

a specifier's guide to the  
**security classification**  
of access control systems



July 2001

---

For other information please contact:

British Security Industry Association  
**t: 0845 389 3889**  
f: 0845 389 0761  
e: [info@bsia.co.uk](mailto:info@bsia.co.uk)  
[www.bsia.co.uk](http://www.bsia.co.uk)

## Contents

Foreword	2
Introduction	3
1. Scope	3
2. Normative references	3
3. Definitions & abbreviations	4
4. System components	5
5. Security levels	5
6. Electro-mechanical locking devices	8
7. Management procedures	8
8. Examples of security levels of access control systems	8
9. Application of security levels to access control systems	10
Annex A Access control doors – physical security classification	11
Annex B Electro-magnetic locks used in access control systems	12
Annex C Machine readable technologies for tokens	14
Annex D Grading of access control systems	15

## Foreword

An access control system offers a highly effective security solution to the management of access to sites and buildings. It is recognised by specialists as a vital element of a structured security strategy in an increasing number of business and residential applications.

However, the suitability of a system for a given situation hinges on the careful selection of compatible products, fit for the particular purpose. This ensures that the system will be practical and effective in use without any unintended compromises in security, operation or the effect of the system on the aesthetics of the building.

Historically, electronic access control has not benefited from a framework of standards and codes as exist in other security sectors such as intruder alarms and many mistakes have been made in the matching of equipment to applications. Typically, uninformed specifying results in systems that are in excess of the requirement or, more dangerously, leave loopholes that allow unauthorised access.

The ABI therefore warmly welcomes the publication of this guide for specifiers. The information on the following pages forms a unique tool that will enable specifiers in insurance, the police and the consultancy, building design and facilities management sectors to identify suitable system components within a rational and practical framework. The information is highly accessible and will benefit specifiers at all levels of experience. The guide will make an important contribution to the quality of specifying decisions, the reputation of the technology and the vital role of access control systems in property risk management.

**Jane Milne**  
**Manager, Household and Property**  
**The Association of British Insurers**

July 2001

## Introduction

An access control system is an effective form of security and its benefits include:

1. An important part of an overall electronic security system
2. Enhanced security of employees, buildings and assets
3. Ability to work with other in-house security measures
4. Reduction in the overall cost of managing security

Specifiers need to be aware of the potential contribution of access control systems when surveying premises, and should understand how and when to specify them to effectively control or restrict access. There is a suite of European standards which have been adopted as British standards and which adequately cover the system design, installation and equipment requirements of access control systems (see Section 2). However, they do not provide guidance on the grading of systems - that is the purpose of this document.

This document has been produced as a guide to assist specifiers in grading access control systems in line with other security applications. It lists the various depths of security that may be required, and identifies what the specifier should take into account when specifying access control systems.

The main determinant of the security level required will be the outcome of the risk assessment of the premises, and this in turn will influence the choice and design of access control system to be used.

## 1. Scope

This guide specifies requirements for different security levels for access control systems and is based on BS EN 50133 – 1 : 1997.

The document details security levels based on:

- Machine readable technologies for tokens
- Electromagnetic locks
- Physical security classifications of doors.

## 2. Normative references

Reference is made in the guide to the following standards:

**BS EN 50133-1 : 1997** System requirements for access control systems

**BS EN 50133-2-1 : 2000** Component requirements for access control systems

**BS EN 50133-7 : 1999** Application guidelines for access control systems

**prEN 12209-1** : Building hardware locks and latches

**BS 6206** : Specification for impact performance requirements for flat safety glass.

## 3. Definitions & abbreviations

### 3.1. Definitions

For the purpose of this guide, the following definitions apply (a full list of access control definitions is listed in BS EN 50133-1).

#### 3.1.1 Access

Action of entry or exit from a security controlled area.

#### 3.1.2 Access point

A door or barrier where entry and/or egress is controlled by the access control system.

#### 3.1.3 Biometric

Information which is referring to unique physiological attributes of the user.

#### 3.1.4 Code

Usually a 4 or 5 digit code which a user has to remember; termed a PIN (personal identification number).

#### 3.1.5 Fail locked

A description of, or state of, an electromechanical locking device that will be locked when there is no power to it, and which requires power to unlock it.

#### 3.1.6 Fail unlocked

A description of, or state of, an electromechanical locking device that will be unlocked when there is no power to it, and which requires power to lock it.

#### 3.1.7 Processing equipment

The comparing of information with pre-set rules to make decisions concerning the granting or denying of access to users and/or the comparing of events with pre-set rules to produce appropriate actions.

#### 3.1.8 Secured side

That side of an access control system to which a user is trying to gain access i.e. by the use of valid codes, tokens etc. **Note:** In such cases it is not possible for an unauthorised person to override the lock control.

#### 3.1.9 Special features

Options, such as anti-passback, which deny access to a valid card or PIN unless there has been an entry followed by an exit.

#### 3.1.10 Token

A device containing recognition data, e.g. cards, keys, tags, etc. Types of token and reader in use are:

##### 3.1.10.1 Biometric reader

A user presents their finger print, retina, etc. to the reader i.e. the user is the token.

##### 3.1.10.2 Contact type reader

A token which has to make direct physical contact with the reader.

##### 3.1.10.3 Non-contact reader

A token that is read at a distance from the reader.

#### 3.1.11 Unsecured side

That part of an access control system where the electronic equipment which controls the lock is on the same side as the user requesting access or egress.

**Note:** In such cases it may be possible for an unauthorised person to override the lock control.

### 3.1.12 User

A person requesting passage through an access point.

### 3.2 Abbreviations

In this guide the following abbreviations are used:

PE	Processing Equipment
kN	Kilo-Newton

## 4. System components

A basic access control system typically includes the following components:

- Processing equipment
- Display equipment
- Programming equipment
- Power supplies
- User identity
- Recognition equipment (tokens and readers)
- Access point interface
- Communication with other systems

Depending on its application, an access control system is designed with some degree of self protection and tamper detection to prevent unauthorised access to the system without the use of special tools. The grading of an access control system will, to some extent, depend on the sophistication of the self protection and tamper detection included.

## 5. Security levels

### 5.1 General

The security of an access control system is determined by a combination of:

- The type of reader(s) used at the access point(s)
- Features employed in the system
- The type(s) of access door(s) and locks used.
- Thoroughness of end user/clients security procedures

Generally the type of access control system and reader used at the access point, and the door or barrier designs determine the security level of the system. However, where special features are included in a system the security level may be increased. The end user or client's procedures covering matters such as the issue of cards and tags, and the upkeep of the system database etc, should be considered as significant in the overall management of security at any site.

Section 5.2 introduces the 4 levels of access control security; the minimum requirements for readers, doors and locks appropriate to these are given in Annex A, B and C. An explanation of the features is given in clauses 5.2 to 5.4. Examples of security levels are given in section 8.

## 5.2 BSIA Security levels of Access Control Systems

The level of security provided by different token / reading technologies, and other system features varies in accordance with the table below. See also comments in section 5.3, 'special features'. A key consideration in the design of any access control system is to relate the level of security at each door to the attendant risk. For example, whilst Level 4 security would be considered for the external entry to premises, levels 2 or 3 may be perfectly acceptable for the internal entries to office areas etc. In the following table, 1 is lowest, 4 is highest. These must be supported by appropriate doors, locks and readers (**see Annexes A, B and C**).

**LEVEL 1** (relates to BS EN 50133 - 1 security classification 1-A or 2-A)

Stand alone PIN pad or token and reader without time based controls or transaction recording capability. The lock control may be on the unsecured side.

**LEVEL 2** (relates to BS EN 50133 - 1 security classification 1-B)

PIN pad with unique code for each user with time based controls and transaction recording capability. The lock controls should be on the secured side.

**LEVEL 3** (relates to BS EN 50133 - 1 security classification 2-B)

A token and reader or biometric reader with unique code for each user with time based controls and transaction recording capability. The lock controls must be on the secured side,

**LEVEL 4** (relates to BS EN 50133 – 1 security classification 3-B)

A system with the same features as LEVEL 2 and LEVEL 3 except with token and reader or biometric reader in association with PIN pads at each access point. To gain entry each user must present a token or biometric as well as inputting a valid pin unique to each user.

**Note 1:** BS EN 50133 – 1 security classification 3-A is not used in this guide, as secure entry without time logging is not believed to be a useful combination for a secure access control system.

**Note 2:** The access control security levels stated above are an interpretation by the BSIA of the "Recognition class" and "Access class" as stated in BS EN 50133-1.

**Note 3:** If lock controls are on the unsecured side the level of security of the system may be increased by the addition of tamper protection to the lock control

## 5.3 Special features

Additional security may be provided by special features such as:

- Anti-passback, where each access point has both entry and egress control.
- Dual-badging where two different tokens are required.
- Video verification, comparing the digital image from the ID pass with the live CCTV to verify that the cardholder is the genuine owner of the pass.
- Card Referral, release of an access controlled door remotely by a control room operator, subsequent to the user request via card swipe.

The above list of special features is not exhaustive and the level of security in such systems would need to be assessed on a more individual basis.

## 5.4 Access doors

### 5.4.1 Types of doors

The main types of doors used in access control systems are:

- Hollow core
- Softwood/uPVC
- Hardwood
- Steel

These doors are graded by the physical strength of the door construction and the locking mechanism fitted. The grading is based on the ability of the door to withstand an applied external force, given in Kilo-Newton's (kN), ranging from 3kN for hollow core door constructions up to 10kN for steel. For details on the grading of doors and locks see Annex A & Annex B

### 5.4.2 Other door constructions

Aluminium doors and frames typically fall between uPVC and hardwood in terms of physical strength, depending on the design and section used.

Anti-ballistic and other very high security door constructions are available for high risk areas such as banks, cash offices etc and these are considered superior to standard steel construction doors.

**Note:** The choice of door construction may be limited by the need for the door to have achieved a fire resistance rating. This can also have an impact on the type of electric locking fitted.

### 5.4.3 External & high risk doors

Preferably these doors should feature controlled entry and exit. However, this is not always practical (particularly on entrance doors) and free egress is often provided. In these instances it is important the device used for exit is properly protected against manipulation from outside. Lever handles, press to exit switches, breakglasses etc should not be fitted near glass panels or letter boxes and ideally should not be visible from outside. If these doors are to allow unrestricted exit during the day then an additional mechanical deadlock or similar may be required to secure the door out of business hours.

Annex B provides a guide to the suitability of various types of door construction and lock mechanism strengths for different applications. Whilst this is not a definitive list, it provides a general guide to the performance requirements.

## 6. Electro-mechanical locking devices

### 6.1 General

Electromagnetic locks used on access control systems should, where possible, conform to EN 12209-1.

The vast majority of electric locks are available with door position monitoring (to detect whether a door is open or closed) in one form or another. A monitored locking mechanism is always recommended and is essential for doors at medium risk or above.

Most electric locking devices operate in one of two modes, fail locked and fail unlocked.

- A fail locked device will be locked when there is no power to it and requires power to unlock. These are generally preferable for higher risk areas
- A fail unlocked device means that with no power to the lock it is unlocked and it requires power to lock. These are better suited to public areas or escape routes

With either type of device, a mechanical means of exit from the secure side is preferable (and may be insisted upon by a fire officer), if it does not compromise security.

Annex C gives general information on the types of electromagnetic locks used on access control systems.

### **6.2 Designated escape routes**

On designated escape routes, the ultimate security of the door may have to be compromised by the use of either a lever handle or full length push bar for exit, or by the requirement for the lock to be connected into the fire alarm system so that in the event of a fire the door unlocks automatically.

## 7. Management procedures

The user should be trained in the management of the access control technology to ensure the integrity of the system. The user should be instructed to ensure:

- There is strict control of the issue and care of tags/cards for staff and visitors.
- Staff changes, lost cards or tags etc are actioned in the database as soon as possible.
- Access to the system's database is strictly controlled.
- The staff / users are fully trained in the use of the system.
- A strict control is kept on the access that individuals have in premises where there are varying levels of access

The end-user or client should have well defined, written procedures for the above. Responsibility for the above should be clearly established.

## 8. Examples of security levels of access control systems

There are many combinations of features that can contribute to the final security level of an access control system, but the large majority will be covered by the security level table shown in section 5.2.

Suggested practical examples of applying security levels are listed below.

### **Coded entry into a staff common room for a small store**

#### **Level 1 or Level 2**

This is a low risk application where coded entry may be preferable as it does not require staff to carry a token. The higher security level may be applicable if the door is heavily used or if staff possessions are left in the room.

### **Access control used for privacy on an office/meeting room door**

#### **Level 1 or Level 2**

When access control is used purely for privacy the construction of the door and strength of locking mechanism are largely irrelevant, provided they are strong enough to cope with the level of use the door is to receive. For privacy purposes a PIN is sufficient, however if a token based system is in use elsewhere in the building it may be more convenient to use this on such doors.

### **Access control for security on a low risk internal office door**

#### **Level 2**

This represents a typical office door inside a company's premises and assumes that to get to this door an individual will have to have already passed either a manned reception or a higher security level of external door. The security level of this type of door may rise to level 3 if a token based access control system is to be used throughout the building (for convenience), or if this were an office door in a public building.

### **Main entrance to a company's premises**

#### **Level 3**

A token only solution to a company's main entrance is acceptable provided that there is a manned reception or that an additional lock secures the door when the building is left unoccupied.

### **Main entrance to a company's premises, in use 24 hours a day**

#### **Level 4**

When a building is to be used 24 hours a day, then a token and PIN system should be used during periods where there is no manned security at reception.

### **Access control into a block of flats**

#### **Level 4**

A grade 4 door may be necessary owing to the likelihood of vandalism and the heavy and abusive usage the door is likely to suffer in this application. Card and PIN is not necessarily required as many residents may find it difficult to remember a PIN, but the use of a token as opposed to a key greatly increases residents security, as previous tenants tokens can be quickly blocked.

### **Rear car park entrance to a building**

#### **Level 4/4+**

Any door in an exposed environment such as this should be of security level 4 construction due to the likelihood of attempted surreptitious entry or vandalism.

### **External warehouse door for high value storage**

#### **Level 4+**

Again, this type of door requires high resistance to physical attack, and card and pin should be enforced outside conventional working hours. For high value goods or cash areas the use of a two door interlock should also be considered - this system prevents both doors being opened at the same time and can help reduce opportunist crime.

## **9. Application of security levels to access control systems**

It must always be borne in mind that electronic access control is an important part of an overall security system. Other measures, including systems such as intruder alarms CCTV, manned patrols, and clients' security procedures etc, must be included in assessing the quality of the overall management of site security.

As with other security measures, a key consideration in the design of an access control system is the potential threat posed to who, or what is contained within the area to be protected.

Any access control system should be designed and installed according to a written specification, preferably accompanied by relevant drawings and plans. In addition, each point of entry into a building, and its associated premises such as car parks, personal accommodation etc, should be assessed in terms of risk. The design of doors and barriers, and the choice of access control equipment should be consistent with those assessments

regarding the security levels set down in section 5.2.

This document is not intended to offer a detailed procedure or criteria for the determination of risk, however such risk assessments should take account of factors such as:

- Probability or threat of personal attack from intruders
- Material value of goods or assets contained within the protected area
- Sensitivity of information or records contained in the protected area, eg personal information, or intellectual property

As stated earlier, the thoroughness of the client's procedures are significant in the management of security, and should be consistent with the particular risks to security.

## Annex A

### Access control doors – recommended physical security classification

Holding force	Hollow Core	Softwood/uPVC	Hardwood	Steel
3kN	<b>Level 1</b> Internal doors used for privacy and not security	<b>Level 1</b> Internal doors used for privacy and not security	N/A	N/A
5kN	N/A	<b>Level 2</b> Low risk internal doors or higher usage privacy doors	<b>Level 2</b> Internal doors in low to medium risk areas	N/A
7kN	N/A	<b>Level 2</b> High usage low risk doors	<b>Level 3</b> External doors supplemented with separate night-time locking; medium risk internal doors	<b>Level 3</b> External/high security doors supplemented with separate night-time locking
10kN	N/A	N/A	<b>Level 4</b> Medium to high risk internal or external doors	<b>Level 4+</b> High risk internal or external doors

**Note 1:** The above table is a general guide to help specifiers determine the type of door construction required to meet the level of access control system installed.

**Note 2:** This document does NOT give security grading of glass doors or glazed panels. Specifiers should refer to the relevant British standard to find the necessary information e.g - BS 6206 – Specification for impact performance regulations for flat safety glass.

## Annex B

### **Electromagnetic locks used in access control systems.**

#### **B.1 Maglocks**

A maglock is a large electromagnet, usually fitted to the head of the doorframe, with a corresponding metal plate fitted to the face of door. The maglock holds the door shut using the electromagnetic attraction (pull) between the magnet and the plate. This typically provides a holding force in the region of 3 to 5kN. Maglocks are always fail unlocked (see definition) in operation.

#### **B.2 Shearmags**

A shearmag is similar to a maglock in that it relies on the attraction between an electromagnet and a plate on the edge of the door to lock. However in this case, the plate has a number of protruding metal pins on the surface, with matching recesses on the face of the magnet. When the door is locked, the electromagnet pulls the plate onto the face of the magnet. In this position the holding strength is then provided by the metal pins which are held within the recesses of the magnet. This provides much greater holding force than a conventional maglock, typically in the order of 7kN and upwards depending on size and type. Shearmags are always fail unlocked in operation.

#### **B.3 Electric strikes**

An electric strike works in conjunction with a conventional mechanical lockcase to retain the latch or deadbolt in the striking plate and then release it on demand. Electric strikes are available to work with either latchbolts or deadbolts, but the basic operation is similar, in that the bolt is held behind a moveable pivot, which is electrically released. Once released, pushing/pulling on the door causes the pivot to swing out of the way allowing the door to open. Electric strikes are available in a wide variety of types with holding forces ranging from 3kN to 10kN plus. Electric strikes are available with both fail locked and fail unlocked mechanisms.

#### **B.4 Solenoid Latch**

A solenoid latch provides similar operation to an electric strike, but in this case it is achieved by the double action latch being freed to move back into the lockcase. When the lock is released the door can simply be pushed/pulled open. Typically these locks only have the option for a key cylinder to provide mechanical override, restricting their use on escape routes. These locks typically have a holding force in the region of 5kN and are usually available either fail locked or unlocked, but this can depend on the manufacturer.

#### **B.5 Solenoid handle locks**

These operate like a conventional mechanical latch lock, but with the ability for either one or both handles to be electrically disabled. When an open signal is sent to the lock the controlled handle is then able to retract the bolts and the door can be opened. Models are available with either one or both handles controlled. The models where only the handle on the insecure side is disabled are suitable for escape routes and any area where there is free exit. Models where both internal and external handles are disabled are suitable for areas where access is restricted in both directions. Solenoid handle locks typically have a holding force in the range of 7-10kN and are available with either fail locked or fail unlocked operation.

#### **B.6 Motor locks**

Motorised locks offer a high level of physical security as they rely on a motor controlled bolt for locking. To unlock, a signal is sent to the lock that pulls the bolt into the lockcase allowing the door to be opened. Due to the time taken for the motor to pull the bolt back and to re-lock, these locks are not usually suited to very high usage areas. Typically motor locks will have a holding force of 10kN plus. Unusually motor locks are neither fail locked or fail unlocked as (for the majority of these locks) with no power to the lock the bolt will stay in whatever position it is currently in, be it locked or unlocked.

**Recommendations for security levels for electromagnetic locks**

<b>Holding Force</b>	<b>Maglock</b>	<b>Shearmag</b>	<b>Electric Strikes</b>	<b>Solenoid Latch</b>	<b>Solenoid Handle Locks</b>	<b>Motor Locks</b>
<b>3kN</b>	Level 1	*	Level 1	*	*	*
<b>5kN</b>	Level 2	*	Level 2	Level 2	*	*
<b>7kN</b>	N/A	Level 3	Level 3	N/A	Level 3	*
<b>10kN</b>	N/A	Level 4	Level 4	N/A	Level 4	Level 4 (+)

**Level** = This is the BSIA recommendation based on the holding force of the electromagnetic lock.

**N/A** = The electromagnetic lock does not currently have the capability of operating at this holding force level.

**\*** = The electromagnetic lock may be used but is normally manufactured for a higher holding force range.

The BSIA recommendation for security levels using electromagnetic locks is based on the electromagnetic locks holding force. The above table has been produced by the BSIA Access Control section and is based on the Section's practical experience gained over many years manufacturing and installing access control systems.

## Annex C

### C.1 Machine readable technologies for tokens

#### Tokens widely available but less secure

- **Magnetic stripe bank cards** - Standard current credit card type.
- **Surface barcodes** – Similar to supermarket produce ID labels.

#### Tokens with more security

- **Weigand** – embedded magnetic wires.
- **Infrared** – hidden optically read codes
- **Watermark** – magnetic stripe with patented security feature to prevent duplication.
- **Proximity** – chip and antenna with unique ID code.
- **Smart Card** – read write chip card which will support multiple applications.
- **Biometrics** – some of the types of biometrics currently available are:
  - Finger recognition.
  - Hand recognition (including vein check).
  - Face recognition (2D & 3D).
  - Iris recognition.

**Note:** There is a difference between full biometrics that only use the unique physiological attributes of the user and a biometric systems that requires a PIN code or card to support it.

### C.2 Type of reader technology

#### Grade 1

Magstripe – contact type

Surface barcode – contact type

#### Grade 2

PIN Pad

#### Grade 3 & 4

Weigand – contact type

Infrared – contact type

Water mark – contact type

Proximity – non contact type

Smart card – contact or non contact type

Biometrics – contact or non contact type

## Annex D

### Grading of access control systems

Type of reader	System features	Minimum door Recommendations	Electromagnetic Locks	Upgrade
<b>LEVEL 1</b>	Stand-alone reader(s) at access point(s) – no data logging. Control of electric lock on “unsecured side”	Hollow core 3kN Softwood/uPVC 3kN	<b>Maglock</b> <b>Electric Strikes</b>	
<b>PIN or token reader</b>	Stand-alone reader(s) at access point(s) – with data logging and/or time/date controlled entry	Hollow core 3kN Softwood/uPVC 3kN		
	Control of electric lock on “unsecured side”			
	Control of electric lock on “secure side”	Softwood/uPVC 5/7kN Hardwood 5kN		<b>Grade 2</b>
<b>LEVEL 2</b>	Stand-alone reader(s) at access point(s) – no data logging. Control of electric lock on “secured side”	Softwood/uPVC 5/7kN Hardwood 5kN	<b>Maglock</b> <b>Electric Strikes</b>	
<b>PIN Pad</b> Each user has unique code	Stand-alone reader(s) at access point(s) – with data logging and/or time/date controlled entry Control of electric lock on “secured side”	Softwood/uPVC 5/7kN Hardwood 5kN	<b>Solenoid Latch</b>	<b>Grade 3</b>
	Control of electric lock on “secure side”	Hardwood 7kN Steel 7kN		<b>Grade 3</b>
	PE controlled system with database management functions, time, date, holiday controls etc.	Hardwood 7kN Steel 7kN		<b>Grade 3</b>
<b>LEVEL 3</b>	Stand-alone reader(s) at access point(s) – no data logging. Control of electric lock on “secured side”	Hardwood 7kN Steel 7kN	<b>Shearmag</b> <b>Electric Strike</b>	
<b>Token</b> User presents token to access point reader	Stand-alone reader(s) at access point(s) – with data logging and/or time/date controlled entry. Control of electric lock on “secured side”	Hardwood 7kN Steel 7kN	<b>Solenoid Handle lock</b>	
	Control of electric lock on “secure side”	Hardwood 10kN		<b>Grade 4</b>
	PE controlled system with database management functions, time, date, holiday controls etc.	Hardwood 10kN		<b>Grade 4</b>
<b>LEVEL 4</b> <b>Token &amp; PIN Pad</b>	Stand-alone reader(s) at access point(s) – with data logging and/or time/date controlled entry. Control of electric lock on “secured side”	Hardwood 10kN	<b>Shearmag</b> <b>Electric Strike</b> <b>Solenoid Handle Lock</b>	
User presents token and enters unique code	Control of electric lock on “secure side”	Steel 10kN	<b>Motor Lock</b>	<b>Grade 4+</b>
	PE controlled system with database management functions, time, date, holiday controls etc.	Steel 10kN		<b>Grade 4+</b>
	Indicates where an increase in the grading for a certain type of reader is required			