

Guide for security of buildings against crime —

Part 3: Storage, industrial and distribution premises

ICS 13.310

Confirmed December 2011

Committees responsible for this British Standard

The preparation of this British Standard was entrusted by Committee B/209, General building codes, to Subcommittee B/209/10, Security of buildings, upon which the following bodies were represented:

- Association of Builders' Hardware Manufacturers
- Association of Building Engineers
- Association of Burglary Insurance Surveyors
- Association of Chief Police Officers
- BRE — Building Research Establishment
- BRE/LPC Laboratories
- British Security Industry Association
- British Woodworking Federation
- Chief and Assistant Chief Fire Officers' Association
- Consumer Policy Committee of BSI
- Council for Aluminium in Building
- Door and Shutter Manufacturers' Association
- Flat Glass Manufacturers' Association
- Glass and Glazing Federation
- Guild of Architectural Ironmongers
- Home Office
- IPSA — International Professional Security Association
- Master Locksmiths' Association
- ODPM — Office of the Deputy Prime Minister
- Royal Institute of British Architects
- Co-opted member

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 19 March 2004

© BSI 03-2004

First edition May 1990
Second edition March 2004

The following BSI references relate to the work on this British Standard:

Committee reference B/209/10
Draft for comment 95/102865

ISBN 0 580 43509 1

Amendments issued since publication

Amd. No.	Date of issue	Comments

Contents

	Page
Committees responsible	Inside front cover
Foreword	ii
Introduction	1
1 Scope	1
2 Normative references	1
3 Terms and definitions	2
4 Planning and design	3
5 Risk management	4
6 Access and control	7
7 Approach and site access	8
8 Security lighting	10
9 External doors	13
10 Security hardware for external and internal personnel doors	19
11 Windows and rooflights	22
12 Roofs and walls	24
13 Internal zones of the building	25
14 CCTV surveillance systems	26
15 Intruder sensors and alarms	27
Annex A (informative) Typical uses for locks and other security hardware	29
Annex B (informative) Intruder detection equipment	30
Bibliography	33
Table 1 — Type and use of luminaires	12
Table 2 — Locking and securing internally installed sliding doors	14
Table 3 — Locking and securing sliding-folding shutter doors	15
Table A.1 — Typical uses of locks and security hardware	29
Table B.1 — Location and type of sensor	32

Foreword

This British Standard has been prepared by Subcommittee B/209/10. It supersedes BS 8220-3:1990 which is withdrawn.

This revision updates the document to reflect current technology. It is also intended to be more user-friendly for the reader. It is hoped that this British Standard will form the basis of any future European Standard that may be drafted.

The other parts of BS 8220 are concerned with the security of the following types of building:

- *Part 1: Dwellings;*
- *Part 2: Offices and shops.*

This standard should not be regarded as a substitute for expert advice; the intention is that it should complement it. Crime prevention should be considered at all stages of the design life of the built environment.

This publication does not purport to include all necessary provisions of a contract. Users are responsible for its correct application.

Compliance with a British Standard does not of itself confer immunity from legal obligations.

Attention is drawn to the following statutory regulations: Occupiers Liability Act 1984 [1], Highways Act 1984, Section 164 [2], Health and Safety Regulations [3], Means of escape requirements in Building Regulations [4], [5], [6].

Summary of pages

This document comprises a front cover, an inside front cover, pages i and ii, pages 1 to 33 and a back cover.

The BSI copyright notice displayed throughout this document indicates when the document was last issued.

Introduction

The cause of crime is a subject which has been well researched. Many factors exist which can influence whether or not an offence is committed. Certain factors, for example, socio-economic conditions are beyond the remit of this standard. Other factors such as neighbourhood layout and building design are covered along with more specific factors such as security management, personal safety, and physical and electronic security.

Most property related crimes are committed because offenders have been given easy opportunities. Easy access to an industrial park or to a single storage premises, concealed areas, no demarcation between public and private space, and poor lighting or landscaping are all features of design which assist the criminal. Careful planning and design can remove these easy opportunities.

The design of the built environment can also influence an individual's perception of the fear of crime. Whilst the perception of crime is very often in excess of the reality, it is important that it is recognized and considered when designing the environment. Fear generators include narrow, dark alleyways; footpaths that are unsupervised and have little natural or formal surveillance; and industrial complexes in which entrances are hidden from view or approached by access roads that feel uncomfortable or have poor lighting. In such cases, factors such as sight lines and vehicle and pedestrian circulation should be considered. Movement generators, for example bus stops, may be positioned within complexes to assist circulation and access.

By understanding the motivation of the offender and balancing this against design features that relate to control of space, sight lines and use of symbolic barriers, combined with specific physical security measures, this British Standard aims to assist designers, planners, owners or managers and crime prevention practitioners in protecting premises from criminal attack. The more vulnerable and at risk offenders feel, the less inclined they are to commit a crime.

1 Scope

This British Standard provides guidance and a recommended strategy for combating burglary, theft, arson and other crimes committed against storage, industrial and distribution premises. It applies to both new and existing property in all localities.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

BS 1186-2, *Timber for and workmanship in joinery — Part 2: Specification for workmanship*.

BS 1245, *Specification for metal door frames (steel)*.

BS 1722-10, *Fences — Part 10: Specification for anti-intruder fences in chain link and welded mesh*.

BS 1722-12, *Fences — Part 12: Specification for steel palisade fences*.

BS 1722-14, *Fences — Part 14: Specification for open mesh steel panel fences*.

BS 3621, *Specification for thief-resistant locks*.

BS 4737-4 (all parts), *Intruder alarm systems — Codes of practice*.

BS 4787-1, *Internal and external wood doorsets, door leaves and frames — Part 1: Specification for dimensional requirements*.

BS 4873, *Specification for aluminium alloy windows*.

BS 5357, *Code of practice for installation of security glazing*.

BS 5544, *Specification for anti-bandit glazing (glazing resistant to manual attack)*.

BS 5589, *Code of practice for preservation of timber*.

BS 6100 (all parts), *Glossary of building and civil engineering terms*.

BS 6262, *Code of practice for glazing for buildings*.

BS 6510, *Specification for steel windows, sills, window boards and doors*.

BS 7412, *Plastics windows made from unplasticized polyvinyl chloride (PVC-U) extruded hollow profiles — Specification.*

BS 7499, *Static site guarding and mobile patrol services — Code of practice.*

BS 7858, *Code of practice for security screening of personnel employed in a security environment.*

BS 7992, *Code of practice for exterior deterrent systems.*

BS 8214, *Code of practice for fire door assemblies with non-metallic leaves.*

BS EN 179, *Building hardware — Emergency exit devices operated by a lever handle or push pad.*

BS EN 942, *Timber in joinery — General classification of timber quality.*

BS EN 1011-1, *Welding — Recommendations for welding of metallic materials — Part 1: General guidance for arc welding.*

BS EN 1011-2, *Welding — Recommendations for welding of metallic materials — Part 2: Arc welding of ferritic steels.*

BS EN 1063, *Glass in building — Security glazing — Testing and classification of resistance against bullet attack.*

BS EN 1125, *Building hardware — Panic exit devices operated by a horizontal bar — Requirements and test methods.*

BS EN 1143-1, *Secure storage units — Requirements, classification and methods of test — Part 1: Safes, strongroom doors and strongrooms.*

BS EN 1935:2002, *Building hardware — Single axis hinges — Requirements and test methods.*

BS EN 12051, *Building hardware — Door and window bolts — Requirements and test methods.*

BS EN 12320, *Building hardware — Padlocks and padlock fittings — Requirements and test methods.*

BS EN 13241-1, *Industrial, commercial and garage doors and gates — Product standard — Part 1: Products without fire resistance or smoke control characteristics.*

BS EN 13724, *Postal services — Apertures of private letter boxes and letter plates — Requirements and test methods.*

BS EN 50131-1, *Alarm systems — Intrusion systems — Part 1: General requirements.*

BS EN 50133-1, *Alarm systems — Access control systems for use in security applications — Part 1: System requirements.*

BS ISO/IEC TR 13335-2, *Information technology — Guidelines for the management of IT security — Part 2: Managing and planning IT security.*

DD 243, *Installation and configuration of intruder alarm systems designed to generate confirmed alarm conditions — Code of practice.*

DD 245, *Code of practice for management of false alarms.*

DD ENV 1627, *Windows, doors and shutters — Burglar resistance — Requirements and classification.*

PAS 24-1, *Enhanced security performance requirements for door assemblies — Part 1: Single leaf, external door assemblies to dwellings.*

3 Terms and definitions

For the purposes of this British Standard, the terms and definitions given in BS 6100 and the following apply.

3.1

building terms and definitions

3.1.1

storage premises

building and adjacent areas on premises concerned with the receipt, storage and dispatch of goods, in which access to storage and associated office areas is controlled

3.1.2**industrial site**

area of land within which a group of storage or industrial premises are situated

3.2**protection**

physical barriers, which may be symbolic, in premises that delay or deter someone attempting unauthorized access

3.3**normal working hours**

period during the day when staff are normally at work, starting with the normal arrival in the morning of first staff and ending with the normal departure time of the last staff

NOTE Normal working hours excludes time of evening or night shift, time when staff are working later than normal, weekends and bank holidays.

3.4**zones of physical security****3.4.1****high security zone**

area that is continuously monitored and to which access is limited to authorized personnel

3.4.2**operations zone**

area to which access is limited to authorized employees and to authorized visitors

3.5**final secured exit door**

exit door used by the first to enter or last to leave a premises, lockable from the outside

NOTE The term "final exit" has been avoided in this part of BS 8220, in order to remove the possibility of confusion with its longer established use in relation to means of escape in case of fire where the term is used to describe the terminal point of an escape route to an open space beyond which persons are no longer in danger from fire and can disperse in safety.

4 Planning and design**4.1 General**

Where a building does not have continuous occupancy, guardianship or natural surveillance, it should be designed to withstand attempts at illegal entry.

Security provisions should be considered at the planning and building design stage. The surrounding environs and infrastructure may all have influences that alter the risk assessment and should be considered at this stage.

4.2 Design

Clear and uncluttered design for both the interior and the exterior of the building can assist security surveillance, especially when coupled with good natural and artificial lighting.

When designing storage, industrial or distribution premises, the appointed design team, which should include amongst others the client's representative and a security consultant, should consider factors that can reduce opportunities to commit crime. The site position of storage units, in many instances, adjoins public rights of way either through the site or against the site boundaries. Ownership of such areas should be clearly defined by use of physical barriers which may be symbolic.

4.3 Natural surveillance

A strong preventative factor to crime is the risk of being seen and identified. Straight and unhindered sight lines along the exterior of a building, and low level vegetation landscaping, assist the use of CCTV and aid surveillance by security personnel from adjoining residential properties and passers by. If units on a site are of mixed use this creates extra movement of employees at varying times of the day, whose surveillance will help to discourage persons who are looking for the opportunity to commit crime.

4.4 Safe environment

Fear of crime, whether real or perceived, should be considered in the design and planning of the environment in which premises are to be sited. Design features such as recessing in the fabric of the building envelope or hidden doors should be avoided in order to reduce the fear of crime. Lighting units established around the site help to increase the safety aspect. First impressions gained by criminals often have a great effect on their decision to offend or not. A site that appears well cared for, neat and tidy can give an impression of affluence. It is equally true that it can give the impression that people who work there take a pride in the area and are more likely to be vigilant and protective.

4.5 Collective control

A commercial development in which occupants are encouraged to work together as a community, to take combined action to improve the environment and defend its territory against criminals, is likely to result in less crime and an improvement in the quality of life for the users. Two methods of achieving this are by defining the development to give it a clear identity and by ensuring the maximum possible surveillance from property to property, as criminals do not like to be seen. Wherever possible it is also advisable to try and obtain a mix of use types and occupant within a commercial development. This may give a variation in occupancy patterns that permits more people to be in the property and therefore exercising informal surveillance.

5 Risk management

5.1 General

Any crime prevention strategy is essentially one of risk management. Consequently, before an effective strategy can be developed, the risk factors involved should be identified and understood.

Distribution centres and storage premises are affected by a variety of crimes. Although burglary is the most common crime, arson, criminal damage and internal theft are also prevalent.

Burglary on industrial sites and storage premises occurs mainly when premises are unoccupied, and tends to fall into two categories.

- a) High-risk premises which are likely to be targeted by well organized and determined professional criminals who undertake premeditated attacks, e.g. stealing in bulk, stealing high value goods or stealing equipment, information or data. An example of this category of burglary is the burglary of a tobacco storage premises in order to steal cigarettes.
- b) Lesser value burglaries committed by opportunists who are able to exploit weaknesses in security precautions. Opportunist burglaries occur more frequently than organized burglaries. An example of this type of burglary is a speculative attack on a unit that offers good clues to the offender that security is lax.

5.2 Security plan

5.2.1 General

To formulate a security plan, it is first necessary to complete an in-depth risk assessment to identify the vulnerability of the premises and its contents.

5.2.2 Risk assessment

In the case of a new build project the risk assessment can be used to assist in the design of the building and its surroundings, for example by designing out unnecessary access points and designing in structural strength to vulnerable areas.

When carrying out a risk assessment the following factors should be considered:

- a) type of business;
- b) attractiveness to the criminal in terms of goods, cash and possible confidential information and data;
- c) degree of inherent security of the premises in relation to its construction;
- d) surveillance provided either by normal public activity or security patrols of the premises or its surroundings;
- e) ease of access from streets, open areas, adjacent roofs, floors above and below the premises (if they are occupied by third parties) and from adjoining premises;

- f) potential escape routes and egress for the removal of stolen goods (these may not be the same as the entry route and may vary according to the time of day);
- g) vulnerability relative to local trends in crime;
- h) seasonal attractiveness of goods and seasonal build up of stock;
- i) risk of arson to the premises and contents, and goods and vehicles stored in the surrounding areas;
- j) requirements of the local authority, fire authority and insurance companies;
- k) possibility of violence to staff.

After the risk assessment has been completed a security plan can be formulated.

5.2.3 Drawing up a security plan

The security plan should be the responsibility of a senior member of staff at the site, whose duties include an annual review of the plan. A more frequent review may be required if the use of the premises or the types of goods stored there changes.

When drawing up a security plan it is important that various layers of protection are considered and that no one type of protection is relied upon to the exclusion of all others.

When deciding upon types of protection to be used it is usual practice to work inwards from the perimeter of the site, considering firstly the fencing and restriction of access, then protections to the buildings and finally inner secure areas and items such as safes.

5.2.4 Protection

The types and levels of protection to be used should be determined by the results of the risk assessment which should take into account anticipated trends in the use of the site and seasonal peaks and troughs in business.

The following types of protection, which are listed for guidance but do not comprise an exhaustive list, can all be used to protect storage, industrial and distribution premises:

- a) external:
 - 1) fencing and gates;
 - 2) electrified fencing;
 - 3) lighting.
- b) external and internal:
 - 1) remotely monitored CCTV;
 - 2) static guarding;
 - 3) mobile guard patrols;
 - 4) physical security;
 - 5) locally monitored and recorded CCTV.
- c) internal:
 - 1) intruder alarm systems;
 - 2) security of communications systems and telephone lines;
 - 3) access control (including visitors, delivery drivers, contractors, and third party maintenance staff);
 - 4) hot work permit systems;
 - 5) smoke generating devices;
 - 6) secure areas;
 - 7) security cages;
 - 8) safes;
 - 9) strongrooms.

5.3 Making potential targets less attractive

Risk management actions which can be taken to make potential targets of theft less attractive include making goods heavier and less portable through bulk storage palletization and marking/labelling goods and equipment to make them less easy to re-sell.

5.4 The immediate neighbourhood

When carrying out a risk assessment, it is essential to give high priority to local factors. This may involve carrying out a diagnostic survey of crime in the immediate neighbourhood, to identify the type of crime reported, where and when incidents occurred and who the victims were. This may be achieved by spatial mapping, the distribution of crime within a geographic area, that will easily identify crime clustering or hot spots. It should be remembered that factors that may influence the opportunity for crime might not necessarily be in the immediate locality, for example a convenient desire route that passes through a commercial area may link two features attractive to potential offenders. Although the features may be some distance away from the site in question, they can influence the possibility of crime.

Where the development is on a new site, it may be that there has been no previous crime problem or that no records exist. In these cases it is important to consider the proposed development in terms of potential crime generation, what crime or anti-social behaviour could reasonably be expected to result from this development being completed.

5.5 Security management

5.5.1 Safeguarding data

It is becoming increasingly important to safeguard information and data from theft or corruption. Whilst a company may be able to replace goods that are stolen or damaged, it is often far more damaging to the company to lose data and information which can cover all aspects of the company operation. Special security measures should be taken to reduce the risk of theft of information and criminal interruption of the power supply to the computer in order to maintain the company's effectiveness.

The greatest risks are of thefts of data held in computer systems. Protection should be provided for computers and terminal links.

5.5.2 Theft and burglary

The overall strategy for preventing burglary and theft in storage, industrial and distribution premises should encompass situations when the premises are open for business and when they are closed. Measures to be taken against crime should be analysed with a view to:

- a) dissuading a person from attempting to attack the building;
- b) denying access should an attempt to enter the building be made;
- c) slowing down or delaying the offender carrying out an attack; and
- d) in the event of a successful attack, increasing the chance of detection by providing appropriate signalling devices to alert the law enforcement agencies.

5.5.3 Arson

All storage, industrial and distribution premises are potentially at risk from arson. Properties at the greatest risk are often isolated or unattended premises or those with little or no physical security. The principal aim of the crime prevention strategy should be to prevent the arsonist from gaining access to the site perimeter and, if this fails, to deny access to the building or to the flammable materials. Fire-resistant materials should be considered as should fire compartmentalization in order to restrict the spread of fire. Fire alarms and extinguishing systems should also be utilized to minimize loss and damage.

Attention should then be given to detail on the actual building, for example gaps beneath doors should either be as small as possible or sealed where practicable in order to reduce the risk of arson. Letterboxes, if fitted, should conform to the requirements of BS EN 13724, be fire resisting and preferably be located outside the fabric of the building. For storage, industrial or distribution premises involved with sensitive operations the use of mail-scanning machines should be considered.

Automatic fire detection and extinguishing systems, e.g. sprinklers, with an automatic alarm transmission facility, conforming to relevant British Standards, should be installed to provide early warning of fire.

Hazardous substances such as flammable liquids and gas cylinders should be locked in secure storerooms, particularly outside of working hours. Unprotected flammable goods, pallets and combustible waste should be stored away from buildings to minimize the risk of an external fire spreading into the building.

6 Access and control

6.1 General

Access and egress of staff and visitors to the storage, industrial or distribution premises should be supervised, either directly by staff or operational management, or remotely by CCTV. In high-risk situations, access doors to both storage and office areas should be supervised.

Staff should be provided with photograph identity cards giving their name and position. Visitors should be given visitor cards which should be tagged on to clothing at all times while they are on the premises, and handed in on leaving.

Staff should challenge anyone on the premises not wearing an identity card or visitor's pass, and should report unauthorized persons to the security office.

6.2 Staff control

Access control systems should conform to BS EN 50133-1. Entry and exit doors for staff should be secured in such a way as to prevent unauthorized access, e.g. the entry and exit of staff should be supervised by an attendant at the door, or monitored by use of CCTV or an access control system. In large storage premises, security can be improved by issuing staff with identity or access control cards. However, electronic access systems alone do not normally provide an acceptable level of security outside normal working hours.

6.3 Visitor control

6.3.1 General

Where possible, storage, industrial and distribution premises should be designed and orientated so as to channel visitors to the site through an office reception area or gate house (see Clause 7).

6.3.2 Access via reception area

Doors for admission of visitors should either be:

- a) supervised by a receptionist and/or security staff;
- b) under continuous supervision by staff, either directly or by the use of CCTV;
- c) kept locked, with admission requested by operating a call button or other suitable device, for example, an entry phone system.

Where appropriate, doors should be fitted with door viewers or other security devices so that callers can be inspected before admittance and unauthorized persons prevented from gaining access. Visitors should not be admitted until their identity has been established.

6.3.3 Vehicle access

Admission of vehicles into high-risk delivery areas should be through controlled doors or gates, the control being exercised by an attendant or security devices. Visiting vehicle users should not be admitted until their identity has been established. Doors should be self-closing and self-locking on release.

Passenger and goods vehicles should use different approach roads within the site perimeter, if possible.

Parking areas for passenger and goods vehicles should be separate, if possible, and separated by fencing.

Industrial and commercial doors and gates should conform to the requirements of BS EN 13241-1.

6.4 Reception zone

Office reception areas should be designed so as to give a welcoming impression to legitimate visitors. However, they should be formal enough to deter an opportunist criminal. Similarly the interior of the reception zone should be laid out to give staff maximum chance of surveillance.

Visitors should enter premises through a door leading directly to an office area (rather than a storage area). Visitors should be escorted by a member of staff at all times.

Theft of personal property belonging to staff or visitors is more likely to occur when facilities are not provided for keeping property secure. In particular the location of storerooms, delivery areas, yards and parking areas should be carefully considered in the design and planning stages of the building.

6.5 Goods vehicle drivers

The following procedures should be used for the control and supervision of goods vehicle drivers:

- a) keeping loading shutters locked until drivers are checked and identified;
- b) requiring drivers to report to a checking point separated from the storage area by a locked door;
- c) providing toilet, telephone and snack facilities for drivers from other organizations outside the storage and main office areas;
- d) providing continuous supervision of loading and unloading operations, if undertaken by drivers from other organizations;
- e) monitoring drivers by CCTV.

7 Approach and site access

7.1 General

Storage, industrial or distribution premises should be provided with clear directional signing, open and uncluttered approaches, unobscured sight lines and appropriate lighting. This applies equally to service roads, delivery areas and car parks. Transport facilities on or near the site should also be considered, for example, the siting of bus stops if on or near the site should be in safe areas with clear surveillance.

Service roads and footpaths to the side and rear of the site should be avoided, if possible. Ideally a number of storage, industrial or distribution premises should be sited together with one secure property backing on to another.

Perimeter barriers should, where possible, permit natural surveillance of the premises.

7.2 Perimeter barriers

7.2.1 Types of fencing

Perimeter fencing should be installed, where appropriate, to provide enhanced protection of the peripheral space around the site or building. It should be a minimum height of 2.4 m. High security and maximum security fences should be a minimum of 3.0 m high. Perimeter fencing may be one of the following types depending on the risk assessment.

- **Chain link and welded mesh fencing:** Anti-intruder chain link or welded mesh fences, with a small mesh size to prevent finger holds, should conform to the requirements of BS 1722-10.
- **Open mesh steel panel fencing:** Open mesh (expanded metal) fences, with a minimum height of 2.4 m, should conform to the requirements of BS 1722-14.
- **Steel palisade fencing:** Steel palisade fences of vertical steel rods, with the top end flattened, split and splayed into sharpened points to deter climbing, should conform to the requirements of BS 1722-12.

7.2.2 Toppings to fences

Where it is proposed to use barbed wire, razor tape or rotating vanes as aids to security of the perimeter fence, attention is drawn to the Occupiers Liability Act 1984 [1] and Section 164 of the Highways Act 1980 [2].

7.2.3 Gates in fences

The provision of gates in perimeter fences, other than those essential for access and egress, should be avoided. In the event that a gate is provided it should be of the same height, material and strength as the adjoining fencing, with no gaps underneath the gate in accordance with BS 1722-14.

Hinges on gates should be designed to prevent the gate from being lifted free. They should also be shielded from use as steps to scale the fencing.

Gates should be secured by a lock conforming to BS 3621 protected by lock protection plates welded to the gate and the frame or by a padlock and padlock fittings conforming to BS EN 12320, grade 5 or 6.