Join us and other experts and become a Committee member

Participating in a BSI committee has its benefits. These include:

- Influencing the content of Standards that will support economic growth, innovation, consumer protection and safety, both nationally and internationally
- Networking with peers in your industry and expanding your circle of contacts
- Developing your skills in communication, negotiation and diplomacy as well as your technical expertise - it’s great professional development

Committee membership work is rewarding. Your expertise, sustained effort and judgment will help derive substantial benefits for the UK and for the people you represent.

How to get involved: if you are interested in participating in any of the Security Committees please visit bsigroup.com/committeemember

Buy the security standards you need today from shop.bsigroup.com/security
BSI’s Security standards

Welcome to our security standards brochure which lists all the important current national and international security standards.

These standards are written by experts and based on best practice. They provide both strategic and practical tools to help organizations minimize their exposure to risk, reduce their insurance premiums, avoid litigation and maintain regulatory compliance.

Please take some time to review the wide range of what’s available. Ultimately security standards will help your organization maintain its reputation and save time, money and potentially lives.

About BSI

BSI is the business standards company that helps organizations all over the world make excellence a habit. For more than a century we have been challenging mediocrity and complacency to help embed excellence into the way people and products work. That means showing businesses how to improve performance, reduce risk and achieve sustainable growth.

As a global leader in helping organizations improve, our clients range from high profile brands to small local companies in 172 countries worldwide.

We are the UK’s National Standards Body (NSB) and were the first national standards body. We represent UK economic and social interests across all European and international standards organizations and in the development of business information solutions for British organizations of all sizes and sectors.
Video Surveillance Systems (VSS), commonly known as CCTV

These standards include the systems that monitor activity in public areas, businesses or commercial buildings for real-time or later review. Some record only video while others include sound. Video surveillance can also be used inside and outside schools and private residences as an extra security measure. Available systems offer varying levels of sophistication within a wide price range.

**Electronic security products**

- Video Surveillance Systems (VSS)
- Access control
- Remote centres
- Installed alarm systems
- Transmission equipment and networks
- Security system components

**BS 8418:2015** Installation and remote monitoring of detector-activated CCTV systems. Code of practice

BS 8418:2015 gives recommendations for the design, installation, commissioning, maintenance, operation and remote monitoring of detector-activated CCTV systems, whether “permanent” or temporary/ portable. It assists in ensuring that the integrity and effectiveness of an installed CCTV system are not compromised.


BS 7958:2015 gives recommendations for the management and operation of CCTV within a controlled environment, where data that might be offered as evidence are received, stored, reviewed or analyzed. It applies to the monitoring and management of public spaces, including automatic number plate recognition (ANPR) and traffic enforcement cameras.

BS 7958:2015 includes “a long awaited update to this important standard for the management and operation of CCTV. Primarily for the public space environment, it equally applies to private schemes where the public have a perceived right of way. This latest update takes account of the work of the Surveillance Camera Code of practice and its 12 guiding principles.”

Dave Wilkinson, Director of Technical Services at BSIA

**BS EN 62676-3:2015** Video surveillance systems for use in security applications. Analog and digital video interfaces

BS EN 62676-3:2015 specifies physical, electrical and software interface (non-IP) specifications of analog and digital video interface in video surveillance systems (so far called CCTV) applications.

**BS EN 62676-4:2015** Video surveillance systems for use in security applications. Application guidelines

BS EN 62676-4:2015 gives recommendations and requirements for the selection, planning, installation, commissioning, maintaining and testing of video surveillance systems (VSS) comprising of image capture devices, interconnections, and image handling devices, for use in security applications.

**BS EN 62676-1-1:2014** Video surveillance systems for use in security applications. System requirements. General

BS EN 62676-1-1:2014 specifies the minimum requirements and gives recommendations for video surveillance systems (VSS) installed for security applications. It specifies the minimum performance requirements and functional requirements to be agreed on between customer, law enforcement where applicable and supplier in the operational requirement.

**BS EN 62676-1-2:2014** Video surveillance systems for use in security applications. System requirements. Performance requirements for video transmission

BS EN 62676-1-2:2014 introduces general requirements on video transmission. It covers the general requirements for video transmissions on performance, security and conformance to basic IP connectivity, based on available, well-known, international standards.

**BS EN 62676-2-1:2014** Video surveillance systems for use in security applications. Video transmission protocols. General requirements

BS EN 62676-2-1:2014 introduces an IP network interface for devices in surveillance applications. It specifies a network protocol for the full interoperability of video devices. On top of the basic layers, protocols are defined to accomplish the full interoperability of video devices.

**BS EN 62676-2-2:2014** Video surveillance systems for use in security applications. Video transmission protocols. IP interoperability implementation based on HTTP and REST services

BS EN 62676-2-2:2014 specifies a compliant IP video protocol based on HTTP and REST services. It leverages the features of HTTP and REST for IP video transmission.

**BS EN 62676-2-3:2014** Video surveillance systems for use in security applications. Video transmission protocols. IP interoperability implementation based on Web services

BS EN 62676-2-3:2014 defines procedures for communication between network video clients and video transmitter devices based on Web Services. This new set of specifications makes it possible to build network video systems with devices and receivers from different manufacturers using common and well defined interfaces.

**BS EN 62676-3-2:2014** Video surveillance systems for use in security applications. Video transmission protocols. IP interoperability implementation based on Web services

BS EN 62676-3-2:2014 defines procedures for communication between network video clients and video transmitter devices based on Web Services. This new set of specifications makes it possible to build network video systems with devices and receivers from different manufacturers using common and well defined interfaces.
Access control
These standards comprise the selective restriction of access to a place, property, building or room by authorized persons. Access control may be enforced either by personnel or a device.

**BS EN 60839-11-31:2016** Alarm and electronic security systems. Electronic access control systems. IP interoperability implementation based on Web services. Core specification

**BS EN 60839-11-32:2016** Alarm and electronic security systems. Electronic access control systems. IP interoperability implementation based on Web services. Access control specification

**BS EN 60839-11-33:2016** defines the Web Services interface for electronic access control systems. This includes discovering components and their logical composition and controlling them. It also defines the Web Services interface for interaction with physical doors. This includes but is not limited to controlling the physical doors and monitoring their state.

**BS EN 60839-11-2:2015** Alarm and electronic security systems. Electronic access control systems. Application guidelines

**BS EN 60839-11-2:2015** defines the minimum requirements and guidance for the planning, installation, commissioning, maintenance and documentation for the application of EACS installed in and around buildings and areas.

Remote centres
Remote centres, known as Alarm Receiving Centres (ARCs), provide reassurance that intruder and fire alarms are monitored 24 hours a day, 365 days a year. Any activation signal goes to a monitoring centre to be filtered for false activations that are neither crime related nor caused by genuine intrusions or fire.

**BS 8501:2014** Remote centres receiving signals from alarm systems. Code of practice

**BS 8501:2014** gives recommendations for the planning, construction and facilities of remote and unmanned service centers and for the operation of alarm receiving centres (ARCs) receiving signals from alarm systems, e.g. fire, social, closed circuit television (CCTV), lone worker and vehicle tracking.

**BS 9263:2016** Intruder and hold-up alarm systems. Commissioning, maintenance and remote support. Code of practice

**BS 9263:2016** gives recommendations for the commissioning, on-site corrective and preventative maintenance, remote system checks and remote support of any intrusion and hold-up alarm system (I&HAS).

**BS 50131-9:2014** Alarm systems. Intrusion and hold-up systems. Methods and principles

**PD CLC/TS 50131-9:2014** is available for use where alarm verification methods are considered necessary. It provides recommendations for the addition and use of alarm verification technology in intrusion and hold-up alarm systems (I&HAS) installed to comply with EN 50131.

**BS 50131-10:2014** Alarm systems. Intrusion and hold-up systems. Application specific requirements for Supervised Premises

**BS 50131-10:2014** specifies requirements for SPT used in intrusion and hold-up alarm systems (I&HAS) to transmit alarm and other messages to a location remote from the supervised premises.

Installed alarm systems
These standards refer to complete installed alarm systems rather than their component parts.

**BS 60839-11-31:2016** Alarm and electronic security systems. Electronic access control systems. IP interoperability implementation based on Web services. Core specification

**BS 60839-11-32:2016** Alarm and electronic security systems. Electronic access control systems. IP interoperability implementation based on Web services. Access control specification

**BS 60839-11-33:2016** defines the Web Services interface for electronic access control systems. This includes discovering components and their logical composition and controlling them. It also defines the Web Services interface for interaction with physical doors. This includes but is not limited to controlling the physical doors and monitoring their state.

**BS EN 60839-11-2:2015** Alarm and electronic security systems. Electronic access control systems. Application guidelines

**BS EN 60839-11-2:2015** defines the minimum requirements and guidance for the planning, installation, commissioning, maintenance and documentation for the application of EACS installed in and around buildings and areas.

**BS EN 60839-11-1:2016** Alarm and electronic security systems. Electronic access control systems. System and components requirements

**BS EN 60839-11-1:2013** specifies the minimum functionality, performance requirements and test methods for electronic access control systems and components used for physical access control and in and around buildings and protected areas. It does not include requirements for access point actuators and sensors.

**BS EN 60839-11-1:2016** Alarm and electronic security systems. Electronic access control systems. Electronic access control systems. Application guidelines

**BS EN 60839-11-2:2015** defines the minimum requirements for setting and unsetting of Intruder Alarm Systems (IAS).

**PD CLC/TS 50131-12:2016** provides recommendations for those methods of setting and unsetting an Intrusion Alarm System (IAS) complying with EN 50131-3. This will reduce unwanted alarm arising from “operator error” in setting and unsetting the IAS and provide confidence that the conditions in which the system is installed are conducive to system reliability during the ‘set’ period.

**BS 8501:2014** was produced as a means to “bridge” the gap left by the publication of EN 50518 and the required withdrawal of BS 5979. The standard allows monitoring applications (other than intruder alarms) to follow current UK expectations, previously covered in BS 5979, but references EN 50518 for intruder alarms to ensure the integrity of the monitoring is aligned to the higher expectations of the European standard.”

Dave Wilkinson, Director of Technical Services at BSIA
Transmission equipment and networks
These standards specify requirements for transmission equipment, otherwise known as ‘notification’ or ‘signalling’ equipment.

BS EN 50136-2:2013 Alarm systems. Alarm transmission systems and equipment. Requirements for Supervised Premises Transceiver (SPT)
BS EN 50136-2:2013 specifies the general equipment requirements for the performance, reliability, resilience, security and safety characteristics of supervised premises transceivers (SPT) installed in supervised premises and used in alarm transmission systems (ATS).

BS EN 50136-3:2013 Alarm systems. Alarm transmission systems and equipment. Requirements for Receiving Centre Transceiver (RCT)
BS EN 50136-3:2013 specifies the minimum equipment requirements for the performance, reliability, resilience, security and safety characteristics of the receiving centre transceiver (RCT) installed in ARC and used in alarm transmission systems.

PD CLC/TS 50136-9:2013 Alarm systems. Alarm transmission systems and equipment. Requirements for common protocol for alarm transmission using the internet protocol
PD CLC/TS 50136-9:2013 specifies a protocol for point-to-point transmission of alarms and faults, as well as communications monitoring, between a Supervised Premises Transceiver and a Receiving Centre Transceiver using the Internet protocol (IP).

Security systems components
These standards refer to the component parts of alarms systems rather than complete installed alarm systems themselves.

BS EN 50131-5-3:2016 Intrusion and hold-up systems. Requirements for interconnections equipment using radio frequency techniques
BS EN 50131-5-3:2016 applies to intrusion alarm equipment using radio frequency (RF) links and located on protected premises. It doesn’t cover long-range radio transmissions. BS EN 50131-5-3:2016 defines the terms used in the field of intrusion alarm equipment using radio frequency links as well as the requirements relevant to the equipment.

PD CLC/TS 50131-2-9:2016 Intrusion and hold-up systems. Intrusion detectors. Active infrared beam detectors
PD CLC/TS 50131-2-9:2016 specifies four security Grades 1 to 4 (in accordance with EN 50131-1) and uses environmental Classes I to IV (in accordance with EN 50130-5). It’s applicable to Active Infrared Beam Detectors (AIBDs) installed inside buildings and used as part of intrusion alarm systems.

BS 4737:3.30:2015 Intruder alarm systems in buildings. Specifications for components. Specification for insulated and sheathed cables for interconnecting wiring
BS 4737:3.30:2015 gives requirements for the construction and performance of insulated and sheathed cables for interconnecting wiring used in alarm systems. It’s applicable to cables intended for use with voltages up to 50 V a.c. or d.c.

Security management systems
These standards give guidance on how organizations can implement systems that holistically manage security requirements across the whole organization. They can also help organizations identify opportunities and gain competitive advantage.

BS 16000:2015 Security management. Strategic and operational guidelines
BS 16000:2015 gives guidance on security management for any organization, whether large or small, public or private, to support its viability, productivity, reputation, sustainability and, ultimately, success. It clarifies the basic principles of security management and demonstrates how security can be embedded in an organization.

BS EN 16747:2015 Maritime and port security services
BS EN 16747:2015 is a service standard that specifies requirements for quality in organization, processes, staff and management of a security services provider and/or its independent branches and establishments under commercial law and trade as a provider with regard to port and maritime security services. It applies according to the laws and the regulations applicable in the territory of every national CEN member adopting the standard.

BS ISO 18788:2015 Management system for private security operations. Requirements with guidance for use
BS ISO 18788:2015 provides a framework for establishing, implementing, operating, monitoring, reviewing, maintaining and improving the management of security operations. It provides the principles and requirements for a security operations management system (SOMS).

BS 16000:2015 ensures that “an organization, whether in the private or public sector, is as protected as it can be relies on the identification of potential risks and threats to its personnel, physical and intellectual property, and other assets. Taking a holistic approach to this issue has certainly become easier since the publication of BS 16000.

BS 16000 brings together the essential aspects of security management in simple, jargon-free language, and it includes the fundamental security management principles on which organisations can gain a better understanding of good security practice. Quite simply, anyone running an organisation will get something out of the information contained within it.”

Mike Bluestone MA CSyP FSpyl, Director at Corps Consult, Vice President at The Security Institute
Vacant property protection services

The provision of investigative services

Keyholding

Lone worker services

The use of general purpose security dogs

The use of detection dogs

Contracted security consultancy

Security guarding services

Security services

The need for BS 8484 to help guide and advise employers of lone workers is more important now than ever. Its review throughout 2015/16 will lead to numerous useful improvements, taking input from industry, the Police, audit bodies and others. BS 8484 is one of the principle reasons why false alarm management in the lone worker industry is well managed and the speed of escalation to Police via URN so quick (when compared to 999). It’s a valuable resource for any employer seeking to remove the risks associated with operating with lone working staff.”

Craig Swallow, Chairman BSIA Lone Worker Section & Managing Director of SoloProtect Limited

“The BS 7984 series “was split into 2 parts with the development of Lone Worker monitoring services (BS 8484: Part 1) covering general recommendations for keyholding and response services and Part 2 specifically for Lone worker response services. Both standards have been developed to provide better harmony with other related security management standards such as BS 7499 and to reflect current practice in this important security sector.”

Dave Wilkinson, Director of Technical Services at BSIA

Steve Hill, Director at NASDU

Eur Ing. Jon Laws, Managing Director and Consultant at The Lyndhurst Consultancy


BS 8549:2016 gives recommendations on management, resourcing and operation for the provision of contracted security consultancy services. It also assists procurers wishing to contract such services to ensure the service fits the end user requirements and risk profile.”

BS 8549 is the essential guidance for security consultancy and their clients to ensure the highest standards possible.”

BS 8584:2015 Vacant property protection services. Code of practice

BS 8584:2015 is for security measures and services introduced when a property is at increased risk of criminal attack because it is vacant. A typical vacant property is a building that has been occupied but is temporarily not in use prior to a new owner or tenant moving in.

BS 102000:2013 Code of practice for the provision of investigative services

BS 102000:2013 gives recommendations for the conduct, management, staffing and operational accountability for the provision of investigative services.

BS 7499:2013 Static site guarding and mobile patrol service. Code of practice

BS 7499:2013 gives recommendations for the management, staffing and operation of an organization providing security guarding services on a static site and/or mobile patrol basis. It isn’t applicable to all security services, for example cash-in-transit services, secure parcel services, keyholding and response services, door supervisors, close protection services, event stewarding and the management and operation of closed-circuit television (CCTV).


BS 8517:1:2016 gives recommendations for the operational use of a dog by a security dog handler when providing passive and proactive detection services e.g. drugs, firearms, munitions, explosives, pyrotechnics, intentionally concealed persons, including records, kennelling/husbandry, dog health and welfare, equipment and clothing, training and operational requirements.


BS 8517:2:2016 gives recommendations for the operational use of a detection dog by a detection dog handler when providing passive and proactive detection services. It recognizes two broad categories of risk that affect LWs: environmental risk and people risk.

The BS 8517 series “enable[s] both suppliers and procurers of either Security Dog or Detection Dog Services, to be aware of the skills knowledge and understanding required to ensure the provision of a professional level of services, as well as ensuring the efficiency, safety and control of Dogs and Handlers.”

Steve Hill, Director at NASDU