NSI Code of Practice for the design, installation, commissioning and maintenance of Access Control Systems

NCP 109 Issue 3

June 2021

National Security Inspectorate
Sentinel House,
5 Reform Road
Maidenhead
SL6 8BY
Website: nsi.org.uk

Contents

1 Scope 4
2 References 5
3 Terms, definitions and abbreviations 5
3.1 Terms and definitions 5
3.2 Abbreviations 9
4 Classification of access points 10
4.1 General 10
4.2 Risk assessment 10
4.3 Access point classification 11
5 Design 14
5.1 Survey 14
5.2 Credentials 16
5.3 Functionality 17
6 Equipment selection and installation 22
6.1 Control 22
6.2 Access point hardware 22
6.3 Environmental protection 24
6.4 Power supplies 24
7 Installation 26
7.1 Cables 26
7.2 Network security 28
8 Commissioning, handover and documentation 29
8.2 Handover 30
8.3 Documentation 31
9 Maintenance 32
9.1 Resources 32
9.2 Preventive maintenance 33
9.3 Corrective maintenance 34
9.4 Records 34

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

Introduction

This Code of Practice is to be read in conjunction with the NSI Regulations relating to approval by NSI, to the NACOSS Gold 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.`

An Access Control System (ACS) consists of credential recognition equipment and user interface(s) such as a token and reader (e.g. Card, token reader, keypad, biometrics etc.), electronically activated entrance release hardware and, in certain systems, means for central control and/or monitoring.

The objectives of this Code of Practice are to:

- establish and maintain minimum standards of best practice for the design, installation, commissioning, handover and maintenance for ACS(s);
- provide a framework to assist purchasers, installers and users in establishing their requirements with suppliers;
- assist specifiers and users in determining the appropriate level of security required for a given application; and
- assist system designers in meeting specifier or user requirements.

The successful operation of an ACS 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 the security of credentials, such as tokens and of information regarding the system, its design, installation and method of operation and to ensuring adequate maintenance, to preserve the security of access.

Your attention is drawn to:

- the Equality Act 2010, which aims to protect disabled people and to prevent disability discrimination, and the Disability Discrimination Act 2005 (as amended), the Disability Equality Duty of which continues to apply;
- relevant national building regulations;

- BS 7273-4 – Code of practice for the operation of fire protection measures. Part 4. Actuation of release mechanisms for doors;
- BS 7671, Requirements for Electrical Installations (also known as the "I.E.T Wiring Regulations"); and
- Loss Prevention Standard LPS 1175, Requirements and testing procedures for the LPCB approval and listing of intruder resistant building components, strongpoints, security enclosures and free-standing barriers.

Note: The BS EN 50133 series of standards have been withdrawn and replaced with the BS EN 60839-11 series of standards. At the time of publishing this document, the BS EN 60839-11 series of standards had not become widely specified due to in part to the lack of component certification, NSI have taken the decision not to implement a certification scheme for these standards.

NSI will keep this decision under review and will develop a scheme if, in future, there is sufficient interest within the marketplace for certification to the BS EN 60839-11 series.

1 Scope

This Code of Practice contains requirements and recommendations for the design, installation, commissioning and maintenance of electronic ACS(s) used for physical access (entry and exit) in and around buildings and protected areas. It is intended for use in security applications for the granting of, or preventing, access and includes requirements for logging, identification and control of information; it does not include requirements for access point actuators and sensors.

The following are outside the scope of this Code of Practice and must not be certificated:

a) Systems where a person makes the decision as to whom may enter or exit the premises or protected area.

   Example: A door entry telephone system used in conjunction with an electrically operated.

b) Lock triggered by a person using a manual switch/button.

c) Where the entire system is housed within a single unit/housing controlling a single access point and located at the access point being controlled, with no interconnections to control equipment or system management database located away from the access point. This exemption does not include systems with more than one access point for the controlled area.

   Note: The recognition device and or request to exit button/switch used for this single access point can be installed external to the single unit/housing.

d) Purely mechanical locking devices.

Note 1: A unit/housing containing a bolt or pin and the striking plate or box into which the bolt or pin is thrown is considered to be a single unit/housing.

Note 2: Electrical wiring, radio links, laser-links, fibre-optic links and mains borne signalling are examples of interconnections (but refer to Note 3 below which allows an exemption for electrical supply failure auto-release facilities).

Note 3: The provision of an auto-release, such that the access point releases in the event of failure of an electrical supply system, is not regarded for the purposes of c) above as amounting to an interconnection to control equipment or system management database located away from the access point.

2 References

The following referenced standards are indispensable for the application of this Code of Practice

BS EN 60529 - Degrees of protection provided by enclosures (IP code)

BS EN 62262:2002 - Degrees of protection provided by enclosures for electrical equipment against external mechanical impacts (IK code)

BS 7273-4 - Actuation of release mechanisms for doors

3 Terms, definitions and abbreviations

3.1 Terms and definitions

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

3.1.1 Access Control System (ACS)

An electronic system restricting entry into and/or exit from a controlled area.

3.1.2 Access Control Unit (ACU)

Device which processes data from the reader to authorise or reject access to the secure area.

3.1.3 Access level

Set of rules used to determine where and when a credential has authorised access to one or more access points and which may include special passage conditions such as specific access point permitted open times.

3.1.4 Access point

The position at which access can be controlled by a door, turnstile or other secure barrier, and includes any associated recognition device, sensors, access point hardware, and physical barrier e.g. a door set.

3.1.5 Access point hardware

Mechanical and/or electro-mechanical devices capable of securing and releasing the access point.

3.1.6 Adversary

Person or persons deliberately attempting to overcome the ACS with malicious intent.

3.1.7 As-fitted document

Document detailing the function and features of the installed ACS.

3.1.8 Biometric

Any measurable, unique physiological characteristic or personal trait that is used as a credential to recognise and verify the identity of an individual's dynamics.

Examples: Fingerprint, hand or face geometry, retinal/eye pattern, voice pattern or signature or keyboarding dynamics etc..

3.1.9 Central processor

Equipment directing the functions of a number of ACUs, changing data for individual ACUs and/or monitoring an ACS.

3.1.10 Commissioning

The completion of installation and final checking of an ACS prior to its handover.

3.1.11 Common code

A sequence of characters (alpha and/or numeric) unique to a particular keypad-operated ACS and used by every user of the system.

3.1.12 Common token

A token unique to a particular ACS, or reader, with all user tokens identical.

3.1.13 Controlled area

The area accessed by the presentation of a valid credential.

3.1.14 Corrective maintenance

Unscheduled maintenance of an ACS, or part thereof, carried out in response to the development of a fault.

3.1.15 Credential

Any token or memorised information or biometric used to identify an individual to an ACS in order to verify user access.

Examples: Access fob, card, mobile phone, etc.

3.1.16 Degraded mode

Operating mode of the ACS where not all processing rules are being applied.

3.1.17 Equal Error Rate (EER) or Crossover Error Rate (CER)

The rate at which accept and reject errors are equal.

See also 3.1.20 and 3.1.21.

3.1.18 Fail locked

The securing of a locking mechanism at an access point in the event of total loss of power to the locking mechanism.

3.1.19 Fail unlocked

The release of a locking mechanism at an access point in the event of total loss of power to the locking mechanism.

3.1.20 False Acceptance Rate (FAR)

A measure of the likelihood that a biometric security system will incorrectly accept an invalid credential.

3.1.21 False Rejection Rate (FRR)

A measure of the likelihood that a biometric security system will incorrectly reject a valid credential.

3.1.22 Global anti-passback

A system feature which applies anti-passback rules at any authorised access point of a controlled area even when the reader is connected to a different access control unit.

3.1.23 Hard anti-passback

A system feature which generates an alert and denies further access to a particular credential following violation of anti-passback rules.

3.1.24 Keypad

A data entry point for the input of a numeric or alphanumeric code into an ACS.

3.1.25 Maintenance company

An organisation providing maintenance of an ACS.

3.1.26 Normal mode

Operating mode of the ACS.

3.1.27 Open time

Time duration for an access point to be open before an alert/indication is generated.

3.1.28 Operational needs

Specific requirements of an organisation that are met by the provision of an ACS.

3.1.29 Personal Identification Number (PIN) code

A sequence of characters (alpha and/or numeric) allocated to an individual user of an ACS.

A PIN code is unique to each user.

3.1.30 Preventive maintenance.

Routine servicing of an ACS carried out on a scheduled basis.

3.1.31 Reader

Device for the input of credentials.

3.1.32 Recognition

Process by which the ACS determines the credentials prior to comparing them against the processing rules.

3.1.33 Release time

The time that the release mechanism is electrically released.

3.1.34 Radio-frequency identification (RFID)

Contactless device for transmitting and/or receiving credential information by radio waves.

3.1.35 Soft anti-passback

A system feature which, upon granting access, generates only an alert following violation of anti-passback rules.

3.1.36 Structured cabling

Cabling installed as part of the network infrastructure of a building to support data and voice services.

3.1.37 System Design Proposal

Document detailing the functions and features of the proposed ACS.

3.1.38 Tamper detection

A means for the detection of deliberate interference with a component of an ACS.

3.1.39 Time zone

A period of time during which system operating requirements are changed, such as refusal of access outside normal working hours or PIN override.

3.1.40 Token

Portable device containing a readable unique identifier (credential) that can be associated with a user's data and access rights stored within the electronic access control system.

3.1.41 Transaction

A recognisable event occurring within an ACS, such as the release of a door following presentation of a valid credential or the generation of a door alarm report.

An example of a door alarm report would be an 'access point held open' alarm.

3.2 Abbreviations

ACS Access Control System

ACU Access control Unit

CIE Control and Indicating Equipment

LAN Local Area Network

PoE Power over Ethernet

UPS Uninterruptable Power Supply

UTC Coordinated Universal Time

WAN Wide Area Network

4 Classification of access points

4.1 General

Access points are classified by the requirements for successful legitimate access and the level of security that they provide.

The access point class can change according to risk, e.g. where the risk is higher during hours of darkness a higher class may be required for that period of time.

For each class, access may be granted using credentials permitted at higher classes, but not when using credentials only permitted at lower classes.

The classification of access points and associated level of security shall be determined as the result of a site risk assessment which may be carried out in conjunction with the customer.

The location and classification of each of the access points making up an ACS must be identified in the system design proposal and in the as-fitted document.

4.2 Risk assessment

A risk assessment shall be carried out and documented as a stand-alone document or as part of the system design proposal.

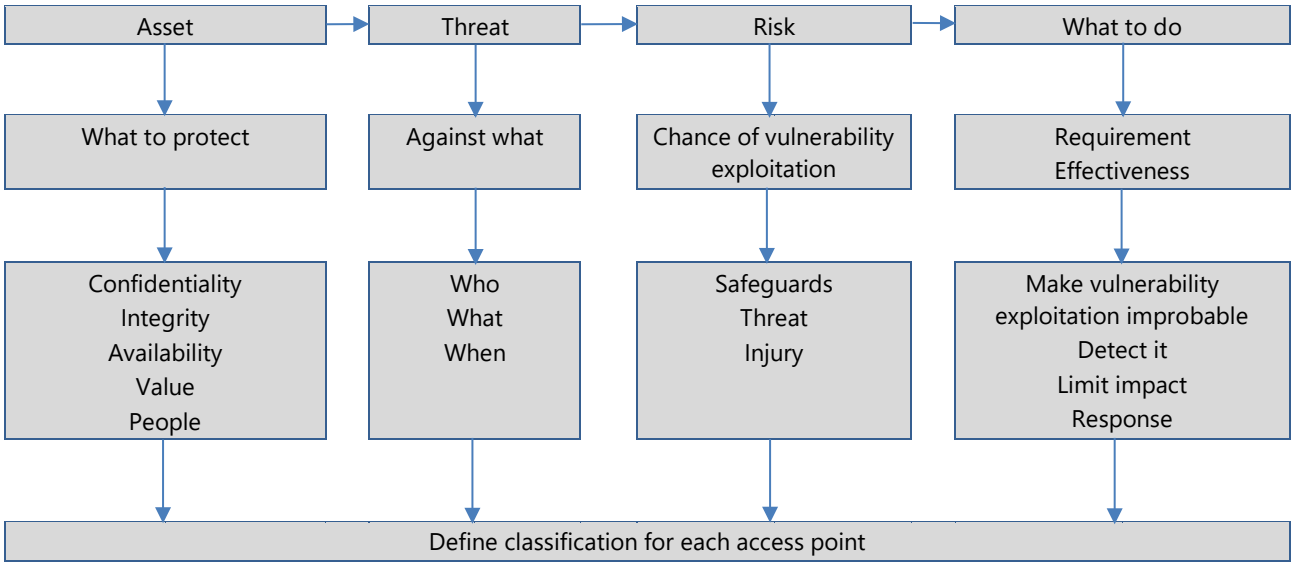
During the risk assessment, consideration must also be given to the threat of the access control system being compromised through accidental or malicious actions.

Any risks to the continuing operation of the system must be mitigated or notified to the customer.

Risks may include vandalism of cables or access point hardware, loss of power, remote access, unauthorised access to the ACS operating system(s) and cyber-security threats.

The key considerations when carrying out the risk assessment are shown in Figure 1.

Figure 1 - Risk assessment chart (Informative)



4.3 Access point classification

The value of the assets requiring protection and the determination (knowledge/skills) and methods of attack of persons intending to bypass the system (adversaries) are to be taken into account when selecting the class of each access point during the risk assessment. Refer to Table 1 for examples of typical applications for each class.

Table 1 - Example classification

Class	I	II	III	IV
Risk Level	*Low*	*Low to Medium*	*Medium to High*	*High*
Application	*Operational needs* *Protection of low value assets*	*Operational needs* *Protection of low to medium value assets*	*Operational needs* *Protection of medium to high values commercial assets*	*Operational needs* *Protection of very high value commercial or critical infrastructure*

Class	I	II	III	IV
Skill level of adversaries/attackers	*Low skill, low knowledge of ACS, low knowledge of token & IT technologies Low financial means for attack*	*Medium skill & knowledge of ACS, low knowledge of token & IT technologies Low to medium financial means for attack*	*High skill & knowledge of ACS, medium knowledge of token & IT technologies Medium financial means for attack*	*Very high skill and knowledge of ACS, high knowledge of token & IT technologies High financial means for attack*
Typical examples	*Hotel*	*Commercial offices, small businesses*	*Industrial, administration, financial*	*Highly sensitive areas (Military facilities, government, R&D, critical production areas)*

Each credential reader must fulfil the requirements detailed in Table 2 according to the defined access point class.

Access shall be denied after each attempt to gain access using invalid credentials.

Suspending access after several sequential incorrect attempts to gain access may be considered.

In normal mode of operation the system shall use complete token information (facility code and card number, or unique card number) for recognition. In degraded mode of operation the system may use partial token information (e.g. facility code only) for recognition.

Where the token identity number is readable on the token, it must not be a direct representation of the credential coding used to gain access.

Table 2 - Recognition requirements

	Class I	Class II	Class III	Class IV
Access granted following the input of a correct common code of not less than 10,000 differs or Access granted following the input of a correct PIN code of not less than 10,000 differs	M	N/P	N/P	N/P

	Class I	Class II	Class III	Class IV
Access granted following the input of a correct PIN code of not less than 1,000,000 differs or Access granted following the presentation of a valid unique token to a reader.	OP	M	N/P	N/P
Access granted following the input of a correct PIN code of not less than 10,000 differs AND the presentation of a valid unique token to a reader or Access granted following the presentation of a valid biometric to a reader.	OP	OP	M	N/P
Access granted following the presentation of a valid biometric to a reader AND the presentation of a valid unique token using radio frequency identification (RFID) *or* Access granted following the presentation of a valid biometric to a reader AND the presentation of a valid unique token to a reader AND the presentation of a correct PIN code of not less than 10,000 differs or Access granted following the presentation of a valid biometric to a reader AND the presentation of a valid unique token to a reader AND the presentation of a correct PIN code of not less than 10,000 differs *(See Note)*.	OP	OP	OP	M
OP = Optional M = Mandatory NP = Not Permitted				

Note:
10,000 differs requires a 4-digit code number such as 1234.
1,000,000 differs requires a 6-digit code number such as 123456.

RFID must not rely on recognising the Chip Serial Number (CSN) only. Also, the code to be read must be stored in the memory of the card.

5 Design

5.1 Survey

A survey may be a physical inspection of the areas to be controlled at the premises, a review of plans or design drawings or a combination of both.

As the performance and reliability of an ACS is determined by several factors, it is of importance that as much information as possible is gathered to produce a robust design, addressing the environmental, physical and the operational needs of the end user.

It is imperative that, wherever possible, all relevant interested parties within the organisation or who provide relevant services to the organisation should be consulted. This may include the IT department or a third-party IT support provider etc.

The classification of each access point shall be determined taking into consideration the needs for control of access and egress, and the overall level of security to be provided at each access point.

Access points of different classes can be used on the same system provided that any common system components for each access point meet the requirements for the highest class that they are associated with.

The suitability of any ACS must be considered in relation to the fire strategy for the premises and the need for safe egress in emergency situations.

Where applicable, the methods to be used to release all the access points (for example green coloured single action emergency exit buttons, or break glass units, on the secure side of access points) must be agreed and these must be documented in the system design proposal and the as-fitted document.

The means to release electronically secured doors and powered sliding doors in the event of a fire should meet the recommendations of BS 7273-4.

Access points must not:

a) conflict with building/fire regulations;

b) restrict exit in such a way as to endanger people in an emergency.

The following aspects must be considered when designing an ACS to meet the risks detailed in the documented risk assessment.

a) The number of access points required to provide the required level of security for the controlled area or areas.

b) How access points will operate in the event of mains power failure and the period, or number of transactions, required in such situations.

c) Whether access points should fail locked or fail unlocked.

Locking mechanisms can have two modes of operation under system failure conditions, 'fail unlocked' and 'fail locked'. Where egress is available by purely mechanical means, the fail locked mode may be acceptable but where exit is granted by electrical means, the 'fail unlocked' mode may be mandatory to meet safety legislation.

d) Whether additional locking devices not controlled by the ACS should be fitted on external doors.

e) Whether a key override is required for any critical doors to facilitate access in an emergency;

In the case of a complete power failure it may be necessary to provide a key override to a critical door(s) with the key(s) kept in a safe place outside the controlled area.

f) Whether ACUs should have a standalone feature and retain data in the event of a communications or power failure.

g) Whether standby power is needed for critical system components, such as servers holding database or application software.

h) Whether a UPS should be provided to any systems that do not reboot to a fully operational condition following a total power failure.

i) The choice of access control technology, including monitoring and additional functionality (e.g. access point left open alarm, door forced alarm, anti-passback, read in/read out etc.) to provide an appropriate level of security for the risk to be protected.

j) The choice of electronic equipment and its siting, taking into account environmental conditions and the potential for malicious damage.

k) The selection of access point hardware, taking into account the volume of traffic, environmental conditions and the level of physical security required.

l) The numbers of users, access levels and time zones required, taking into account both present and predicted numbers of users and their needs.

m) The need to site equipment in a secure area e.g. controllers and printers.

n) The implementation of suitable security controls to prevent unauthorised access to the system.

This may require system components to be physically protected and/or technical measures taken to protect the network, operating and application systems that make up the ACS.

o) Whether existing LAN and/or WAN infrastructure is suitable for use.

p) Any arrangements for network access and additional security features or protocols that may be required.

q) Account should be taken of any client's requirements or restrictions for connecting devices such as laptops directly to the client's network.

r) Where applicable, written permission should be obtained from the user to retain any user account and password information and permission to remotely access the system if these are necessary for ongoing maintenance purposes.

s) Ease of access to ACUs and power supplies for preventive and corrective maintenance.

5.2 Credentials

Credentials may be thought of in terms of something you know (code), something you have (token) or something you are (biometric).

The security, size and durability of a credential are dependent upon the technology used to encode it and the equipment required to read it.

Credential technology should be selected as appropriate to the protected risk and the needs of the customer.

Listed below are some examples of common types of available credential:

- *Memorised information such as common codes and PIN codes, which are input by hand onto a keypad*
- *Radio Frequency Identification (RFID)*
- *QR Code / Barcode*
- *Near Field Communication (NFC)*
- *Biometric*

When selecting a battery powered active token, the life span of the battery as well as the environment in which the token will be required to operate and the frequency of its use must be taken into account.

5.3 Functionality

Access control equipment must provide appropriate levels of functionality for each class of access point in accordance with clauses 5.3.1 to 5.3.7.

Where functions are indicated in the table associated with each section as being optional, their inclusion or omission must be determined by the risk assessment and/or operational requirement.

5.3.1 Time synchronisation

The system time must auto update for changes between any daylight-saving offsets and UTC unless otherwise specified.

Where there is a requirement to maintain an accurate system time, this may be provided using a network time source or the provision of instructions to the user on how to manually update the system time.

5.3.2 Access control

Access into a controlled area must be provided and granted conditional upon credential validity.

Access control functions must be provided in accordance with the classification of the access point in accordance (see Table 3).

Table 3 - Access control functions

	Class I	Class II	Class III	Class IV
Anti-passback	OP	OP	OP	M
Anti-passback override/disabling	OP	OP	OP	M
Credential expiry date	OP	OP	M	M
OP = Optional M = Mandatory				

5.3.3 Release timing

The access point must re-lock on expiry of the release time.

The release time of the access point must operate in accordance with the classification of the access point (see Table 4).

Table 4 - Release timing

	Class I	Class II	Class III	Class IV
The release time shall be system defined	OP*	OP*	NP	NP
The release time shall be configurable per access point	OP*	OP*	M	M
OP* = One of the options in the identified grouping (gray area) should be considered M = Mandatory NP = Not Permitted				

5.3.4 Access point status monitoring

The status of the access point must be monitored in accordance with the classification of the access point (see Table 5).

Table 5 - Access point status monitoring

	Class I	Class II	Class III	Class IV
Access point secure / insecure status monitoring.	OP	OP	M	M
Access point held open time (Door held open)	OP	OP	M	M
Door forced monitoring	OP	OP	M	M
OP = Optional M = Mandatory				

5.3.5 Overriding requirements

The ACS shall not prohibit the free exit triggered by emergency systems (e.g. fire alarms).

The user requirements or risk assessment may identify a need for manual commands that override the pre-configured rules of the ACS.

5.3.6 System self-protection requirements

Components of the ACS that provide central control, processing and indicating functions must be installed in a suitably secure location(s) offering protection against tampering or be provided with means to detect and notify users when tampered with.

Access point equipment that is installed outside of the controlled area or that could be accessed from outside of the controlled area must be provided with an adequate level of tamper protection in accordance with Table 8 where opening of the enclosure or removal from mounting would allow manipulation of the internal components resulting in access being granted.

Tamper detection shall occur before the tamper mechanism can be defeated.

Means of access to the internal elements of components of an access control system shall require the use of a tool in accordance with Table 6.

Note: A key could be considered as a tool if it is proprietary to the manufacturer.

The customer should be advised to ensure physical access controls are in place to prevent unauthorised access to the secure location.

Following a total loss of power, automatic restart of the access control system is required upon power source restoral.

If full functionality of any of the access control system components cannot be restored (e.g. data corrupted or lost) following the automatic restart, a trouble condition shall be notified.

Either failure or restoration of the communication channel with any CIE shall not result in the release of an access point.

Where an ACS incorporates equipment for central indication, logging and control (e.g. networked PC), the loss of communication between the access point controller and the central equipment should not prevent the access decision.

This would require the processing rules to be stored within the access point controllers or for there to be a replicated database within each access point controller.

Where access point configuration is stored in access point readers (e.g. via dip switches) they should not be visible external to the reader once the reader is installed.

Visual or audible indication of keystrokes shall not be able to identify which key is depressed but shall all be identical in pitch and duration for each key action.

System administration including configuration shall only be logically accessed with the use of valid credentials (e.g. password, token).

Any default ACS passwords must be changed prior to handover to the client and where required, the client must be notified of the new password(s).

Consideration should be given to using secure password management practices.

There shall be levels of access hierarchy that categorize the ability of operators to perform a range of functions in the system relevant to their roll.

Consideration should be given to having a timer to prevent configuration access after a period of inactivity.

In all classes, where data is encoded within tokens then this must be protected against unauthorised change, for example, by requiring an authorised person to enter a password to gain access to software at the central processor where changes are made.

In all classes, PIN codes shall be protected from repeated attempts to enter the correct code, for example, by limiting to a maximum number of attempts.

The features detailed in Table 6 must be provided according to the access point classification.

Table 6 - System self-protection requirements

	Class I	Class II	Class III	Class IV
Detection of opening of enclosure.	OP	M	M	M
In case of loss of communication between the access control unit(s) and the CIE, the access point control unit should be capable of storing and subsequently transmitting upon restoration of communications a minimum number of events per access point	N/A	OP	M	M
Communication between control unit and the ACS components shall be monitored.	N/A	OP	OP	M
Access to the components shall require the use of a tool.	OP	M	M	M
OP = Optional M = Mandatory N/A = Not Applicable				

When biometrics are used, the system will normally have a decision threshold adjustment that can modify the False Acceptance Rate (FAR) and False Rejection Rate (FRR). These settings should be discussed with the user to ensure the balance between the need for security and the need for operability is met. If the FAR is high, it will be more likely that an unauthorised person will be able to gain access using their biometric. However, if the FRR is set too high, this may make the system too sensitive and prevent authorised users accessing the secure location.

Where the customer has been provided with the means to adjust biometric readers, the access to the means of adjustment must be protected against unauthorised change (for example by requiring an authorised person to enter a password) and sufficient information to enable them to understand the consequences of making adjustments must also be provided.

For example, the customer might be provided with information about the adjustments of their biometric readers that are acceptable and/or unacceptable for their security application.

5.3.7 Indication and annunciation

Visual and/or audible indication must be given at each access point when access is granted or denied.

Indication of the lock status at each access point may also be required based on the risk assessment.

Central indication and annunciation facility requirements in Table 7 must be provided according to the access point classification.

Table 7 - Central indication & annunciation

	Display	Alert	Log	Class I	Class II	Class III	Class IV
When access is denied	●		●	OP	M	M	M
When access is granted			●	OP	M	M	M
Access point open status following access granted			●	OP	OP	M	M
Access point remain closed status following access granted.	●	●	●	OP	OP	OP	M
Scheduled or manual (through control system) access point status change			●	OP	OP	M	M
Power supply fault/failure	●	●	●	OP	OP	M	M
Primary power restoration	●		●	OP	OP	M	M
Entering and leaving configuration mode	●		●	OP	M	M	M
Loss of communication between access control unit and central processor	●	●	●	OP	M	M	M
Restoration of Access point held open/forced			●	OP	OP	M	M
All events shall be identified by type, location, time and date of occurrence			●	OP	OP	M	M
Tamper detection (where applied)	●	●	●	OP	M	M	M
Access point forced open	●	●	●	OP	M	M	M
Access point held open	●	●	●	OP	M	M	M
Reader off-line condition	●	●	●	OP	OP	OP	M
Locking device abnormal status	●	●	●	OP	OP	OP	M

	Display	Alert	Log	Class I	Class II	Class III	Class IV
Alerts received at the central processor/monitor that require acknowledgement and are subsequently acknowledged by the operator.	●	●	●	OP	OP	M	M
All operator initiated changes			●	OP	OP	OP	M
OP = Optional M = Mandatory NP = Not Permitted The requirement to display, alert and/or log a particular event is indicated by a "●" in the relevant column.							

6 Equipment selection and installation

6.1 Control

Control equipment must be capable of providing the required functionality that has been determined by the risk assessment and survey during the design process.

6.2 Access point hardware

Access point hardware must be capable of providing the required functionality and degree of physical security that has been determined by the risk assessment and survey during the design process.

Any manual emergency release controls should be clearly distinguishable from any installed fire alarm call points and should meet the requirements of BS 7273-4

The risk assessment must consider the physical strength and suitability of any existing or customer provided hardware associated with each access point and identify any potential shortcomings that may require attention or action by the end user. Any such findings must be documented in the risk assessment.

When considering the physical strength of access points, account should be taken of the following:

a) The strength of doors and frames.

b) The physical fit of the door in the frame.

c) The strength of hinges and supporting fixings.

d) The effect that the access point hardware may have of the physical strength of the access point.

Access point hardware such as locking mechanisms should be selected appropriate to the strength of the door and its frame.

The physical strength of the access point should not be reduced by the fitting of such hardware.

Where the fitting of access point hardware to meet the specific class of access point, as identified in the risk assessment, would result in a reduction in the physical strength of the access point, there should be consultation with the end user to ensure that suitable reinforcement of the access point is undertaken.

Where the reinforcement of the access point is not possible, the classification of the access point may need to be reduced. (e.g. where the risk assessment identifies that an access point of class III is required, but the physical strength of the access point would only permit the fitting of access point hardware meeting the requirements of class II etc.). Any such circumstance should be documented in the system design proposal, as-fitted documentation and risk assessment.

e) The minimum holding force of any powered locks required.

f) The holding force required should be suitable to protect against the risk identified in the risk assessment.

Holding forces per access class are typically considered to be:

- *Class I Holding Force = 3kN/300kg or more*
- *Class II Holding Force = 5kN/500kg or more*
- *Class III Holding Force = 7kN/700kg or more*
- *Class IV Holding Force = 10kN/1000kg or more*

g) The characteristics of the door such as rebate and double rebated doors.

h) Any necessary safety precautions for glass or other special doors.

i) Door closing devices should be sufficient to close and lock the door under normal circumstances.

j) The fire resistance of the access point.

Not all access point hardware (e.g. locks and locking mechanisms) is suitable for use on fire doors, therefore particular regard should be given to the integrity of the fire resistance and how it may be affected by the fitting of the access point hardware and any associated cabling etc. Advice should be sought from the fire door manufacturers regarding the possible effect on the integrity of the fire door when fitting access point hardware.

6.3 Environmental protection

Except where otherwise specified, equipment must be selected and installed to withstand the following air temperatures:

Internally sited equipment, 0 ºC to +40 ºC

Externally sited equipment, -20 ºC to +50 ºC

Wider temperature ranges may be specified for some applications.

Equipment exposed to direct sunlight can exceed these temperatures and appropriate shielding may be required in such circumstances. Where the temperature is not well maintained internally in premises, temperature may vary between -10 ºC to +40 ºC and consideration should be given to using equipment suitable for external use or similar. In all cases equipment should be suitable for use in the environment in which it is installed.

Environmental housings must be used, classified according to BS EN 60529, which must be appropriate for the location in which they are installed.

ACS components mounted in external locations would be expected to have a suitable IP rating appropriate to their location. Exposed areas would require equipment to have a higher IP rating than those in relatively sheltered areas etc.

All equipment housings and enclosures must offer protection against the intrusion of solid objects larger than 1mm. (e.g. wires, nails, screws, larger insects and other potentially invasive small objects such as small tools etc.).

This would necessitate a minimum IP rating of IP4x (where x is the moisture protection rating etc.).

All equipment housings and enclosures must offer suitable protection against damage from impact.

This would necessitate a minimum IK rating of IK04 in accordance with BS EN 62262.

6.4 Power supplies

Power supplies, including PoE switches and injectors, must be capable of meeting the largest load likely to be placed upon them under normal operating conditions.

Manufacturer's recommendations for the use of PoE switches, injectors and cabling must be followed.

All equipment housings must be clearly marked with the operating, or supplied, voltage except where access to the inside of the housing leads only to sealed components carrying the required markings.

Where ACUs use external power supplies, ACU input voltages should not exceed 50VAC or 75VDC unless unauthorised access to both power supply and ACU are prevented.

Certain release mechanisms associated with an ACS, such as those for roller shutters, may operate at mains voltage and specific electrical safety requirements will apply to these.

Where safety and security considerations do not require continued operation of a system during a mains supply failure, the public mains supply via a safety isolating transformer may be the sole supply for the system. A 'clean' source for this may be required in electrically noisy environments.

It is preferable for the ACS to have its own dedicated final mains circuit.

Power supply units must be located within controlled areas and in positions secure from tampering. Additional security must be provided for power supply units that support fail unlocked hardware.

Additional security measures to be considered may include installation of equipment above false ceilings, enclosures that can only be opened by means of a special tool (i.e. a tool not likely to be carried by a member of the general public) or using tamper proof or monitored enclosures etc.

The mains power supply must be permanently connected to the ACS via an un-switched fused spur, dedicated to the ACS.

Extra low voltage cables must not enter a power supply enclosure through the same entry point as any low voltage (mains cables).

Where continued operation of all or part of the ACS is essential during mains supply failure, standby power supplies, with the capacity to support the system for not less than the minimum period agreed with the customer, must be provided according to the access point classification in Table 8.

Table 8 - Power supplies

	Class I	Class II	Class III	Class IV
Standby Power Supply	OP	OP	M	M
OP = Optional M = Mandatory				

Some types of actuators may be excluded from the standby power supply requirements/calculations (e.g. directly AC powered and/or for high power consumption) provided it has been agreed with the user and recorded in the system design proposal and as-fitted document.

7 Installation

Readers must be mounted:

a) securely in position; and

b) adjacent to their access points and in positions convenient for all users to use, including those with disability.

Attention is drawn to relevant national building regulations.

When fitting access point hardware (including locks, latches and locking plates) to fire door sets, guidance from the manufacturer of the fire door sets must be followed.

Access point hardware (including locks, latches and locking plates) should not introduce any hazards that could result in injury (e.g. head injury due to frame hung locking device etc.)

The following must be taken into consideration when siting control equipment:

a) Ventilation

b) Access for maintenance.

c) User access for archiving, etc.

d) Noise from associated printer.

e) Physical security and supervision.

f) General visibility to unauthorised people of any displayed data.

7.1 Cables

7.1.1 General

Attention is drawn to BS 7671 (the I.E.T Wiring Regulations).

Cable types selected must meet manufacturer's recommendations or have the required performance to meet the electrical characteristics required to support the connected devices and be suitable for the environment in which they are installed.

Where practicable, cables must be installed within controlled areas and be concealed or in containment.

Where cables are exposed to possible mechanical damage or tampering, or are outside controlled areas, they must be mechanically protected.

All interconnecting wiring must be supported and its installation must conform to good working practice.

Particular attention is drawn to BS 7671 (the I.E.T Wiring Regulations) in respect of the requirements for cable supports that resist premature collapse in the event of fire.

All extra low voltage cable joints must be made in suitable junction boxes using either soldered, crimped, or screw-terminals.

Extra low voltage signal cables should not be run in close proximity to mains power cables or other low or high voltage cables.

Where it is not possible to separate cables or where mains or other cables may be installed with signal cables in the future, for example where signal cabling is run in open cable trays, the cable insulation of the ACS cables must be rated at or greater than the highest voltage of adjacent cables.

Where cables are part of the 'critical path' for door release mechanisms the recommendations of BS 7273-4 should be followed.

BS7273-4 defines 'critical signal path' as: "all interconnections and communications between a fire alarm system and the input terminals on, or within (a) device(s) provided to open, release or unlock a door, or between CIE and other control equipment by which such devices are controlled".

7.1.2 Data cables

Cables for the transmission of data or other low-level signals must have the required performance to support the load, rate of data transfer and protect against any anticipated levels of electromagnetic interference.

Where the installer of the ACS is responsible for the installation of the network, cabling must as a minimum be tested for the correct wire mapping (including split pairs), short and open circuits. Test results must be documented.

Where more complex networks are installed, e.g. a structured network, or where it is defined in the user requirements the structured cabling should be subject to certified testing.

Cables, connectors, patch panels, termination blocks and outlet sockets must be compatible, i.e., Cat 5e and Cat 6 components and cables should not be mixed.

Care should be taken to ensure bend radius, as defined in the manufacturer's documentation, is not exceeded.

Network devices should be connected to interconnections via patch panels or outlet sockets using stranded pre-terminated patch cables.

Cabling must be clearly and unobtrusively labelled at each termination point with source and destination identities to facilitate future maintenance and servicing.

A cross-reference chart or running out diagram showing the relationship between cables and devices must be created and held by the installing company.

In very simple point to point systems where the relationship between devices and cables can be reasonably determined, a cross reference chart or running out diagram may not be necessary. Patch cables having a specific colour unique to the ACS is recommended.

7.1.3 Extra low voltage and low voltage cables

Extra low voltage signal cables and low voltage cables from both mains and standby power supplies to remote equipment must be of sufficient rating to permit satisfactory operation of the equipment at the end of any proposed length of cable run.

7.2 Network security

Suitable physical, technical and cyber security measures must be put in place to prevent unauthorised direct or remote access to any part of the ACS or the client's network.

There should be consultation with the customer to determine if there are any particular security requirements they may have with regards to connecting the ACS to their network(s).

The system design proposal or as-fitted document should identify who holds the responsibility to provide critical security updates and security updates relating to system software and firmware.

Access to all system components, applications and operating systems from internal access points must be restricted to authorised individuals or processes using authentication protocols and access controls.

External access to the network must be restricted to authorised individuals and processes using suitably configured firewalls and/or routers and switches and/or proxy servers, authentication protocols and access controls.

The impact of cyber-attack in the following areas should be assessed and mitigated or managed:

- *Boundary firewalls and internet gateways*
- *Security of configuration*
- *Access control measures*
- *Malware protection*
- *Patch management*

The capability of all system products should be assessed to ensure these can be made secure against cyber-attack; for example, by using encryption, user authentication, complex passwords, etc.

If wireless networks are used by the ACS, then suitable security measures should be taken to prevent unauthorized access to the network. Such measures could include

changing/hiding the Service Set Identifier (SSID), changing default passwords and IP addresses and using suitable encryption protocols.

7.2.1 Shared networks

If sharing a network with other applications and devices, consideration must be given to implementing VLANs or end point security of all connected network devices to prevent these devices from being compromised.

Permission must be granted by the customer prior to the connection of any external devices, such as laptops and memory sticks, to the customer's network

All external devices must have the latest anti-virus software and operating system updates installed and have been scanned using the latest anti-virus software.

Where a network is being shared, it should be determined whether the customer has any IT policies or requirements that may need to be considered or complied with.

8 Commissioning, handover and documentation

8.1.1 Commissioning

The following must be checked and verified during the commissioning process:

a) All wiring is correctly terminated.

b) Voltage and resistance at all appropriate points (e.g. where voltage drop or high resistance would have an adverse effect on the operation of the ACS) of the system are correct and recorded.

c) Alignment and operation of access point hardware and of release and closure mechanisms at each access point is operating correctly.

d) Emergency release mechanisms at all the access points operate correctly and manual controls are clearly identifiable and labelled.

e) Emergency release mechanisms operate correctly under fire alarm conditions.

f) Operation of each reader is correct.

g) Release time for each door is correct.

h) Specific security requirements, such as time of day operation and event notifications, such as door held open, door forced, anti-passback, etc., all function correctly.

i) Correct authorisation of access is verified by the input of appropriate data.

j) ACS continues to work when mains supply disconnected (if specified).

k) All system security measures are functioning correctly.

l) All system application and operating software is at the correct and up to date version with any outstanding application and security patches and appropriate upgrades installed, subject to any software configuration controls the customer may have in place.

m) Any standby power supplies required to support the system in the event of a mains failure are verified as being capable of supporting the system for the required duration and the results recorded.

n) All unused TCP/UDP ports should be closed.

o) All unused system protocols should be disabled e.g. port 23 (typically Telnet).

At the end of commissioning, all unused user accounts must be deleted or disabled and details of accounts and passwords provided to the user.

Permission for the installing company to retain details of user accounts and passwords for ongoing maintenance activities must be agreed in writing.

8.2 Handover

The following must take place during the handover process:

a) Ensure there is a facility to record any system events (e.g. this could be in the form of an electronic event log or hardcopy logbook).

b) Ensure the end user is aware of how to report any issues that require attention by the maintenance company.

c) Demonstrate all aspects of system operation to the customer, including any necessary safety precautions and any standby power facilities.

d) Ensure that the correct documentation (see 8.3) is given to the customer to enable the system to be correctly operated, adjusted and maintained.

e) Provide details and training of end user maintenance responsibilities for the system, with particular emphasis on:

- regular system back-ups;
- database management & password security;
- Cyber Security
- visual checks on door furniture;
- periodic maintenance of door furniture and correct operation of door closers;
- correct release of access point on activation of the fire alarm system (where applicable) during the weekly fire alarm test;
- correct operation and resetting of any manual override switching.

f) Provide the user with any software and or software licenses purchases by the customer.

g) Ensure that users are aware of any procedures to be followed in the event of a system malfunction.

These may be additional physical measures to maintain the level of security normally provided by the ACS

h) Advise the end user of their obligation to comply with any legal requirements under the Data Protection Act and UK GDPR.

i) Ensure that written permission has been obtained where a user code(s) are to be retained by the installation/maintenance company for ongoing maintenance purposes.

Any such arrangements should have been determined at the design/survey stage.

j) Where an ACS is managed remotely, the details of this should be included in the documentation (see 8.3), for example the means to interface to the system, the level of access and details of sites with remote access.

k) Issue a NSI Certificate of Compliance in accordance with NSI Regulations.

8.3 Documentation

A documented risk assessment must be produced as part of the design process.

A system design proposal must be developed that includes all the customer's requirements, features and functionality of the ACS as well as any limitations or exclusions (based on risk assessment). Any user responsibilities or provisions should also be included.

Where a standby power supply facility is to be provided, the system design proposal must include either the minimum duration of the standby supply in hours or the minimum number of actuations per hour for each applicable access point.

BS EN 60839-11-2, Annex B gives information on how battery standby capacity can be calculated.

The system design proposal must be agreed with the user or their representative prior to commencement of the installation.

Upon completion of installation of the ACS an as-fitted document, including the following information, must be provided:

a) The address of the premises where the ACS is installed.

b) The location and classification of each access point and the type and location of each controller and its associated hardware (for example the type of token/reader technology).

c) The type and location of power supplies.

d) Power supply standby periods where relevant.

e) Details of those access points which the customer has the facility to override.

f) The type and location of any warning device.

g) Configuration settings.

h) Manufacturer's documentation relating to equipment, software, operation and security functions.

i) Details of the methods adopted for emergency override for safe escape.

j) Details of any mechanical components in an ACS, such as locks and hinges, which may require routine preventive maintenance by the user more frequently than once per year.

k) Firmware and software versions installed.

l) The as-fitted document must be agreed with the user or their representative and a copy provided to them.

Some of the information required for the as-fitted document may be provided in the form of a diagram of the installed system.

The customer should be advised to keep all documentation for the ACS in a place where access is restricted to authorised people.

9 Maintenance

9.1 Resources

9.1.1 General

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

The organisation responsible for the maintenance of the ACS must have the means, including spare parts and documentation to comply with this Code of Practice.

This recommendation does not place an obligation upon customers to have their ACS maintained, maintenance is a matter of agreement between the installing company and the customer or between the customer and a separate maintenance company. However, where an ACS controls access points that are also fire exits the customer should be advised to put a maintenance agreement in place to ensure the system continues to operate correctly.

Where a computer based system is installed, the customer should be advised to consider having a support agreement with the software supplier, where the organisation

responsible for the maintenance of the ACS does not provide the necessary software support this is to ensure updates to the application and technical support can be provided.

The organisation responsible for the maintenance of the ACS must ensure the safe custody and control of all equipment and documentation pertaining to installations, which is within their control.

9.1.2 Test equipment

Each service technician must have access to tools, test instruments and other equipment to enable them to perform their functions satisfactorily. Specialist tools, test equipment and plant must be available as required.

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.

9.2 Preventive maintenance

9.2.1 Frequency of visits

Preventive maintenance visits must be carried out every twelve months (+/- one month) from the month of commissioning

A greater frequency may be required due to user requirements, environmental conditions or issues identified in the risk assessment.

Where there are any mechanical components in an ACS, such as locks and hinges, which may require routine preventive maintenance by the user; this should be documented in the system design proposal and/or the as-fitted documentation.

9.2.2 Inspection

During each preventive maintenance visit, the following should be inspected and any necessary corrective action should be carried out in agreement with the customer:

a) The installation, location and siting of all equipment and devices against the as-fitted document (see 8.3).

b) The satisfactory operation of all equipment.

c) All flexible connections.

d) The normal and standby power supplies, for correct functioning.

e) The control equipment, in accordance with your procedure.

f) The operation of any warning device in the system

g) The correct operation of all system security functions

h) System application and operating software is at the correct version with the latest security patches and critical updates installed, subject to any software configuration controls the customer may have in place.

i) Verify customer responsibilities have been carried out, and inform the customer of any required corrective actions.

Those items of inspection and rectification which are not carried out during the preventive maintenance visit must be documented and agreed with the customer. These should be completed as soon as practicable, subject to the customer agreement.

Any reduction in the level of security identified during the preventative maintenance visit must:

- be recorded on the maintenance visit;
- be subject to a review of the risk assessment; and
- be rectified as soon as is practicable.

Rectification of any issues resulting in the reduction of the level of security may be outside of the scope of the maintenance organisation.

Where the risk assessment has not been made available to the maintenance organisation, a new assessment may need to be undertaken.

9.3 Corrective maintenance

The corrective maintenance (emergency service) facility must be so located and organised so that, under normal circumstances, the company's technician attends the premises within the time agreed in the contract with the customer.

9.4 Records

9.4.1 General

The organisation responsible for the maintenance of the ACS must maintain records relating to the ACS it maintains, including the information required as detailed in sections 9.4.2 to 9.4.5. It is essential that these records are protected from unauthorised access.

Attention is drawn to the General Data Protection Regulation (GDPR) and the 2018 Data Protection Act (DPA). In those cases where records contain information concerning individuals.

You must retain information in respect of contracts (including survey, design, quotations, amendments and commissioning/handover documents for the life of the contract plus a minimum of two (2) years.

9.4.2 As-fitted document

An as-fitted document will have been generated on completion of the system and may include previous information from the system design specification. The organisation responsible for the maintenance of the ACS must keep this document up to date and the document must be available to maintenance technicians for use at each maintenance visit.

The updated as-fitted document does not need to include the number of keys, codes, tokens, etc. where the customer has control of these.

When taking on a contract to maintain a system that has been installed by others, the as-fitted documentation should be obtained. Where this is not possible, a new document should be produced.

Where it is necessary for a new as-fitted document to be produced, it is preferable that this is done as soon as practicable and it is reasonable to expect that it could be done at the initial visit. However, it may be compiled over several maintenance visits, particularly in the case of large and/or complex systems.

9.4.3 Preventive maintenance record

A preventive maintenance visit record must be produced for each preventive maintenance visit.

A preventive maintenance record must include the details of the work undertaken, including any modifications or remedial works.

Parts of the system that could not be fully tested should be recorded on the maintenance record, together with the reasons for their omission and the signature of the client or representative.

A record of checks and work carried out must either be provided to the customer at the time of maintenance or within 10 days of the maintenance visit or as agreed with the customer.

The organisation responsible for the maintenance of the ACS must retain preventive maintenance records for a minimum period of 15 months after the preventive maintenance visit has taken place.

9.4.4 Corrective maintenance record

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

A corrective maintenance visit record must be produced for each corrective maintenance visit.

A corrective maintenance visit record must include the details of the reason for the corrective maintenance visit and the work undertaken, including any modifications or remedial works.

Any corrective maintenance work not completed should be recorded, including the reason why and accepted by the client or their representative.

A record of checks and work carried out must be given to the customer at the time of maintenance or provided within 10 days or as agreed with the customer.

The organisation responsible for the maintenance of the ACS must retain corrective maintenance records for a minimum period of 15 months after the corrective maintenance visit has taken place.

If a preventive maintenance inspection is made at the same time as the corrective maintenance visit, these should be recorded as separate records.

9.4.5 Temporary disconnection record

The organisation responsible for the maintenance of the ACS must keep a record of any temporary disconnection of the system or of any component part(s) of it. This must identify which part(s) of the system and the associated equipment is not operable. The reason for the disconnection must be given and the date and time of disconnection and of subsequent reconnection. A signed authorisation for each disconnection must be obtained from the customer or their representative.

Authorisation from the customer for temporary disconnection must be kept for at least three (3) months after reconnection.

National Security Inspectorate
Sentinel House, 5 Reform Road,
Maidenhead, Berkshire SL6 8BY

Telephone: 01628 637512
E-mail: nsi@nsi.org.uk
Web: www.nsi.org.uk