# A guide to
# integrated security
# management systems



April 2017

# Contents

Contents

# 1. Scope

Security managers wishing to procure new security systems for their organisation today are presented with a complex range of technical options. This guide aims to assist consultants, integrators and security managers in defining an integrated security system. It will assist navigation through some of these issues and explain the benefits and opportunities of implementing a truly integrated system to meet the needs of the organisation.

# 2. Overview

Security systems are changing at an ever-increasing pace and are becoming standard Information Technology (IT) products running over a Local Area Network (LAN), Wide Area Network (WAN) or wireless. As a result of using standard protocols such as Transmission Control Protocol/Internet Protocol (TCP/IP), the opportunity has arisen for manufacturers to develop new generations of integrated systems. These systems are often called Integrated Security Management Systems (ISMS) as they bring together the management of all aspects of an organisation's security. This brief document does not aim to cover all the possibilities, but will explain most of the opportunities for integration into a single management system.

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. The benefits that an integrated system can provide include the ability to view alarms from all systems in a single user interface and the ability to link access and intrusion events to video recordings. This can make investigation much more straightforward and reduce the need to send security officers out to respond to security breaches.

It is not always necessary to purchase all the components of a system from one supplier. Manufacturers of Security Management Systems realise that the customer wants choice and will often link to components from other specialist manufacturers. Many manufacturers provide integration modules and protocols such as BACnet and OPC, and data integration methodologies such as eXtensible Markup Language (XML), ActiveX and others, which can in theory link to almost any business system. You will need to talk to individual suppliers to discover what development tools such as Software Development Kits (SDK) and Application Programming Interfaces (API) are available for integrating systems.

As part of a Smart Cities approach the ISMS can bring together security elements (access control, video, intruder & hold up alarms), life safety (Fire systems), building management systems (HVAC, lighting) and various other aspects of an organisation's facilities management requirements. We will look at more of the possibilities later in this document. Any one of these systems can form the central "glue" that connects the various systems together.

The system you choose should not only meet your requirements today, but should also be adaptable enough to meet your needs into the future. This is a difficult challenge, but you need to be able to predict how your organisation may change and grow and ensure that the systems that you are looking at have the scope to expand to meet these needs. Manufacturers will not stand still as technology evolves. You should expect:

- More use made of wireless devices.
- More of the system to connect directly to your network.
- To run the security for the whole organisation from a single location via your Wide Area Network (WAN) or the internet.
- Changes in access token formats (this may include greater use of biometric technologies) and a greater level of integration than you see today.
- More use of apps (via a smart phone or other device) to manage, monitor and control the ISMS.

In the future, all systems will match the performance of the best systems of today, which provide a totally integrated solution for your security needs.

# 3. System integration opportunities

There are a number of advantages to be gained in both the security and commercial aspects of designing and adopting an integrated system. This section lists some of the advantages that may be considered when combining separate systems into an integrated solution.

## 3.1. Access control systems

Access control is typically specified to provide protection to both property and employees. Generally it is thought of in terms of managing doors. However, it often extends to public areas when coupled with turnstiles, gates and barriers, or highly sensitive areas when coupled with biometrics. By integrating access control with other systems many advantages may be realised. For example:

- Fire Alarm mustering – know where your employees are at a given time.
- Know which doors / areas employees are entering, or trying to enter.
- Link CCTV images with access control events.
- Link Time & Attendance monitoring using the same badge / token software.
- Link Visitor Monitoring with Access Control & CCTV using badge / token software.
- Increase security through systems such as dual card access or access using a biometric technology.
- Integration with intruder & hold up alarm systems.

## 3.2. Time & Attendance (T&A) monitoring

The same badge/token used to identify a person in Access Control can register them on and off work with time & attendance monitoring. Also as more integrated software systems become available, use of the same software to handle access control, time & attendance and visitor monitoring can be achieved. Remember, however, that just because a person went through an access control door does not mean they are registered for work, especially under Working Time Directive (WTD) requirements. You will need separate T&A clocking stations, albeit on the same network, to monitor working hours and software to calculate employee hours, monitor absences and WTD hours and infringements.

## 3.3. Visitor Management Systems (VMS)

For many companies and organisations a manual paper-based VMS will suffice, providing visual identity of visitors. However, computerised systems linked to Access Control and Time & Attendance systems are the natural bedfellows for integrated security systems. These not only print ID passes, but can also incorporate biometric identification and the scanning of visitor/contractor documentation, licences, certificates and insurance certificates.

## 3.4. Lift control

By integrating lift control with the access control system, access to certain floors in a building may be restricted, particularly outside normal working hours or in multi-tenanted buildings. Also, modern lifts, can take a data feed from the access control system and advise the user which lift car they should go to. This is known as "elevator despatch", this improves efficiency of the lift system and reduces energy usage.

## 3.5. CCTV systems

By integrating CCTV and other systems such as access control, the benefits of more than one system can be coupled to provide a more efficient and usable solution for the end user. For example:

- Live camera views can be integrated with the access control software, equally access control or other data can be integrated with the CCTV system.
- Access control and other security detection systems can initiate pre and post-event video recording, linking the video recording with the event information. This makes searching for events on the Digital Video Recorder (DVR) more effective as only the event needs to be searched, for example 'door forced – stores door' or 'zone 3 – perimeter breached.'

- Track individuals and record their access details against the recording to track suspect users or stolen card users.
- Initiate camera presets when specific pre-determined events occur, e.g. when entering a room in a bank, switch the camera to zoom into the door to identify the individual.
- Use CCTV with time & attendance system to detect / eradicate 'buddy-clocking', a practice where employees clock each other on and off work.

### 3.6. Intruder alarms systems

By integrating intruder with other systems, the benefits of more than one system can be coupled to provide a more efficient and usable solution for the end user. For example:

- Set / unset the intruder system using an access reader. No need to use the intruder keypad.
- No entry delay time if main door forced. The entry timer is bypassed thus providing an instant alarm.
- Disabling of access readers when the intruder system is in the armed state, to prevent false alarms due to unauthorised entry into an armed area.
- Using an occupancy count from another system, the intruder & hold up alarm system can be notified that there may be persons present in the building when the system is being set. False alarms will reduce your credibility with the National Police Chiefs' Council (NPCC) or Police Scotland Security Systems Policies.

### 3.7. Fire systems

By integrating fire with other systems, the benefits of more than one system can be coupled to provide a more efficient and usable solution for the end user. For example:

- In the event of a fire, all emergency exit doors on the fire escape route need to be automatically released from an electrical point of view, but physical quick release locks may be in place to maintain security and still allow people to escape. It is common practice to install a relay in series with the electric locking mechanism controlled by the fire panel. An alternative is to feed a fire input into the access control system, which then automatically releases 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.
- In addition to providing hardware control during a fire situation, it may be necessary to provide a 'roll call' or 'muster' report to list all people in the building at the time of the fire alarm.
- CCTV cameras may also be linked to software to detect smoke or fire and provide a good early warning of fire.

### 3.8. Building Management Systems (BMS)

Building management systems are responsible for monitoring and controlling the environment of a building, for example lighting, heating and ventilation (HVAC). In the current climate of energy saving, why leave lights on when an area is unoccupied? By integrating access control systems with BMS systems, the lighting can be automatically controlled by recording when people access an area. The system can also be configured to control the heating by reducing the room temperature when no one is present rather than leaving it on all day and off at night. The use of mobile device apps to remotely control building systems is becoming more popular.

### 3.9. Human Resources (HR) / Payroll

Why enter data twice? When a new employee joins a company their personnel details are often entered into both the appropriate HR system and then again into the security system. By integrating these two systems, a subset of the employee data can automatically be transferred into the access control system when an employee joins. Alternatively, when an employee leaves, their rights can be automatically deleted from the access control system, again reducing effort and increasing security.

Access rights held within HR systems can automatically update the access control system when changes are made ensuring instant security updates. This reduces the risk of the access control system not being informed of employee changes.

### 3.10. Car park management

Where access to a car park is restricted, the ISMS can automatically monitor the number of spaces left for each tenant or department and regulate access accordingly. For example:

- Visually through CCTV.
- Audibly through an intercom system.
- Automatic number plate recognition.
- Access Control tokens.

### 3.11. External perimeter detection

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 CCTV or access control 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.

### 3.12. Logical security

Logical access control is the brother of physical access control but is often limited to secure PC logon. Integrating these two elements can significantly increase your security. For instance, you can restrict PC access to only those who have a smart card and use this to logon to your IT network. Alternatively, you can inhibit network logon if the person is not in the building, further enhancing your security. One example is to use the CCTV system and access system to monitor and lock doors during a denial of service (DOS) attack at the same time as sending a message to the security guards. Quite often physical and logical attacks go hand in hand.

### 3.13. Asset management

This subject can cover many areas but as a starting point, consider linking alarms associated with company assets into the ISMS, for example:

- By logging assets against employees you can automatically raise an alarm if an asset is moved outside a designated area (or building) without its owner e.g. a laptop.
- By using CCTV automatic number plate recognition (ANPR) systems vehicles could be tracked and logged in and out of sites.

### 3.14. Audio / video intercom

By integrating your intercom system with your ISMS, you can provide notification that an intercom call has been initiated or the caller can be visually verified.

### 3.15. Guard tour

By using a guard tour package that integrates with the ISMS the door readers can be used to define and monitor a tour by a specific guard, providing a real time indication if the guard does not reach a set point in time (or even if he arrives too early) – equally integration with the CCTV system can provide visual verification of the guard's location and wellbeing. Many time & attendance systems incorporate guard tour functions as part of their software package.

### 3.16. Vending

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.

# 4.    Integration connection methods

The type and level of integration will depend on the user requirements. Options to consider are detailed below and they range from using a common access card through to systems where two or more software applications are 'merged' as one.

Note: British Standard DD CLC/TS 50398:2009 Alarm systems - Combined and integrated alarm systems - General requirements, gives recommendations for interconnected systems.

### 4.1.    The non-integrated approach
When considering integration, the not so obvious option might be to keep all systems completely separate from each other. An integrated solution might not be appropriate for the operator, or if the nature of the business is such that two or more functions are operated in separate areas of a building.

### 4.2.    Using a common token
Companies often have several systems in operation, each requiring verification using some form of identification card. Examples are an access control system, a library book loan system, a photocopier control system etc., all of which can be managed from a single Smartcard.

Smartcard technology allows data to be stored in any of the sectors on the card. This means that a standard card can support as many systems as there are sectors on the card.

### 4.3.    Interconnected systems
An interconnected system, typically using inputs and outputs, is often referred to as a low level interface. Two or more systems operate independently of each other, but there is a link where the outputs from one system connect to the inputs of another system. This is often the way a fire alarm panel is connected to an access control system. The fire alarm panel has a regulatory approval for fire warning/protection, whereas the access control system may not. Should the fire system detect an alarm, an output relay on the fire system is connected to the input of the access control system. This means the alarm is reported as a fire alarm on the access system. This is the full extent of the interface.



**Interconnected System**
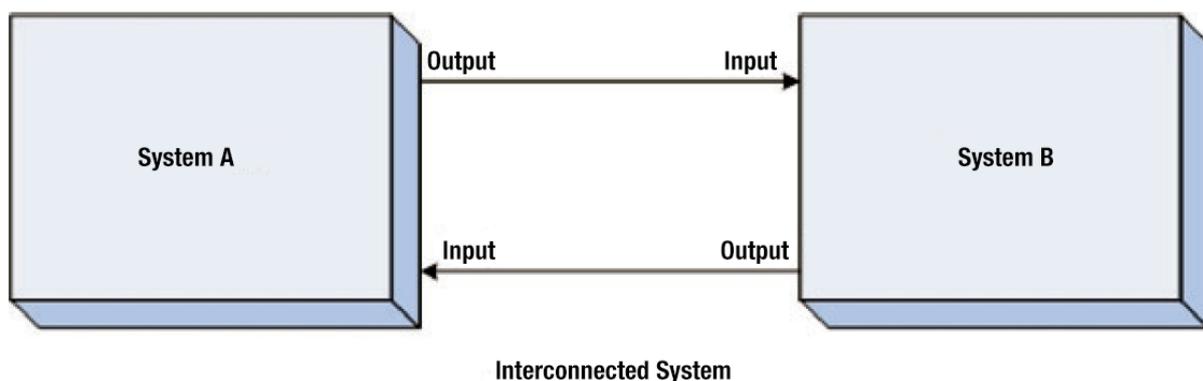
## 4.4. Data communication

Data may be shared between systems using common connection/protocols such as Ethernet with TCP/IP protocol data or other data transfer methods. This allows data flow in both directions so that not only is event data received, but control data may also be sent in each direction. An Ethernet connection across the LAN is capable of providing a more sophisticated integration and can be location independent. A simple example of this process is an access control system connected to a CCTV system, where an access control event generates a data string and passes this to the CCTV system. The CCTV system has been pre-programmed to recognise the string so that on receipt, it switches a specific camera to a specific monitor.



**System A**    ← **Communications Interface** →    **System B**

**Data Communication**
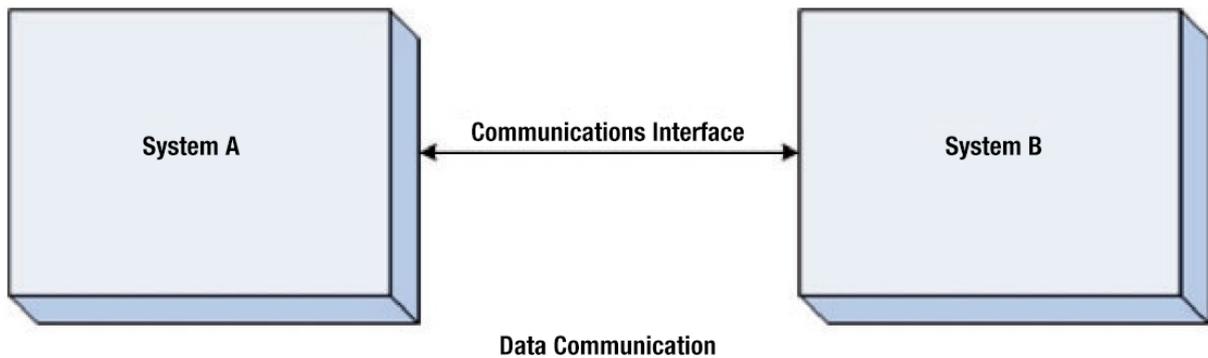
## 4.5. Common User Interface

Although, as above, data may be shared between systems using common connection/protocols such as Ethernet with TCP/IP protocol data or other data transfer methods, a Common User Interface is used, this is a single map-based graphical user interface (GUI) that shows the location and real-time status of every security device. This would also include a single consolidated alarm/event stack, or history.



**System A**    **System B**

**Communications Interface**    **Communications Interface**

**Common User Interface**
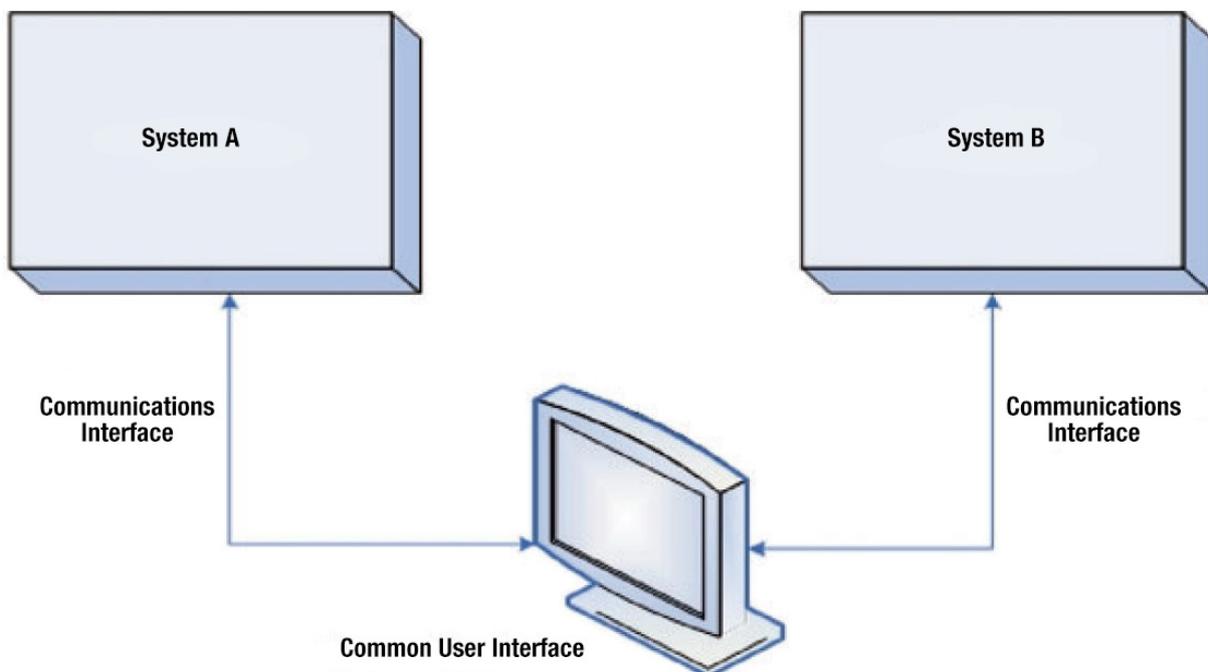
### 4.6. Multifunctional system

In a multi-function system, a common platform provides many of the main elements of the ISMS. These types of systems offer a number of advantages:

- Common user interface.
- Single contact for support.
- Deeper integration between systems.

### 4.7. Physical Security Information Management (PSIM)

PSIM is software that provides a platform and applications that are designed to integrate multiple non associated security applications and devices and control them through one comprehensive user interface. It collects and correlates events from security devices and information systems (CCTV, access control, sensors, analytics, networks, building management systems, etc.) to empower personnel to identify and proactively resolve situations. The benefits of PSIM integration are increased control over security, improved situation awareness and management reporting.

### 4.8. Hybrid systems

It also may not be practical or viable to fully integrate systems due to compatibility or infrastructure issues, in these cicumstances it may be possisble for some level of integration, using some of the techniques described above, creating a hybrid security management system.

# 5. Considerations

### 5.1. Audit trails

When considering integrated systems, it is important to look at the depth of integration not only of the main user interface, but also of the security trails on the system. A completely integrated system will allow operator security checks to be made from one centralised point. For instance, if a camera is tampered with and a guard checks it out then both camera alarm and guard response should be available on the same report and a history file should be available on camera tamper, guard response and who printed out the report.

### 5.2. Data security / encryption

Open integrated systems rely on open system architecture to achieve integration and share their working environment with other systems – computer databases for instance or LAN cable structures. Different parts of a system that are connected by open cable structures can be vulnerable to hacking by anyone who has access to the network. In order to minimise this risk, integrated systems have forms of encryption on messages that are passed between the different constituent elements. This encryption can range from simple proprietary message codes and checksums to complex multi-bit encryption algorithms. For added system security, a completely separate communications structure can be used.

The security of the computer where the security system is installed needs to be managed and IT security measures considered, for example:

- The use of vulnerability checks such as Cyber Essentials that requires organisations to complete a self-assessment questionnaire, with responses independently reviewed by an external certifying body.
- If required, further more in-depth vulnerability tests such as Cyber Essentials PLUS that, additional to the requirements of Cyber Essentials, carries out tests of the systems by an external certifying body, using a range of tools and techniques that analyses, identifies and classifies the security vulnerabilities in a computer, server, network, or communications infrastructure.

### 5.3. Data integrity / bandwidth

When using integrated systems that require messages to be passed on communication paths – Internet links for instance – care must be taken that there is sufficient bandwidth available for messages to be transmitted correctly. Data integrity / response will be commensurate with the type of data (e.g. video or alarm) and the communication method (e.g. LAN or modem). The use of picture and video data over a network will need to be looked at carefully as calculations of bandwidth usage are complex and require a degree of knowledge. If sharing an existing network, high volumes of video data may cause other services on the network to be slowed down. It is vital to involve your company IT manager at an early stage of your planning to ensure full compatibility between the ISMS and the existing information technology infrastructure.

### 5.4. LAN / WAN availability

Not all communication links are available all the time. You should not rely on Local Area or Wide Area Networks being able to transmit every message in real time. A well designed integrated system will also be able to run as separate entities if communication is not available. This should be invisible to the user and once communication is available again, the different system parts should be able to send stored messages and carry on running as if nothing has happened.

### 5.5. Recovery from power failure

Any system should be designed and configured to ensure that all relevant applications associated with the integrated system automatically start following a power fail or re-boot. This will ensure minimum down time and reduced risk to security by negating the need for the user to understand the complexity of the system configuration. Any such events should be logged for later evaluation.

### 5.6. Fault intolerance

In any ISMS, consideration should be given to minimising single points of failure and defining a disaster recovery policy when designing the system to ensure maximum availability and rapid resolution of any failures. The following forms of resilience should be considered:

• N+1 Redundancy
• Cold standby
• Warm standby
• Hot standby
• Active standby

# 6. Standards & legislation

Both British and European standards are available for associated equipment and their constituent parts. DD CLC/TS 50398:2009 (Alarm systems - Combined and integrated alarm systems - General requirements) forms part of these, but there are also industry specifications (e.g. ONVIF and PSIA), codes of practice and legislation for privacy and data protection that you need to be aware of.

The BSIA is well placed to obtain information about which standards apply to your particular configuration of system components. The standards themselves are available from the BSI (British Standards Institute).

BSIA companies have to demonstrate compliance with standards and therefore, we would strongly recommend that you choose one of these companies who can demonstrate to you a track record of installation of complex integrated systems. You also need to ensure that your installer / integrator and maintainer have the in-depth capability to be able to install, commission and maintain the system into the future.

# 7. Steps in defining an Integrated Security Management System

Think through the basic requirements and talk to potential users of the system in other job functions throughout the organisation including Human Resources and IT. You should be prepared to continually add to your list of requirements as you talk to potential suppliers because today there are opportunities to add additional functionality that you probably would not have thought possible. You can also reduce cost by linking to other applications within the organisation – for example, automatically importing details of new employees from the payroll system.

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 an ISMS 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.

When talking to suppliers you need to be prepared to ask detailed questions about what is and is not possible and to ask for the system to be demonstrated in a configuration that closely matches your needs. At first glance many of the systems available appear quite similar and it is only when you look more closely and ask questions that the differences start to appear. There is a range of manufacturers of these systems and many are members of the British Security Industry Association (BSIA).

The definition and design of any ISMS requires careful consideration. Due care and attention should always be given when evaluating operational requirements to ensure that the system integrity is not compromised.  As a minimum the following should be considered:

- Required level of integration (i.e. interconnected systems, SMS, PSIM).
- Range of equipment to be integrated (i.e. availability of device drivers).
- Scale (number of systems/points, number of workstations, number of maps).
- Maps (how many maps, how often do they have to be updated, can they be updated without support from the manufacturer).
- Ease of use.
- Reports (how many reports are available, can these be customised to meet your individual requirements).
- After-sales service & support.
- Cost (both up-front and recurring costs).
- Cost benefit / return on investment.

# 8. Further information

To source an ISMS from a BSIA member company, visit the BSIA website at **www.bsia.co.uk**

This document was created by the technical groups and committees 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.

In order to provide guidance and simplification in the complex area of integrated security management systems, the BSIA is very active in the European & International standards arenas and also develops its own guides and codes of practice where currently standards do not exist.

The technical groups and committees encourage debate on new developments and concerns within the security industry. In doing so it seeks to ensure that all stakeholder interests are represented including: security companies, users, the police, inspectorates and insurers.

As a security company, 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.