RISCAuthority

administered by

FPA Fire Protection Association

S29: Guide to Electronic Access Control Systems (EACS)

Version 01 Published 2016

Symbols used in this guide


Good practice


Bad practice


Discussion topic

Frequently asked question

Acknowledgements

The assistance of TDSi UK with the inclusion of illustrations is gratefully acknowledged.

Contents

Summary of Key Points

Increasingly recognised as an essential security control	• Access control should be seen as a natural and indispensable component of a security strategy, particularly where the volume of human and/or vehicular traffic makes reliable monitoring and control challenging for traditional methods.
Tailor the system to the security and business need	• The need for a careful risk assessment is as important for this solution as any of the other security technologies and the owner is recommended to research the benefits of the various optional features that add value to the basic function of controlling access.
System owners benefit from being involved	• System owners should liaise closely with the provider and satisfy themselves that the type and grade of equipment match the requirement and that emergency escape and disabled access have been adequately taken into account.
Complements and supports other security technologies in operation	• The effectiveness of a system is optimised when it is integrated with fire and intruder alarm systems and any CCTV or security guarding service already on the premises.
Recognise the system's role and limitations	• Access to and within the protected location will be managed and controlled in a very effective and sophisticated way but owners should recognise that these systems are not a substitute for such robust conventional security measures as may be necessary outside normal working hours.
Technically advanced	• This is a state-of-the-art security technology that has benefited from developments in user authentication which most criminals would be hard pressed to overcome.

1 Introduction

Access control is the term understood in the security context as referring to a class of mechanical or electromechanical products able to control access to and/or egress from a physically enclosed place such as a building, a part of a building or a compound, by persons or vehicles. That is to say, to permit authorised users to enter and/or leave a controlled area and to deny passage to non-authorised users. Strictly speaking, products operated by an occupier to remotely control (say) a door, usually supported by an audio or audio/video channel, come within this description as do simple mechanical devices which are released when a legitimate user enters a code on the device by pressing buttons.

Electronic Access Control Systems (EACS) are often an essential component of business premises security and building management, particularly for those medium to larger operations with significant numbers of people legitimately visiting or working on the premises. This is a security solution that is familiar to the general public but deeper understanding of the range of implementation issues and benefits is variable amongst security specifiers.

This may be due to the fact that whilst EACS are very effective in controlling human movement they are usually not designed primarily to exclude well-equipped intruders working outside normal hours which is often the main focus, for good reasons, of those responsible for security. Indeed, it is historically the case that most insurance policies covering theft from commercial premises are limited to claims arising from forcible and violent entry, or exit from, unattended premises. As a result, recommendations for EACS do not often feature in the security strategies typically proposed or sought by insurers.

Nevertheless, there is an increasing recognition that sound, state of the art security, confronting all forms of crime risk, is important to the creation of a “hard target” that will tend to divert criminals seeking to infiltrate or enter the premises, whether aiming to spy, steal, disrupt, damage, injure or commit arson.

2 Scope

This guide examines the principal components, design, operation, benefits and limitations of automatic electronic access control systems. Reference is also made to other methods for controlling access but they are mentioned only in passing. Although the guide should assist security practitioners wishing to add to their knowledge of the technology, it should also be comprehensible to the non-technical reader eg the potential EACS purchaser.

3 Overview

This guide is focused on those products usually associated with the mainstream electronic access control system sector of the security industry. These products themselves control, without any additional action on the part of an occupier or guardian, the movements of identified persons or vehicles legitimately entitled to pass through. It does this through assigning access rights to individual users or groups of users. The concept is now familiar to most people through the access control technology in use at their place of education, work or lodging, usually requiring possession of an object eg an access card and/or knowledge of a code, these being examples of a ‘credential’. Thus the correct recognition of users is achieved by comparing the credentials brought to the portal (the access point) by the user and those recorded in the system as signifying the right to pass through. A credential may be a tangible interface ie something possessed (eg a token such as a card), something known (eg a PIN number), a biometric quality ie a bodily characteristic or personal trait (eg a fingerprint or pattern of keyboard entry) or any combination of these.

In the absence of an EACS those responsible for the security of assets within a defined perimeter would need to ensure that:

- each portal (eg door) was subject to some form of controlled access eg through the use of locks and keys or a human guardian;
- keyholders would be prevented from passing through the portal during periods that access was unauthorised;
- keyholders leaving the organisation always surrendered all keys in their possession;
- all associated locks would be changed in the event of compromised key security;
- a forced entry through a controlled portal was detected and communicated;
- records were available as far as possible in relation to the accessing of critical assets at material times (eg between the last time the asset was known to be safe until the time of discovery of a security breach).

Being able to effectively address these issues in a way that eliminates many security weaknesses and reduces both management time and cost would themselves be reason enough to install electronic access control, but there are additional benefits as the remainder of this guide will explain.

4 Elements

Most electronic access control systems consist of several dispersed, discrete components that, when interconnected, are capable of exercising highly discriminatory control of movements at a location. The ubiquitous component familiar to most people these days, namely the access point control device – typically an electronic card presented to a card reader, is generally to be found in control of portals at various points around the location. The anatomy of such an access control system can be viewed as a number of distinct components and functions that are networked and driven by software applications. The essentials have been tabulated below).

Component/system function of typical system	Purpose
Portal (access point) actuator, eg an electrically actuated locking device	• To permit physical passage through the portal according to pre-set rules
Monitoring of access point	• To report/log within the system whether the portal is open or closed and whether the control device is secure or released
User interface: method used to identify users requesting access (eg keypad, token reader or biometric reader)	• To permit access to those users in possession of the correct access device and/or PIN code or who are biometrically recognised
Local controller	• To determine, according to pre-set rules, whether access should be granted or denied according to data from the reader, control device and sensing devices monitoring the portal
Alert (alarm) function	• To raise an alert in the event of an irregular event eg an abuse of, or attack on, the system and to generate a log entry
Duress function	• To generate an alert should an authorised user be subjected to coercion at the user interface
Monitoring console	• To centrally control the system and allow the system operator or administrator to program/ configure the system and follow alerts and events that are displayed/logged.

5 A typical system

Readers

These are located at each controlled portal and their purpose is to determine the unique credential(s) (identifiers) associated with each user's data and access rights stored within the system. A typical example being a device that can read the electrical signals when the user presents an access card. The 'grade' of reader (ie according to the international standard, designated in UK as BS EN 60839-11-1: *Alarm and electronic security systems. Electronic access control systems. System and components requirements* – see Section 6) determines whether audio and visual feedback is given to the user as to whether access has been granted or denied.

Access point actuating and locking devices

The most common of these devices, electrically driven mechanical devices that permit access through the portal, eg release of a door, is the door release – aka 'electric strike'. A description of this and other devices can be found in Section 8.

Local controller

A local controller, working in conjunction with reader(s) and the main controller ie the monitoring console, determines whether a given request for access should be granted according to the conditions and rules programmed into the system in relation to that particular individual or entity. Causes of access denial include: access privileges not extending to the particular portal, the particular time period, the particular day, the particular holiday, the particular location code; memorised information incorrect or not provided in time; anti-passback violation (see below); credential expired, not effective or not programmed in the system. After a predetermined number of unsuccessful attempts the access rights for the particular token may be suspended for a pre-set duration.

To avoid compromising the security of the monitoring console/host PC, locate it in a locked room or similarly secure environment.

Monitoring console/main controller

This is the heart of most systems to which the readers/local controllers are connected and where a database is maintained containing the rules that determine whether a user is allowed access through a particular portal at a given date and time. The component is also the place where the operator or system administrator can monitor logs and indications and can program and configure the entire system. However, in the event of an interruption of communication between a reader and the local controller/monitoring console, or where there are practical difficulties with continuous communication between these points, a reader may assume 'stand-alone' mode in which case it is self-contained with its own database and can operate without connection to a local controller and monitoring console.

6 System design

The sophistication, security functionality and range of features vary between the offerings of the suppliers. However if a given system conforms to BS EN 60839 it will have been designed to match one of four grades and the standard guides the specifier or purchaser by recommending the applications considered suitable at each level as follows:

- G1 Hotel;
- G2 Commercial offices, small businesses;
- G3 Industrial, administration, financial;
- G4 Highly sensitive areas (military facilities, government, R&D, critical production areas).

The situations indicated for each grade are merely to illustrate the general consensus on the functionality and security required for typical situations at each level (ie the value of the assets requiring protection and the knowledge/skills of a hypothetical adversary) but it is of course entirely a matter for the owner as to whether the organisation in question merits a higher or lower level than might be assumed from this guidance. For example, there is a school of thought that, given the potential for theft in hotels, they should be graded in the same category as offices and small businesses. Furthermore it is permissible that access points within a system differ in selected security grade. However, in this case common system components must meet the requirements of the highest security grade access point with which they are connected.

In arriving at a suitable grade the security risk assessment should take the following into account:

- the organisation's activities and access control policy;
- the assessed threat (target attraction/adversarial determination and skills);
- points of enhanced exposure (eg specific assets);
- security grade for each access point in light of previous item;
- access levels (authorisation) for each area zone;
- user flow (number of persons in a period of time);
- the need to allow for users with disabilities;
- means of safe escape (eg in event of fire);
- management of visitors and vehicles;
- selected recognition technology eg pin/token/biometric or a combination of these.

7 Interface recognition technology

The purchaser of an electronic access control system may have difficulty determining the relative merits of each technology. A balance needs to be struck between purely practical issues (convenience, ease of programming etc) and security. The selected technology may well differ from portal to portal if the risks of the system failing to reject an authorised user significantly differ between the various portals/control zones. The available methods are defined as follows:

- **Memorised information:** 'Information known to the user'. Example: PIN code.
  Comment: If memorised information is the only technology in use at the reader then the reader would be considered of low security value as there are a number of ways a PIN code might be revealed to an unauthorised person. BS EN 60839 requires that memorised information is used on its own only at grades 1 and 2.
- **Token:** 'Portable device containing a readable unique identifier (credential) that can be associated with a user's data and access rights stored within the electronic access control system'.
  Comment: the ubiquitous swipe card is an example of a token and an obvious security risk is that the token is found or stolen and used illegitimately. However use of a pin code in combination with a token has the potential to uplift the basic security of the token on the basis of "something owned, something known". This would be an example of what is referred to as 'two factor authentication' (see Figure 3).

Figure 1: A token in use with a reader working on a proximity basis

Figure 2 A fingerprint reader with a keypad for a PIN

- **Biometrics:** 'Any measurable, unique, physiological characteristic or personal trait that is used as a credential to recognise and verify the identity of an individual's dynamics'. Examples: facial verification, fingerprint, hand or face geometry, retinal / eye, face, voice, signature or keyboarding dynamics.
  Comment: biometric recognition potentially provides ultimate security (particularly where used with memorised information) but, as a general principle, as the accuracy of recognition demanded of the system is increased, so is the possibility of false rejection, to the point that a customer may view the system as unfit for the particular purpose. The other side of that coin of course being the risk of an unacceptably high false acceptance rate from the quest for tolerable performance. That said, where demanded by onerous risk, the biometric solution clearly has the advantage over the other options.

  However, ease of use, accuracy and cost vary greatly between the technologies and manufacturers/brands and a reliable provider needs to be identified with whom the assessed risk and options may be discussed. And finally on this topic, there needs to be an acceptance that there is the possibility of resistance on the part of those required to use the equipment and from whom biological data will be extracted, retained and processed. Furthermore, even if subjects are merely hesitant at the outset, attitudes to the technology could easily change over the life of the installation eg in the event of negative coverage in the media. A greater investment in initial and ongoing consultations with users than would be necessary with the other, traditional technologies, is perhaps called for.

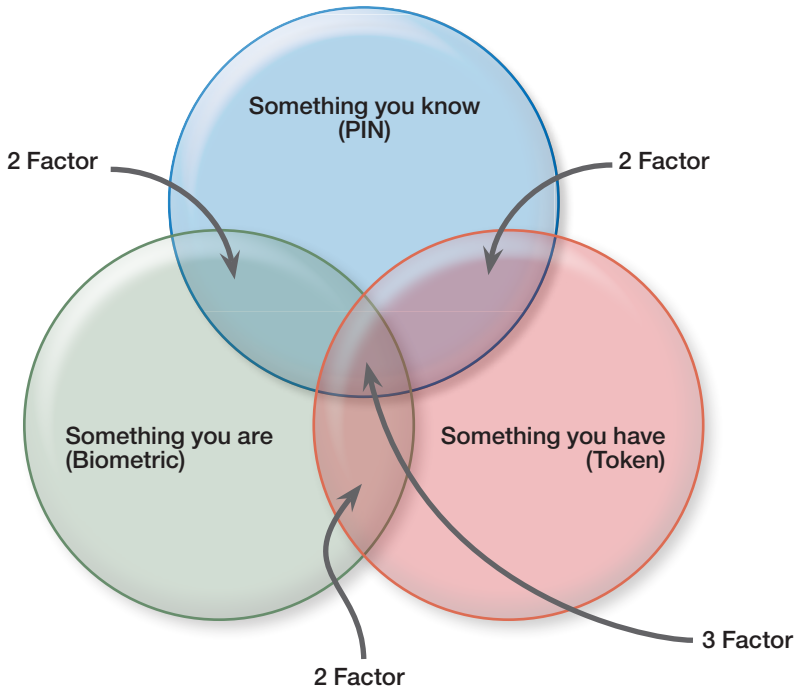

Figure 3: User authentication

If suggested by the assessed security risk the recognition technologies outlined above may be used in any combination thus uplifting single factor authentication to two or three factor authentication. Furthermore, it's worth being reminded that the presence of an electronic system should not debar some element of verification by a responsible human being in ultimate control of the portal. This human controller can have remote control of the portal, possibly supported by an audio link to it whereby the user may be interrogated and/or the controller can have access to both a live and recorded facial image of the individual. In this way an additional check by a human intelligence on an individual being passed by the system might be seen as a valuable confirmation of the legitimacy of the permitted access with the added benefit that abuses and crime such as 'tailgating', deception, intimidation, hold-up etc may be detected (see Section 9 for more information).

8 Portals and release options

In most cases the portal to be controlled by the EACS is a conventional hinged door fitted with a door closing device (a device designed to automatically return the door to the closed position after the door has been released/opened).

Exceptions to this are usually found for reasons of aesthetics and/or higher throughput and/or better control than might be possible with a standard hinged door. These exceptions nearly always involve the use of a 'turnstile'. For the purpose of this description, by turnstile we simply mean a portal, in whatever form, designed to physically limit passage to one person at a time. This degree of physical control varies according to the type of turnstile selected. Obviously, a full height turnstile is more likely to effectively control passage through it than a half height turnstile or a half height 'speedgate' but then, for the sake of appearance and speed of use, and where there is a degree of supervision, solutions less than full height may be preferred by the specifier and be fit for purpose. However, the full height turnstile minimises the critical tailgating risk and, in combination with biometrics, ensures credentials cannot be duplicated or passed to others. If a turnstile is contemplated the need for a suitable means of emergency escape and consideration of whether a method of disability access must be provided (see also the observations in the paragraphs that follow), should receive special attention and be discussed if necessary with the system provider.

Perhaps the ultimately secure turnstile solution is the so-called 'security booth' or 'security cubicle' of the type that works on the principle of an airlock. This is formed by a cubicle of dimensions sufficient to accommodate just one person which allows the user to enter through an opening on the unsecure side and exit on the secure side, the two openings never being unsecured at the same moment.

The mechanical device that releases and re-secures a portal is an 'access point actuator'. The turnstiles as described here are their own actuator through their very operation as commanded by the local controller, unless of course a turnstile is of the passive type, functioning purely to allow passage in one direction, eg typically used at the exits of sports stadia.

However, portals consisting of conventional doors need to be secured by some form of remote-controlled locking device. The circumstances of each portal need to be considered in the selection of a suitable device, for example:

- The device and portal type should be commensurate with the security grade of the portal as determined for its zone and the physical qualities of the barrier (eg surrounding internal wall) accommodating the door opening.
- Safety issues (eg in the event that the portal is to form a means of safe escape in an emergency).
- The ability of persons with disabilities to use the portal.

Descriptions of three important types of device, and the considerations involved with each, follow.

Electric strike

This is probably still the most popular release device due to its simplicity and low cost, plus the fact that it often works in combination with a lock that is already fitted to the door. The device, a type of keep fitted on the door frame on the locking side, receives the latch of a lock in the door and releases it on command from the controller. Although stronger, higher security versions are available, the type generally fitted provides very limited resistance against the use of physical force on the door. As a result, if the situation of the door exposes it to attack by intruders, it is vital that a routine is in place to ensure that the door is secured by an adequate lock outside the normal operating hours of the premises. The insurer should be consulted if necessary.

Along with certain others, these devices work in one of two ways, depending on whether electrical power is available or has failed. These two fundamental principles of operation are as follows:

- 'Fail-safe': the device is designed to automatically release upon power failure. Devices operating on this principle are mandatory for portals required to allow passage in an emergency such as a fire.
- 'Fail-secure': the device is designed to remain secure upon power failure. Devices operating on this principle are typically selected in high security applications and where escape in an emergency is not a requirement.

Whether working on the principle of fail safe or fail secure there should be available a manual door release switch – essential where the door has been identified as a means of escape in an emergency – see below.

Regular inspection and maintenance of doors and release devices are vital to maintaining the integrity of the system.

'Maglock'

An energised electromagnet and a metal plate are in contact when the door is closed but released (when power is withdrawn) on command from the controller. The design has the benefit of no moving parts that could fail but alignment is critical. A so-called 'Shearmag' is a similar device but its design provides a greater holding force than a Maglock. Like the electric strike, product types vary in the strength with which the magnet and plate are held together. However, as this device inherently fails-safe (ie fails unsecure) it may not be suitable in high security applications. Once again, it could be vital that the door is adequately locked by another device outside normal hours.

Motorised lock

In contrast with the electric strike, in which the operating component is in the door frame, the motorised lock is essentially similar to a mortice deadlock and the operating component is a moving dead bolt which is driven by an electric motor. This endows the device with a greater level of inherent security than an electric strike and, despite its much higher cost, it might be considered where the portal enjoys limited supervision when the EACS is in control.

Failure of power to the lock will cause the bolt to remain in position, whether secure or unsecure. Furthermore, the device does suffer from slow operating speed making it unsuitable for portals with high levels of traffic. Various other types of electric lock are available but they do not work on this principle and, all things being equal, the motorised lock tends to provide superior security if the slow operating speed can be tolerated. However, depending upon the strength of the device and the security requirement, a conventional lock may still be needed for use outside normal hours. The insurer should be consulted.

Egress options

A simple 'request-to-exit' push button or rocker switch is usually all that's required to release a controlled door from the secure side and permit uncontrolled exit. If there is a pressing need for this function to be provided by a movement sensor then it is important to ensure that the device only responds to persons at the exit and not simply passing by. If exit from the premises needs to be controlled then a second reader will be required on the secure side to permit this. In this case, since emergency egress must not require an access control system to operate, a 'breakglass' device must be installed close to the portal to allow the release of the locking device.

Perform a fire evacuation drill at an early opportunity after installation of the system.

If the premises have a fire alarm system then the default configuration is that, in the event of its activation, all points of access are automatically released. In certain high risk situations eg art galleries holding very valuable exhibits exposed to the risk of criminal activation of the fire system, a compromise sometimes arrived at is configuration on a fail-safe basis alongside emergency breakglass devices and having a CCTV image showing the released portal(s) displayed to security staff.

When it comes to hardware, system design must take full account of the premises' escape routes and reflect the following basic principles established in the applicable national documents dealing with escape according to the categories of premises and occupiers.

Panic escape devices are particularly prone to sabotage and to misoperation resulting from damage or lack of maintenance and regular inspection is vital.

In a small business, with a stable workforce and no public areas, and assuming the exit doors are used by a limited number of staff familiar with the layout of the premises, use of exit devices, with keyless egress, ie where the lock bolt can be operated by handle or knob from the inside, is normally acceptable. In all other cases, the choice of suitable emergency exit door hardware will normally be restricted to panic or emergency bolts and latches.

For information on the conditions placed on use of these devices reference should be made to *Building Regulations Approved Document B, BS EN 1125: Panic exit devices operated by a horizontal bar and BS EN 179: Emergency exit devices operated by a lever handle or push pad*.

Specialised escape devices, electrically connected to the system, can be included according to the circumstances.

9 Additional features

The risk assessment, in terms of both the overall level of security required for the location and the measures necessary to manage the movement of personnel at various points, will suggest which of the following features should be included:

Duress alert

An authorised user has an opportunity to enter a duress code on a keypad in the event of threat or coercion. A silent warning is generated eg at the monitoring console (but, in the UK, is not permitted to generate an automatic alarm signal to police unless integrated with an intruder alarm system meeting national police rules).

Portal forced open alert

An alert signal is generated when an access point is opened without access being granted.

A 'blind eye' turned to the practice of propping open a monitored door undermines the system; special arrangements should be made with the provider for any staff required to carry awkward sized objects between zones.

Portal open for too long alert

An alert signal is generated when an access point open time is exceeded after access is granted.

Anti-passback alert

This feature eliminates the abuse whereby a user, having gained access, passes back the credential to a confederate. It does this by requiring user validation when leaving the controlled area in order to be able to re-enter. 'Hard anti-passback' generates an alert and denies further access to a particular credential following violation of anti-passback rules whilst 'soft anti-passback' generates only an alert in these circumstances. In the 'area controlled anti-passback' mode the user is required to be present in a designated security controlled area in order to be able to enter another security controlled area. 'Timed anti-passback' traces an individual credential access request to a given area for which an access granted was not followed by an exit granted, or an exit granted was not followed by an access granted within a predetermined time period.

What is seen by users and abusers alike as the 'Achilles heel' of the average access control system? Tailgating would be high on the list!

Anti-tailgating alert

Tailgating occurs when a person or entity passes through an access point without using credentials by following a person or entity for whom access has been granted. This function prevents or detects attempts at gaining access in this way. However the only completely reliable way of actually preventing simple tailgating is to resort to a full height turnstile (see Section 8).

10 Other optional benefits

Time and attendance

The reliability of the data evidencing identity and presence allows an access control system to record employee hours and feed information to the company's payroll system.

Automatic number plate recognition (ANPR)

This special application uses CCTV and optical character recognition to capture the alpha-numeric information on a vehicle licence plate. The vehicle is illuminated with IR light to allow operation in all light conditions. In effect the index number is the interface credential and, provided the number appears on the system's database, access (eg to a car park) will be granted automatically (the access point actuator being an electrically powered barrier), provided any other zonal and time window rules are met. Obviously, the access control of vehicles is perfectly possible through a human controller or, automatically, the use of other interface devices that bear more similarity to the devices carried by personnel – of which the tokens used to admit vehicles onto toll roads are an example.

Fire roll call

A fire roll call application reports the identity and location of persons within a building should there be an emergency.

Integration with an intruder alarm system

One practical benefit of integrating with the alarm system is to be able to exclude unauthorised people from set areas thus avoiding unnecessary false alarms.

Visitor management

Through integration with CCTV and/or the issue of specifically programmed temporary tokens, the movements of legitimate visitors can be managed and tracked. An associated function requires a visitor to be accompanied by a token holder with defined credentials for access to be granted.

Presence check

The ability of a system to confirm the number (maximum, minimum) of persons within a security controlled area.

Vulnerable person management

The configuration may provide for an alert to be generated should the number of staff within a defined zone be reduced to a single lone worker. Similarly, a system can be configured such that a minimum of two persons are present whenever the zone is occupied.

Lift (elevator) control

In this case the system restricts the operation of a lift/elevator car to those token holders to whom the privilege has been assigned. In emergency situations it is normally the case that the lift car is sent to the ground floor and parked. This function could be controlled through an access control system or the fire detection system itself.

11 Conclusion

Electronic access control technology is a security solution ideally suited to present day network technology and is continuously evolving, developing and widening its benefit to the security of business premises. For all practical purposes its function cannot be fully replicated by any other method of control, irrespective of cost and it is often an invaluable component of the security strategy of, particularly, the larger operation. It naturally complements other forms of electronic security such as CCTV and intruder alarm protection and there are few applications where it should not be considered as a useful component of overall site security.

12 RISCAuthority guides containing additional guidance

The following selected guidance documents contain additional information of relevance to those interested in the security of occupied business premises and access control:

- S11 Security of emergency exit doors in non-residential premises
- S18 Cash risk assessment – an insurers' guide
- S19 Security guidance for defence against robbery
- S20 Essential principles for the protection of property
- S22 Cash security – a user's guide

In addition to these, a wide range of guidance documents covering other aspects of security is also available.

Documents may be downloaded free of charge from the website: www.riscauthority.co.uk and those available in hard copy form may also be purchased from the Fire Protection Association.

RISCAuthority

administered by FPA Fire Protection Association

Fire Protection Association
London Road
Moreton in Marsh
Gloucestershire GL56 0RH
Tel: +44 (0)1608 812500
Email: info@riscauthority.co.uk
Website: www.riscauthority.co.uk