bsia
british security industry association

A specifier's guide to access control systems

April 2016

For other information please contact:

British Security Industry Association
t: 0845 389 3889
e: info@bsia.co.uk
www.bsia.co.uk

Form No. 132 | Issue 4

Table of Contents

BACnet® is a registered trademark of American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE).

Bluetooth® is a registered trademark of Bluetooth SIG

Fieldbus® is a registered trademark of Fieldbus Foundation

LonWorks® is a registered trademark of the Echelon Corporation

Mifare® is a registered trademark of NXP Semiconductors

Modbus® is a registered trademark of Schneider Automation, Inc.

ONVIF® is a registered trademark of Sony Corporation

Profibus® is a registered trademark of Profibus Nutzerorganisation e.V.

Wi-Fi® is a trademark of the Wi-Fi Alliance

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. 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.

Design of the access control system should take account of the Equality Act and Disability Discrimination Act so that physical aspects permit goods and services to be accessible to disabled people.

For the first time this version of Form 132 takes into account the BS EN 60839-11 series of standards for access control. The component and system requirements in BS EN 60839-11-1 and the application guidelines given by 60839-11-2 were developed by the worldwide international standards body IEC and replace the older European standards (EN 50133 series). As a new series of standards the 60839-11 series has not immediately become the accepted practice but increasing use is expected over time. This document refers to some aspects of the standards in particular where the standards allow for varying quality of systems to allow for different levels of risk. This is done by the use of grading. Grade 1 is associated with weaker security and Grade 4 with stronger security.

Where this guide is used in conjunction with a recommendation to comply with Secured by Design requirements then specifiers should consult with Police Crime Prevention Design Advisors (CPDA).

For further information about Secured by Design refer to www.securedbydesign.com

1. Scope

This guide provides details of security grading for access control systems. It covers system components including tokens, barriers, doors and interconnection methods. The document provides security levels for:

- Reader / Token Technology
- Physical security classification of doors
- Electromechanical locks
- System Software

2. Referenced Documents

See also Section 21 Further Reading which includes BSIA Forms and Guides.

BS EN 60839-11-1 Alarm and Electronic Security Systems – Electronic Access Control Systems – Systems and Components Requirements.

BS EN 60839-11-2 Alarm and Electronic Security Systems – Electronic Access Control Systems – Application Guidelines.

BS EN 50486 Equipment for use in audio and video door-entry systems.

EU Working Time Directive (officially: Directive 2003/88/EC of the European Parliament and of the Council of 4 November 2003 concerning certain aspects of the organisation of working time).

BS 7671 IET Wiring Regulations (latest edition).

LPS 1175 Requirements and testing procedures for the LPCB approval and listing of intruder resistant building components, strongpoints, security enclosures and free standing barriers, LPCB.

NCP 109 NSI Code of Practice for Planning, Installation and Maintenance of Access Control Systems, NSI.

PAS 24: 2012 Enhanced security performance requirements for door assemblies, British Standards.

PAS 68: 2013 Impact test specifications for vehicle security barriers, British Standards.

SSAIB Code of Practice for Access Control Systems, SSAIB.

STS201: Enhanced security requirements for doorsets and door assemblies for dwellings to satisfy the requirements of PAS23 and PAS24, Warrington Certification.

STS202: Requirements for burglary resistance of construction products including hinged, pivoted, folding or sliding doorsets, windows, curtain walling, security grilles, garage doors and shutters, Warrington Certification.

Disability Discrimination Act 1995 (for Northern Ireland).

Equality Act 2010.

Regulatory Reform (Fire Safety) Order (FSO) 2005.

3. Terms and Abbreviations

3.1 Terms

Access	Action of entry or exit from a security controlled area.
Access control installation	The hardware part of the access control system in combination with the management software.
Access control system	An electronic system restricting access (i.e. entry into and/or exit from a security controlled area).
Access group	A number of users sharing the same access level.
Access level	User authority based on a set of rules used to determine where and when a credential has authorized access. This may include special conditions such as specific allowed times.
Access point	The location at which access can be controlled by a door, turnstile or other secure barrier.
Access point hardware	Mechanical or electro-mechanical devices used to restrict entry/egress through the access point.
Access request	The presentation of a credential to attempt to gain entry or egress.
Access request response time	The time taken from presentation of the credential to activation of the access point hardware.
“Airlock”	Although commonly called an “airlock” this is technically incorrect. Preferred terms are: Interlocking doors / Man trap / Person Trap / Personal transfer units / Security Booth / Security Vestibule / Commodity transfer units. A combination of two or more doors, turnstiles, barriers, etc required to be used in sequence in order to gain access to a controlled area. The release of a subsequent door is conditional upon the closure of the previous door used. This design may be used in combination with surveillance methods to combat piggybacking and tailgating. It can also be applied to vehicles. Some arrangements of interlocking doors are intended for transfer of goods such as money or commodities.
Alarm / Alert	An event following an exception to prompt intervention.
Anti-loiter	A feature that monitors the progress of a user through a security controlled area. (see also Card Trace).
Anti-passback	A feature that traces individual credential access requests to a given area. It checks for granting of access not preceded by granting of egress (or vice versa) to check that the credential has not been “passed back” to another user. Also refer to hard anti-passback, soft anti-passback, logical anti-passback and timed anti-passback.
Anti-tailgate / Anti-piggybacking	A system function that is designed to detect or prevent a second person from gaining access without presenting a credential.
Area controlled anti-passback	See Anti-passback.
Authentication	The system recognition process comparing a user’s credential with recorded credentials.
Audit trail	A list of system events (e.g. credentials used at an access point).
Badge	Another name for a Token.
Biometric	Any measurable, unique physiological characteristic or personal trait used as a credential. (e.g. fingerprint, hand or face geometry, retinal/eye, face, voice, signature or keyboarding dynamics).
Break glass	A device, similar to a fire alarm call point, used to release a door in the event of an emergency.
Card	Another name for a Token.

Card Blocked / Card Lost	See Credential Suspension.
Card Trace	A feature used to track the movement of a user through a security controlled area (see also Anti-loiter).
Central processing	See On-line Processing.
Chip Serial Number (CSN)	A number stored at manufacture in an RFID device or Proximity token otherwise known as a Unique ID or UID.
Code	Usually a 4 or 5 digit code which a user has to remember See also Common code, Group code, PIN.
Commodity Transfer Unit	See “Airlock”.
Common code	A code used by all users of a single access control system or access point.
Common token	A token unique to a particular access control system, or reader, with all user tokens identical.
Configuration	The process or the result of enabling/disabling systems functions and/or changing values as allowed by pre-set rules.
Controlled area / Protected area / Security controlled area	The area protected by the access points and accessed by the presentation of a valid credential.
Credential	Any token/memorized information/biometric image used to identify an individual to an access control system in order to verify user access rights. See also badge, token, biometric, code, PIN.
Credential suspension	The temporary removal of access permission for a particular credential (e.g. following the report of a lost token). Also known as Card Blocked or Card Lost.
Degraded Mode	A mode of operation where part of the system is inoperative but some control is still possible. An example being the loss of communication to a central controller for an on-line system where individual access points can provide authentication to a limited number of users.
Door	A general term referring to a hinged, sliding or revolving barrier intended to prevent a user from gaining access to or egress from a secured area. May also refer to a hatch, lift door, or turnstile. (see also Portal, Turnstile).
Door Entry System	See 3.2.
Door forced	Unauthorised opening of an access point.
Door Held Alarm / Door opened too long	Detection that a door has not closed within a defined time after access has been granted.
Door Status	Information obtained by detectors or sensors monitoring the door that allows the system to know whether a door is open or closed. A typical sensor (a “door contact”) consists of a magnet mounted on a door and a magnetically controlled switch on the frame. See also Lock Status.
Dual Access / Dual Badging	A function granting access only after two sequential authorised access requests are made within a programmable limited time period. Sometimes known as “dual custody”, “supervisor mode”, “multi-tap”, “four eyes”.
Dual Occupancy	A function, which counts the number of users entering and leaving the area and grants egress only if at least two authorised users remain in the area at all times.

Duress alarm / alert	An alarm/alert generated by a user being coerced into providing access. The alarm is hidden at the access point and typically generated by use of an alternative PIN that also grants access.
Egress	The action of leaving the security controlled area.
Elevator Control	See Lift Control.
Elevator Dispatch	Directing users to appropriate lift cars for efficiency.
Fail locked / Fail secure	The securing of a locking mechanism in the event of an access control system failure (usually power failure).
Fail open/ fail safe / fail unlocked	The release of a locking mechanism in the event of an access control system failure (usually power failure).
Fail Maintained	Locking device to which the removal of power does not change the locked or unlocked mode.
False acceptance	The granting of access to an unauthorised user.
False Acceptance Rate (FAR)	Percentage of erroneous recognition of users granting access.
False Match Rate (FMR)	Percentage of erroneous verification of users against other ID (for biometric verification methods) resulting in granting of access.
False rejection	The denial of access to an authorised user.
False Rejection Rate (FRR)	Percentage of erroneous recognition of users denying access.
Forgive	A function applied when anti-passback is in use to overcome a situation where the credential is inadvertently located on the opposite side of the access point /door to that the system believes it to be. Thereby allowing the user to gain access or egress and thus correcting the location. (see Global Forgive).
Free Access	A condition in which the door is allowed to open, or is held open, to permit access or egress without presentation of a credential. Used for example during building maintenance, escorted deliveries, emergency evacuation.
Global Forgive	A forgive function applied to all credentials (for example following an emergency evacuation).
Group code	A code used by a defined group of users of a single access control system or point (similar to having multiple common codes).
Guard Tour	A feature of a system that enables the defined route of a guard to be combined with the access control system (e.g. by permitting access only in a certain sequence).
Hard anti-passback	A feature, which generates an alert and denies further access following violation of anti-passback rules.
Human Image Verification / Human Identity Verification	A method where, when a credential is read, instead of the access point being unlocked a security operator is informed who then checks that a live image of the user matches a stored image from a database and allows or denies access remotely.
Interlocking doors	See “Airlock”.
Keypad	A data entry point for the input of a numeric or alphanumeric code (PIN) into an access control system.
Lift Control	A functionality restricting the use of a lift (elevator) car.
Lock Status	Information obtained by sensors monitoring a lock that allows the system to know whether a lock is locked or unlocked. Note that knowledge of the lock status does not necessarily imply the door it is attached to is locked shut. See also Door Status.

Logical anti-passback	Operating mode which requires user validation when leaving a security controlled area in order to be able re-enter and vice versa.
Man trap / Person trap	See “Airlock”.
On-line Processing / On-line System	An access control system where all access points are linked to a central controller that records events and (in normal usage) carries out the authentication process. Compare with Stand-alone System.
Personal identification number (PIN)	A sequence of characters (code) allocated to an individual user of an access control system keypad.
Personal (or Personnel) transfer unit	See “Airlock”.
Portal	An alternative general term for Door, Hatch, Turnstile, etc.
Power supply	That part of an access control system which provides power for the operation of the system or any part of thereof.
Proximity token	A credential using a radio frequency token where the identification number is fixed into the card.
Primary Battery	A battery that is not rechargeable.
Protected area	See Security Controlled Area.
Push-button Lock	A lock that opens when buttons on it are operated together or in sequence. Not normally considered to be an access control “system”.
Reader	An input device, which “reads” a credential consisting of specific identifying characteristics.
Request-to-Exit (REX)	A device used to initiate free egress.
RFID	Radio Frequency Identification. Normally used in the context of a small device (the credential) that transmits information using radio frequencies to a reader. The data on the card (including user identification) can be changed by the system. Commonly known as a “smart card”.
Security Booth / Security Vestibule	See “Airlock”.
Security Controlled Area	The area protected by the doors, hatches, turnstiles, etc included by the access control system.
Soft Anti-passback	A system feature, which grants access but generates an alert following violation of anti-passback rules.
Stand-alone System	A system in which the credential authentication and control of granting of access is applicable to a single door (e.g. decision making is within the reader). Compare with On-line System.
Standby	In relation to power supply, refers to the operation of the system (perhaps with reduced functionality) when the mains supply is unavailable. Usually this is achieved with a battery backup.
Status	See Door Status, Lock Status.
Unique ID / UID	See Chip Serial Number (CSN).
Tailgating / Piggybacking	When a person, without using a credential, passes through a portal with a person for whom access has been granted.

Tamper detection	A means for the detecting unauthorised interference with a component of an access control system.
Tamper protection	Methods used to protect an access control system or part thereof against deliberate interference.
Time and Attendance	A facility where the use of credentials is monitored for the purposes of tracking the hours when an employee is on site. For this purpose additional readers may be used that do not form part of the access control system.
Time Scheduled Free Access	A period of time according to pre-set rules for which the system does not control access.
Timed Anti-passback	A system feature, which denies a second access in violation of an anti-passback rule to the same area to a credential until a defined period of time has elapsed.
Token	A credential containing a readable unique identifier. e.g, cards, keys, tags, etc. Tokens can be read from a distance (non-contact or proximity tokens) or by contact (where the token must physically touch a reader).
Transaction	An event corresponding to the release of a door following an access granted by the system.
Turnstile	A type of physical entrance device that mechanically restricts entry to a single person.
Uninterruptible power supply (UPS)	A device that maintains power to equipment (typically a computer) for a short period after mains failure. Its use is intended to prevent loss or corruption of data.
Visitor Escort	A feature that permits a credential temporarily assigned to a user (the visitor) to grant access or egress but only when used close in time to a credential belonging to a normal user (the escort).
Wiegand	A method of sending information between components. See 12.1.

3.2 Door Entry Systems compared to Access Control

There is often confusion between the terms door entry system and access control. This is in part because access control often includes door entry control as a feature and many systems sold as door entry systems include simple elements of access control.

A basic door entry system consists of a method by which a person inside a building can remotely open a door to allow entry to a visitor without the effort of going to the door. To achieve this they are typically coupled with microphones and sometimes cameras so that the operator can tell who entry is being given to. This type of system is fundamentally used to provide convenience. The security of the door is reliant on the locks fitted and on the users of the door. Tailgating is a common problem with such systems.

With older door entry systems the opening of the door from outside the secure area would usually have been done using a traditional lock and key and would not have involved the electronic controls. When the electronic system is used, for example by adding a keypad outside the building and the property owner gaining entry using a PIN or a proximity token, then some aspects of access control may be included.

In some cases a standalone door entry system might be used with an access control system.
Care should be taken that wiring that controls locks for a door entry system are protected and located on the secure side of the door.

There is a standard for door entry systems: BS EN 50486 “Equipment for use in audio and video door-entry systems” but this may be replaced in the near future by a new series of standards developed by the international standards body, IEC, in the 62820 series.

Abbreviations

ANPR	Automatic Number Plate Recognition
BS	British Standard (from BSI British Standards Institute – www.bsigroup.com)
CSN	Chip Serial Number
DDA	Disability Discrimination Act
EN	European Norm (standard, see BS)
FAR	False Acceptance Rate
FMR	False Match Rate
FRR	False Rejection Rate
ID	Identification
LAN	Local Area Network
LPCB	Loss Prevention Certification Board (www.redbooklive.com)
LPS	Loss Prevention Standard (from LPCB)
NSI	National Security Inspectorate (www.nsi.org.uk)
PAS	Publicly Available Specification (see BS)
PC	Personal Computer
PIN	Personal Identification Number
PSU	Power Supply Unit
REX	Request-to-Exit
RFID	Radio Frequency Identification
SLA	Service Level Agreement
SSAIB	Security Systems and Alarms Inspection Board (www.ssaib.org)
STS	Security Technical Schedule (from Warrington Certification – www.warringtonfire.net)
T&A	Time and Attendance
UID	Unique Identity (see CSN)
UPS	Uninterruptible power supply
WAN	Wide Area Network
WCL	Warrington Certification Limited

4. Reasons for fitting access control

4.1 Introduction

Whilst users of access control may simply consider it to be a part of the building security there are many other reasons to use access control systems. Many of these not only provide a useful and convenient feature but can also serve as a way of reducing costs or enabling compliance with regulations. This section highlights some of the reasons why an access control system is useful. A specifier should consider whether any of the possible reasons might affect the system design.

4.2 Security

Access Control is a 24/7 electronic security solution providing physical and operational security whilst your premises is open or closed.

- A physical deterrent at perimeter access points reducing walk-in theft and attack
- A means of restricting access to company data and assets
- Keeping untrained/unauthorised persons from hazardous areas
- Replaces cost and management of physical keys
- Overcomes need to replace locks if keys lost/stolen
- Control and audit of authorised persons – instant granting or removing access rights
- Controls and monitors who goes where and when

4.3 Environmental

Often overlooked, the environmental benefits of a well deployed access control system can include:-

- Determination of building occupancy and usage to increase efficiency
- Control of lighting and heating based on occupancy
- Door monitoring can help prevent heat loss
- Remote barrier/door control can reduce the need to visit unattended sites to provide access
- Reduce wastage by control of printers, copiers and ancillary equipment.

4.4 Health & Safety

Controlled access to areas and equipment based on competency can assist in compliance with health and safety objectives.

- Limit access to areas and equipment to authorised and trained users
- Integrate with training and competency systems
- Update access based upon competency and training
- Provides detailed H&S access reports
- Can be used to monitor exposure in hazardous areas
- Limit access to areas containing dangerous or hazardous equipment/materials
- Restrict access to contaminated areas or areas under construction.

4.5 IT

Integrate with IT Systems to control access through a single system.

- Use Active Directory to manage your users
- Control Single Sign On access based upon users location
- No more orphaned users in the access system
- Use existing IT infrastructure to reduce installation cost and disruption
- Centralised control and monitoring of remote and multiple sites.

4.6 Integration

A variety of systems can be integrated with access control providing benefits including the following:

- Lift Control – restrict access to unauthorised floors (e.g. hotel floors)
- Elevator Dispatch – efficient direction of users to lifts
- CCTV – link access events with CCTV (e.g. door forced or secondary verification)
- Fire – control of doors and site plan integration
- Intruder Alarms – preventing false alarms (by accidental entry or setting occupied area)
- Building Management System (BMS) – for environmental control using occupancy information
- HR – integration of personnel data with access profiles
- School and student management systems – integration of student data with access profiles
- Cashless Vending – common card for vending and access
- Library systems – common card for lending and access control
- Visitor management systems
- Car park systems – common cards and shared restrictions
- IT / Logical security access (e.g. prevent log on to PC if not logged into building)
- Asset management – control movement of assets and link to user
- Audio video intercom – combined use of readers, remote visitor access, etc
- Guard Tour – use access control readers to manage guard behaviour.

See also Section 18 Interoperability

4.7 Finance

Access Control saves you money by reducing losses, securing assets including staff & property and reducing potential health and safety claims.

- Provides a return on investment by reducing the risk of losses and claims
- A secure environment improves staff morale, productivity and efficiency
- Reduces the risk of financial claims (see Health and Safety)
- Reducing lost revenue from expired memberships
- Reduce wastage by control of printers, copiers and ancillary equipment
- Identify and allocate usage to cost centres (e.g. copiers)
- Identify building usage to reduce costs (e.g. canteen needs)
- Restrict access to private company/hotel car parks
- Monitor contractor hours on site.

4.8 Personnel Management (HR & Time & Attendance)

Commonly integrated with Access Control, Time and Attendance (T&A) is a system to record when employees start and stop work and what jobs they may be working on.

- Improve punctuality and reduce unscheduled breaks
- Increased efficiency by removing manual time sheets
- Know who is working in your organisation and what they're doing
- Centralised HR, AC and T&A reducing administration and increasing security.

4.9 Duty of Care

Control access or limit egress to demonstrate Duty of care.

- Limit access to areas containing dangerous or hazardous equipment/materials
- Restrict access to contaminated areas or areas under construction
- Protection of personal assets (controlled access to locker rooms /staff only areas)
- Record working hours for time on site and time spent in restricted areas etc.
- Prevent off street walk-ins protecting lone or vulnerable staff.
- Restrict access to walk-in freezers
- Wandering patient protection
- Protection of infants and children in nurseries/schools
  – Restrict access by unauthorised members of public
  – Prevent unauthorised egress by unaccompanied minors
- Control of equipment or tools in and out of hazardous / restricted areas
- Restrict access to private company/hotel car parks
- Supervisor mode for teachers restricting pupil access to classrooms / workshops / swimming pools
- Supervisor mode to escort visitors/contractors into restricted areas
- Dual access for opening high risk areas to ensure individuals are not put at risk
- Record additional information against user credential in custom field e.g. Next of Kin, blood group, known health risks, emergency contact numbers etc.

4.10 Compliance & audit

The access control system can provide reports to aid compliance and audit requirements.

- Automatically log which areas users are accessing and when for compliance purposes
- Automatically reports which areas users have accessed
- Records access denied attempts by areas
- Set alarms on occupancy count for fire loading compliance
- Record working time for each user
- Operator audit logs for change monitoring
- Compliance with industry regulations (e.g. food safety, financial trading, border security).

4.11 Facilities Management

Access Control provides an essential support package to facilities management teams. Aside from day to day access management, additional benefits include:-

- Monitor contractor hours on site
- Ensure only qualified and trained operatives gain access to sensitive / hazardous areas
- Permit-to-Work management
- Manage public holiday and non-business hours access
- Visitor Management
- Fire roll call reports for emergency mustering

5. System Components

5.1 Access control system components and their operation

An access Control System typically consists of a number of components from those that identify a person to those that authorise access. This section defines the main components in the system.

5.2 Credentials

A credential is a physical or tangible object, a piece of knowledge or a facet of a person's physical being that enables an individual to gain access to a controlled area. Typically, credentials can be something you know (such as number or PIN), something you have (such as an access token), something you are (such as a biometric feature) or any combination of these. The typical credential is an access card, key fob, or other token.

5.2.1 Codes

A code is something that you know. Normally codes are either common (common code or group code) or personal (PIN). Codes are normally 4, 5 or 6 characters long and are usually numerical only. Care must be taken when using codes to identify individuals as they can be easily copied. When used to verify individuals, codes can provide higher levels of security – e.g. used with another credential. If used by themselves then the number of different PINs on a reader must be kept low in order that a PIN cannot be guessed by chance. BS EN 60839-11-1, Table 4, requires that, when PINs are used alone, there should be at least 1000 times more possible PINs than there are users (i.e. actual PINs).

5.2.2 Tokens

A token is something that you have. There are a large number of tokens available and they vary in both characteristics and price.

- **Swipe** – Swipe cards use a variety of technologies including magnetic strip to hold identification data. This is read into a reader by swiping or inserting. Swipe cards are usually cheap but easily copied and deteriorate over time, needing to be replaced quite often.
- **Contact** – These are cheap cards or tags that have contacts on the surface e.g. a chip and pin bank card. More difficult to copy than swipe cards but do deteriorate over time.
- **Passive proximity** – These are relatively cheap cards or tags that have small chips inside. They can transmit the user number a short distance (normally less than 15cm) to a reader. These are less easy to copy and relatively long living since they receive less wear and the chip is protected inside the card.
- **Active proximity** – These cards use batteries to give a longer range than passive cards. The batteries are normally long life but depending on use may need to be replaced every few years. Active cards and tags can be used for longer range access control for vehicle access, comply with the DDA or for "hands free" access. Typical reading ranges from 0.5m to 10m.
- **RFID** – In access control terms RFID normally refers to contactless smart cards. These cards act very like passive proximity cards and tags except that they can hold much more data and the reader can write this data to the card. This enables multiple uses for the card. This type of card can also be used in off-line access control systems.
- **Mobile devices** – Devices such as phones can operate as a token in a variety of ways. They can use NFC or Bluetooth Low Energy (BLE) to provide an identity over a short range.

5.2.3 Biometric

Biometric data is something that you are. Again, there are a large number of different biometric reading technologies available. In each case there is a secondary consideration to make on whether to use biometric identification or biometric verification.

Biometric Verification (Also known as “One to One” (1:1) technology) is where the user’s biometric sample is compared to a single template stored by the biometric system. The user identifies themselves to the system (e.g. via a keypad, smartcard, etc), and then a biometric feature is scanned. The system then verifies that the biometric feature matches the information stored against the user already identified. This method is usually quick because the biometric system does not need to search through all records stored to find the user’s template.

Biometric Identification (Also known as “One to Many” (1:N) technology) is where the recorded biometric feature is compared to all biometric data saved in a system. This method is referred to as identification due to the user being unknown to the system prior to providing a biometric sample. If there is a match, the identification is successful, and the corresponding user name or user ID may be processed subsequently. The speed of identification can deteriorate proportionally with the greater number of users enrolled.

Verification is normally faster than identification and more secure but requires multiple reading technologies at the access point. Care must be taken with biometric readers where high security is required that there is an acceptably low FAR (False Acceptance Rate) for identification or low FMR (False Match Rate) for verification. Manufacturers’ data should be checked carefully for this figure as it can vary greatly. In particular if comparing manufacturers it should be checked that values quoted are based on a like-for-like measurement.

Table 1 – Comparison of Biometric Technologies

Biometric characteristic	User Acceptability	Accuracy	Costs
Fingerprint	HIGH	LOW to HIGH*	LOW to MEDIUM*
Facial recognition	MEDIUM	HIGH	MEDIUM
Iris	MEDIUM	HIGH	MEDIUM
Retina	LOW	HIGH	HIGH
Hand geometry	MEDIUM	MEDIUM	MEDIUM
Vein Recognition	HIGH	HIGH	MEDIUM
Voice	HIGH	LOW	MEDIUM
* Depends on the quality of the system and its FRR and FAR NOTE: This table was correct at the time of writing but technological advances may cause this to change.			

There is a trade-off between accuracy and costs that often means fingerprint technology is used for access control. Care must be taken on availability since not everyone has a fingerprint whereas almost everyone has a facial geometry that can be read. Iris scanning is the most secure but also the most expensive.

The BS EN 60839-11-1 standard gives requirements for biometrics based on False Acceptance Rates (FAR). They refer to FAR and FAReff (effective FAR). The latter takes into account the number of users because a system with more users is more likely to have an approximate match to an unauthorised user. This is not relevant if two factor authentication is used because it then requires a match of the biometric measurement to the user identified by the other means.

FAReff = n x FAR where “n” is the number of registered biometric templates (users). So if a piece of equipment has a FAR of 0.001% and the system has 1000 users then the FAReff is 1%.

The requirement is for the FAR (with two or more factor authentication) or the FAReff to be better than the following.

Table 2 - Maximum False Alarm Rate by Grade

Grade	1	2	3	4
FAR or FAReff	1%	0.3%	0.3%	0.1%

5.3 Human Verification

5.3.1 General

Human verification is a procedural method by which access through a door is granted by a person either at the door or remotely. When used as the sole method of permitting access this is not considered part of an access control system. It can however be used as an extra security measure so that the user is initially identified by an electronic system but only the subsequent verification by a human operator permits the door to open. This method also allows for checks against tailgating.

Event audit trails can provide information on who allowed access, answered or initiated a call, the call time, date, relevant door, duration and action taken.

5.3.2 Human image verification

To increase the security of a system, a challenge or video verification mode is often available. When a token is presented at a reader, an operator at a PC is presented with the stored photograph of the user, together with a live image from a camera viewing the reader. Depending on whether the operator identifies the person in the live image against the displayed photograph, access can be manually granted or denied.

Specific personal data (name, details etc.) may also be displayed to the operator to aid identification.

5.3.3 Other human identity verification methods

Alternative method that does not use an image can be employed. For example, systems can provide human verification via audio means by integrating with multiple IP based intercoms for remote door control.

5.4 Readers

Access control readers may be classified by functions they are able to perform:

5.4.1 Standalone readers and keypads

These have all the necessary inputs and outputs to control door hardware, as well as the memory and processing power to make access decisions independently. A standalone reader usually has one credential (e.g. common code) and anyone knowing that code is allowed access through the door. The access decision logic can be made on the unsecure side of the access point.

5.4.2 System readers

These devices read the credential from a card, or a PIN from a keypad and forward the data to a controller. Most also provide an audio and visual method of feedback to indicate to the user whether access has been granted or denied.

5.4.3 Combined reader / controller

As the name suggests, some system readers combine the functions of the reader and the controller in a single device. They hold a copy of the user database allowing them to make the decision to grant or deny access even if the controller cannot access the network. The access decision logic can be made on the unsecure side of the access point.

5.4.4 Offline Readers

An offline reader differs from a combined reader / controller in that it does not maintain a database. With offline readers, the card itself holds the information that defines which doors are valid, and the times that access is allowed. The offline reader analyses this information and grants or denies access as appropriate.

5.4.5 Online Readers

An online reader differs from a combined reader / controller in that it does not maintain a database. With online readers the access decision is typically made by a connected computer which then sends an open command if authenticated or the decision may be made within the reader itself and immediately communicated to the central system. The advantage of online readers is ease of installation but with real-time door and event monitoring.

5.5 Reader Interfaces

In some systems, one or more readers and the relevant door hardware are connected to a reader interface (see Figure 1 - Reader Interface). The reader interface analyses the data from the readers and transfers it to the system controller (see 5.6 Controllers). Control of the door hardware is run from the reader interface which is normally in close proximity to the access point and will act depending on signals from the controller it is connected to.

The reader interface may also contain a small number of specific users in order that access can still be granted in degraded mode if there is a problem with the main system controller.

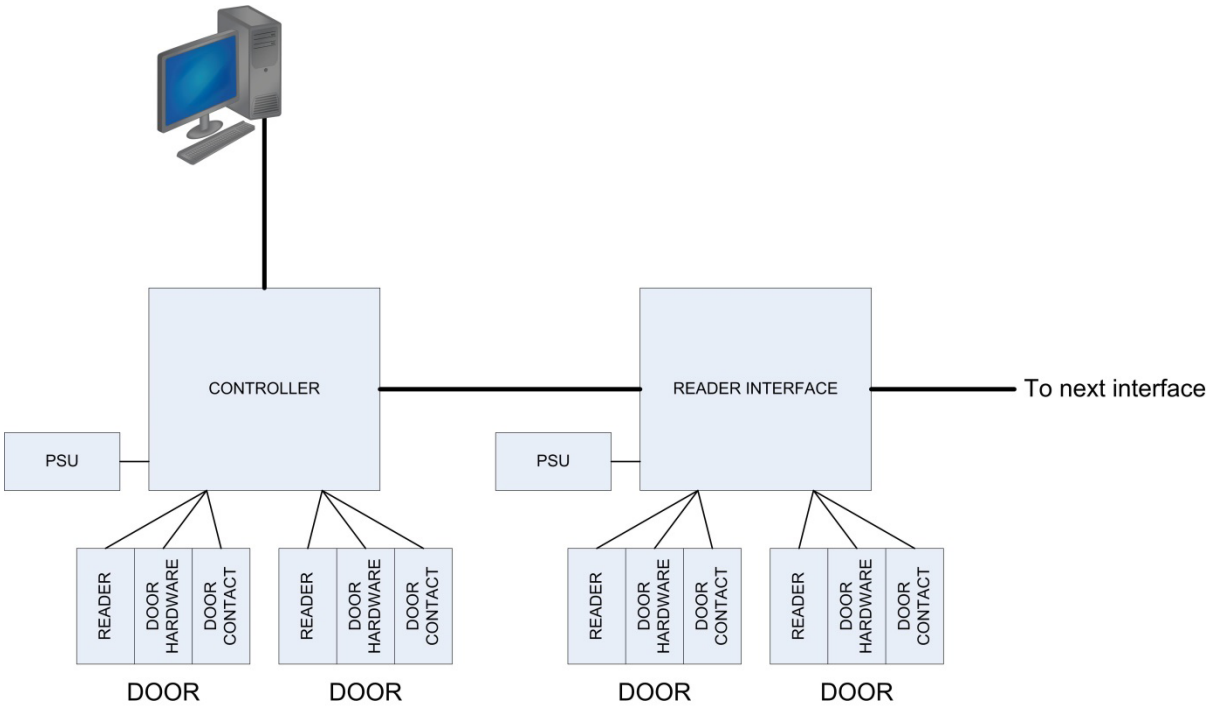


Figure 1 - Reader Interface

5.6 Controllers

In some networked systems, one or more readers and the relevant door hardware are connected directly to a controller (see Figure 1 - Reader Interface). Otherwise the controller will connect to reader interfaces (see 5.5).

These intelligent devices hold information in a local database required to decide whether a user is allowed through a door at a given date and time. The controller should also be capable of working off-line should the network communications fail for any reason.

Controllers can be connected to a PC through a variety of interconnection methods. Subject to how the controllers communicate, alarm events and card transactions may be passed to other controllers. This communication can be used for event driven actions, such as activating a sounder in a different area, or for access control features such as anti-passback. This communication is often dependent upon the PC or master controller being operational and full communications being on-line.

In addition to storing credentials, access groups and time zones, controllers will also store transactions should the system go off-line. Then, once the communication path with the system PC or master controller is re-established, the audit trail of access and alarm events will be uploaded with date & time stamp.

Operation of the system is highly dependent on the controller, so consideration should be given to the number of readers connected to any one device. Failure of one controller could affect a large number of controlled points depending on the system design.

5.7 Power Supply Units (PSUs)

The power supply requirements should be carefully checked to ensure that all necessary door hardware, including the chosen locks, can be supported simultaneously. It may be necessary to utilise a separate power supply for controlling the lock hardware.

If a controller does not contain its own power supply then a suitable PSU should be provided in accordance with the manufacturers recommendations.

It is recommended that systems be provided with battery back-up in the event of mains failure. The duration of standby should be agreed with the end user. It is recommended that the power supply standby batteries are monitored.

5.8 PC & Software

The system software may range from a simple standalone solution installed on a PC in an insecure area to a secure solution installed on a server in a controlled area. Web/App based systems are also available which allow an authorised person to gain access from any PC or mobile device. Careful consideration should be given to the level of access available, and the location of the software or any terminals.

It is important to ensure that the PC provided for the system meets the minimum specification recommended by the manufacturer.

In place of a standard PC or server, some systems now provide a controller with an industrial grade PC pre-loaded with the system software. This will be battery backed overcoming issues caused by mains failure. These devices are connected directly to either a dedicated or existing LAN/WAN or can be used in more traditional wiring configurations.

For more information about IP Based Networks refer to the BSIA Guides listed in 21 Further Reading.

In addition to access control features, the software may offer ID badging, integration with intruder or video surveillance systems, lift control etc. There are a wide variety of options available providing a better return on investment and a system that is easier to use and manage.

Some access control systems are now ‘hosted’, with the software located offsite. Administration of the system can be handled by the end user via a web browser, or it may be fully managed by a third party on behalf of the end user, reducing the need for on-site user training, PC hardware and ID badge production equipment.

5.9 Programmers

If a system is not PC based, then a means of programming the system must be supplied, with a minimum requirement of adding and deleting cards. This could be via a hand held device, or keypad and display forming part of the master controller.

These devices should be password controlled and are often very simple to operate by means of Yes/No questions, allowing basic access to be granted which can also include day/time schedules on larger systems. For many entry level applications this solution is adequate for the level of security required BUT manual records of card holder details must be kept so that lost/stolen cards can be deleted as it is unlikely the user record will be 'named'. The system may also lose the facility to provide historical reports of who went where and when.

5.10 Door Status Monitoring

A door contact is used for sensing opening and closing of a controlled door. Typical door contacts are made up of two component parts: the contact switch that is installed on the door frame; and a magnet that is mounted on the door.

Door contacts are used to monitor events such as:

- Door forced alarm – a door being opened without the use of the reader or normal egress device
- Door held alarm – someone holding the door for another party or blocking the door for delivery or to return later if they have no card.

Door contacts are recommended for higher grades of security (see Section 6.1). BS EN 60839-11-1 requires the monitoring of doors in grades 2 to 4.

Use of Door Contacts by Grade	Grade 1	Grade 2	Grade 3	Grade 4
	Optional	Mandatory		

Table 3 – Use of Door contacts

5.11 Lock Status Monitoring

Lock monitoring is used to indicate whether a closed door is locked or not. This is not an alternative to monitoring the door and should only be used in addition to door contacts.

5.12 Egress devices

Having replaced (or disabled) standard lock sets in most access control installations, a means of providing controlled and authorised egress may be required so that any door monitoring contact is isolated for the approved period of the door release. This is commonly achieved with a simple Request-to-Exit switch, a movement sensor or a reader.

Also refer to disability anti-discrimination regulations relating to control of doors.

5.12.1 Normal Egress

Egress buttons are the most common form of device used. These can be simple light duty rocker switches, heavy duty buttons or a touch sensitive switch – all of which send a signal to the controller to release the door lock. A variation of the egress button is the monitored handle where the egress is requested by a switch in the exit handle that is activated every time the door handle is depressed.

If a movement sensor is used this should be designed for the purpose. The detection pattern must be fully adjustable to ensure that the door release is only signalled by a person wishing to leave and not simply walking past the door or standing in the general vicinity.

In addition to normal egress, a means of override will be required from the secure area and possibly from outside of the controlled area.

For fail safe locking, such as a maglock or shear lock, where no key override is supplied, then a means of removing the power from the lock from the unsecure side may be required if this is the only entrance into the secure area – or if all doors are controlled (see 5.12.2).

5.12.2 Emergency Egress

To comply with local authority and building regulations and to meet local fire officer requirements, emergency egress must not depend on the operation of the access control systems controller, software etc. In the case of Fail Safe locks this is normally provided by a green break glass device. Operation of this device will remove power from the lock and the door is no longer secure. This device should be monitored to show its operation. Opening an access control monitored door in this way would generate an alarm event (Door Forced). A green break glass device should not be used alone when there is a requirement for a single action mechanical override (see BS 1125 and BS EN 179) to allow for means of escape through doors on an emergency escape route.

It is considered best practice to use a double or even triple pole break glass units to ensure both positive and negative connections are released and reporting of break glass activation in the case of the triple pole unit.

It is the responsibility of the site's 'responsible person' to carry out an audit as required by the Regulatory Reform (Fire Safety) Order 2005.

5.13 Operation

For an on-line system, when a credential is presented to a reader, the information is sent to a door controller. The controller compares the credential to a list of authorised users in the database. If there is a match (taking account of the day/time of the request if applicable), the controller will send a signal to release the door lock, gate, barrier or turnstile. The controller will then ignore a door open signal generated by a monitor contact to prevent an alarm. A signal is sent to the reader to provide audio/visual feedback to the user to show that access is granted.

For an off-line system, when a credential is presented to a reader, the reader checks with the data on the credential if the user is allowed through the access point at that time. If access is allowed the reader will allow access and then update the credential with this information. At some point the credential must be used at a reader connected to a controller so that all transaction data on the credential can be logged and any changes in access rights can be written to the credential.

Generally entry is controlled and exit is uncontrolled. If exit is to be controlled, a second reader is needed on the secure side of the door; otherwise, a Request-to-Exit push button is normally used.

An important safety feature to consider is the ability to exit a door if the access control system is unavailable – this is called mechanical free egress. This is usually achieved with a green break glass device that removes power from the lock. This must always conform to local authority building regulations and fire officer requirements.

6. Security Levels

6.1 Security Grading

Access control points are graded according to the type of business and risk associated with the premises being secured. The grade applies to the protected area and not the overall system, therefore mixed grades may be utilised within any premises.

6.1.1 Access Point Grading

There are four grades:

Grade 1 (Low Risk)
A standalone lock (code, PIN or token), or off-line system, controlled in a public area for low risk situations.

Example token technology: Proximity and Mifare Classic card technologies.

Typical examples: Internal doors or areas where you want to stop the public wandering in.

Grade 2 (Low to medium risk)
An on-line system utilising tokens or PINs to prevent access to the premises. Events are received in real-time on the monitoring software.

Example token technology: Proximity and Mifare Classic cards should not be used due to the issue of cloning that is available. Mifare PLUS SL3 or higher technology should be utilised.

Typical examples: Commercial offices and small businesses, hotels.

Grade 3 (Medium to high risk)
An on-line system using two factor authentication or single-factor biometric to prevent access to the premises. Events are received in real-time on the monitoring software.

Example token technology: Mifare PLUS SL3 or DESfire.

Typical examples: secure areas of commercial business such as server rooms, data centres.

Grade 4 (High risk)
An on-line system using two (or more) factor authentication, one of which should be biometric or human image verification to prevent access to the premises. Events are received in real-time on the monitoring software. When using biometrics careful selection of the quality to reduce FAR shall be made. (See section 5.2.3)

Example token technology: Mifare DESfire

Typical examples: High security areas, such as MOD, Government, research labs.

The grade applied to each point may increase with time according to the requirements, for example, card only during office hours and card and PIN outside hours.

For more information refer to BSIA Form 198, A Guide to Token and Reader Technology in Access Control Systems

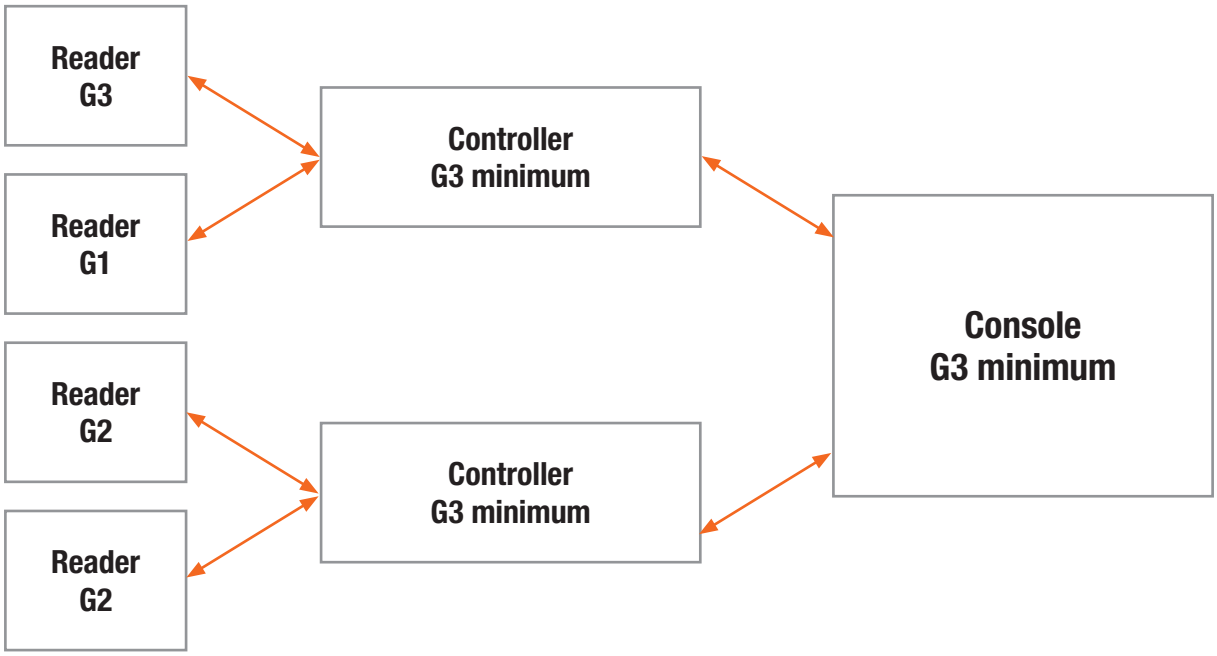
6.1.2 How grading is used to comply with the 60839-11 series of standards

This is described in BS EN 60839-11-2.

The starting point for grading is to assess the relevant risk at each door (or access point) to the building. The equipment used to provide access control at that door should then meet all of the requirements needed to meet that grade.

Any parts of the system that are shared by more than one door must then have a grade equal to or better than the highest graded door.

If this can't be achieved for practical reasons then the recommended approach is to have more than one access control system.



6.1.3 Other components

Within any system the main components that control and monitor the system, for example the PC and software must meet the highest grade installed. The following should also be considered for all systems:

- PC / software access, auto lock when operator away from PC
- UPS on PC
- Battery backup of controllers
- Logical access
- Encryption
- Physical location of PC

6.1.4 System Passwords

Consideration should be given to the use of complex passwords that conform to the latest recommendations for IT security.

It has been said that "The only secure password is the one you can't remember"[1]

Any password that you define and use for accessing your security system should be strong. A strong password is one that is long and random (in terms of both character and sequence). Tools such as LastPass and KeyPass should be used for managing passwords. You should not use the same password for multiple systems and never write the password down. Remember, even though the system may be inside the corporate firewall, access to the system could allow a 'hacker' to change or assign access privileges.

6.2 Cross reference of grading to other schemes

Table 4 shows the approximate relationship between the recommendations for grading in this guide, the security classification used in the BS EN 60839-11 series and the classification used by NSI in their Code of Practice for Planning, Installation and Maintenance of Access Control Systems NCP109.

Access Security Grade	NSI NCP109 Classes	Permitted at BS EN 60839-11-1 Grade	Access Grade
4	4	1, 2, 3, 4	3 factor including biometric / human image verification
4	4	1, 2, 3, 4	2 factor (see Table 10- Reader applicability) including biometric /human image verification
3	3	1,2, 3, 4	2 factor (non-biometric)
3	3	1,2, 3, 4	1 factor biometric
2	2	1,2, 3, 4	Token
1, 2	1, 2	1, 2	PIN
1	1	1,2, 3, 4	Standalone lock with token
1	1	1, 2	Standalone lock with code

Table 4 - Security Grading Cross Reference

[1] Troy Hunt 21/3/2011 (http://www.troyhunt.com/2011/03/only-secure-password-is-one-you-cant.html)

7. Door Types

There is an obvious association between the security provided by a door and its frame and the associated access control system. It can however be recognised that the access control system may be supplemented outside normal opening hours by extra security provision. The following table gives an indication of the relationship between the holding force applied by the access control locking system and the materials of a door together with any testing and certification of the door.

Holding Force	Hollow Core	Softwood / uPVC	Hardwood	Steel
3kN	Internal door – not security, privacy only	Internal door – not security, privacy only		
5kN		Internal door – not security, privacy only	*PAS 24, STS201* Internal door – low risk only	
7kN		Internal door – not security, privacy only	*PAS 24, STS201* *LPS 1175 SR 1, STS 202 BR 1* Low risk external doors (use with separate night locking) Medium risk internal doors	*PAS 24,* *LPS 1175 SR 2, STS 202 BR 2* Medium risk external doors (use with separate night locking) Medium risk internal doors
10kN			*PAS 24,* *LPS 1175 SR 2, STS 202 BR 2* (depending on door) Medium risk external and internal	*PAS 24,* *LPS 1175 SR 2, STS 202 BR 2* Medium risk external and internal
12kN			*PAS 24,* *LPS 1175 SR 2, STS 202 BR 2* (depending on door) Medium risk external and internal	*LPS 1175 SR 3, STS 202 BR 3* Medium / high risk external

Key:
LPS 1175: Certified by LPCB to LPS 1175 with Security Rating (SR) as indicated. (SR can be from 1 to 8)
PAS 24: tested to meet PAS 24 (published by British Standards)
STS201: Certified by Warrington Certification to PAS 23/24 (formerly WCL1)
STS202: Certified by Warrington Certification to STS 202 (formerly WCL2) with Burglary Rating (BR) as indicated. (BR can be from 1 to 6)
For details of Warrington Certification and LPCB see 2. Referenced Documents

Table 5 – Door types and holding force

kN	Pounds (lbs)	kg
0.45	100	45.4
1.0	225	102
1.5	337	153
3.0	674	306
5.0	1125	509
7.0	1570	713
10.0	2250	1020
12.0	2700	1220
15.0	3370	1530
Note: Conversions are approximate		

Table 6 - Comparison of forces in lbs, kg and kN

Table 7 shows the recommended holding force for a door by grade.

Holding Force	Grade
3kN	1
5kN	2
7kN	3
>=10kN	4

Table 7 - Holding Forces - recommendation by grade

8. Lock Types

8.1 Precautions regarding types of lock and fire escape

It should be noted that Electrically Controlled Locks as mentioned can be either:-

- Fail Safe (fail open) = Voltage applied to lock
- Fail Secure (fail locked) = Voltage removed to lock

Therefore it is paramount that the lock choice consideration should be well thought out before installing on a Fire Door which is part of the exit route.

The recommended solution is FAIL SAFE Voltage Removed as this can be easily achieved by installing an Emergency Call Point (Break Glass) to cut the supply voltage.

However applying a voltage to open a lock in an emergency situation is not recommended therefore if a FAIL SECURE lock is to be used then there has to be a manual solution to open the door i.e. Door Handle / Panic Bar etc.

8.2 Maglocks

Description

An electric magnet is perhaps the simplest means of remotely locking and unlocking doors. These again can vary tremendously in cost and performance ranging from 1kN to 14kN holding forces. The principle is very simply an electro-magnet and a ferrous plate that are in contact when the door is closed. The magnetic field is only on when an electric current (12v dc) is passed through the electromagnet. Because of this they are only available as fail unsecure (unlocked) and this reason alone they are generally seen as low security solutions.

Security

Security is generally low as power failure to the magnet will release the door. Often only one magnet is used at the head of the door (top). The door can become vulnerable if attacked at the base through either the door failing or sufficient leverage being gained to break the holding force on the magnet.

Installation

Installation of the electromagnet is generally very easy and straight forward with power only being required to the frame. It is important for the alignment between the electro magnet and the ferrous plate to be correct to achieve the specified holding force. If the electromagnet is mounted on the top of the doorframe it is important that it does not restrict the height through the door sufficiently for it to become a health and safety issue. There have been a number of incidents where people have injured themselves on overhead electromagnets mounted on the doorframe.

Applications

The electromagnet is generally used on low security doors with medium to heavy traffic. It is suitable on internal doors or external doors if there is a further mechanical lock for use at night or outside normal business hours.

8.3 Shearmags or Shearlocks

A shearmag or shearlock 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 and often require larger amounts of power to operate.

8.4 Electric strikes

Description

An electric strike, or as it is sometimes described an electric release, is perhaps one of the most popular methods of unlocking a door electrically. It works on the principle of a solenoid which, when powered, moves a small pin that in turn engages or disengages a blocking mechanism which then allows a moving plate (usually referred to as the staple) to be released. This allows the release of a lock's latch from the keep in the frame.

Security

The electric release is not always seen as the most secure means of electrically locking a door. They do however vary tremendously in their holding power from 1.5kN of side force up to 14kN or more on some of the higher security versions. Some versions are available with a monitoring switch that can detect whether the latch is engaged. This can save the need for a door monitor. The fact that the release is fitted to the doorframe also means that the doorframe material and size affect the security. Most strikes can be specified fail secure (locked) or fail insecure (unlocked), this being the status of the lock when power is withdrawn.

Installation

Generally easy to install as the strike is mounted in the door frame in the place of a conventional lock strike, so it is relatively easy to get electrical power (usually 12V dc) to the unit. It is important that the latch on the lock is of the correct dimensions to work with the strike and the fitting needs to be precise to ensure the two units engage and work correctly without binding.

Applications

The electric strike is generally used on low to medium security doors with medium to heavy traffic. It is suitable on internal doors or external doors if there is a further mechanical lock for use at night or outside normal business hours.

8.5 Solenoid Locks

Description

A solenoid lock works in a similar way to an electric strike but the mechanism is contained within the lock case. The solenoid moves a pin, which engages or disengages the handle movement to the latch. In the locked position the handle will move as normal but will not connect to the latch, so the handle moves freely but has no effect. In the unlocked position the lock will respond like a conventional lock with movement on the handle pulling the latch in.

Security

This type of lock can achieve quite high levels of security as the lock will behave much like a traditional lock under attack. Most of these locks operate with a deadlocking latch lock, which in most instances will not give quite the high level of engagement as a standard deadlock. Like an electric release these can be specified as fail secure or fail insecure. These can be specified with different functions inside to outside. For example the inside lever handle can always be active (for emergency egress) but the external handle is only engaged when the solenoid is operated.

Installation

Installation can be a bit more involved and specialist, the main challenge is to get cabling to the back of the lock mortise on the door where the lock is to be installed. This will involve a door loop to transfer the cable from the frame to the door leaf. On a timber door this may also involve drilling a 5mm hole across the width of the door leaf. One of the benefits of the solenoid lock is that it appears to be a conventional lock from outward appearances and will match closely other locks and door furniture on a site.

Applications

The solenoid lock is generally used on medium security doors with medium to heavy traffic. It is suitable on internal doors or external doors up to a medium security application. Some solenoid locks have a built in mechanical deadbolt for dead locking for out of hours.

8.6 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.

8.7 Motor locks

Description

In outward appearance they appear very similar to a solenoid lock but rather than a solenoid have an electric motor that drives a dead bolt.

Security

This type of lock can achieve as high a security level as any mechanical single point lock generally and will behave much like a traditional lock under attack. Most of these locks operate with a deadbolt, which in the correct door and frame installation can achieve high levels of security. In the event of a power failure the lock will remain in the status it was in at the time of the power failure.

Installation

Installation can be more involved and specialist, the main challenge is to get cabling to the back of the lock mortise on the door where the lock is to be installed. This will involve a door loop to transfer the cable from the frame to the door leaf. On a timber door this may also involve drilling a 5mm hole across the width of the door leaf. One of the benefits of the motor lock is that it appears to be a conventional lock from outward appearances and will match closely other locks and door furniture on a site. On many motor locks they require a small control box, which usually needs to be fitted in the vicinity of the door, often above a false ceiling on the secure side of the door.

Applications

The motor lock is generally used on higher security doors with medium to low traffic. This is because the lock takes a few seconds to withdraw the deadbolt. For an office entrance at peak times it would not be the best choice. It is suitable on both high security internal and external doors.

8.8 Electronically controlled multi-point lock

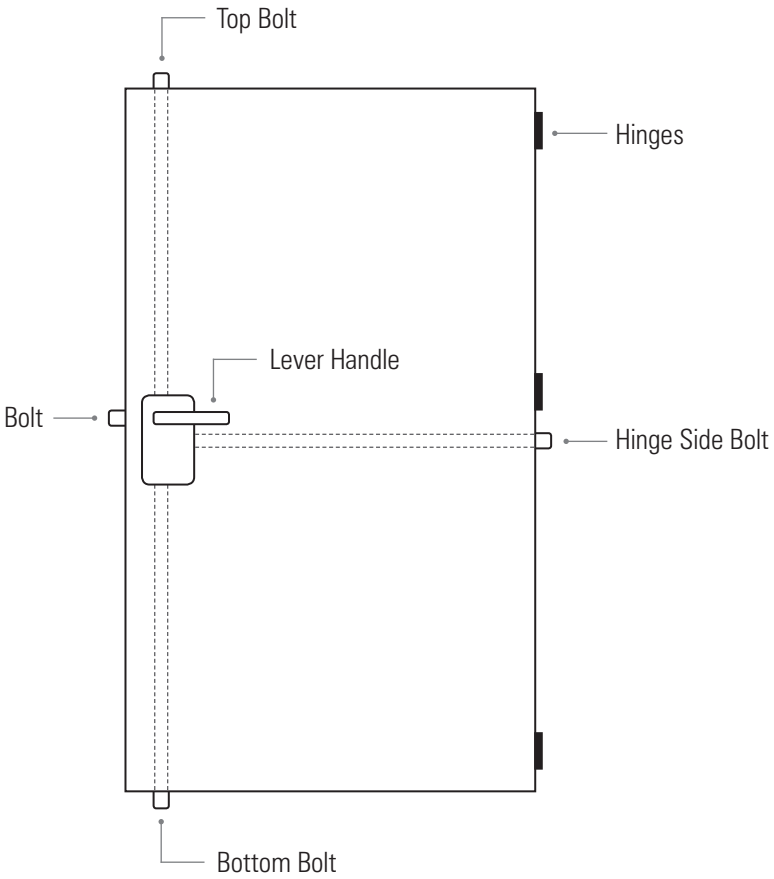
Description

For high security applications, multi-point locking mechanisms should be used. These would normally have a three point configuration, bolts at the top, bottom and non-hinge side of the door.

For very high security areas, this can be extended to four or five points to include the hinge side. These are usually installed in applications involving critical national infrastructure and government high security areas.

From an authorised input from the access control system, the operation is normally via a lever handle on the non-secure side to drive all the locking bolts inwards. The door is opened, and on closing the bolts would normally lock and automatically dead lock.

Egress can be via a handle which can be released via an egress button, or by the handle alone for emergency exit applications. The movement of the egress handle from the inside would signal an exit request to the main system.



9. Entrance Control

Entrance control includes pedestrian gates, barriers, turnstiles and doors.

Entrance control solutions form a part of the overall access control security classification. Entrance control products require an access control reader to be integrated with them so that users can present their credentials. The entrance control product increases the security level of the access control system by either providing a physical barrier to restrict unauthorised access or by providing a method of detecting unauthorised access and generating an alarm.

9.1 Door Type v Grading

The following table defines the type of allowable physical security based upon grade of access system.

Access Point Types (Entrances)			
Grade 1	**Grade 2**	**Grade 3**	**Grade 4**
Hollow Core external door	UPVC, Full or part glazed external door	Solid hardwood door	Steel doors
Softwood external door	Hollow Core internal door	Full height pedestrian entrances.	High security doors
Single arm pedestrian barrier	Softwood internal door	Roller shutter doors	Interlocking Doors e.g. Personal transfer units or commodity transfer units
Single arm vehicle barriers	Low-level pedestrian entrances	Top and bottom skirted vehicle barriers meeting a full height perimeter wall / fence	Deep vehicle road blocker / Rising kerbs (see PAS 68:2006)
	Roller shutter doors with windows or access doors	Full height sliding vehicle gate	
	Bottom skirted vehicle barriers	Surface or shallow Vehicle road blocker / Rising kerbs (see PAS 68:2006)	

Table 8- Entrance Selection

9.2 Turnstiles

The major difference between turnstiles and doors is that they restrict passage, usually allowing only one person to pass at a time. They can also enforce a single direction of passage and can stop people that have not paid a fee or presented correct identification. There are numerous ways that they can be used and in addition to access control they can be used for direction control (e.g. single direction exit from a property so that visitors must go to a controlled entrance) and revenue control (e.g. at a barrier requiring use of a ticket or coin).

Turnstiles are used in a variety of locations such as public-transport stations, office lobbies, toilets, visitor attractions, stadiums, etc.

As a security feature some turnstiles offer much greater security than others. For example, a full height turnstile can hinder a person from gaining access at an unattended location whereas a half-height turnstile can be jumped over. The latter may be suitable in an office lobby environment where access to the building lobby will have required entrance through a lockable door and reception staff can monitor the turnstile use.

Turnstiles can be used as the main method of access control (e.g. in a lobby) or be used in combination with access control of other entrances and exits (e.g. to permit people to leave without use of the access control system but enter using only an access controlled entrance).

Many designs of turnstile are available. Some of these have advantages over other types and overcome problems in usage. For example, the temporary need to open the turnstile entrance to allow free flow of people or goods may be impossible with certain designs.

Purchasers should consider many features of a turnstile before purchasing.

- How easy and obvious should it be to use?
- How will the turnstile be supplied, delivered and erected?
- How easy is it to supply power to the turnstile?
- Is appearance important?
- How fast should it operate? The slower the throughput, the more lanes will be required.
- How many lanes are required? Will they fit in the available space?
- Will the restrictions of the turnstile need to be removed from time to time or are there alternative routes?
- Would the turnstile prevent access or exit in the case of a fire?
- How tall should it be (to prevent jumping or climbing)?
- How strong should it be? How high a force should it resist?

It is particularly important to consider legislation relevant to avoiding discrimination against persons with disabilities (See BSIA Form 173, Access Control and Disability Discrimination).

9.2.1 Types of Turnstile

Tripod Barrier – A turnstile of traditional appearance where three arms on a base (like a three legged stool) rotate to allow passage.

Tripod Barrier

Optical Turnstile – These do not have a traditional barrier and instead use a detection method (e.g. infrared beams) and sound an alarm if unauthorised access is attempted.

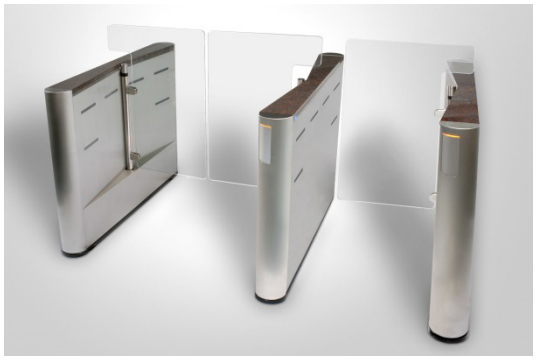
Optical turnstiles are the safest pedestrian solution as there are no moving barriers that will cause injury. This also makes them the ideal solution for wheelchairs. They could also be considered the most discreet and aesthetic solution. However, they are intended for use in well-managed reception areas where aesthetics is a priority.

Optical Turnstile

Speedgates – These have a form of motor driven barrier that is **Rising, Swinging** or **Sliding** depending on its method of moving into or away from the passage lane. These combine optical detection technology with a physical barrier. They can be normally open, in which case they close in front of an unauthorised person, or normally closed, opening when a person is authorised.

9.2.2 Types of Speedgate

Rising barrier



Swinging barrier

Sliding barrier

Entrance gate – This is a motor driven gate that swings to allow passage. Frequently these are now made of glass. Some models may have detection beams but most do not. The lack of detection before or after the barrier means that these products are not ideal for high throughput areas; they are usually installed as additional devices for wheelchair users or occasional wide deliveries.

Entrance turnstile – This is constructed like three gates attached to a vertical pole (like a short revolving door).

Entrance gate

Entrance turnstile

Full height turnstiles – These are usually rugged metal constructions tall enough to walk through and often associated with football stadiums.

Full height turnstile

“Airlock” / Security booth

“Airlock” / Security booths – These are constructions that work on a principle often described as an airlock. The person passes the first door which then closes before a second door opens. These can also be constructed using a rotating screen with an opening; the user steps through the opening into its centre and waits for the opening to rotate to the opposite side before leaving.

Revolving security door – Similar in appearance to a standard revolving door but incorporating access control and of higher strength.

Turnstile Type	DDA Compliant[1]	Physical Security Level[2]	Typical Appearance	Speed[3]	Ease of Use	Typical Cost	Emergency Egress[4]
Tripod Barrier	No	Medium	Prominent	Slow 15-25	Medium	Low – Medium	Hindered
Optical Turnstile	Yes	Low – Medium	Low Key	Fast 60	Easy	Medium	Unhindered
Rising Barrier	Yes	Medium	Medium	Fast 60	Medium	Medium – High	Unhindered
Sweeping Barrier			Medium	Fast 60	Medium		Unhindered
Sliding Barrier			Medium	Fast 60	Medium		Medium
Entrance Gate	Yes	Low – Medium	Low Key	Slow 15-25	Medium	Low – Medium	Medium
Entrance Turnstile	No	Medium	Medium	Slow 15-25	Medium	Medium	Hindered
Full Height Turnstile	No	High	Highly Prominent	Slow 15-25	Awkward	Medium	Hindered
"Airlock" / Security Booth	No	High	Highly Prominent	Slow 6-10	Awkward	High	Hindered
Revolving Security Door	No	Medium – High	Highly Prominent	Slow 10-15	Medium	High	Hindered

Key:

1. Shows whether a product of this type is typically DDA Compliant. Products may vary and compliance can be dependent on other circumstances.
2. Level of physical security compared to other turnstile types.
3. Speed measured in persons per minute.
4. Difficulty of gaining emergency access through the turnstile for a typical product of the type.

Table 9- Comparison of Turnstile Types

10. Reader / Token Technology

There are a number of different technologies that can be used as a token reader within an access control system. Each technology has a different level of security from the lowest (common code) through to highest (biometric with good FAR). Table 10 defines the suitability of the different reader technologies according to the grade of system being installed.

	Grade 1	Grade 2	Grade 3	Grade 4
Single Factor Authentication Options				
PIN (Common or Unique – minimum 10,000 differs)	XR	NP	NP	NP
PIN (Unique – 100,000 differs)	R	R	NP	NP
Magnetic or Proximity or RFID	R	R	P	P
Biometric	R	R	R	P
Two Factor Authentication Options				
Magnetic/Proximity/RFID & PIN (Unique)	R	R	R	P
Biometric & PIN (Unique)	R	R	R	P
Biometric & Magnetic/Proximity	R	R	R	P
Biometric & RFID	R	R	R	R*
Three Factor Authentication Options				
Biometric & PIN (Unique) & Magnetic/Proximity/RFID	R	R	R	R
Key: XR = Not permitted by BS EN 60839-11-1 NP = Not permitted by BE EN 60839-11-1 and not recommended by the BSIA R = Recommended P = Permitted by BS EN 60839-11-1 but not recommended by BSIA * with RFID, use of CSN alone is not recommended as the number can be read directly from the card. With other smartcard formats (e.g. MiFARE and DESFire) security keys are used to protect the data from unauthorised access.				
Note: When PIN is used in Two or Three Factor Authentication, a minimum of 10,000 differs is required.				

Table 10 – Reader applicability

Consideration should also be made to the possibility of duplication of the card number used. The type of technology used will determine the probability of a duplicate number occurring and its potential for being used to gain access to the system.

Note: When using a biometric system the manufacturers FAR and FRR figures should be checked to ensure that they can meet the system requirements.

10.1 Passive / Active

Tokens can be obtained in either a passive form (no batteries) or an active form (with batteries). Active tokens typically provide a longer read range (> 10m), however they will require replacing over the lifetime of the system with the frequency dependent upon their usage.

11. Special Features

This section covers a number of security and non-security related features that may be utilised to enhance the security of the system. The choice of additional features should be discussed with the end user.

- What it is
- How it works
- Advantages
- Disadvantages

11.1 Security related

11.1.1 Anti-passback

Anti-passback is designed to detect whether a user's credentials are used to enter an area when the system already believes the user to be in that area. This feature can be useful to stop a user who has entered an area from passing their token to another person outside the area. Three forms of anti-passback exist, namely hard, soft and timed.

Anti-passback rules are generally reset after a preset period after valid entry, at a fixed time each day, on exit from site or manually as an over-ride.

11.1.2 Anti-tailgate

Anti-tailgate is a feature designed to prevent a situation where an unauthorised person attempts to enter or exit a security controlled area by passing through the access controlled point at the same time or immediately after a valid user. Two forms of anti-tailgate exist, namely hard anti-tailgate and soft anti-tailgate:

- Hard anti-tailgate employs physical means such as turnstiles to restrict movement
- Soft anti-tailgate does not prevent the unauthorised person but uses detection methods to generate an alarm.

11.1.3 Multi card usage

The system may need to be flexible enough to support different token technologies (e.g. Mifare®, Magstripe, 125Khz) to grant access on a single system. In this instance, each registered user should be capable of having multiple tokens assigned to them.

11.1.4 Lift Control

Lift control is an extension to the concept of access control, using the user's credentials to grant access to floors, rather than granting access through a door.

For instance a token reader is fitted in each lift cab, using technologies compatible with the rest of the system. Depending on the user's access rights, access to one or more floors may be granted. If the user does not have access to a given floor, the button for that floor is disabled. "Free access" is sometimes provided to allow anyone access to certain floor(s) (e.g. ground floor).

For maximum flexibility, the lift control system may be capable of controlling multiple lift shafts simultaneously.

11.1.5 Automatic Number Plate Recognition (ANPR)

Access into and/or out of car parks can be automated by the use of ANPR. A camera is used to capture an image of the vehicle's number plate, and this number is recognised and compared against a list of authorised vehicles stored in a database.
To improve the reliability of an ANPR system, the camera should be located where vehicles are lane controlled or constrained by a narrow width, where the vehicles are viewed head on and as close as possible.

Tailgating can be a problem, so measures are recommended to restrict this possibility (e.g. speed hump, barrier or electric gates).

11.1.6 Long Range readers for vehicle identification

Some readers are available which have an extended reading range, often over 10m (33ft). In addition, some readers can successfully read a passing tag at speeds up to 200km/hr (125mph).

When using such readers, it is important to consider their position and use, to avoid a single token being detected by multiple readers, as this may activate multiple barriers.

11.1.7 N Factor Authentication

User authentication in an access control system requires recognising certain data related to the user. Typically, credentials can be something you know (such as number or PIN), something you have (such as an access token), something you are (such as a biometric feature) or any combination of these.

Depending on the required security of the system, one or more of these factors may be used in combination to provide single, dual or multi-factor authentication:

- Single factor authentication is where the user is identified against one element, e.g. something you are, such as a biometric.
- 2 factor authentication is where the user's credentials are checked between two of the elements, e.g. something the user is and something the user knows such as biometric + PIN.
- 3 factor authentication is where the user's credentials are checked between all three elements, e.g. something the user is, has and knows such as biometric + card + PIN.

Using a card or PIN reader in combination with a biometric reader reduces the possibility of false acceptances.

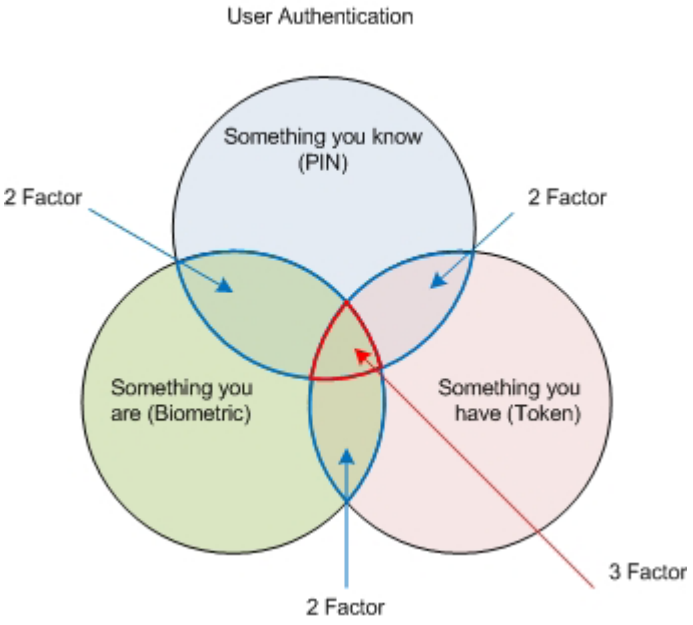


Figure 3 – User Authentication

11.1.8 Logical Access Control

Logical access control enhances the security of a computer network by restricting a user from logging onto a computer system unless the access control system has previously granted that user access into the relevant area. This requires a close integration between the access control system and the computer login system to ensure that the credentials for each can be cross referenced.

Logical access can also be useful to detect “hackers” by identifying attempts by a user to remotely access a computer system, when the user is physically on the premises.

11.1.9 Visitor Management

Visitor management allows visitors to a site temporary access to some or all areas within that site. It is important that visitor details can be quickly entered onto the system, often by pre-registration. Information to be considered for pre-registration includes the person being visited, visitor arrival and departure times, access rights to be given to the visitor and possibly even the visitor’s photo-ID image. A visitor badge is then printed on a card or label printer when the visitor arrives.

Visitor details can be made valid for a single visit, or for a predetermined period (e.g. contractors).

If visitor data is not pre-registered, the relevant information must be entered when the visitor arrives. Groups of visitors are often selectable as a group, and their status processed as a single action.

Some systems typically assign dual access for the visitor token such that the visitor and host must present their tokens to gain access to an area. This prevents the visitor from freely accessing areas without the host being present whilst providing an audit trail of the visitor’s whereabouts.

11.1.10 Route Enforcement

Route enforcement is a method of enforcing access through selected access points in a specific order.

11.2 Non Security

11.2.1 Time and Attendance (T&A)

A time and attendance system logs and monitors the arrival and departure times of staff and calculates number of hours worked and numbers of outstanding hours to be worked that day / week / month. Reports can then be issued by user, department etc.

When required, the system should meet standards set by the EU Working Time Directive.

Such systems can be a standalone dedicated T&A solutions or use information taken from integration with a suitable access control system. In either case, they should be capable of making flexible calculations on hours worked to suit bespoke site requirements. These include basic/overtime hours worked, flexi time calculations, complex and varied shift patterns and administer planning for labour and forecasting. Holiday and absence pre scheduling and booking are often possible.

A facility to export T&A data to a company payroll system improves the overall usability of the system.

12. Interconnection Communication Requirements

A variety of methods exists for connecting components together in an access control system, each with their own advantages and disadvantages. These components can be connected either with cables (WIRED interconnections) or with RF signals (WIRELESS interconnections).

12.1 WIRED Interconnections

- **Wiegand** is rarely used other than for interconnections between readers and controllers or reader interfaces. It is a 1:1 connection (i.e. one Wiegand port on a controller is connected to one reader), with a maximum length of around 50m.

- **RS232** is a more general type of interconnection than Wiegand, so can be used in a wider range of applications. It is limited in distance to around 15m between devices, and requires a 1:1 connection (i.e. one RS232 port on a host is connected to a single device). The speed of data transfer is typically 20K bits per second (bps), but can be as high as 100Kbps. It is important to note, however, that its susceptibility to electrical noise increases as the data transfer rate and distance between devices increases.

- **20mA Current Loop** uses current rather than voltage, so is less susceptible to noise than RS232, allowing it to be used over longer distances (tens of kilometres). It is possible to connect more than one ancillary to a single host to provide a very basic network. Some cable integrity checking is also provided in that data is signalled by switching between 4mA and 20mA, so if the current drops to 0mA, the connection must be broken. Data transfer speed is low, around 300bps for long connections, although speeds up to 19.2Kbps are possible over short distances.

- An **RS485** bus can typically support up to 32 devices, each with an address to identify it to other devices. Unlike RS232, an RS485 bus is capable of covering up to 1.2 Km end to end, using twisted-pair cables. The maximum data transfer speed is dependent on the implementation, but can be between 100Kbps and 10Mbps. An RS485 bus can offer good immunity to electrical noise, making it ideal for interconnecting components around buildings.

- Several other standardised bus systems and protocols exist, including CANbus, Modbus®, Fieldbus®, PROFIBus®, Lonworks® and BACnet®, and consideration should be given to the advantages / disadvantages of each prior to specifying their use. These are mainly used for building automation and industrial process control systems and are, as yet, rarely used in access control applications.

- **IP** interconnections can be limited to a single Local Area Network (LAN) whereas a Wide Area Network (WAN) can connect multiple LANs together to communicate with users and computers in other locations. A LAN has the advantage of covering a large physical area, allowing buildings to be connected together, with a WAN covering an even greater area allowing countries to be connected together. The following BSIA documents include a wealth of useful information on IP interconnections such as advantages / disadvantages, bandwidth and security considerations.

  – Form 210 – An installer's guide to internet protocol (IP) in the security industry
  – Form 211 – A user guide to the use of internet protocol (IP) in the security industry

- **ONVIF** (Open Network Video Interface Forum), is a global open industry forum with the aim of faciltating the development and use of an open standard for the interface of IP-based security products. The group is working to create a standard for how IP products within video surveillance, access control and other security products can communicate with each other.

12.2 WIRELESS Interconnections

- **Proprietary** wire-free connections are common in intruder alarm systems, but less so in access control. Wireless security products usually use 868MHz, but range and data transfer speeds will depend on the specific product design. There are also system components that utilise 433MHz and 2.4GHz. The choice of wireless frequency will depend upon the building infrastructure.

- **Wi-Fi®** is a trademark of the Wi-Fi Alliance that denotes that a product complies with the requirements for a Wireless Local Area Network (WLAN) based on the IEEE802.11 series of standards. Wi-Fi systems are intended as a replacement for LAN cabling using RF transmissions at 2.4GHz or 5GHz. Data from a Wi-Fi receiver is usually transferred to a LAN or WAN for onward transmission. The range of a Wi-Fi connection depends on the transmitter power, the aerial design and the sensitivity of the receiver, typically 30m (indoors) for IEE802.11b/g and 60m (indoors) for IEE802.11n. Typical data transfer rates of 50Mbps is common using Wi-Fi, although 600Mbps is possible.

- **Bluetooth®** (also Bluetooth Low Energy, BLE) is a short range wireless connection using the 2.4GHz frequency band. It is used extensively in mobile phone technology, but little used in security. Typical range between Bluetooth devices is 10m (Class 2), but it is possible for Bluetooth to cover 100m (Class 1). Typical data transfer rates are 1Mbps (v1.2), 3Mbps (v2.0) and 24Mbps (v3.0 and v4.0).

- **NFC** (short for Near Field Communication) is a short-range wireless communication technology which enables the exchange of data between devices over about a 10cm distance. NFC is mainly used when an electronic device (such as a mobile telephone) is used to emulate a smartcard although data can be exchanged between NFC devices

- **GSM, GPRS, 3G, and 4G** connections use mobile phone transmission technology to send data into a wireless network at 900MHz or 1800MHz. Range depends on the location of the nearest 'base station', as well as the power and sensitivity of the transmitter and receiver. Typical data transfer rates are 50 to 100Kbps for a 2G GPRS connection, or over 200K bps for an EDGE connection.

Note: Consideration should be given to whether the security of wireless technology for connection between reader and door controller and door controller to PC is adequate for higher risk areas.

12.3 Interconnection Security

Consideration should be given to the use of encryption on any communication method that is utilised to enhance the security of the system.

13. Building Access

13.1 Access equipment locations

All access control system devices should be located to suit all of the system users. Readers should be placed at a height that allows correct usage by all users, this can require dual readers being installed at some entrances e.g. vehicle barriers may need dual height readers for car and HGV heights. Entrances that are used by disabled and able-bodied may require the access control devices to be located at a suitable height for both types of users, or two readers may be required.

13.2 Escape routes

Emergency exit should be considered in the system design to enable escape from the site appropriate to the amount of building users and how familiar the building users are likely to be with the building escape procedures. There are two emergency escape scenarios that should be considered in the access control system design.

- **Panic escape**

  Where members of the public use buildings or where there are high numbers of employees, there is a heightened risk of panic during an emergency evacuation. Users of the escape route may not be familiar with the operation of the escape hardware, they must be able to easily find and operate the hardware located on the exit door (see BS EN 1125).

- **Emergency escape**

  Where the building users are all familiar with the site and the emergency exits, panic during an emergency evacuation is less likely. Operation of emergency exit devices and handles are acceptable as long as it is with one single operation to release the locking device (see BS EN 179).

14. Installation Requirements

Consideration should be given to industry codes of practice and any relevant standards as defined in section 2.

15. Configuration

The configuration of access control systems is carried out by the use of various system software tools. According to the authority of the system user, functions may be enabled and disabled, system values may be modified.

Typically, an access control system configuration may be seen as falling into two categories:

- System hardware configuration, i.e. readers, controllers and other control equipment – this step is carried out by the installer.
- User database configuration, i.e. cardholder details, time schedules, access levels etc. – this step is usually carried out by the customer or end-user.

The system user database will contain information about personnel probably including a photographic image which may be printed onto a suitable credential. Additional information may be printed on the reverse of the access control credential, this may be site safety information e.g. fire emergency procedure instruction. There may also be information about what to do with the card if found.

Use of the system application software is restricted by passwords and/or PINs which may be simple, user generated, or may be time limited with complexity enforced or be linked to the user's operating system password rules.

16. System Management

As with any system, efficient management is key to ensuring the security and operability of the access control system is maintained. This section covers some of the main elements that shall be considered within any system.

16.1 Backups

An on-line access control system should have a suitable backup regime defined to ensure that in the event of any failure of the IT hardware, configuration and historic events can be recovered if required. This can take the form of a simple backup from the access control system through to a fully automated nightly backup of the server.

16.2 Resilience

All door controllers should be battery backed to provide continuous operation in the event of a power failure. If the server is critical for operational use, for example, fire alarm mustering, then this should also be provided with a suitable UPS. Controllers should retain any audit trail information in the event of a power failure.

BS EN 60839-11-1 and -2 have requirements for standby battery operation at Grades 3 and 4.

16.3 Token Management

The management of tokens is critical to the secure operation of the system. The control and security of access to the system should be password protected to ensure that the registration of new users is controlled.

16.4 Reporting

To ensure that the system remains efficient regular reports should be run that check a range of events from the system, such as unauthorised access attempts, usage lists etc.

16.5 Data Protection

As the access control system will be storing personal data then it must be documented within the company's Data Protection Policy.

16.6 Information Security

Access to any terminals and servers that run the access control system must be secured from inadvertent access.

17. Service and Maintenance

To ensure the continued efficiency of any access control system throughout its lifespan, they should be regularly maintained.

A Service Level Agreement (SLA) should be agreed with a qualified maintenance provider (check the BSIA website for member companies). The SLA should include a preventative maintenance schedule (at least once per annum) detailing what is to be: tested, tightened, lubricated, replaced etc and the frequency. The SLA should also include a reactive maintenance agreement detailing what response times and repair times are expected.

The end user should ensure that the chosen maintainer is authorized by the manufacturer to service and maintain the system.

Due to the variety of components that are used in some access control systems, there is often a requirement for more than one maintenance contract to cover all of the system components. For example, electronic access control and vehicle barriers could be from different maintenance providers. To ensure consistency with the maintenance service it may be a consideration to have only one maintenance contract and allow that maintenance provider to contract out the other maintenance contracts that are required to fully maintain the access control system (back to back contracts).

For software based systems, most software manufacturers will offer a Software Support Agreement (SSA). This will provide your systems integrator to maintain your software to the latest version available. This provides you with the latest features but most importantly compatibility and testing with the latest releases of operating systems on the market.

18. Interoperability and Integration

- Over the years, systems from different manufacturers have started to use common methods of interconnecting components, LAN technology being a common example. In addition, common communication protocols such as TCP/IP have also been developed. These developments have led to an increasing likelihood that systems from different disciplines can be integrated to give a common benefit. This is called interoperability.

- An integrated security solution can reduce cost and provide a return on investment by eliminating costly manual processes. However, the major benefit is the improved security that can be provided at a time when security is a great concern to all organisations whether they are in the public or private sector.

- Any system chosen must meet today's requirements, but must also fit the customer's needs into the future This is a difficult challenge, which requires predicting how the organisation may change and grow and ensure that the systems have the scope to expand to meet these needs.

- There are many advantages to integrating systems, the following list representing some of the major benefits:

  – Different disciplines may be operable from a common user interface, where the operator can see access control events, intruder alarm activations and video activity on a single screen. This can make investigation much more straightforward and reduce the need to send security officers out to respond to security breaches.

  – Access control and fire allows fire alarm mustering – know where your employees are at a given time. Furthermore, the access control system can monitor the fire alarm system to automatically release the appropriate electric locking mechanisms. The proposed link between the access control system and the fire system should be evaluated as part of the fire risk assessment.

- Access control and other security detection systems can initiate pre and post-event video recording, linking the video clip with the event information. This can make searching for events more effective as it is much quicker to search for an event in the alarm log, rather than search through hours of video.

- Intruder and hold up alarm system control functions can be managed by the access control system – allows the intruder alarm system to be unset on presentation of a card before entry is granted. If the user is not authorised to unset the system, access is denied.

- Initiate camera presets when specific pre-determined events occur, e.g. when entering a room in a bank, switch the camera to zoom onto the door to identify the individual.

- Use video with time and attendance system to detect / eradicate 'buddy-clocking', a practice where employees clock each other on and off work.

- Using an occupancy count from the access control system can reduce false alarms - the intruder and hold up alarm system can be notified not to set if the access control system is aware that not all users have exited the building.

- Building management systems (BMS) are responsible for monitoring and controlling the environment of a building, for example, lighting, heating and ventilation (HVAC). By integrating access control systems with BMS systems, the lighting can be switched on and the temperature can be increased to normal when a user enters an area.

- One of the fundamental objectives of a security system is to provide protection at the outermost perimeter of a property. A perimeter intruder detection system can be used, linked with video to provide early warnings and increased security through verification in the event of a breach. For example, external doors could be automatically locked if the perimeter system detects an abnormal event.

- By using smart card technology, cashless vending becomes a reality. The same card that gets you into the building can also hold money for the vending machines or canteen.

- Part of the definition of any system is the evaluation of risk within the business. Any system should evaluate and mitigate these risks by the careful selection of components and analysis of the requirements. The resulting system should aim to reduce any risks within the business that are associated with both people and property.

- When reviewing the opportunities for integration of different system components, consideration should always be given to the real advantages and benefits that integration brings to the customer in their specific situation in terms of increased security, increased efficiency, and reduced cost. If a clear business benefit cannot be identified then there is no requirement for integration.

- The definition and design of any integration requires careful consideration. Due care and attention should always be given when evaluating operational requirements to ensure that the system integrity is not compromised.

19. Example Applications

19.1 Grade 1

Application: Retail store, public area to private area
Number of Doors: Low
Number of Staff: Small
Risk level: Low
Customer Requirement: Low cost solution, no audit trail
Lock Type: Electric strike
Door Type: Hollow core
System Description: A standalone system utilising PIN or token access to secure the private areas from the general public

19.2 Grade 2

Application: Hospital
Number of Doors: Medium to high
Number of Staff: Medium to high
Risk level: Medium
Customer Requirement: Networked solution with audit trail and integration capability
Lock Type: Maglock
Door Type: Solid wood
System Description: A networked solution with tokens allowing full audit trail and definition of areas to allow varying access rights across the estate. The system allows for the remote control of the access point through the central software along with integration to other systems such as CCTV for remote monitoring of specific access conditions, such as door forced.

Specific areas may utilise higher security doors and locks depending upon the risk level and area to be protected.

19.3 Grade 3

Application: Data Centre
Number of Doors: Low
Number of Staff: Low
Risk level: Medium to high
Customer Requirement: Networked solution with multi factor authentication to secure access to the data centre
Lock Type: Shearlock or motorised
Door Type: Solid hard wood
System Description: A system providing two factor (i.e. card and PIN) or single factor biometric for increased security accessing the servers. This is coupled with a airlock to restrict access to one person at a time.

19.4 Grade 4

Application: Airport cargo screening (airside)
Number of Doors: Small to Medium
Number of Staff: Medium to high
Risk level: High
Customer Requirement: Biometric solution with full audit trail and integrating CCTV
Lock Type: Turnstile (full height)
Door Type: Steel
System Description: Turnstiles provide very secure access for one person at a time reducing the risk of tailgating. This coupled with biometrics ensures credentials cannot be duplicated or passed to other staff.

20. Appendices

20.1 Appendix A – Interconnection bus system definitions

Several other bus systems exist, but these are mainly used for industrial process control and are, as yet, rarely used in access control applications. These include:

- **CANbus** was originally designed for automotive applications, so works well in electrically noisy environments. The bus can support up to 64 devices, and its length varies depending on the data transmission speed, from 40m @ 1Mbps to 10Km @ 5Kbps.

- **Modbus®** is an open protocol for connecting industrial electronic devices, the main advantage being that it allows different types of devices to use a common serial bus. Unlike RS485 or RS232, Modbus defines the communications protocol, rather than the physical bus structure.

- **Fieldbus®** is a digital, serial communication system capable of supporting up to 16 devices per segment. Two implementations exist, H1 which has a data transfer speed of 31.25Kbps over a distance of 1.9Km, and HSE (High Speed Ethernet) with a data transfer speed of 100Mbps.

- **PROFIBus®** is a supplier-independent network standard, whose interface permits a vast application in processes, manufacture and building automation. PROFIBus is a communications protocol that can be used on physical buses such as Ethernet and RS485.

- **LonWorks®** is a networking platform for connecting a large number of devices using standard bus structures such as RS232, RS485 or Ethernet, with data transfer rates in excess of 78Kbps (depending on the bus used).

- **BACnet®** (short for Building Automation and Control network) and allows communication over a variety of networks including Ethernet, ARCNET and RS-485. BACnet then simplifies the interoperability of devices on the different buses.

20.2 Appendix B – Summary of recommendations by grade

Access control points are graded according to the type of business and risk associated with the premises being secured. The grade applies to the protected area and not the overall system, therefore mixed grades may be utilised within any premises.

The standards, BS EN 60839-11-1 and BS EN 60839-11-2, contain a significant number of requirements that vary according to grade.

If an installation is made to accord to the standards then grade related requirements will apply otherwise these are recommendations. This appendix repeats the requirements and recommendations that vary according to grade and are to be found in this document.

Clause 6.1 describes the four grades:

Grade 1 (Low Risk)	A standalone lock (code, PIN or token), or off-line system, controlled in a public area for low risk situations. Example token technology: Proximity and Mifare Classic card technologies. Typical examples: internal doors or areas where you want to stop the public wandering in.
Grade 2 (Low to medium risk)	An on-line system utilising tokens or PINs to prevent access to the premises. Events are received in real-time on the monitoring software. Example token technology: Proximity and Mifare Classic cards should not be used due to the issue of cloning that is available. Mifare PLUS SL3 or higher technology should be utilised. Typical examples: commercial offices and small businesses, hotels.
Grade 3 (Medium to high risk)	An on-line system using two factor authentication or single-factor biometric to prevent access to the premises. Events are received in real-time on the monitoring software. Example token technology: Mifare PLUS SL3 or DESfire. Typical examples: secure areas of commercial business such as server rooms, data centres.
Grade 4 (High risk)	An on-line system using two (or more) factor authentication, one of which should be biometric or human image verification to prevent access to the premises. Events are received in real-time on the monitoring software. When using biometrics careful selection of the quality to reduce FAR shall be made. (See section5.2.3). Example token technology: Mifare DESfire. Typical examples: high security areas, such as MOD, Government, research labs.

Clause 6.2 (in Table 4) includes a cross-reference to other graded schemes

Table 2 – Maximum False Alarm Rate by Grade can be found in 5.2.3

Grade	1	2	3	4
FAR or FAReff	1%	0.3%	0.3%	0.1%

Table 10 in Clause 10 gives recommendations about the reader and token types appropriate to each grade.

	Grade 1	Grade 2	Grade 3	Grade 4
Single Factor Authentication Options				
PIN (Common or Unique – minimum 10,000 differs)	XR	NP	NP	NP
PIN (Unique – 100,000 differs)	R	R	NP	NP
Magnetic or Proximity or RFID	R	R	P	P
Biometric	R	R	R	P
Two Factor Authentication Options				
Magnetic/Proximity/RFID & PIN (Unique)	R	R	R	P
Biometric & PIN (Unique)	R	R	R	P
Biometric & Magnetic/Proximity	R	R	R	P
Biometric & RFID	R	R	R	R*
Three Factor Authentication Options				
Biometric & PIN (Unique) & Magnetic/Proximity/RFID	R	R	R	R
Key: XR = Not permitted by BS EN 60839-11-1 NP = Not permitted by BE EN 60839-11-1 and not recommended by the BSIA R = Recommended P = Permitted by BS EN 60839-11-1 but not recommended by BSIA * with RFID, use of CSN alone is not recommended as the number can be read directly from the card. With other smartcard formats (e.g. MiFARE and DESFire) security keys are used to protect the data from unauthorised access.				
Note: When PIN is used in Two or Three Factor Authentication, a minimum of 10,000 differs is required.				

Table 7 in Clause 7 recommends the minimum holding force applied by locks to doors by grade.

Grade	Holding Force
1	3kN
2	5kN
3	7kN
4	>=10kN

Table 8 in 9.1 recommends the type of doors thought appropriate to each grade.

Use of Door Contacts by Grade (AS recommended and according to BS EN 60839-11-1) (from Table 3 in 5.10)

Use of Door Contacts by Grade	Grade 1	Grade 2	Grade 3	Grade 4
	Optional	Mandatory		

BS EN 60839-11-1 and -2 have requirements for standby battery operation at Grades 3 and 4.

Appendix C

BS EN 60839-11-2 recommends for Operational Consideration (Clause 7.3.2.2) that the following items are considered.

a) Manufacturer's recommendations;
b) The threat(s);
c) Specific assets requiring protection;
d) Activities undertaken at the site/building;
e) Access control measure philosophy;
f) Security grade for each access point;
g) User flow (number of persons in a period of time);
h) Operation of the access control system while under fault conditions (e.g. the need for a second source of power, equipment cable infrastructure, loss of communication, etc.);
i) Access control for users with disabilities;
j) Safety requirements (e.g. emergency exits, fire protection, etc.);
k) Environmental and EMC conditions of the site;
l) Redundancy, disaster recovery plans for monitoring console;
m) Location of the equipment (control unit, user interface, monitoring console);
n) Co-operation of users (motivation, training, etc.);
o) Training of operators;
p) The cable routes, the type of cable, the maximum cable length;
q) The communication links (availability, reliability, security, performance);
r) Tamper detection;
s) Alarm/alert reporting method;
t) Throughput of personnel (staff and visitors);
u) Management of visitors;
v) Response force (e.g. police) arrangements;
w) Vehicle access;
x) Access levels (authorization) for each area zone.

21. Further Reading

BSIA Guides – www.bsia.co.uk

BSIA Form 151 – User Guide to Access Control
BSIA Form 152 – An Installer Guide to Access Control
BSIA Form 173 – Access Control and Disability Discrimination
BSIA Form 181 – Users practical guide to biometrics
BSIA Form 198 – A Guide to Token and Reader Technology in Access Control Systems
BSIA Form 203 – Integrated Security Management Systems Guide
BSIA Form 210 – An installer's guide to Internet Protocol (IP) in the security industry
BSIA Form 211 – A user guide to the use of Internet Protocol (IP) in the security industry
BSIA Form 242 – A Guide to Access Control for Manufacturing Sites
BSIA Form 246 – A Guide to Access Control for Offices
BSIA Form 261 – Installation of Access Control Systems Using IP Technology
BSIA Form 269 – A Guide to Access Control for the Education Sector
BSIA Form 293 – A Guide to Access Control for the Healthcare Sector

Approvals and Certification

Loss Prevention Certification Board (LPCB) – www.redbooklive.com
Secured by Design – www.securedbydesign.com
Warrington Certification – www.warringtonfire.net

Acknowledgments

The BSIA acknowledge the assistance given by the following member companies for the development of this guide.

ADT Fire and Security

Bradbury Security

Chubb Fire and Security

Gallagher Security (Europe Limited)

G4S Technology

Kaba

RGL Electronics Ltd

Romec Fire and Security

TDSi

This page has been intentionally left blank

This document was created by the Access and Asset Protection Section of the British Security Industry Association (BSIA).

The British Security Industry Association is the trade association for the private security industry in the UK. Our members provide over 70% of UK security products and services and adhere to strict quality standards.

The British Security Industry Association's Access and Asset Protection Section brings together companies involved in areas of security providing physical products to stop unwanted people from accessing property or valuables and the electronic measures that can, optionally, control them.

The section includes member companies involved in the manufacture, supply and installation of solutions that restrict, control and monitor the movement of people, assets or vehicles in, out and around a building or site. This includes physical protection methods, such as security doors, fencing, locks, barriers, safes and strong rooms, rising screens, etc and the electronic access control systems that control them and allow authorised persons in and keep undesired people out.

Access control products are subject to fast-moving technological development. The section aims to raise awareness amongst end-users and specifiers of the different types of equipment that are available, the applicable standards and the most appropriate environments for using them.

The Access and Asset Protection Section sits in a strong position when it comes to lobbying for consistent standards and regulations. Access control products are subject to fast-moving technological development. A major focus of the section is to raise awareness amongst end-users and specifiers of the different types of equipment that are available and the most appropriate environments for using them.

BSIA membership will raise your company profile and ensure that your business is at the heart of influencing the future of the security industry. You will become part of a unique group of high quality and professional companies which are well-respected and well-represented to government, end users, specifiers, standards and legislative bodies. For more information contact the BSIA.

BSIA Ltd
Kirkham House
John Comyn Drive
Worcester
WR3 7NS

t: 0845 389 3889
e: info@bsia.co.uk
www.bsia.co.uk

@thebsia

bsia
british security industry association