

3.1.62 tamper detection

detection of deliberate interference with the SAS, or part thereof

3.1.63 tamper protection

methods or means used to protect SAS, or part thereof, against deliberate interference

3.1.64 transom

tube that rests on ledgers at right angles

Main transoms are placed next to the uprights. They hold the uprights in place and provide support for the boards. Intermediate transoms are placed between the main transoms to provide extra support for the the boards.

3.1.65 unset

status of SAS, or part thereof, in which an alarm condition cannot be notified

3.1.66 unboarded lift

lift without boards

3.1.67 unwanted alarm

alarm conditions not generated by an intrusion or attempted intrusion into the supervised premises or site

3.1.68 upright

vertical tube that transfers the mass of the scaffolding structure to the ground

Vertical tubes (also known as "standards") rest on base plates to spread the load.

3.1.69 user

person authorized to operate SAS

Example: Operators of SAS and/or alarm company personnel.

3.1.70 warning device (WD)

a device that gives an audible alarm in response to a notification

A warning device may also provide alert indications providing such indications are easily distinguishable from an alarm.

3.1.71 wire-free interconnection

interconnection conveying information between SAS components without physical media, for example using RF techniques

3.1.72 zone

area of the supervised lift (or lifts) where an intrusion or attempted intrusion may be detected by a SAS

A zone may contain any number of detectors.

3.2 Abbreviations

For the purposes of this document, the following abbreviations apply.

ACE Ancillary Control Equipment

APS Alternative Power Source

ARC Alarm Receiving Centre

ATS Alarm Transmission System

CE Control Equipment

PIR Passive Infra-Red

PS Power Supply

PPS Prime Power Source

SAS Scaffolding Alarm System (Basic and Enhanced)

SPPS Supplementary Prime Power Source

SPT Supervised Premises Transceiver

WD Warning Device

4 SITE SAFETY, SECURITY SCREENING AND RECORDS

Your staff must adhere to site safety requirements at all times.

When arriving on site your staff should make contact with the person responsible for overall site safety, obtain permission to carry out the work on site, and complete any safety induction training required.

Your staff must be suitably trained to work at height, including the use of steps and ladders, and they must hold all relevant qualifications for working on scaffolding as may be applicable.

You must keep records of all training and qualifications.

Your staff must be competent to assess whether the scaffolding upon which the SAS will be installed is suitably and safely constructed for them to use.

You should specify (for example in your quotation) the standard of the scaffolding upon which the SAS will be installed. Typically you might specify boarded lifts with 4 or 5 boards, guard rails and toe boards.

Your staff must not work on un-boarded lifts.

We draw your attention to the Construction (Design and Management) Regulations 2007 (CDM) which place legal duties on people involved in construction work.

You must ensure that all staff visiting sites are security screened to BS 7858 and carry identification cards, which must include a photograph of the bearer, their signature, the name of your company and a date of expiry.

Everyone in "relevant employment", as defined in BS 7858, needs to be security screened, not just staff visiting sites.

5 SYSTEM DESIGN

5.1 Categories of SAS

This code of practice specifies two categories of SAS, basic and enhanced. Except where otherwise stated in this code of practice, SAS means basic and enhanced SAS.

The category of SAS depends upon the performance required as determined by the alarm company in agreement with the client.

5.1.1 Basic SAS

A basic SAS does not need to include remote notification of alarms to a BS 5979 Category II compliant ARC.

A basic SAS must include at least one local audible warning device, except that including such a warning device is optional if remote notification of alarms to a BS 5979 Category II compliant ARC is included.

5.1.2 Enhanced SAS

An enhanced SAS must include remote notification to a BS 5979 Category II compliant ARC.

An enhanced SAS does not need to include a local audible warning device, but it is common to include such a device, in addition to remote notification to the ARC.

5.2 Site survey

The importance of an adequate survey for installation is paramount. The survey can be carried out on site or remotely depending on the complexity of the site, whether the scaffolding has been erected or not, and the ability (or otherwise) to use remote means such as satellite images to gain sufficient information. Site surveys are necessary for large or complex systems for example in order to establish how power will be supplied and/or to establish if the installation will need to be carried out in several stages.

You must survey the site to be supervised in order to determine the extent of the SAS and to select equipment and components of the appropriate functionality and performance, including their suitability for the environment in which they will be installed.

You must ensure that the design of the SAS complies with either the basic or enhanced category of SAS as agreed with the client.

You must establish the dimensions and the complexity of the lifts to be supervised by the SAS including any ladder access points requiring supervision.

You must determine the number of lifts to be supervised and the elevations associated with each lift.

It is typical to supervise the first boarded lift and any ladder access points. However other lifts may need to be supervised, for example if access to the scaffolding is possible at other levels (for example from adjacent buildings).

You must consider the potential for an intruder to gain access to the scaffolding:

a) for example via external stairwells, fire escapes, balconies, the roof and so on; or

b) from adjacent premises including using scaffolding on adjacent premises that may

or may not have an installed SAS.

5.3 Supervision

You must determine the type and location of all the equipment and components required for the SAS including the detection required on each elevation of each lift and the associated cabling needed for interconnections.

The technology chosen must provide adequate supervision of the lifts to be supervised and the ladders used to gain access to these lifts.

You must consider the detectors available to detect an intruder gaining access to the scaffolding:

a) for example via external stairwells, fire escapes, balconies, the roof and so on; or

b) from adjacent premises including using scaffolding on adjacent premises that does not have an installed SAS.

These considerations may lead you to install the SAS on more than one lift in order to provide adequate supervision of the scaffolding.

You must provide detection for the full length of each elevation of each lift to be supervised.

Typically this may be achieved using beam interruption devices if the range is over 10 metres or passive infra-red detectors if the range is less than 10 metres.

Depending on the premises a lift may have complex elevations and the number of detectors required to supervise these elevations will increase with the complexity.

You must provide WD(s) and/or ATS(s) according to whether the SAS is basic or enhanced.

You must:

- install end stops on the lowest supervised lift.
- consider whether end stops need to be installed on other lifts.
- offer the client additional end stops if there is the possibility of intrusion from adjacent premises, for example via scaffolding on adjacent premises that does not have an installed SAS.

This Code of Practice does not require alarm confirmation technology to be used (for example using two independent detectors to cause a sequentially confirm alarm to be generated). However, this is not to say that alarm confirmation technology cannot be used, for example if there is a need to reduce false alarms from debris netting and/or other materials used to provide protection for the scaffolding.

5.4 Installation planning

You must determine:

- whether the installation of the SAS will need to be carried out during one site visit or over several site visits;
- the length of time that the scaffolding will be required to be supervised;
- whether the supervision will need to change over time and if so when it will need to change (for example if the scaffolding is to be adapted during the course of the project);
- how much cable will be required taking into account the length and location of cable runs and the need to ensure that any voltage drops are within required tolerances;
- the need for a documented plan for carrying out the installation, particularly if it is a large and/or complex installation.

5.5 System design proposal

You must prepare a system design proposal (which can be part of a quotation) for submission to the client. The proposal must include:

a) **Client details** – The name, address, and the trading name, if different from the name of the client, and any other information necessary to clearly identify the client.

b) **Supervised premises details** – The name and address of the premises where the SAS is to be located and a brief description of the use of the premises, for example shop, factory, school, business or home.

c) **Category** – The category of the proposed SAS, either basic or enhanced.

d) **Environment** – The environment under which each system component will operate.

e) **Schedule of equipment** – A schedule of the type and location (in words or diagrammatic form) of all equipment and a statement relating to the expected range and/or area coverage of intrusion detectors in relation to where the lifts are installed or expected to be installed.

f) **Notification** – Details of the proposed notification equipment, the type and location of WD and SPT and whether or not alarms will be remotely notified to an ARC.

g) **Legislation** – Details of any claims of compliance of system components in relation to any local or national standard (for example noise pollution).

h) **Standards and codes of practice** – A reference to this Code of Practice, NCP 115.

i) **Intervention** – Planned response to alarm activations and or faults, for example key-holder, intervention service or private response company.

j) **Preventive maintenance** – Recommendations for any scheduled maintenance of SAS or particular system components including details of the frequency of any maintenance visits and a list of the work to be carried out during each visit.

k) **Corrective maintenance** – Details of the proposed repair service to be provided including contact names and daytime and twenty four hour telephone numbers.

Any changes to the system design proposal, for example during installation, must be agreed with the client and the documentation amended accordingly.

5.6 Selection of equipment and components

You must determine the environmental conditions in which the equipment and components are expected to operate. You must then select and install equipment and components that will operate correctly in these environmental conditions.

Guidance on environmental conditions is given in 5.6.1 to 5.6.4 below.

It is not necessary for the equipment and components of SAS to hold environmental classifications, though it is helpful if they are classified. Where there are no classifications then manufacturers' literature should confirm the environmental conditions under which the equipment and components are expected to operate correctly.

5.6.1 Outdoor – General (Class IV)

Out of doors, when components are fully exposed to the weather, temperatures may be expected to vary between -25 °C and +60 °C with average relative humidity of approximately 75 % non-condensing. For 30 days per year relative humidity can be expected to vary between 85 % and 95 % non-condensing.

5.6.2 Outdoor – Sheltered or indoor extreme conditions (Class III)

Out of doors, when components are not fully exposed to the weather, or are indoors where the environmental

conditions are extreme, temperatures may be expected to vary between -25 °C and +50 °C with average relative humidity of approximately 75 % non-condensing. For 30 days per year relative humidity can be expected to vary between 85 % and 95 % non-condensing.

5.6.3 Indoor – General (Class II)

Indoors, when the temperature is not well maintained (for example in corridors, halls or staircases and where condensation can occur on windows and in unheated storage areas or warehouses where heating is intermittent), temperatures may be expected to vary between -10 °C and +40 °C with average relative humidity of approximately 75 % non-condensing.

5.6.4 Indoor (Class I)

Indoors, when the temperature is well maintained (for example in a residential or commercial property), temperatures may be expected to vary between +5 °C and +40 °C with average relative humidity of approximately 75 % non-condensing.

5.7 Housings

You must use environmental housings according to BS EN 60529 so as to afford appropriate protection (for example to IP54 or IP65 as applicable) where the possibility of penetration by solid objects, dust or water exists. This applies to all equipment and components including any external power supplies.

You must consider whether certain equipment and components may need to be protected against malicious damage such as vandalism and/or physical attack. Where this is relevant you must select equipment and components that are resistant to such attack.

The degree of vandal and/or attack resistance is not defined in this code of practice but the resistance should be suitable for the application and agreed with the client.

5.8 Interconnections

You must select interconnections to enable the SAS to perform correctly and reliably under the prevailing environmental conditions including temperature and humidity (see 5.6) and any sources of electromagnetic interference.

5.8.1 Wired interconnections

Where wired interconnections (cables) are used you must take into account the relevant electrical specifications and the equipment manufacturers' recommendations.

The rating of cables must be such that they permit satisfactory operation of the equipment at the end of any proposed length of cable run.

The voltage delivered to any system component should not be less than the minimum specified operating voltage, when measured in the maximum current condition, with the minimum power supply voltage.

To facilitate rapid tracing of faults in interconnecting wiring you must ensure that all cables are identifiable at their ends. Sufficient test points, contained in junction boxes, must be provided for efficient fault identification, for example colour coded insulation or labelling.

5.8.2 Wire-free interconnections

Where wire-free interconnections are used you must make sure that they meet statutory regulations and that they will work reliably under all the environmental conditions in which they are installed, including interference from other electromagnetic sources.

5.9 Means of setting and unsetting

You must select the means of setting and unsetting the SAS to suit the requirements of the site and the needs of the client.

For example SAS can be set and unset at CE/ACE located inside the premises where the scaffolding is erected or at external ACE located on the scaffolding.

5.10 Notification

5.10.1 Warning devices (WDs)

You must give consideration to the number of local audible WDs and their location.

You must locate WDs within or above supervised lifts.

5.10.2 Alarm transmission systems (ATSs)

Many communication formats exist for the transmission of data between SPT and an ARC. You must take care to ensure the ARC can accept signals from the SPT to be installed and process all signals correctly.

You must locate SPT within or above supervised lifts.

5.11 Remote monitoring

If you contract to provide remote monitoring you must use only ARCs that hold NSI ARC Gold approval for the monitoring of intruder alarms (or other ARCs approved by an independent third-party approvals organisation acceptable to NSI and complying with the requirements of BS EN ISO 9001 and BS 5979 for the monitoring of intruder alarms).

5.12 Power supplies (PSs)

You must select power supplies to meet the largest load placed upon them under both normal and alarm conditions including when the APS is being recharged.

When power is normally derived from a mains supply with an alternative power source (APS) as backup, you must ensure that the capacity of the alternative power source is capable of powering the SAS for a minimum of 12 hours for an enhanced SAS, or for a minimum of 8 hours for a basic SAS.

You must locate any external power supplies within or above supervised lifts.

5.13 Response

You must agree and document the planned response to alarms generated by the SAS.

For example the ARC may contact the client and/or a private guarding company to provide response.

6 FUNCTIONAL SPECIFICATION

6.1 General

SAS must include the functional requirements specified in this code of practice according to the category (see 5.1) of SAS selected.

SAS must include means to operate the SAS (for example set/unset), to detect an unauthorized person or hazard, to process the information and to notify alarms.

Additional functions may be included in SAS provided they do not influence the correct operation of SAS.

Components of other applications (such as detectors) may be combined or integrated with SAS provided the performance of the SAS components is not adversely influenced.

Examples of other applications may include smoke or heat detection, flood alert, gas detection and so on.

6.2 Detection of intruders, tampering and the recognition of faults

SAS must include means for the detection of intruders, tampering and the recognition of faults necessary to meet the requirements of this code of practice.

6.2.1 Intruder detection

An intruder alarm signal must be generated when an intrusion detector has been activated. The duration of the signal must be sufficient to ensure that communication with CE is achieved under normal conditions.

Detectors may be configured so that two (or more) activations are required to generate an alarm condition. For example this might be required in some cases in order to minimize false alarms

6.2.2 Tamper detection

SAS components must incorporate tamper detection as specified in Table 5.

A tamper signal must be generated when tamper has been detected. The duration of the signal must be sufficient to ensure communication with CE is achieved under normal conditions.

6.2.3 Recognition of faults

SAS must recognise the fault conditions specified in Table 1.

Table 1 – Faults

Faults	Basic	Enhanced
Detector(s)	M	M
Prime power source	M	M
Alternative power source	M	M
Interconnections	M	M
Alarm transmission systems	OP	M
Warning devices	M	M
M = Mandatory OP = Optional		

A fault signal must be generated when a fault has been detected. The duration of the signal must be sufficient to ensure communication with CE is achieved under normal conditions.

The requirement for SAS to recognise detector, ATS and WD faults does not imply such equipment is required to provide a dedicated fault output. For example such faults may be derived from failure of periodic communication. In the case of beam interruption detectors, misalignment of the detectors should give rise to a fault condition.

6.3 Operation

6.3.1 Access levels

SAS must provide a minimum of two user access levels, one for operators of SAS, the other for alarm company personnel.

Additional access levels may be provided, for example for private response company personnel, or else such personnel should have their own codes as operators of SAS within the relevant access level.

6.3.2 Authorisation

Access to functions of SAS (for example set/unset) must be restricted by user authorisation codes or equivalent means.

Authorisation code requirements for SAS must be a minimum of 10,000 differs for logical keys and 3,000 differs for physical keys.

Logical keys require a 4 digit code number such as 1234 to achieve 10,000 differs.

6.3.3 Setting

User access to the means of setting must be restricted through the use of authorisation codes (see 6.3.2).

There must be an audible or visual indication to indicate when the setting procedure is in progress and/or has been completed.

The CE must be configured such that signals from detectors on the exit route (if any), activated during the setting procedure, are not processed as alarm conditions.

It is not always necessary to have an exit route for the SAS. Setting of the SAS can be carried out outside the area(s) being supervised, for example inside the premises where the scaffolding is erected.

6.3.3.1 Enhanced SAS

Enhanced SAS must have the facility to set automatically if a user has not set the SAS before a time agreed with the client.

Whether this facility is used or not depends on the agreement between you and the client.

If any part of the SAS is not operating normally at the time of setting automatically, the relevant part (for example a detector) must be inhibited and the inhibition must be notified to the ARC.

Sometimes this inhibition is called a "false set" ("false arm") even though the remaining parts of the SAS have set.

You must agree with the client the actions that the ARC must take upon receiving notification of inhibition.

6.3.4 Prevention of setting

SAS must not set if any intrusion detector (except for any detector on a designated entry/exit route) is in active condition and/or if any tamper or fault has been detected.

An exception to this is where the SAS sets automatically (see 6.3.3.1).

6.3.5 Overriding prevention of setting

Users are permitted to override conditions preventing setting provided the overriding is limited to each set period and is recorded in the event log.

It must not be possible to override a prevention of set condition if overriding would result in the generation of an alarm condition.

6.3.6 Set state

When the setting procedure has been completed satisfactorily there must be a time limited completion of setting indication to show that the SAS or part thereof has changed to a set state.

6.3.7 Unsetting

User access to the means of unsetting must be restricted through the use of authorisation codes (see 6.3.2).

There must be an audible or visual indication to indicate when the unsetting procedure is in progress and/or has been completed.

The CE must be configured such that signals from detectors on the entry route (if any), activated during the unsetting procedure, are not processed as alarm conditions.

It is not always necessary to have an entry route for the SAS. Unsetting of the SAS can be carried out outside the area(s) being supervised, for example inside the premises where the scaffolding is erected.

6.3.7.1 Unsetting completed outside supervised area(s)

SAS can be unset from outside the area(s) supervised by the SAS, for example by unsetting the SAS at a keypad or CE located inside the premises associated with the SAS.

6.3.7.2 Unsetting completed inside supervised area(s)

Alternatively SAS can be unset by having a defined entry route whereby unsetting is initiated outside the area(s) supervised by the SAS and then completed within a maximum time. If so, a route from the entry point to the means of unsetting must be defined. Provided the correct entry procedure has been initiated only detectors in the defined route must be ignored so as to permit access to the unsetting device.

The maximum time to complete the unsetting procedure must be 60 seconds. There must be

an entry indication during this time. An alarm condition must be notified (locally and/or remotely) if unsetting is not completed within the maximum time.

When the unsetting procedure has been satisfactorily completed there must be a completion of unsetting indication to show that the SAS, or part thereof, has changed to the unset state. The completion of unsetting indication must be time limited in the case of an enhanced SAS.

If an intruder alarm condition occurs during the unsetting procedure (from a detector not on the entry route) the alarm condition must be notified by a warning device or indicated. When remote notification is included in the SAS, the alarm condition must be remotely notified if and when the entry timer expires.

6.3.8 Restoring

SAS must include the means necessary to restore the SAS or part thereof following an intruder, tamper or fault condition. Access to the means of restoring must be restricted through the use of authorisation codes (see 6.3.2).

6.3.9 Inhibit

SAS may include the means necessary to inhibit the functioning of individual or groups of functions. Access to the means of inhibiting must be restricted through the use of authorisation codes (see 6.3.2).

6.3.10 Isolate

SAS may include the means necessary to isolate individual or groups of functions. Access to the means of isolating must be restricted through the use of authorisation codes (see 6.3.2).

6.3.11 Test

SAS must include means for a user to carry out a functional test of intrusion detectors provided such tests are non destructive.

A walk test facility is an example.

6.3.12 Other functions

SAS may include the means necessary to carry out other operations not included in this code of practice provided these operations do not affect the mandatory operations of the SAS.

6.4 Operation

Processing and indication of intruder, tamper and fault signals must be in accordance with Table 2.

Table 2 – Processing and indication of intruder, tamper and faults signals

Category		Basic			Enhanced		
SAS status	**Inputs / Outputs**	**Intruder**	**Tamper**	**Fault**	**Intruder**	**Tamper**	**Fault**
Set	Indication	M	M	M	M	M	M
	Audible WD	M[(a)]	M[(a)]	NP	M[(a)]	M[(a)]	NP
	ATS message type [(b)]	Intruder	Intruder or tamper	OP as fault	Intruder	Intruder or tamper	OP as fault
Unset	Indication	M	M	M	M	M	M
	Audible WD	NP	NP	NP	NP	NP	NP
	ATS message type [(b)]	NA	OP as tamper	OP as fault	NP	OP as tamper	OP as tault
Key:	M = Mandatory, NP = Not Permitted, OP = Optional, NA = Not Applicable						
(a)	There may be circumstances where the audible WD remains silent (see 6.6).						
(b)	Applies to basic SAS when an ATS is included.						

6.5 Indications

6.5.1 General

The indications specified in Table 3 must be provided.

Table 3 – Indications

Indications	Basic	Enhanced
SAS set/part set	M	M
SAS unset	M	M
Intruder alarm condition	M	M
Intruder zone identification	M	M
Inhibited	OP	M
Isolated	M	M
Fault condition	M	M
Tamper condition	M	M
Setting*	M	M
Completion of setting*	OP	M
Entry indication (if applicable)*	M	M
Completion of unsetting*	OP	M
* These indications are time limited.		

6.5.2 Availability of indications

All indications specified in Table 3 must be available to users (operators of SAS and alarm company personnel).

The indications in Table 3 may be seen by non-users except for intruder alarm condition, intruder zone identification, inhibited, isolated, fault condition and tamper condition and except for SAS set/part and SAS unset in enhanced SAS.

SAS set/part set and SAS unset indications may be seen by non-users in basic SAS.

6.5.3 Cancelling indications

Indications, except time limited indications (*), specified in Table 3 must remain available until cancelled by a user.

6.6 Notification

SAS must include notification as shown in Table 4.

Table 4 – Notification requirements

Notification (Note 2)	**Basic**	**Enhanced**
Audible warning device (WD)	M (Note 1)	OP
Alarm transmission system (ATS) signalling to ARC	OP	M
Note 1: Having an audible WD is optional in a basic SAS if an ATS is included. Note 2: Additional WDs and ATSs may be included in basic and enhanced SAS.		

The average sound level at 3 metres from the audible WD must be not less than 70 dB(A).

Audible WD must operate for a minimum of 90 seconds unless a shorter period is demanded by local or national regulations. The maximum operating period must be 15 minutes unless a shorter period is demanded by local or national regulations. This applies to each operation of the WD.

If a strobe light operates the strobe can operate indefinitely until manually cancelled by a user.

Following the operation of audible WD, the SAS must re-arm so that the WD can operate again if another alarm condition occurs. However, the SAS must not re-arm more than twice within the same set period.

When a WD is installed as well as an ATS, operation of the WD may be delayed for a period of up to 10 minutes, or suppressed completely, providing the circumstances are agreed with the client.

It is not a requirement of this Code of Practice that the ARC has to confirm receipt of an alarm signal from the ATS before the operation of the WD is delayed or suppressed. Therefore such delay or suppression should be implemented with care and only by agreement with the client.

Remote notification of PPS faults may be delayed for a maximum of 1 hour.

Remote notification of PPS faults is not required for basic SAS.

6.7 Tamper security

6.7.1 Tamper protection

SAS components must provide means to prevent access to internal elements to minimise the risk of tampering.

All terminals and means of mechanical and electronic adjustment must be located within SAS component housings.

Housings must be sufficiently robust to prevent undetected access to internal elements without visible damage. Normal access must require the use of an appropriate tool.

Access to means that are provided to adjust the field of view of a detector must be made inaccessible to unauthorised persons.

6.7.2 Tamper detection

Table 5 specifies the types of tampering to be detected. Tamper detection must function in both set and unset states for all SAS.

Table 5 – Types of tampering to be detected

SAS Components	Basic	Enhanced
CE	O + R (Note 1)	O + R (Note 1)
ACE / PS / SPT	O	O
WD (Note 2)	O + R	O + R
Intrusion detectors (wired)	O	O
Intrusion detectors (wire-free)	O	O
Junction boxes	O	O
Key: O = Opened by normal means R = Removal from mounting		
Note 1: Detection of removal of the CE from the surface the CE is mounted on.		
Note 2: Detection of removal of the WD from the surface the WD is mounted on.		

6.8 Interconnections

Interconnections must be suitable for purpose and designed to provide a reliable means of communication between SAS components. Interconnections may be wired or wire-free.

Communication must be established between SAS components to verify that the communication necessary for the correct functioning of SAS can be accomplished as and when required (for example when an alarm signal or message is generated).

Interconnections must be monitored so that a failure of an interconnection is detected within the following time periods:

- Basic SAS - 4 hours
- Enhanced SAS - 2 hours

For SAS using wire-free interconnections there must be a method of monitoring that detectors are connected to the SAS when the setting procedure takes place.

6.9 SAS timing performance

6.9.1 Timing requirements

Intruder and tamper signals with an active period exceeding 400 milliseconds must be processed.

Fault signals with an active period exceeding 10 seconds must be processed.

Intruder, tamper and fault messages need only be present for the period necessary to ensure communication is successful.

6.9.2 Processing

Intruder, tamper and fault signals must be notified (by WD and/or ATS) within 10 seconds.

6.10 Event recording

The events specified in Table 6 must be recorded.

Table 6 – Events to be recorded

Event	Basic	Enhanced
Set/unset	M	M
Intruder alarm condition	M	M
Intruder zone identification	OP	M
Tamper condition	M	M
Detector fault	M	M
PPS fault	OP	M
APS fault	M	M
Interconnections fault	M	M
ATS fault	OP	M
WD fault	M	M
Overriding prevention of setting conditions	M	M
Changes to time and date	OP	M

The means used to record the mandatory events must be protected against the accidental or deliberate deletion or alteration of the contents.

The means of recording events must have a capacity complying with the requirements of Table 7.

Table 7 – Event recording - Memory

Capacity and endurance	Basic	Enhanced
Memory capacity – Minimum number of events	10	500
Minimum endurance of memory after SAS power failure	30 days	30 days

When the capacity of the means of recording is finite and the event recorder reaches maximum capacity, further events may cause the oldest events to be erased.

Enhanced SAS must record, in addition to the event, the time and date at which the event occurred.

Basic SAS do not need to record the time and date.

6.11 Power supply (PS)

6.11.1 Types of power supply

PS included in SAS may be of the following types:

Type A: A PPS, for example mains supply, and an APS recharged by the SAS, for example a rechargeable battery automatically recharged by the SAS.

Type B: A PPS and an APS not recharged by the SAS, for example a battery not automatically recharged by the SAS.

Type C: A PPS with finite capacity, for example a battery.

Where the PPS has finite capacity (e.g. a battery) the PS is considered to be Type C.

6.11.2 Requirements

The PS must be capable of supporting the SAS in all conditions including when recharging storage devices (batteries) within the periods specified.

The PS may be placed in one or more SAS components or in a separate housing.

A changeover between the PPS and the APS and back again, must not create an alarm condition, or otherwise influence the status of the SAS.

For SAS having a Type C PS, the PPS must be capable of powering the SAS for a minimum of 6 months in all the conditions of use. Type C PS must generate a fault signal before the voltage falls below the level required for the normal functioning of the SAS.

In all SAS using Type A or B PS, in case of failure of the PPS, the APS must be capable of powering the SAS for the periods specified in Table 8.

During the periods specified in Table 8, the PS must be capable of providing the power required for normal functioning of the SAS, including sufficient power to ensure the generation of all mandatory indications and notifications resulting from the processing of two separate intruder alarm signals.

Table 8 – Minimum duration of APS

Types of PS	Basic	Enhanced
Type A	8 hours	12 hours
Type B	24 hours	24 hours

For Type A and B PS, when a SPPS with automatic change over between the PPS and the SPPS is provided, the period the APS must power the SAS may be reduced to 4 hours.

7 ELECTRICAL SAFETY

7.1 General

SAS equipment and components must provide protection against electrical shock and consequential hazards by achieving compliance with the requirements of EN 60950-1 or EN 60065.

7.2 Portable appliance testing

Relevant SAS equipment and components must be tested at regular intervals.

It is recommended that relevant SAS equipment and components are tested at least every three months due to the environment in which they are installed and the fact that they are re-used on other sites.

8 INSTALLATION

8.1 Location of equipment and components

8.1.1 Location of CE and ACE

You must locate CE and ACE such that access by unauthorised persons is prevented, for example internally behind a locked door to the premises where the scaffolding is erected.

It is permissible to install ACE externally provided the ACE is within a lockable container with suitable environmental protection and the container is located within or above a supervised lift. The container must be securely fixed to the scaffolding and the lock on the container must have at least 1,000 differs.

A code lock requires a 3 digit code number such as 123 to achieve 1,000 differs.

8.1.2 Location of SPT

You must fix SPT securely to the scaffolding either within or above a supervised lift. In addition, you must locate SPT in positions consistent with reasonable access for servicing or repair.

SPT using radio telecommunications must be located such that the signal strength is strong

enough to ensure reliable notification of alarms to the ARC.

8.1.3 Location of detectors

You must locate detectors in accordance with manufacturers' recommendations and to provide the range and area of coverage determined as being necessary during the design stage.

8.1.4 Location of WD

You must fix WD(s) securely to the scaffolding either within or above a supervised lift. In addition, you must locate WD so as to give effective local audible notification of alarms and in positions consistent with reasonable access for servicing or repair.

When more than one WD is installed you must give consideration to installing the WDs at different locations.

8.1.5 Location of PS

You must locate PS such that access by unauthorised persons is prevented, for example internally behind a locked door to the premises where the scaffolding is erected.

You must ensure that there is adequate ventilation for PS and associated equipment so as to minimise the possibility of overheating.

You can connect SAS to the mains power supply either via an unswitched fused spur or via a plug and socket connection. Where a plug and socket connection is used it is advisable to include means (such as a socket cover) to prevent inadvertent disconnection from the mains power supply.

It is permissible to install PS externally provided the PS is within a lockable container with suitable environmental protection and the container is located within or above a supervised lift. The container must be securely fixed to the scaffolding and the lock on the container must have at least 1,000 differs.

8.2 Interconnections

All cables used for interconnections must be adequately supported and their installation must conform to good working practices. You must tie cables at regular intervals (for example to scaffolding poles). You must not wrap cables around the scaffolding poles and/or the fittings.

You must run cables in positions where there is the least risk of physical damage. If risk of physical damage exists you must consider whether the cables need to be provided with tamper protection, for example ducting, trunking or conduit.

It is good practice to tie cables to the inside ledger because outside ledgers often have cross braces to limit swaying of the scaffolding and these cross braces can cause damage to cables.

When tamper protection is made of conductive material, you must ensure that the materials are correctly earthed.

Electrical interference may cause unwanted alarms. You must ensure that extra low voltage signal cables do not run in close proximity to mains power cables or other low or high voltage cables.

Except where it is impractical to avoid doing so, you must not bring extra low voltage cables into a power supply container through the same entry point as any low voltage (mains) cables.

You must make all joints in interconnecting wiring in suitable junction boxes using either soldered, crimped, or screw-terminals.

9 INSPECTION AND FUNCTIONAL TESTING

9.1 Inspection

On completion of the installation you must inspect the SAS to confirm that the SAS has been installed in accordance with the system design proposal and the installation plan (if prepared).

You must record any deviations from the system design proposal such that you have a complete record of all the equipment and components that have been installed. This record must be available to office staff and to anyone visiting site (for example to carry out maintenance).

9.2 Functional testing

You must test the following to ensure that the SAS meets this code of practice, the system design proposal and the installation plan (if prepared):

- all wiring is correctly terminated;
- voltage and resistance at all appropriate points of the system are correct, which must be recorded (enhanced SAS only);
- alignment and operation of all detection equipment;
- configuration of the SAS including correct authorisation of access via input of appropriate data/codes;
- operation of the SAS including activation of any notification equipment (WD and SPT);
- SAS continues to work when the mains supply is disconnected.

You must make any necessary adjustments to detectors to achieve the required detection.

Movement detectors may require adjustment of range or coverage. Other types of detector may also require final adjustment prior to commissioning.

You must ensure that debris netting or similar used to cover the scaffolding for protection purposes does not interfere with the range and/or area of coverage of the detectors.

Debris netting or similar may need to be tied back or otherwise adjusted to ensure that it does not interfere with the range and/or area of coverage of the detectors.

Where SPT is installed you must check with the ARC to ensure that the test signals were successfully received.

10 COMMISSIONING AND HANDOVER

10.1 Commissioning

On completion of the testing you must place the SAS into operational mode ready for handover.

You must ensure that the SAS is fully operational before handing it over to the client or the client's representative (for example an authorised user of the SAS).

10.2 Handover

A person in your organisation with the appropriate training and experience must handover the SAS to the user. They must:

- demonstrate all aspects of the SAS operation to the client, including any necessary safety precautions;
- explain the procedures with the ARC (if applicable);
- provide clear and concise operating instructions;

  These could be written instructions given to the client/user or the instructions could be on stickers fixed to the CE/ACE (not including authorisation codes).
- train the users in the correct operation of the SAS and how to avoid unwanted alarms;
- arrange for any further training if necessary;
- ensure that users know the procedure for summoning assistance in the event of

system malfunction;

- ensure that the correct documentation (see 11.3) is given to the client to enable the system to be operated, adjusted and maintained.

10.3 Acceptance

Following the successful completion of the handover, where applicable the ARC must be informed that the SAS is fully operational. The responding company must also be informed and where necessary provided with any keys or authorisation codes.

Where possible you must request the client/user to sign a handover certificate stating the SAS has been installed in accordance with the system design proposal (including any agreed changes) and operates accordingly and that sufficient instruction and training has been provided to ensure the proper operation of the SAS.

If the client/user is not present at the time of handover, your handover person may sign the handover certificate indicating that the client/user was not present to sign the certificate.

You must leave a copy of the handover certificate with the client/user and/or otherwise send the client/user a copy of the handover certificate as soon as practicable.

11 DOCUMENTATION AND RECORDS

11.1 As-fitted document

You must prepare an as-fitted document for any SAS that will be installed for more than 3 months. The as-fitted document must be based upon the system design proposal and amended to reflect any changes to SAS design found to be necessary during the installation process.

The as-fitted document needs to be an accurate record of the installed SAS including all information relating to the equipment installed and its location.

If warranted by the size and complexity of SAS the as-fitted document must also include details of the types of cables used and their routing.

The as-fitted document must be made available to maintenance and service personnel.

You must keep track of all changes to the SAS during its period of service either by updating the as-fitted document when changes occur and/or by maintaining a complete schedule of all the equipment and components used in the SAS.

11.2 Schedule of equipment and components

If the SAS does not warrant an as-fitted document, due to the installation being for less than 3 months, you must maintain a complete schedule of all of the equipment and components used in the SAS including whenever a change takes place.

The schedule of equipment and components must be made available to maintenance and service personnel.

11.3 Documentation for client

You must provide the following documentation to the client:

(i) as-fitted document (for SAS installed for more than 3 months);

(ii) system operating instructions (which could be stickers affixed to CE/ACE);

(iii) name and telephone number of the installation and maintenance company, including details of the emergency call-out number (if different);

(iv) details for contacting the ARC responsible for initiating a response to the SAS;

(v) handover certificate.

Details of client procedures (if any) relating to audio, sequential and/or visual confirmation of alarm conditions may need to be provided if alarm confirmation is included in the SAS.

12 MAINTENANCE

12.1 General

It is advisable that you as the installing company should also carry out the maintenance.

Whatever arrangements are made, you as the maintaining company must have the means, including spare parts and documentation (see 11.3) to comply with this Code of Practice.

This recommendation does not place an obligation upon clients to have their SAS maintained; maintenance is a matter of agreement between you and the client or between the client and a separate maintenance company.

You must ensure the safe custody of all equipment and documentation pertaining to installations that are within your control.

Each service technician you employ must carry a range of tools, test instruments and other equipment to enable them to perform their functions satisfactorily. Specialist tools, test equipment and plant must be available for deeper investigation as necessary.

Not all eventualities can be foreseen and, in exceptional circumstances, a system or part(s) of a system may have to be left inoperable or disconnected whilst tools or replacement components are obtained (see 13.6).

Your organisation must be staffed so as to ensure that the requirements of this part of the Code can be met at all times. You must take the following factors into consideration the:

a) number of installations to be serviced;

b) complexity of the installations;

c) geographical spread of the installations in relation to the location of the maintenance company, its branches and its service personnel;

d) method of calling out service personnel outside normal office hours.

Service personnel must be adequately trained and training must be updated whenever appropriate.

12.2 Preventative maintenance

12.2.1 Frequency of visits

You must offer your client preventative maintenance in the case of every SAS that is installed for over three months.

Preventative maintenance visits should occur every 8 weeks though the frequency can be varied by agreement with the client.

Your representative must make preventative maintenance visits to the premises at the frequency that is agreed with the client.

SAS installed for a limited period of time (less than 3 months) might not require preventative maintenance.

12.2.2 Inspection

During each preventative maintenance visit, inspection of the following, with all necessary tests, and those rectifications which are practical at the time, must be carried out:

a) the installation, location and siting of all equipment and devices against the as-fitted document (see 11.1) or the complete schedule of all equipment and components installed (see 11.2);

b) the satisfactory operation of all equipment and components;

c) all cabling to ensure that it is properly secured at regular intervals;

d) the normal and standby power supplies, for correct functioning;

e) the CE, in accordance with your procedure;

f) the operation of any WD;

g) the operation of any ATS along with test signals through to the ARC.

Any items of inspection and rectification which for any justifiable reason are not carried out during the preventative maintenance visit must be completed as soon as practicable (typically within a maximum of 7 days).

Those parts of a system or any environmental conditions which are found during preventative maintenance to be the potential cause of reduced security (for example the erection of scaffolding without an SAS on an adjacent building) must be identified on the maintenance visit record (see 13.4).

12.3 Corrective maintenance

An emergency service must be available for all your installed SASs and you must keep the client informed of the telephone number for your emergency service facility.

You must locate and organise the emergency service facility so that, except under abnormal circumstances, your representative reaches the premises where the SAS is installed within the time period that you have agreed in writing with the client.

The time period for reaching the premises should not normally exceed 2 hours.

13 RECORDS OF MAINTENANCE

13.1 General

You must establish, retain and maintain a system of records relating to all the SAS you maintain including the information required by 13.2 to 13.6. It is essential that these records are protected from unauthorised access.

We draw your attention to the Data Protection Act in those cases where records contain information concerning individuals.

13.2 As-fitted document

You must keep the as-fitted document (or the schedule of all the equipment and components installed) up to date and the document (or schedule) must be available to your maintenance technician for each corrective or preventative maintenance visit.

13.3 Historical record

You must keep a historical record with the date of every visit, any faults found and the action taken. Details of every fault reported to you must be included, together with details of any action taken, and, if known, the cause.

You must keep this information for at least 2 years after the last event to which it refers.

13.4 Preventative maintenance record

You must enter the results of a preventative maintenance inspection on a maintenance visit record. A record of checks and work carried out must either be given to the client at the time of maintenance or provided within 10 days.

This record may be in electronic form if acceptable to the client.

You must keep this information for at least 15 months after the inspection to which it refers.

13.5 Corrective maintenance record

You must keep a record of the date and time of receipt of each request for emergency service, together with the date and time of completion of corrective maintenance and the necessary action(s) carried out.

You must keep this information for at least 2 years after the emergency call to which it refers.

You must enter the result of a corrective maintenance inspection on a maintenance visit record. A record of checks and work carried out must either be given to the client at the time of maintenance or provided within 10 days.

This record may be in electronic form if acceptable to the client.

You must keep this information for at least 15 months after the inspection to which it refers.

If a preventative maintenance inspection is made at the same time as the corrective maintenance visit, you should complete separate visit records.

13.6 Temporary disconnection record

You must keep a record of any temporary disconnection of the SAS or of any component part(s) of it. This must identify which part(s) of the system and the associated equipment is not operable. You must give the reason for the disconnection and the date and time of disconnection.

An example of a disconnection would be where a detector is not operating correctly and a replacement is not available at the time.

Wherever possible you must obtain a signed authorization for each disconnection from the client or their representative.

You must keep this authorization for at least 3 months after reconnection.

You must always seek to resolve a disconnection as quickly as possible. You must record the time of reconnection and also confirm to the client that the SAS is operating normally in full working order.

14 MANAGEMENT OF UNWANTED ALARMS

14.1 System design

System design has a bearing on unwanted alarms. Therefore your design proposals must seek to minimise unwanted alarms from installed SAS.

14.2 Installation

Installation has a bearing on unwanted alarms. Therefore your installation methods must seek to minimise unwanted alarms for example by tying back debris netting and/or other materials used to provide protection from the scaffolding.

14.3 Administration

You must appoint a person within the company who is responsible for the performance of SAS. The appointed person must have a right of direct access to the Chief Executive/ Managing Director and have sufficient experience and authority within the company to achieve the objectives of monitoring, analysing and reducing unwanted alarms. In the case of a small company, the Chief Executive/Managing Director may personally undertake this role.

The appointed person is referred to as the Systems Performance Manager (SPM).

The SPM must ensure that the following tasks are carried out effectively:

a) Monitoring of the standards of surveying and installation to ensure that:
    1) system design proposals meet the requirements of your company's policies and result in systems which are unlikely to generate unwanted alarms;
    2) clients are instructed on how to minimise unwanted alarms;
    3) comprehensive training for your staff is maintained.

b) Maintenance of all SAS at intervals in accordance with NCP 115.

c) Identification of abnormalities and trends likely to lead to unwanted alarms.

d) Identification of troublesome systems, equipment and practices.

e) Identification of transmission path problems.

f) Keeping statistics on unwanted alarms.

g) Monitoring of client complaints.

h) Monitoring trials on new equipment, with particular reference to unwanted alarms.

i) Working with operational management to keep unwanted alarms to a minimum.

14.4 Documentation and training

For each installation, you must provide the client representative(s) with sufficient written instructions, reinforced by adequate training, to ensure correct operation can be achieved.

You must ensure that each service call following notification of an alarm condition is recorded in an appropriate manner, for example by using a corrective maintenance form, identifying any unwanted alarms.

You must aim to establish the prime cause of the unwanted alarm and record this on the corrective maintenance report, as the report forms a source document for the monitoring and categorization of unwanted alarms.

You must have a system of categorizing unwanted alarms in order to establish and monitor the main reasons for unwanted alarms.

Each office at which corrective maintenance call-out requests are received and recorded must have a system in place for monitoring all remotely notified alarm conditions and all other alarm conditions (e.g. local audible) reported to the alarm company.

The monitoring system may be manual or computerized but, as a minimum, it must:

a) form the source document for the identification of troublesome systems and the analysis of recurring defects;

b) in the case of remotely notified SASs, require the ARC to report daily;

In the case of Saturdays, Sundays and public holidays, the report may be delayed to the following office day.

c) provide a register of all remotely notified alarm conditions and of all other alarm conditions (e.g. local audible) that have been reported to you, and discriminate between genuine alarms and unwanted alarms for monthly analysis.

In all documentation and reports, the prime cause of the unwanted alarm must be reported, not its effect.

14.5 Statistics relating to remotely notified SAS

You must compile and collate a record of all remotely notified alarm conditions as follows:

a) You must record details of all remotely notified alarm conditions and categorize them as either genuine alarms or unwanted alarms.

b) Monthly alarm reports must be compiled on an overall company basis, and for each office, including categorization of unwanted alarms so that common problems can be identified. Each office must retain copies of the statistics relating to its own area of responsibility, which must be made available for inspection.

c) The SPM must oversee the production of the monthly analyses and ensure that the information is sent to senior executives and others within the alarm company, as appropriate.

14.6 Management procedure for unwanted alarms

You must have in place a documented process by which the occurrence of unwanted alarms is identified.

This process must include a means by which any installation giving rise to an unwanted alarm, or more than three unwanted alarms in a rolling 30 day period, is identified and reported to the appropriate levels of management for information and action. The aim of the management procedure for unwanted alarms is to identify troublesome installations and to overcome the problem as quickly as possible.

14.7 Diagnosis of unwanted alarms

You must provide personnel involved in the execution and management of corrective maintenance with training in both the means to identify unwanted alarms and the necessary escalation procedures for their management. This training must be documented and the records retained.

National Security Inspectorate
Sentinel House, 5 Reform Road
Maidenhead, Berkshire SL6 8BY
Telephone: 01628 637512 Fax: 01628 773367
E-mail: nsi@nsi.org.uk
Web: www.nsi.org.uk