ACCESS CONTROL
GAI SPECIFIER'S GUIDE

The specifier's guide to understanding electronic access control and specifying the correct solutions.

Guild of Architectural Ironmongers

RIBA · CPD PROVIDERS NETWORK · RIBA · CPD PROVIDERS NETWORK ·

Guild of Architectural Ironmongers

SEPTEMBER 2024

ACCESS CONTROL
GAI SPECIFIER'S GUIDE

Based on the RIBA Approved CPD of the same name, the specifier's guide to Access Control develops the wider understanding of electronic access control and specifying the correct solutions.

To ensure that your project meets the latest standards, regulation, legislation and best practice, it is strongly recommended that the ironmongery should be specified by a GAI Registered Professional such as a Registered Architectural Ironmonger (RegAI). All RegAI's have successfully completed the GAI Diploma in Scheduling qualification, and continue to maintain and update their knowledge through the GAI continuing professional development (CPD) programme. RegAI status is a clear demonstration of professional competence in matters which are critical to building safety, accessibility and security. Visit www.gai.org.uk/RegAI.

If you would like to receive a presentation of the CPD, this is available through GAI member companies. Please visit the GAI website (www.gai.org.uk) for more details.

CONTENTS

Guild of Architectural Ironmongers

1. WHAT IS ACCESS CONTROL?

DEFINITION

Access control is the selective restriction of access to a place or other resource. Its purpose is to ensure that authorised people are free to move around authorised areas of a building at authorised times, while unauthorised people are prevented from entering those parts of a building where or when their presence is not permitted.

TYPES OF ACCESS CONTROL

Control of access in and out of a building is enforced by the following means each with their own issues:

- **People -** With people, you are reliant on a person's judgement which has the potential for human error, there is also a potential lack of diligence, as well as distraction. There is an inevitable higher financial overhead as well as the fact that humans are a limited resource who can only be in one place at any given time.
- **Mechanical locks and keys -** With mechanical lock and keys, whilst cheaper than electronic access control, they can at times be fiddly and inconvenient to use. Some keys can be easily copied at a local locksmith or heel bar, and there is an inevitable cost and time implication if the key is lost or stolen.
- **Electronic access control.**
- **Mixture of all of the above.**

ADVANTAGES OF ELECTRONIC ACCESS CONTROL

- Allows only employees and other authorised personnel to conduct their legitimate business in areas where they are authorised to do so.
- Reduces risk to an acceptable level and provides awareness of risks when they arise, thus giving the ability to act quickly if a security threat is found.
- Copying the "key" or card/token used in place of a key is difficult and if using biometrics, it is practically impossible.
- Stolen "key" or means of entry can be programmed out of the system, removing security risks quickly and easily.
- Audit trails can be provided. In essence it is a log showing who has been where and at what times.
- Entry to the system can be restricted to certain times, allowing timed free access or lockdown on specific doors. This is particularly useful for schools when entrance doors can be set before classes, break time and lunch times.
- Manufacturers have started to use common interconnecting components and communication protocols through the Internet of Things. This has allowed systems such as fire alarms, intruder alarms, CCTV cameras, time and attendance systems, vending machines and building management systems to be integrated with access control software.

Guild of Architectural Ironmongers

2. SPECIFICATION OF ACCESS CONTROL

Access control turnstiles

SPECIFICATION QUESTIONS

When commencing the specification of an access control system, it is useful to find out the answers to the following questions:

- **How many people are using the system?**
  This will impact the system selection.
- **How many doors require access control?**
  This will impact the system and hardware selection.
- **Are the doors fire rated?**
  This will impact the hardware and whether it has been previously tested on fire doors.
- **Are the doors escape doors?**
  Will the hardware selected be suitable for an escape scenario? If so it must be tested to BS EN 179.
- **What is the budget available?**
  This will impact all aspects of the specification from hardware to software selection.
- **What type of electric locking is required?**
  Will it be simple mechanical or fully electronic? If electronic what type to use for each scenario as a mixture can be used depending on the situation.
- **Are there any specific security requirements?**
  Such as "dynamic lockdown" which enables a building or an area to be quickly locked down e.g. in the event of terrorist activity.
- **What type of reader technology is to be used?**
  Will it be PIN, card/token or even biometric?
- **Read in/read out or read in/free egress?**
  Will it require a reader on both sides of the door or must one be free to escape at all times?
- **Is it a stand alone or networked system?**
  The amount of users and doors will impact this and if networked it will require a PC.
- **Are there any integration requirements with other systems through the Internet of Things?**
  Does this need tied in to building management, CCTV or alarm? – if so further discussion with these parties must be had prior to specification in order to check compatibility.
- **Is the Access Control specified in more than one package?** It maybe that the Mechanical and Engineering (M&E) Consultant has already dealt with this so ensure that it is not being double counted.

Electronic escutcheon

ORDER OF SPECIFICATION

In ironmongery there is a natural order of specification which starts with hanging then closing then locking and finally furnishing the door.

When specifying access control, there is a natural order of specification. A useful way of ensuring that nothing is left out is to use the acronym **SCARPER.**

- **S**ecure the door - Select the electronic locking device that will hold the door locked.
- **C**lose the door - It is important to remember that a door is not secure if it is not shut.
- **A**ctivate the door - What will act as the 'key' to get users through the door?
- **R**elease the door - How do I usually get out from the inside?
- **P**ower the door - Check that, if it needs power, this has been supplied.
- **E**scape through the door - Check what happens in an escape situation.
- **R**eview the specification - Look at your door and think about how you would use it. This is a good way to check if you have missed anything.

Guild of Architectural Ironmongers

3. SECURE THE DOOR

It is important to consider the functionality and the level of physical security required for the application when selecting the electronic locking device that will hold the door shut.

MECHANICAL DIGITAL LOCKS

Mechanical Digital access control solution are the simplest form of access control and are offered on a single door, whereby all the programming and system set up is carried out at the door. Whilst identical sets can be installed on other doors within a site, there is no direct interface or connection between this door and any other or to a computer system for transfer of data.

They can look somewhat bulky but newer versions are available combining aesthetics with functionality.

SOLENOID LOCKS

A solenoid lock is similar to a conventional mortice lock but a solenoid blocks or enables the outside handle that is used to release the deadbolt and latch. The appearance and functionality is that of a normal lock and is generally aesthetically pleasing and acceptable to users.

A split follower allows separate control of the inside from the outside handles with the internal handle always free for egress. The lock will automatically deadlock when the door is closed. Key override functions are available to mechanically withdraw the bolts or throw the deadbolt by key.

MOTOR LOCKS

An electric motor drives the lock bolt to retract or project it. They require less power to operate than a solenoid using power only whilst retracting or projecting the bolt so they are suitable for battery powered devices. Some examples feature mechanical retraction of the locking element by lever handle to allow them to be used for exit on escape routes.

Mechanical override by key or thumbturn is common. Motorised locks are as secure as a mechanical deadlock but are expensive. They are considered to be heavy duty devices and are usually specified where reliable operation over an extended period is required. The door must be correctly aligned when operating so as to prevent binding, often used with door automation.

Both solenoid and motor locks fall under the scope of BS EN 14846 which is a harmonised standard therefore must be CE marked .

Guild of Architectural Ironmongers

3. SECURE THE DOOR CONT'D

Electronic escutcheon

ELECTRO MAGNETIC LOCK

An electro magnetic lock is one of the simpler means of electronically locking and unlocking doors. It consists of two items; the magnet itself and an armature.

The maglock as it is commonly called, has a core of nickel plated steel around which is wound coils of insulated copper wire. This is encased in epoxy resin to hold it together and housed in a metal casing. When a current is passed through the coil the unit becomes a powerful magnet and will provide enough force to hold a steel plate, called the armature, with sufficient strength to be suitable for securing doors. When the current is switched off the magnetic field collapses immediately releasing the armature.

They are only available as fail unsecure (unlocked) and for this reason they are generally seen as low security solutions. They can be used on inward and outward opening door depending on bracketry used.

ELECTRONIC ESCUTCHEONS

Electronic 'escutcheons' are an electronic access control solution allowing multiple doors to be linked to each other but not online to a computer. Powered through battery which can have up to a 3 year lifespan it has flexibility in that it can be used with a number of locks.

The programming and system set up is carried out at a master controller which distributes the operating parameters to relevant controllers as data is transferred via the media. They can be linked with other forms of access control and communication to PC can be done through a series of wireless hubs.

ELECTRIC STRIKE

An electric strike, or electric release, is perhaps one of the most popular methods of unlocking a door electrically. Access is allowed by electrically operating a solenoid to release the jaw so that, as the door opens, the latch bolt pushes the spring-loaded jaw which pivots out of the way. The jaw returns to the secure position as soon as the latch bolt has cleared it and the solenoid relocks the jaw.

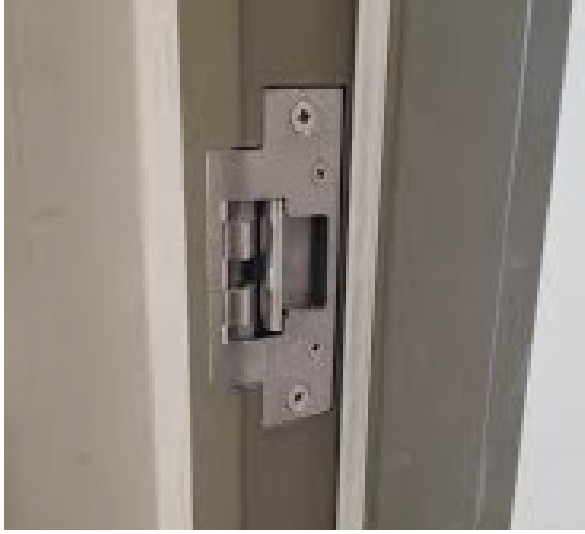
Any sideload can cause the strike jaw to fail to release properly requiring the user to push or pull the door to gain access. Electric strikes are not recommended for use on doors fitted with sound or smoke seals which are compressed when the door shuts or in situations where a strong draught may prevent closure of the door. Strikes are available as light, medium and heavy duty.

ELECTRICALLY CONTROLLED MULTI POINT LOCK

This features motor-driven latch bolt retraction and is a module added to a mechanical multi-point locking mechanism. Any access control system can be used in conjunction with this lock in order to release it and it can also be opened mechanically by key in cylinder. This is particularly useful in a domestic scenario.

RFID CYLINDERS

RFID cylinders are often deployed as part of a wider access controlled solution that will incorporate electronic escutcheons (lever handles with built-in proximity readers) and wall readers to form a total solution.
The RFID cylinders are designed to work with a suitable mechanical lockcase. They are battery powered and often the batteries are located in the internal Knob on the secure side of the door. These can usually be replaced without removing the cylinder from the door.



Electric strike

MECHATRONIC CYLINDER

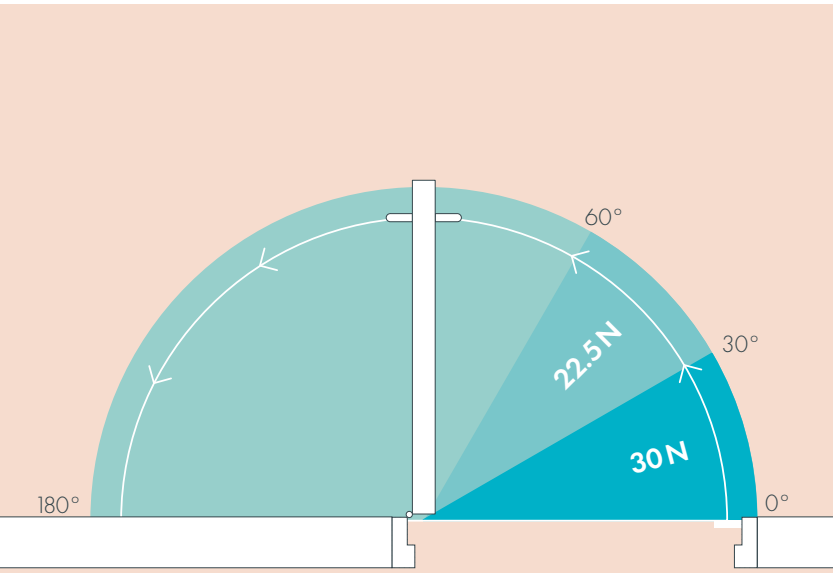
A mechatronic cylinder is a hybrid of conventional mechanical cylinder design and the electronic functionality of an access control product. This allows the cylinder to still retain the existing fittings such as lock case and lever set whilst providing an electronic answer for access control. In some cases the technology can be applied to other locking products such as padlocks or furniture locks. They usually have built in batteries to provide power and operate a clutch mechanism for access. In some cases these cylinders draw power from an external source.

MECHANICAL & ELECTRONIC KEY BASED PRODUCTS

Mechanical and electronic key based products also combine these two technologies. These solutions work whereby the power and communication is all carried out by the keys. Audit information, time schedules and validation periods are all programmed into the key. This allows for installations in remote areas without the need for power or networking. Updaters placed in common areas allow users to frequently download new profiles for their keys and upload audit trail information.

Guild of Architectural Ironmongers

4. CLOSE THE DOOR



Opening resistance for door closers

It is essential that closing devices are adequate for the particular purpose.

- Be certain that you know the size and weight of the door, particularly if it is a fire door.
- Consider the door width and the possibility of wind pressure.
- Closers on fire doors must conform to BS EN 1154 and be CE marked.
- Consider which type of door closer you wish to specify will it be a face fixing pattern or concealed type. They can also be floor mounted as a floor spring.

RECOMMENDED OPENING FORCES FOR DOORS

BS 8300-2 states "For most disabled people to have independent access through single or double swing doors the opening forces when measured at the leading edge of the door should be:

- not more than **30N** from **0°** (the door in the closed position) **to 30° open**.
- not more than **22.5N from 30° to 60°** open.

It is also stated that it is preferable that backchecks should not operate before about 80° open and that the maximum closing force should occur between 0° and 15° of final closing.

Motion sensor controlled power operated door

SELF-CLOSING SWING DOORS

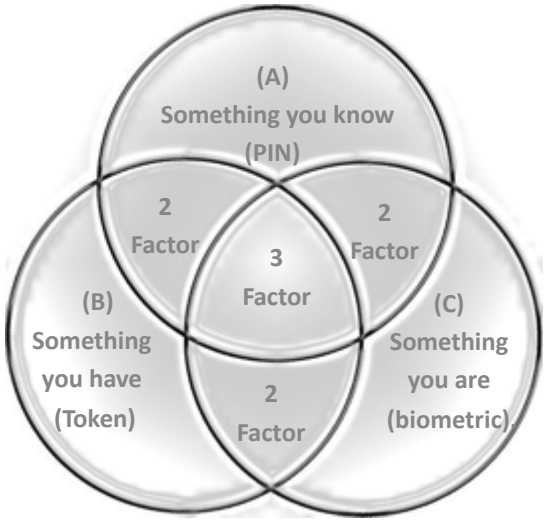
Where it is not possible for a controlled door closing device to close an entrance door and keep it closed against external forces without exceeding the opening force limits as mentioned in BS 8300-2, then a power-operated option may be used. This can either sliding, folding, balanced or swing, which should be one of the following types:

- A manually activated door controlled by a push pad, coded entry system, card swipe or remote control device.
- An automatically activated door controlled by a motion sensor or a hands-free proximity reader.
- An entrance lobby or airlock system of inner and outer doors.

These can also be connected to act alongside and in conjunction with an access control system.

Guild of Architectural Ironmongers

5. ACTIVATE THE DOOR



An access control system needs to identify the user and it does so by using one or more of these three methods.

- **Something you know -** Such as a PIN or digital code.
- **Something you have -** For example a card, token or key.
- **Something you are -** Physical characteristics such as voice recognition, fingerprint, weight, retinal or iris scan.

You can have single factor authentication which is where the user is identified against one element, i.e. something you are, such as a biometric.

Two factor authentication is where the user's credentials are checked against two elements, i.e. something the user is and something the user knows (biometric + PIN).

Three factor authentication is where a user's credentials are checked against something the user knows (PIN), has (Card) and are (biometric).

SOMETHING YOU KNOW

A PIN (Personal Identification Number) code is something that you know. Codes are usually 4, 5 or 6 characters in length and are normally numerical only. This is seen as the lowest form of access control.
A digital electronic keypad is an example of a device that is preprogrammed with one (or more) PIN (Personal Identification Number) codes. When the user enters the correct PIN code the device allows access. PIN Codes can be combined with another credential to provide higher levels of security.

Proximity card

SOMETHING YOU HAVE

Magnetic Strip or Swipe Cards are something you have and they utilise differing types of of technologies to hold identification data. In operation, the magnetic code in the stripe is read by the reader when the card is swiped through the reader. With a mag stripe system the reader does not communicate with the card but the reader just reads what is encoded on the card. Swipe cards are usually cheap but easily copied and often need to be replaced.

There are various features and benefits of magnetic stripe readers in that they are fast and easy to install, card cost replacement is low, they are robust and reliable and are available in internal and external options.

Proximity cards and readers provide contactless technology with robust reliable performance and can be used internally and externally. Combining proximity readers with keypad provides extra security. They are also available in different sizes so they can be used on narrow mullions.

Proximity cards are also something you have. These can be either passive proximity (which transmit a short distance) or active proximity which give a longer range.

Bluetooth devices such as your mobile phone can be utilised to release a lock. This is becoming more popular in hotels but is also available for smart locks used in the home.

Guild of Architectural Ironmongers

5. ACTIVATE THE DOOR CONT'D

Biometric finger reader

Biometric finger reader

SOMETHING YOU ARE

Biometric reading technologies has come a long way. From the very first commercial application for a fingerprint reader in 1984 the market has regularly seen the introduction of new products and applications.

Biometrics is measurement and analysis of the unique physical or behavioural characteristics used to recognise humans. It works by unobtrusively matching patterns of live individuals' data in real time, against enrolled records.

Biometric data is initially read with an 'enrolment' reader and the data is then 'encoded' into a template which is usually stored in an access control database or on a smartcard for later use. The encoding process ensures that the data cannot be reproduced from the template, only compared against a recently read sample for a pass/fail result.

There are a number of different options available for Biometric readers:

- Finger.
- Vein scanner.
- Multi-format biometric reader.
- Iris recognition.
- Facial recognition.
- Hand geometry.

TYPES OF ACCESS CONTROL SYSTEMS

Access Control systems can vary in complexity, depending on the application and the building. These vary from simple standalone systems, through to more complex fully online system as well as virtual network systems which are a hybrid of both.

A standalone system is an electronic access control solution, on a single door, whereby all the programming and system set up is carried out at the door. Whilst identical sets can be installed on other doors within a site, there is no direct interface or connection between this door and any other or to a computer system for transfer of data. Different locking mechanisms are available for this.

An online system is an electronic access control solution allowing multiple doors to be connected whereby the system is linked to a computer for programming and administration. Depending on the complexity of the building, it can be tailored as varying sizes and capabilities are available. Each door or series of doors is connected to a door controller which is connected to the computer system to provide total management control. This enables changes to the system to be instantly notified to the doors via the controllers and also provides real time monitoring and data transfer.

Virtual networks are access control systems that are a hybrid of both standalone and networked systems. The Smart card/token carried by the user updates or retrieves information from a reader instead of someone going to each and every reader to programme, upload or download information. By using the user card to transport data there is no need for any cabling.

In addition, as the readers are battery operated, there is no need for power supplies and mains connections, which means the cost of installation is significantly reduced.

Virtual network reader

Guild of Architectural Ironmongers

5. ACTIVATE THE DOOR CONT'D

Smart lock

Smart digital lock

THE INTERNET OF THINGS

This is a concept where not only people but objects and devices are able to network and communicate with each other. Smart homes, buildings and even cities are increasingly using modern systems to provide a practical way of controlling electronic devices. This can include internet connected safety and security systems such as electronic locks, monitors, cameras and even alarm systems. Newer products are being brought to the market including the following:

SMART DOOR LOCKS

Smart Door Locks means a home can be secured without the need to carry keys. The door can be opened in a variety of ways, including a PIN code, remote fob, or even a smartphone when connected to a smart home system. It is also possible to have a smart lock installed on a doorset which has been successfully tested on a PAS 24 Doorset.

SMART DIGITAL LOCKS

Digital locks had previously been seen as an elementary form of access control, but all that has now changed. It is now possible to generate time sensitive codes which can allow temporary access through locks. Short, medium or long-term codes for a specific date, time and duration can be set and generated via an app or online. Codes can be sent via email or SMS. Using an audit trail, it is possible to view a lock's history including which codes were used at what time.

SMART LOCKING AND ACCESS CONTROL

There is an intelligent combination of electronics, mechanics and wireless access control available which uses smartphone application. This technology for the locking industry provides unique identification for every opening through encrypted communication. The Battery inside the key provides wireless function of time and calendar with complete audit trail. Specialist keys can be updated with a smartphone application and allows the ability to update access rights in the field. A Cloud-based Web Manager allows the ability to change access rights anytime anywhere required.

BUILDING AUTOMATION SYSTEMS

There is also a management system available which intelligently integrates door, window and safety technology into building management systems. The interface module allows integration of emergency exit systems, smoke and heat extraction systems, hold open door systems and automatic doors. It can be used as an independent building automation system (stand-alone solution) or integrated into a higher-ranking building management system. The applications for this are browser-based and can therefore be operated on every IP competent terminal; No matter whether you use a PC, tablet, or smartphone.

VIRTUAL REALITY 360 DEGREE CITY

New Virtual Reality technologies are being exploited to engage with customers. Through the 360 degree City it allows the customer to digitally experience the usability of products in real life situations. this includes security and locking solutions. This virtual world will illustrate where and how a range of products can be used with their solutions displayed in a 3D environment from a user's perspective. This is all accessible via an app.

Guild of Architectural Ironmongers

6. RELEASE THE DOOR

In order to exit through the door, there needs to be a means to release the electronic lock. Where electric strikes or electrically activated lever sets are specified then a manual lever handle may suffice. For 'read out' situations, where access control is required to both sides of a door, a second reader will be required. In other instances, one of the following release mechanisms will be needed.

REQUEST TO EXIT BUTTON

If a door does not have a mechanical means of exit, e.g. a lever handle or push bar, an electronic method is used, known as a 'Request to Exit' (RTE) button. There are a range of different shapes and sizes but all have the same function. When pushed they send a signal to the device controlling the door which then releases the locking mechanism allowing exit.

KEY SWITCH

If the locking function needs to be turned off for periods of time, this is usually done through use of a 'key switch' and the cylinder can be suited with others in the building.

BREAK GLASS UNIT

A break glass unit is a means of releasing the locking mechanism, but unlike a request to exit button it will leave the door unlocked until reset. When operated, it disconnects the power to the locking device thus releasing the door, assuming the device is fail unlocked. In access control the break glass unit is always wired after the door controller and before the locking device.

When operated the BGU disconnects the power to the locking device and assuming the device is fail safe/fail unlocked, the device releases the door. A unit that combines the request to exit with the break glass unit is available as a single item. This has the advantage of wiring to a single point and a Perspex flap over the emergency release to prevent accidental use.

Request to exit button

Key switch

Break glass unit

Guild of Architectural Ironmongers

7. POWER THE DOOR

All access control systems will require a power source. The power source will depend on the device and the manufacturer but will normally be either 12 or 24 volts DC. Some devices, notably hotel door locks, may be powered by an internal battery only, while door operators usually operate from a mains supply of 230v AC.

The power supply should have a 'fire alarm relay' so that power is also cut if the fire alarm is activated.

The system design will need to take into consideration the power requirements for not only normal operation but also backup for emergency situations such as in the event of mains power loss.

Backup is usually by means of a battery sufficient to power the system for a given length of time located in the power supply unit (PSU) 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.

Power Supply Unit (PSU)

Battery backup

Guild of Architectural Ironmongers

8. ESCAPE THROUGH THE DOOR

Access control must not inhibit escape through a door on final escape route. The use of a panic bolt, lever or push pad may overcome the electronic locking already in place, but access control can be used alongside panic or escape hardware.

SOLENOID RELEASE EXIT DEVICES

These exit devices look like conventional touch bar panic latches, are aesthetically pleasing and easy to operate. They are suitable for panic egress in public areas but incorporate a solenoid powerful enough to draw back the latch to allow access.Some versions control vertical rod Pullman latches.

Solenoid release exit devices are usually linked to an external access control device to allow entry for authorised personnel.

They must comply to the harmonised standard BS EN 1125 and be CE marked.

Solenoid release exit device

BS EN 13637

There is a European Standard which covers electrically controlled exit systems for both panic and emergency escape entitled BS EN 13637:

- This specifies requirements for performance and testing of electrically controlled exit systems, specifically designed for use in an emergency or panic situation on escape routes.
- This standard also covers electrically controlled exit systems that are either manufactured and placed on the market in their entirety by one manufacturer or assembled from sub-assemblies produced by more than one manufacturer and subsequently placed on the market as a kit in a single transaction.

The BS EN 13637 Standard provides clarity and testing methodology on solutions for electrically operated systems which incorporate time delay and denied exit but only under strict guidelines and should only be used where building control allow this usage.

An Electrically Controlled Exit System may be combined with mechanical exit hardware – provided they have been tested to BS EN1125 or BS EN179. Exceptional cases allow inward opening doors such as hospitals, classrooms where local building regulations allow by way of exceptions.

Guild of Architectural Ironmongers

9. REVIEW THE DOOR

CHECKLIST

- Make sure that the ironmongery you have used is compatible with the access control specification – for example, lever handles should not be used on a door secured with an electromagnetic lock.
- Review against any current BS and EN Standards, particularly on harmonised mandatory standards such as BS EN 14846.
- Check the access control package is not contained in both the architect's and M&E packages which would mean it is counted twice.
- Check integration with other packages e.g. door operation to ensure the correct locking is specified with door automation.
- Think about other items your system may need and ensure that they are included – software, management control devices, swipe or proximity cards, etc. It can be very costly to overlook these in a specification.

STANDARDS

The following is a list of relevant BS EN and TS standards which all relate purely to access control locking and equipment:

BS EN 14846 - Electromechanically operated locks and striking plates – which is a harmonised standard under the CPR.

BS EN 13637 - Electrically controlled exit systems for use on escape routes - not yet harmonised but has been published.

BS EN 15684 - Mechatronic Cylinders.

BS EN 16867:2020 - Building hardware - Mechatronic door furniture - Requirements and test methods.

BS EN 16864:2017 - Building hardware - Mechatronic padlocks - Requirements and test methods.

BS EN 60839 - A series of standards specifically on access control.

BS 8607 - Mechanically Operated Push Button locks which is a British and not a European Standard.

TS 010 - Electro magnetic locking devices - Performance Requirements.

TS 621 - Thief resistant Electronic door locking devices.

Guild of Architectural Ironmongers

The Guild of Architectural Ironmongers (GAI) is the only trade body in the UK that represents the interests of the whole architectural ironmongery industry - architectural ironmongers, wholesalers and manufacturers.

Formed in 1961, the GAI is internationally recognised and respected as the authority on architectural hardware, building its reputation on three key pillars; education, technical support and community.

Its technical information service is the only specialist service of its kind, providing comprehensive advice on issues relating to the legislation, regulations and standards governing the use of architectural ironmongery and related hardware.

, Ironmongers' Hall, Shaftesbury Place, Aldersgate Street, London, EC2Y 8AA **T:** +44 (0)20 7033 2480 **E:** technical@gai.org.uk **www.gai.org.uk**