

Secured by Design



Official Police Security Initiative



# COMMERCIAL DEVELOPMENTS 2015

VERSION 2



## Introduction

Secured by Design (SBD) is a crime prevention initiative operated by the Police Services of the United Kingdom. *Secured by Design Commercial 2015* is one of several guidance documents that aim to reduce crime in the built environment. Secured by Design continually evaluate the effectiveness of all guidance and periodically amends the various guides in response to research findings and changing standards. This new guidance for commercial developments incorporates numerous new and improved security standards that have been developed to address emerging criminal methods of attack.

A sensible and practical level of security, which will not adversely affect the efficiency of a business, is essential for a successful and profitable business. The majority of criminal incidents in commercial development relate to property crime. This is because the modern business contains a vast array of portable and desirable goods with a ready market, such as plant and machinery and raw materials, personal computers, laptops, and other valuable electronic equipment. Other crimes that regularly occur include acts of vandalism, such as graffiti and arson and occasional assaults on members of staff.

The Police Service places great importance upon the need to build sustainable developments. This not only includes the need to use environmentally friendly products, materials and construction methods, but also the need to raise awareness of the fact that

crime prevention is a positive sustainability issue. Academic research conducted on behalf of SBD has confirmed that crime committed in the UK is responsible for the release of at least 6,000,000 tonnes of CO<sup>2</sup> into the atmosphere each year. It therefore follows that the achievement of an SBD certificate for commercial premises not only indicates that the designer has made a significant effort to create a secure working environment, but has also vastly reduced the carbon footprint of the development. To that end applicants are also encouraged to build to the Building Research Establishment's environmental and sustainability standard BES 5052: Issue 4.1. The standard's requirements can be found in the BREEAM UK New Construction: Non-domestic Buildings Technical Manual: SD5076: 2.1 2014

It is also important that the benefits of a new secure commercial building are complemented with a clear management & maintenance programme and a business continuity and resilience plan to ensure a safe and secure working environment. Further information about risk management in both new and existing commercial buildings can be obtained from the SBD partner initiative 'Secured Environments' at [www.securedenvironments.com](http://www.securedenvironments.com).

# Contents

	Page		Page
<b>Introduction</b>	<a href="#">2</a>	<b>19 Signage and unit identification</b>	<a href="#">17</a>
<b>How to use this document</b>	<a href="#">5</a>	20 Vehicle Parking and Access	<a href="#">18</a>
<b>Scope of SBD Commercial</b>	<a href="#">5</a>	<i>Two-wheeled motor vehicle parking</i>	<a href="#">19</a>
<b>Applying for the SBD Commercial Award</b>	<a href="#">5</a>	<i>Bicycle parking</i>	<a href="#">19</a>
<b>Policy and strategic guidance in support of Secured by Design</b>	<a href="#">6</a>	<b>External security issues</b>	<a href="#">19</a>
<b>Design &amp; Access Statements</b>	<a href="#">6</a>	21 Landscaping	<a href="#">19</a>
		22 External furniture and litterbins	<a href="#">20</a>
		23 Natural surveillance and recessed doorways	<a href="#">20</a>
		24 Temporary buildings	<a href="#">21</a>
		25 Wind turbines and photovoltaic installations	<a href="#">21</a>
		<b>Storage facilities</b>	<a href="#">22</a>
		26 Equipment storage	<a href="#">22</a>
		27 External waste storage	<a href="#">22</a>
		28 Fuel storage	<a href="#">22</a>
		29 Cleaning equipment storage	<a href="#">22</a>
		<b>Utility services and mail delivery</b>	<a href="#">22</a>
		30 Telecommunications access covers, ducting and utility meters	<a href="#">22</a>
		31 Mail delivery arrangements	<a href="#">23</a>
		<b>Building shell</b>	<a href="#">23</a>
		32 Windowless building elevations	<a href="#">23</a>
		33 Automatic opening window systems and vents	<a href="#">24</a>
		34 Walls – facades, apertures and graffiti	<a href="#">24</a>
		35 Roof design and access and aids to climbing	<a href="#">25</a>
		<b>Internal layout issues</b>	<a href="#">25</a>
		36 Entrances into the building	<a href="#">25</a>
		37 Reception area and visitor control	<a href="#">26</a>
		38 Internal doorsets	<a href="#">27</a>
<b>SECTION 1: The Development – Layout and Design (planning and external issues)</b>	<a href="#">7</a>		
1 Creating a sense of place	<a href="#">8</a>		
2 Relevant planning policy and requirements	<a href="#">8</a>		
3 Phased or speculative developments	<a href="#">8</a>		
4 Location and adjoining land use	<a href="#">9</a>		
5 Configuration of buildings	<a href="#">9</a>		
6 Outdoor amenity spaces	<a href="#">9</a>		
<b>Roads and footpaths</b>	<a href="#">9</a>		
7 Vehicular and pedestrian routes	<a href="#">9</a>		
8 Through-roads and cul-de-sacs	<a href="#">10</a>		
9 Footpath design	<a href="#">11</a>		
10 Planting next to footpaths	<a href="#">11</a>		
11 Lighting of segregated footpaths	<a href="#">12</a>		
12 Phased developments and footpaths	<a href="#">14</a>		
<b>Perimeter security and site access</b>	<a href="#">14</a>		
13 Enclosed commercial developments	<a href="#">14</a>		
14 Open commercial developments	<a href="#">14</a>		
15 Boundary types	<a href="#">15</a>		
16 Security fencing	<a href="#">16</a>		
17 Gates	<a href="#">17</a>		
18 Defensive hedging	<a href="#">17</a>		

	<b>Page</b>		<b>Page</b>
<b>Security lighting</b>	<a href="#"><u>28</u></a>	55 Roof lights and sun tubes	<a href="#"><u>42</u></a>
39 External Lighting	<a href="#"><u>28</u></a>	<i>Roof lights</i>	<a href="#"><u>42</u></a>
<b>40 Internal lighting</b>	<a href="#"><u>28</u></a>	<i>Sun tubes</i>	<a href="#"><u>43</u></a>
<b>SECTION 2:</b>			
<b>PHYSICAL SECURITY SPECIFICATIONS</b>			
<b>Introduction</b>	<a href="#"><u>31</u></a>	56 External doorset apertures	<a href="#"><u>43</u></a>
41 Levels of security standards	<a href="#"><u>31</u></a>	<i>Avoiding door recesses</i>	<a href="#"><u>44</u></a>
42 Unknown occupiers and risk	<a href="#"><u>31</u></a>	57 Locking systems for doorsets and gates	<a href="#"><u>44</u></a>
<b>Perimeter and external areas</b>	<a href="#"><u>31</u></a>	58 Glazing within doorsets and secure vision panels	<a href="#"><u>45</u></a>
43 Fencing	<a href="#"><u>31</u></a>	<i>Secure vision panels</i>	<a href="#"><u>46</u></a>
<i>Specification for timber or steel security fencing for normal crime risks</i>	<a href="#"><u>32</u></a>	59 Door installation	<a href="#"><u>46</u></a>
<i>Standard for security fencing for higher security risks</i>	<a href="#"><u>33</u></a>	60 Security glazing	<a href="#"><u>46</u></a>
44 Gates	<a href="#"><u>33</u></a>	61 Electronic access control systems	<a href="#"><u>46</u></a>
45 Security bollards (including those intended for Hostile Vehicle Mitigation)	<a href="#"><u>34</u></a>	<i>Electronic access control standards</i>	<a href="#"><u>47</u></a>
46 Vehicle Parking	<a href="#"><u>35</u></a>	<i>Electronic access control and security staff</i>	<a href="#"><u>47</u></a>
<i>Underground car parking</i>	<a href="#"><u>35</u></a>	62 Protection of window apertures	<a href="#"><u>47</u></a>
<i>Bicycles</i>	<a href="#"><u>36</u></a>	<i>Secondary glazing</i>	<a href="#"><u>49</u></a>
<i>Two-wheeled motor vehicle parking</i>	<a href="#"><u>37</u></a>	63 Mail delivery	<a href="#"><u>49</u></a>
47 Telecommunications and utility access covers	<a href="#"><u>37</u></a>	<b>Internal security considerations</b>	<a href="#"><u>49</u></a>
48 External lighting standard requirements	<a href="#"><u>37</u></a>	64 Intruder alarms systems	<a href="#"><u>49</u></a>
49 Closed circuit television (CCTV)	<a href="#"><u>38</u></a>	65 Public address systems	<a href="#"><u>49</u></a>
<b>Building shell security</b>	<a href="#"><u>40</u></a>	66 Physical security standards for computers and server rooms	<a href="#"><u>49</u></a>
50 Wall construction	<a href="#"><u>40</u></a>	67 Secure Internal doorsets	<a href="#"><u>50</u></a>
51 Glazed curtain walling and window walls	<a href="#"><u>40</u></a>	68 Safes and strong rooms	<a href="#"><u>50</u></a>
52 Roller shutters and grilles	<a href="#"><u>41</u></a>	<b>Other security considerations</b>	<a href="#"><u>51</u></a>
53 Roller shutter doors providing vehicular access	<a href="#"><u>41</u></a>	69 Security staff manned guarding and guard houses	<a href="#"><u>51</u></a>
54 Roof construction	<a href="#"><u>41</u></a>	70 Arson and fire protection	<a href="#"><u>51</u></a>
		80 ARGUS professional	<a href="#"><u>52</u></a>
		90 Buildings with undercrofts	<a href="#"><u>52</u></a>
		<b>GLOSSARY OF TERMS</b>	<a href="#"><u>55</u></a>
		<b>REFERENCES</b>	<a href="#"><u>58</u></a>

## How to use this document

SBD Commercial differs somewhat from other SBD documents in that it does not provide the reader with a menu of requirements in order to gain SBD approval. Since the scope of the document covers all types of commercial premises from a small storage unit to multi use business parks or leisure centres, and, since the risks associated with commercial premises vary considerably from a corner shop containing low value goods to an iconic business hub that may attract the unwarranted attentions of international terrorists, there is no 'one size fits all' solution.

However we have endeavoured to produce as much information as possible in order that an initial assessment of the building or proposed new development can be made prior to contacting the police Crime Prevention Design Advisor (CPDA). The following paragraphs both set the political theme by providing a broad understanding of the planning requirements intended to reduce crime and provide guidance within the 'Scope' and 'Applying for a Secured by Design Commercial Award' paragraphs. Further detailed advice is contained within the following two sections:

- Section 1: Deals with the development layout and design and all external features
- Section 2: Provides the detailed technical standards for various elements of the building

**It cannot be stressed enough that if full SBD Accreditation of the development is required then the CPDA must be contacted at the earliest possible opportunity, preferably at concept stage and definitely before submission to planning for a new development or prior to commencing work on the refurbishment of an existing building or development.**

## Scope of SBD Commercial

This document encapsulates both commercial developments where the public have no formal access e.g. factory or office buildings, and those where public access is integral to the commercial use such as retail premises, leisure centres and public buildings. Such developments may range in size from a single building with a defined use to a group of buildings with multiple uses.

This document provides design guidance and specification requirements for reducing the risks for crimes against the person and property. Typically this will include burglary, theft, arson, vehicle crime and assault. Provision has also been made for the prevention of terrorism. The same advice is also intended to reduce the fear of crime and the incidence of anti-social behaviour. Consequently, consideration is given to both environmental design and physical security. This is best achieved through negotiation with the designers of new commercial building development or major refurbishment at pre-planning stage. Where acts of terrorism and or extremist activity are of a concern to the business owner, the developer, or their agent, such concerns should be communicated to the police Crime Prevention Design Adviser dealing with the Secured by Design application, who will in turn notify the relevant security experts. In some circumstances it may be the police service that identifies vulnerable buildings or commercial activities that require detailed counter terrorism advice, this will be communicated to the relevant applicant and the earliest possible opportunity.

Section 1 of this document addresses the development – layout and design issues together with general external environment issues, whilst Section 2 deals with the specific physical crime prevention requirements. Compliance with both sections is required to achieve Secured by Design certification.

SBD operates throughout England, Scotland, Wales, Northern Ireland, The Isle of Man and the Channel Islands.

## Applying for a Secured by Design Commercial Award

In order to stand the best chance of achieving SBD award it is of the utmost importance to consult the relevant Crime Prevention Design Adviser (CPDA) prior to a planning application being made. In some areas the CPDA is entitled Architectural Liaison Officer (ALO), however all subsequent references within this guidance will refer to the process being administered by a CPDA.

Should you wish to apply for SBD Award please complete an application and checklist form,

which can be found at [www.securedbydesign.com](http://www.securedbydesign.com) Send the application to the relevant CPDA whose details can also be found on the website.

## Policy and strategic guidance in support of Secured by Design

Secured by Design reflects the established principles of designing out crime. The application of these principles, the design details and specifications for the particular development, must be agreed between the developer and/or the developer's agent and the police Crime Prevention Design Adviser (CPDA).

Local planning conditions, crime risk assessment and other statutory provisions such as both national and local planning policies that may influence the measures to be adopted, should be addressed. Such as:

- The National Planning Policy Framework (NPPF) and accompanying National Planning Practice Guidance (NPPG) in England.
- For Scotland, PAN 77 Designing Safer Places applies, available at [www.scotland.gov.uk](http://www.scotland.gov.uk)
- In Wales TAN 12 Design applies, available at [www.wales.gov.uk](http://www.wales.gov.uk)
- In Northern Ireland Secured by Design is referenced in the government guidance for new buildings.

The advice given by the CPDA will be dependent upon the outcome of a crime risk analysis and an understanding of local crime occurrence. Consequently, specific measures recommended to address particular types of crime may vary from one site to another. It is important to note that the national SBD guidelines are minimum requirements and in areas of higher risk, greater crime resistance will be required. Therefore it is inevitable that the advice given to design professionals may occasionally vary according to crime risk whilst still maintaining a consistent approach.

## Design & Access Statements

Still a requirement for many development schemes, compliance with the Secured by Design award scheme criteria can be a major indication that a proposal has adequately addressed the crime prevention component

required to be included in Design and Access Statements (DAS).

As 'crime' has a potentially adverse economic, social and environmental impact upon a development, and the National Planning Policy Framework requires that crime and the fear of crime should not undermine quality of life or community cohesion, 'crime' should be afforded due consideration within the DAS. Insufficient or inadequate crime prevention information within the DAS may hinder the application.

Where acts of terrorism or extremist activity are of a concern reference to consultation documents: '*Safer places: a counter-terrorism supplement*', '*Working together to protect crowded places*' and '*RIBA Guidance on Designing for Counter Terrorism*' are recommended. These documents are available from [ww.gov.uk/government/publications](http://ww.gov.uk/government/publications)

It is important to note that the national SBD guidelines for the security of commercial buildings are set at a minimum level and in areas of greater crime risk a higher level of crime resistance may be required. The advice given and requirements made by the CPDA will be dependent upon the outcome of a crime risk assessment and an understanding of local crime context. Consequently, specific measures addressing particular types of crime or anti-social behaviour may vary from one site to another. It is important therefore that frequent and continued dialogue exists between the CPDA and those responsible for design and construction to ensure that any local site specific and/or additional requirements are met.



**SECTION 1:**  
DEVELOPMENT  
– LAYOUT & DESIGN  
(Planning and external specification issues)

# Urban design and planning policy

## 1 Creating a sense of place

- 1.1 Creating an easily legible sense of place where employers, employees and legitimate visitors are able to go about their daily routine without undue fear of crime is a key element of the SBD initiative for commercial developments. Crime and anti-social behaviour are facilitated by a lack of definition of ownership of space.

## 2 The Planning System and Crime Prevention

- 2.1 National Planning Policy Framework 2012

The National Planning Policy Framework (NPPF) states that “Planning policies and decisions should aim to ensure that developments create: ...

- Safe and accessible environments where crime and disorder, and the fear of crime, do not undermine quality of life or community cohesion (para.58)...
- Safe and accessible developments, containing clear and legible pedestrian routes, and high quality public space, which encourage the active and continual use of public areas” (para.69)

Creating a sense of place where businesses and legitimate business users are able to go about their daily routine, without undue fear of crime or insecurity is a key element of the Secured by Design initiative.

The police service supports seven key attributes as integral to achieving sustainable communities. It is essential that developers demonstrate that these attributes have been considered and applied within the design of the development regardless of the geographical location within the United Kingdom.

Crime and anti-social behaviour are more likely to occur if the following seven attributes of sustainable

communities are not incorporated:

1. Access and movement: places with well-defined and well used routes with spaces and entrances that provide for convenient movement without compromising security
2. Structure: places that are structured so that different uses do not cause conflict
3. Surveillance: places where all publicly accessible spaces are overlooked
4. Ownership: places that promote a sense of ownership, respect, territorial responsibility and community
5. Physical protection: places that include necessary, well-designed security features
6. Activity: places where the level of human activity is appropriate to the location and creates a reduced risk of crime and a sense of safety at all times
7. Management and maintenance: places that are designed with management and maintenance in mind, to discourage crime in the present and the future, encouraging businesses and legitimate business users to feel a sense of ownership and responsibility for their surroundings can make an important contribution to community safety and crime prevention. Clarity in defining the use of space can help to achieve a feeling of wellbeing and limit opportunities for crime.

## 3 Phased or speculative developments

- 3.1 It is recognised that some commercial developments or mixed use (domestic and commercial) may be either phased; developed when the market allows, or speculative; the developer provides the infrastructure but there are no specific building designs available. Neither of the above circumstances will necessarily preclude achievement of SBD certification provided that there is a continuous dialogue with the CPDA.



## 4 Location and adjoining land use

- 4.1 Security requirements will be influenced by the location of new or existing commercial and non commercial buildings, both in the immediate vicinity and in the surrounding area, the hours of business operation, the type of business, by the numbers of employees working on site and others visiting the site and by transport links to and from the local area.
- 4.2 Security may be affected by the type of land use or property immediately adjoining the site. Wooded areas or open fields can make the grounds easier to access by trespassers. In contrast, houses with gardens adjoining the boundary can generate natural surveillance increasing the likelihood of crime or anti-social behaviour being observed and reported.
- 4.3 In planning new commercial areas or when re-developing such areas, sustainable design principles should be utilised, including the relationship of the commercial development with other facilities in the local area. Security will be significantly improved if the new buildings benefit from natural surveillance from existing occupied buildings. Such measures create conditions in which potential offenders feel vulnerable to detection. However, reliance on natural surveillance alone is not a guarantee of lower crime. Natural surveillance has to work in tandem with defensible space and the presence of persons who can act as potential deterrents and/or witnesses.

## 5 Configuration of buildings

- 5.1 It is important to consider the crime risks that a large number of commercial buildings might inadvertently create, such as numerous paths behind buildings for emergency exit and large areas set aside for car parking. Legitimate activity on industrial estates for example can be very low at weekends, and at night, and this inactivity can attract criminals.

Configuring buildings to maximise natural surveillance is of great importance, careful layout can help resolve many of the crime problems associated with in these developments. SBD recognises that there will often be site constraints or other considerations, such as solar energy efficiency gain requirements which may influence the orientation of buildings.

## 6 Outdoor amenity spaces

- 6.1 The location of seating areas and other recreational spaces provided for the use of the employees or the public must be carefully planned. Such amenity should be within view of occupied rooms from surrounding buildings (see *glossary of terms*). Recreation spaces may encourage trespass outside normal business hours and may require additional fencing or other security measures and should be discussed with the CPDA.

## Roads and footpaths

## 7 Vehicular and pedestrian routes

- 7.1 It is desirable that vehicular and pedestrian routes are designed in a way that ensures they are visually open, direct, and well used. They should not undermine the defensible space of commercial developments. Design features can help to identify the acceptable routes through a development and appropriate areas for public access, thereby encouraging their greater use, and in doing so enhance the feeling of safety. Where it is desirable to limit access/use to employers, employees and legitimate visitors features such as rumble strips, change of road surface (by colour or texture), pillars or narrowing of the carriageway may be used. This helps to define the defensible space, psychologically giving the impression that the area beyond is private.



## 8 Through-roads and cul-de-sacs

8.1 There are advantages in some road layout patterns over others especially where the pattern frustrates the searching behaviour and limits escape opportunities of the criminal. Whilst it is accepted that through routes may be included within commercial development layouts the designer must ensure that the security of the development is not compromised by excessive permeability, such as allowing the criminal legitimate access to the rear or side boundaries of buildings or providing too many or unnecessary segregated footpaths (Note 8.1).

*Note 8.1: It is generally accepted that routes for pedestrians, cyclists and vehicles should, in most cases, run alongside one another, and not be segregated. Movement frameworks based upon 'primary routes' and shared spaces, remove the need for under-used alleyways, short-cuts, footpaths and a large number of minor access points that can become vulnerable to/or facilitate crime.*

*A review of available research in this area concluded that: "Neighbourhood permeability... is one of the community level design features most reliably linked to crime rates, and the connections operate consistently in the same direction across studies: more permeability, more crime. Several studies across several decades link*

*neighbourhood property crime rates with permeability versus inaccessibility of neighbourhood layout. Neighbourhoods with smaller streets or more one-way streets, or fewer entrance streets or with more turnings have lower property crime rates..." Source: Taylor R B 2002 "Crime Prevention through Environmental Design (CPTED): Yes, No, Maybe, Unknowable, and all of the above" in Bechtel RB (ed) "Handbook of Environmental Psychology", John Wiley, New York, Pages 413 – 426. Cited by Professor Ted Kitchen Sheffield Hallam University.*

8.2 Good surveillance of the street from buildings has been proven to reduce the opportunities for crime.

8.3 Cul-de-sacs on commercial developments should be short in length and not linked by footpaths so as to create safe environments where premises can benefit from low crime. Research shows that features that generate crime within cul-de-sacs invariably incorporate one or more of the following undesirable features:

- backing onto open land, railway lines, canal towpaths etc, and/or
- are overly long and/or
- linked to one another by footpaths.

If any of the above features are present in a development additional security measures may be required.



## 9 Footpath design

- 9.1 Routes for pedestrians, cyclists and vehicles should run alongside one another and not be segregated. All planned routes should have a rational purpose and follow natural 'desire lines'. They should be well overlooked and integrated. Unsanctioned direct routes such as underused alleyways, shortcuts and a large number of minor access points can create hiding areas and anonymity for offenders.
- 9.2 Public footpaths should not run to the rear of, and provide access to industrial units, rear yards or neighbouring buildings (commercial units or dwellings) as these have been proven to generate crime. Private footpaths that serve as emergency exit routes at the rear of industrial premises should be secured with gates of steel construction (See section 2 paragraphs 44.2 and 44.3 for appropriate standard) and locking systems that restrict access but still facilitate emergency egress where required.
- 9.3 Where a segregated footpath is deemed to be essential, designers should carefully consider the possible impact on crime. Such routes have in the past been proven to facilitate crime, hence they must be straight, wide, well lit, avoid potential hiding places and be overlooked by surrounding buildings and activities. Physical barriers may also have to be put in place where unsanctioned 'desire lines' would place

a pedestrian in danger such as at a busy road junction. It is important that the pedestrian has good visibility along the route of the footpath. The footpath should be as carefully 'designed' as the buildings.

- 9.4 Where necessary and where space permits, segregated footpaths should be at least 3 metres wide (to allow people to pass without infringing each other's personal space), with at least a two-metre verge on either side. Some footpaths may be designated as an emergency access route and if so should be wide enough to allow the passage of emergency vehicles, service vehicles and have lockable barriers.
- 9.5 Keeping pedestrians and vehicles at the same level avoids creating intimidating spaces such as subways, footbridges and underpasses. If a subway is essential it should be as wide and as short as possible with a clear line of sight to the exit. Chamfering the access points can help reduce areas of concealment.

## 10 Planting next to footpaths

- 10.1 In general, planting next to a footpath should begin at the outer edge of the verge, starting with low growing plants with taller shrubs and trees to the rear. Planting immediately abutting the path should generally be avoided as the plants could have a tendency to grow over the path creating pinch points,

places of concealment, reduction of visibility and unnecessary maintenance.

10.2 Where footpaths run next to buildings or roads the path should be open to view. This does not prevent planting, but will influence the choice of species and the density of planting. Public footpaths should not run immediately next to doors and windows, therefore buffer zones should be created to separate a path from a building elevation. This is particularly important in areas with a known graffiti or anti-social behaviour problem where the use of defensive planting may be appropriate.

10.3 Careful selection of plant species is critical in order not to impede natural surveillance and to avoid an unnecessarily high maintenance requirement. Some hedging plants, for example, will require trimming twice a year, whereas other species might only need one visit every two years. Trees on appropriate root stocks can provide a more reliable means of reducing the likelihood of impeding natural surveillance. The potential cost savings of a reduced maintenance requirement could be substantial.

## 11 Lighting of roads and segregated footpaths

11.1 Roads and segregated footpaths for adopted highways and footpaths, private estate roads and car parks must comply with BS 5489-1:2013. Where conflict with other statutory provisions occurs, such as developments within conservation areas, requirements should be discussed with the CPDA and the local authority lighting engineer. Please note bollard lighting will not be compliant with BS5489:2013 or give sufficient light at the right height to aid the reduction of the fear of crime as they do not light people's faces sufficiently (*Note 11.1*).

*Note 11.1: It is recognised that some local authorities have 'dark sky' policies and deliberately light some of their rural, low crime areas to very low levels of*

*illumination and that others are currently experimenting with switching off street lamps in low crime areas between certain hours of the night in order to save energy costs and reduce CO2 emissions. If such policies exist then these must be brought to the attention of the CPDA at the time of application. The Institution of Lighting Professionals (ILP) does not encourage switch off unless a full risk assessment has been carried out and it should never be implemented purely for cost saving. A variable controlled lighting level is the preferred option.*

11.2 Landscaping, tree planting and lighting schemes shall not be in conflict with each other and lighting column positions should take priority over tree positions on new developments. Where trees are existing they shall be cut back and maintained so as not to impede the spread of light from the street lighting at any time.

11.3 The Overall Uniformity of light for an SBD development is expected to achieve a level of ideally above 15% for P classes, however the spacing window which is detailed in BS5489:2013 means that bad uniformity is not possible as a maximum average has to be achieved along with a minimum. As long as the scheme is BS 5489:2013 compliant it will have suitable uniformity.

Conflict areas such as roundabouts of a certain size and shared surfaces will require a higher uniformity which will be determined by compliance with BS5489:2013.

Major roads going through residential areas come under a different criterion of M classes with light levels measured in Candelas. Compliance to BS 5489:2013 will ensure a quality lighting scheme.

11.4 The Colour Rendering qualities of lamps used in an SBD development should achieve a minimum of at least 60Ra on the Colour Rendering Index (*Note 11.4*).

*Note 11.4: The Colour Rendering Index, scaled from 0 to 100 indicates the colour rendering qualities of lamps. 0*



is a non-existent ability to render colour under illumination, such as low pressure sodium lamps (SOX) (not allowed under BS5489:2013), and 100 is the colour rendering qualities of daylight. The 'Higher the RA the better the colour rendition qualities. Properly optically controlled white light (higher than RA60) will enable humans to see more clearly and improves facial recognition than if the light has an RA of lower than 60 such as High Pressure Sodium (SON). This is because it falls into the Mesopic range of vision and therefore the eye uses both rods and cones to determine the image. The British Standard has different levels of lighting as part of its P classes which now take into account the Mesopic properties of each type of lamp and its effect on the human eye. This is called an S/P ratio and will be an additional factor when the designer is choosing the lighting class. Please note that C classes and M classes are not affected by this and do not have the scope to lower lighting levels due to the use of white light.

- 11.5 The CPDA should always be provided with a 'Lux Plan' which shows both contour lines and lux points in order that the lighting system can be assessed. Additionally a risk and environmental assessment (EMS) for the CDM designer compliance requirements must be included. The plan should be compiled by a "competent" independent designer with at least level 3 or 4 competency under the ILP guidance notes (see additional documentation). The designer

should be MILP and either IEng or CEng to be deemed competent to be able to design under CDM regulations. Manufacturer designed schemes without risk or environmental assessments will not be accepted as they do not cover the CDM designer risk elements which are required.

*Note 11.5: The details on the plan must include the maximum average, minimum and average lux levels proposed. The plan must also show the Uniformity (U<sub>o</sub>) and colour rendering (Ra) values for the scheme.*

- 11.6 Light Pollution must be minimised (Note 11.6)

*Note 11.6: All living things adjust their behaviour according to natural light. The application of artificial light has done much to improve our experience of the night-time environment, but if this light is not properly controlled both physiological and ecological problems may occur. Minimising light emitted in directions where it is neither necessary nor desirable is extremely important. Obtrusive lighting from the private elements of the scheme is deemed a statutory nuisance (public lighting is not covered) and illuminating areas unintentionally is wasteful. SBD requires that only luminaires with suitable photometry serving to reduce light spill and upward light may be used.*

*In terms of sustainability consideration must be given to the consequences of*

turning off street lights. Such a measure may be counterproductive in terms of CO2 emissions and lead to the greater use of motor vehicles because residents are too afraid to use unlit streets. Crime levels, and in particular fear of crime levels, must also be carefully monitored to see what impact such an action has made to the community. The alternatives to switching off are Central Management Systems (CMS) which allow varying lighting levels for different times of the night and are centrally controlled by a Web based system. Also stand alone dimming equipment can be pre-set to dim after an agreed time when most residents are asleep. Both systems are preferable to switching off. Some light sources are more controllable than others and these should be considered where possible. The most controllable light source with the correct RA is LED, it also has no UV or IR so therefore does not impact as heavily as other light sources on wildlife and birdlife.

Presence sensing should not be considered unless in bin stores or rarely used areas as it can produce nuisance switching and become a problem to residents. Varying light levels via a CMS or stand-alone system reduces CO2, energy consumption and light pollution so is preferable where cost is not prohibitive and where the Council specification allows.

Glare is also an issue and is defined by direct view of the light source. Luminaires without good optical or lens control should not be used in residential areas.

## 12 Phased developments and footpaths

- 12.1 Where the construction of a footpath will be delayed because of phased development or long term planning policy, it may be prudent not to complete the footpath until such time as the full implications of its interaction with its environment can be understood. This will avoid in the short to medium

term the creation of an underused and possibly isolated movement route.

## Perimeter security and site access

### 13 Enclosed commercial developments – industrial and office use

- 13.1 Secured by Design supports single and multiple unit commercial developments that are contained within secure perimeters with access controlled entrances (industrial use only).
- 13.2 SBD recommends the use of one main entrance into an enclosed commercial development serving both vehicles and pedestrians or separate entrances that are located next to one another to aid mutual supervision. There should be clear demarcation between the roadway and the footway and a safety barrier between the two may be necessary to protect pedestrians from large vehicles/plant. In some cases an additional entrance may be required to service emergency access/egress. In these circumstances it may be prudent to provide additional electronic access control with CCTV.
- 13.3 For an extensive site and/or where there are higher risk security considerations, a staffed gatehouse may be required at the entrance. Such arrangements will invariably include the use of powered vehicular and pedestrian access gates. The CPDA should be consulted at the earliest possible opportunity in order to ascertain whether the risk analysis for the local area supports such a requirement (See Section 2 paragraphs 43 to 44 for further advice regarding perimeter security standards and specifications and Section 2 paragraphs 69 for standards relating to security guards and buildings).

### 14 Open commercial developments – office and industrial use

- 14.1 Ideally, no part of a commercial building should immediately abut a public footpath, road or other public area. This



Photo: Jacksons Fencing

is to prevent a vehicle borne attack to penetrate a wall, door or window or to prevent parking of high sided vehicles close enough to the building to allow climbing to less secure windows or flat roofs.

- 14.2 In open planned developments a defensible area can be created between the unit and the public road through the introduction of visitor and staff car parking and measures such as high kerbs, dwarf walls and hard and soft landscaping. Access for pedestrians or vehicles along the side of a building must be controlled through the use of fencing and/or gates, thus allowing access for emergency vehicles and staff where appropriate and means of escape when required. Physical barriers, such as 'anti-ram' bollards, may also be required to protect vulnerable building elevations, doors, roller doors and shutters when the business is closed (see Section 2 paragraphs 45 for standards for bollards).

- 14.3 Soft landscaping to the front of commercial units is acceptable provided it is set back from paths and placed to avoid obstructing visibility of doors, windows or any other access points. Generous hard paving in front of the unit may reduce the likelihood of plants growing to excess and obscuring vulnerable areas.

- 14.4 Casual approaches to windows can be deterred through the creation of uneven hard surfaces such as cobbles or angled

brick sets set in concrete. Specifiers should take particular care when specifying the type of gravel or loose surface treatment in developments so as not to provide missiles which will create criminal damage opportunities.

## 15 Boundary types

- 15.1 Boundaries fall into three main categories:

- 15.2.1 Psychological: Those that are intended to psychologically define ownership of space and distinguish between private and public land using features such as rumble strips, change of road surface (by colour or texture), road markings, and landscaping

- 15.2.2 Controlled: Normally a low fence, wall, hedge or other boundary treatment intended to help staff manage a site by physically restricting casual intrusion onto the site and channelling visitors to a formal entrance point in the perimeter. These types of boundaries are generally not high enough or sufficiently resistant to intrusion to be classified as a secure boundary.

- 15.2.3 Secured: A fence, wall, hedge or other boundary treatment intended to physically prevent climbing and or penetration into restricted parts of the site. A secure boundary around the site, or in the case of open planned developments, to the rear and or side of a building will also frustrate the intruder intent on breaking into the building out of hours and or limit the quantity



Photo: Jacksons Fencing

or type of goods that can be stolen. Secure boundaries can also provide for the security of industrial plant and machinery during the working day and keep unauthorised persons off a potentially dangerous site (See Section 2, paragraphs 43 to 44 for standards and specifications).

## 16 Security fencing

16.1 Security fencing is effective at delaying or deterring intrusion because of the need to climb over or penetrate the fence. It is therefore important that there are no structures close to or over the fence that will aid climbing, e.g. trees, lamp columns or buildings.

16.2 Security fencing materials may include welded mesh and expanded metal available in numerous coloured coatings, which are sometimes used in conjunction with timber. Railings of various designs can be used to good effect and all fencing types can be fitted with toppings to deter climbing. Whilst SBD recommends that security fencing should be effective without creating a 'fortress' impression it is accepted that certain business locations or business operations may actively seek to promote the security of their premises and hence utilise fencing that creates a strong visual deterrent.

16.3 Surveillance of and over the site from any surrounding streets, footways

and occupied buildings can help to deter potential offenders who may fear that their presence on the site will be reported to the police. It is therefore recommended that, where appropriate, security fencing systems are transparent to facilitate observation from outside the site and efforts are made by the occupiers to develop good relationships with their neighbours. The use of dark coloured coatings on metal fencing systems reduces the reflection of light and makes it easier for passersby to observe activity through the fencing.

16.4 It is accepted that some security rated fencing systems can be both costly and unsightly. However, the type of fencing that is required in order to gain SBD recognition must ultimately be determined by local crime risks. For example, in an average crime risk location, where the perimeter of the site is very large, it may be more appropriate to use a fence type matching the specification found in Section 2 paragraph 43.4. Indeed, in some locations it may prove to be more effective to install an inner security fence and then reduce the specification for the outer site boundary fence. There are many options that can be considered and they must be agreed on a site by site basis with the CPDA (see also paragraph 18.1).

16.5 Public footpaths immediately outside the boundary fencing can affect security.





If the footpath already exists and cannot be re-routed, the use of defensive planting in addition to fencing should be considered. However, this should not block natural surveillance from the footpath.

- 16.6 A party or shared boundary should not compromise security and maintenance. It may be advisable to erect a separate security fence inside the party boundary, ensuring access for maintenance of both existing and new structures. It is important to take account of neighbours' amenity in the choice of structure, as they will be more likely to act as deterrents or witnesses in helping to maintain site security. This arrangement may create a new path around the boundary and measures may be required to obstruct this path at vulnerable points.

- 16.7 When the building is closed and unoccupied, it must be possible to lock all entrance gates onto the site. During partial occupation, whether by employee, cleaners or security staff perimeter gates should be operable by appropriate means of secure access control.

## 17 Gates

- 17.1 The design, height and construction of any gates within a perimeter fencing system should match that of the adjoining fence and not compromise the overall security of the boundary (See also Section 2, paragraphs 44).

## 18 Defensive hedging

- 18.1 In some locations it may be a planning requirement to use or retain a defensive hedge, such as hawthorn, as a means to protect a site perimeter or to further bolster the security of an existing or proposed fence. Obviously it can take several years for a new hedge to develop into an effective barrier and therefore a temporary fence will be required in the short to medium term. When the hedge has matured to provide an effective barrier the fence can either be left in place (lost) or removed. Species selection is important, as hedging will require periodic maintenance.

## 19 Signage and unit identification

- 19.1 The commercial building's reception entrance and car park should be clearly signposted from the entrances onto the site. People found wandering around the forecourts of industrial buildings will often use the excuse that they could not find their way to the reception and the presence of clear signs will go some way to dismiss this excuse and help security staff and the police establish the legitimacy of the claim. Likewise, signs that identify areas that are not open to public access can act as a reminder that unauthorised persons should be challenged.
- 19.2 Site maps for industrial estates, if required, that identify road names and unit numbers should be correctly

orientated for the visitor and be protected from graffiti using a replaceable or cleanable transparent cover if the risk is present. Alternatively they can be located at a height that reduces the risk of damage or treated with an anti-graffiti coating to allow easy removal. Such maps should be located adjacent to a lay-by to reduce the impact on industrial estate traffic.

- 19.3 Clear numbering of individual units, which can be seen from the estate roads (too often absent in existing industrial estates) is essential to assist users, customers, postal workers and the attendance of emergency services.

## 20 Vehicle Parking and Access

- 20.1 The routes from the site entrance to the reception and to the car parks and delivery points should be clearly defined and benefit from as much overlooking from the reception and other occupied offices as possible.

- 20.2 It is highly likely that a new industrial estate road system will be designed to allow the easy operation of emergency vehicles and may include turning points and or space between buildings for large vehicles to operate. These arrangements may need to be matched with security measures to alleviate crime opportunities and it is recommended that a dialogue takes place with the fire service at an early stage.

- 20.3 Identifiable parking for staff should be provided in view of occupied offices and, where possible, identified visitor parking should be similarly located. In areas of high crime or where there are special security considerations, it may be prudent to secure the parking facility with appropriate fencing and an automatic access-controlled gate.

- 20.4 It is recommended to provide a parking space for emergency vehicles, such as an ambulance, close to the entrance of the building.

- 20.5 It is good practice to ensure that commercial buildings are designed to

allow secure deliveries and collections of material and goods. This will dictate the height of the bay delivery floor and its overall dimensions/design. Depending on risk, monitoring by CCTV may be necessary together with other security measures such as the provision of a secure delivery compound. It is recommended that this matter is further discussed with the CPDA.

- 20.6 The design criteria for car parks should follow the principles laid down in the police owned 'ParkMark' initiative. Full registration to 'ParkMark' is not a requirement of this document. The CPDA will be able to offer additional advice. Further information can be found at [www.parkmark.co.uk](http://www.parkmark.co.uk)



- 20.7 The purpose of 'Parkmark' is to:
- Reduce crime and the fear of crime in parking facilities.
  - Provide guidance to owners/operators and developers of parking facilities, both new and existing, on how to establish and maintain a safe and secure environment through the introduction of proven management processes, physical measures and site security systems, having considered the crime risk in the immediate vicinity.
  - Raise awareness with staff and visitors when parking their car, bicycle, motorcycle, etc, that the owner/operator has considered, and where appropriate, has taken action to reduce crime and the fear of crime within the parking facility they have chosen to use.
  - Provide a design framework for architects and developers of new parking facilities.



Photo: Cyclepods

## Two-wheeled motor vehicle parking & bicycle parking

- 20.8 Secure motorcycle, moped and scooter parking should be made available for staff. Such parking provision should benefit from surveillance from an occupied industrial unit or warehouse, be provided with secure ground anchors and be lit after dark when in use (See also Section 2 paragraph 46 for security standards).
- 20.9 Secure bicycle parking should be provided in view of an occupied industrial unit or warehouse with stands to which the bicycles can be secured. In order to encourage cycling to work and therefore reduce car journeys, it is recommended that the cycle parking provision is contained within a securable, roofed building. The building should be lit and secured during operating hours.
- 20.10 Further information about the parking of both motorised vehicles and bicycles can be found in Section 2 paragraphs 46. For lighting of the same see Section 2 paragraphs 48.
- 20.11 Where terrorism measures are being considered there should be sufficient 'stand-off' provision from the perimeter of the building; for vehicles the recommended distance is a minimum of 30m.

## External security issues

### 21 Landscaping

- 21.1 The planting of trees and shrubs in new developments to create attractive commercial environments will be supported and is encouraged providing:
- The layout allows sufficient space to accommodate the planting.
  - Future maintenance requirements are adequately considered at the design stage and management programmes are put in place to ensure that the maintenance will be properly carried out.
  - The planting design takes full account of opportunities for crime
- 21.2 The selected use of plants such as spiny or thorny shrubs can help prevent graffiti, casual approaches to the external face of the building, loitering and create or enhance perimeter security. Defensive planting is not just about prickly shrubs. It is about selecting the right type of plant for the right aspect and environment. For example, open branched and columnar trees can be used in a landscape scheme where natural and formal surveillance is required. Climbing plants can be used to cover walls that may be used as canvases for graffiti and carefully selected trees and shrubs can be used to "green up" the most hostile of environments providing both



horizontal and vertical interest without adding to crime risks.

- 21.3 Planting should not impede the opportunity for natural surveillance and must avoid the creation of potential hiding places. Although plant growth above 1m and below 2m should be absent to provide a window of surveillance, this does not preclude the use of hedging plants and feature shrubs and trees, providing surveillance opportunity is maintained. Plant growth below 500mm will be required in respect to car parks to deter vehicle interference.
- 21.4 The planting of new trees should be considered in tandem with the installation and the operational requirement of any specified CCTV system. Likewise, locate new trees so that they do not reduce directed light from lamps or provide climbing aids over boundaries or onto buildings.
- 21.5 Species selection of trees and shrubs should take account of their future maintenance, as poor maintenance can impact on site security. Mature, slow growing plants, although often more expensive to purchase from the outset, are normally much less expensive to maintain in the long term. It is recommended that a landscape architect is consulted about these matters.

## 22 External furniture and litterbins

- 22.1 External furniture such as benches and

planters should be of robust vandal and graffiti resistant design. Furniture should be fixed into the ground in order to prevent its theft and reduce the possibility of it being used for climbing or as a tool to break through the shell of the building. External furniture should not be located at or close to a building line where it can be used to climb onto roofs and nor should it be located against boundary fences.

- 22.2 Litterbins can also be used to assist climbing and the contents used to start fires. It is preferable that the bins are of a type that can be locked onto a fixed base and that they are located away from the buildings. Under no circumstances must litterbins be wall mounted beneath windows or on walls covered in combustible material.
- 22.3 Building or commercial activities where terrorism is a threat, the use and positioning of litter bins should be carefully considered so as not to provide for the placement of an improvised explosive device which may compromise public safety or building security.

## 23 Natural surveillance and recessed doorways

- 23.1 For new buildings it is important to avoid the creation of areas and building features (such as recesses) that cannot be overlooked from another occupied building or room. Recessed doorways can obstruct surveillance and also



collect windblown litter that can be used to start fires. Designing in an unobservable recess and then providing CCTV surveillance of the recess is not a sustainable solution (See Section 2 paragraph 56.10 to 56.12).

- 23.2 Where a recessed doorway is unavoidable because of site constraints, e.g. where an emergency exit door opens onto an 'out-of-site' fire path and has to be recessed due to the safety of those using the path, it would be prudent in this specific scenario to use a secure doorset (refer to Section 2 para.56 for appropriate standard) with emergency exit hardware and in-built secure vision panel. The secure doorset would resist most forms of attack and the vision panel would allow the recess to be checked for obstructions before opening the door (See Section 2 paragraph 58.5).

## 24 Temporary buildings

- 24.1 Temporary buildings, such as portable buildings, are notoriously difficult to secure due to their construction and the fact that they are outside the secure envelope of the permanent building structures. The voids under many of these buildings must be secured to prevent litter collecting underneath, which may be used to start a fire.
- 24.2 Temporary buildings should not be used for the storage of high value equipment such as computers and cash unless the building is security rated (Note 24.2).

All such buildings should be included within the main building's intruder alarm system. If practical and possible, additional temporary buildings when required should be linked to each other to form one larger continuous building, thus avoiding the creation of blind spots in between the buildings. It is expected that the use of non security rated temporary buildings will be discontinued as soon as possible after the main building has been enlarged (or possibly rebuilt).

*Note 24.2: SBD is currently working with interested parties to develop temporary buildings certificated to the Loss Prevention Certification Board's standard LPS 1175 Security Rating 2. Once such buildings become available they will be referenced within this guide*

- 24.3 Portable buildings should be constructed of non-combustible materials.
- 24.4 The location of temporary buildings must be discussed with the local fire authority to ensure that the spread of fire to other buildings is minimised and that the fire service's access is not hampered.
- ## 25 Wind turbines and photovoltaic installations
- 25.1 Consideration must be given to protecting wind turbines, photovoltaic installations (PVs) and biomass boilers from vandalism through the use of

access control, appropriate fencing and the removal of any climbing facility that may aid access.

- 25.2 PV panels are susceptible to criminal damage from thrown missiles and are likely to be the subject of theft as their installation becomes more commonplace. Therefore PVs should be located on roofs that are difficult to access, other than by legitimate means, and should be secured onto the roof with theft resistant fastenings. Landscape design should never include the use of loose pebbles for obvious reasons.

## Storage Facilities

### 26 Equipment storage

- 26.1 Plant and material should be protected from theft and criminal damage and stored within the main building when possible, otherwise external storage in a secure, roofed compound will be required. CCTV coverage may also be required if the value/nature of the stored items suggests heightened crime risk.

### 27 External waste storage

- 27.1 Waste containers, particularly those with wheels, can be used for climbing and the contents used to start fires. Therefore, consideration should be given to using waste containers with lockable lids. Additionally they should be kept inside a secure, externally accessed store in the main building or in a secure, roofed compound located well away from the buildings. Advice in respect to safe stand off distances, fire and smoke detection devices and fire sprinkler systems should be sought from the appropriate fire authority. In general, combustible materials should not be stored within 10 metres of the outside of a building (*See Section 2 paragraph 70*).
- 27.2 Adequate secure provision (as above) for temporary storage of materials to be recycled should be included.

- 27.3 Bin stores for kitchen waste (very large business operations) should be located in a similar way to paragraph 27.1 above, although it is accepted that for convenience during business hours the bin(s) may be kept outside and close to the kitchen areas.

### 28 Fuel storage

- 28.1 Fuel, such as central heating oil and cans of fuel used for grounds maintenance and plant machinery should be stored in a secured building located well away from the main building. Where there is insufficient space and the fuel has to be stored inside the main building advice should be sought from the appropriate fire authority as in paragraph 27.1 above. It may also be desirable to store biomass fuel close to the boiler plant in which case the appropriate fire authority should be consulted.

### 29 Cleaning equipment storage

- 29.1 A secure store, or stores, inside the building must be provided for the safe storage of cleaning equipment and cleaning fluids, given that many of these will be flammable and possibly toxic. Advice should be sought from the appropriate fire authority as in paragraph 27.1 above.

## Utility services and mail delivery

### 30 Telecommunications access covers, ducting and utility meters

- 30.1 Utility access covers, protecting access to drains, sewers, telephone cables, electricity cables and other services, must be secured to prevent access and damage by unauthorised persons (*Section 2 paragraph 47 for recognised standards*).
- 30.2 The ultimate security of the development and business continuity may be reliant upon the intruder or fire alarm's ability

to signal to an alarm receiving centre via a secure telephone line. It is therefore highly important to provide sufficient secure ducting into the site with an appropriate number of secure access covers. It may also be necessary to provide enough additional capacity to cater for speculative developments.

- 30.3 Utility meters must be sited in a secure building, such as a plant room, and where possible should allow for meter reading without having to enter the main building. Alternatively, instructions should be given to utility providers to carry out their readings during hours of occupancy or by prior appointment, so that access can be arranged without unnecessary disruption or security risk. Smart meters that automatically send readings along a data line or can otherwise be read remotely are encouraged.



## 31 Mail delivery arrangements

- 31.1 For the majority of commercial buildings it is expected that mail delivery will take place during business hours and that the mail will be handed in at reception. For out of hours deliveries please refer to Section 2 paragraphs 63 for standards for various methods of mail delivery.

## Building Shell

## 32 Windowless building elevations

- 32.1 A common feature of many industrial units and warehouses are long runs of elevations that have no windows for potential observation over the site. This arrangement is commonly found along the side and rear elevations of a unit. These same elevations will usually have at least one, windowless emergency exit doorway (often recessed) which can present opportunities for crimes such as graffiti, burglary and arson and also inappropriate loitering (See Section 1 paragraphs 23.1 and 23.2).
- 32.2 It is clearly sensible to keep unauthorised persons away from such building elevations. The way this is achieved will be different from one site to another and will depend to a large extent on the number and size of individual units and their orientation to each other. Common problems and potential solutions are discussed below:
- 32.2.1 Where units are separated by pathways designed for emergency exit from the doorways on the side and rear elevations it is important to place gates at the entrances to these pathways level with the front building line. During times when the building is occupied it must be possible to exit through these gates without the use of a key (See Section 2 paragraphs 44.2 and 44.3 for standards).
- 32.2.2 Where a unit's blank building elevation is next to a footpath or road to which the public have access create a 1m or greater separation between the footpath/road and the building using a 1.8m fence. A welded mesh or



expanded metal fence would be useful in this setting to maintain surveillance over the wall from the footpath or road. It is possible to use a 'defensive' hedge, such as hawthorn instead although the new hedge will have to be supported by the aforementioned fence until maturity and periodically maintained to control its height and spread.

32.2.3 Where there is insufficient space for a buffer zone and there is public access to the elevation then the wall structure and the standard for the doorset together with the use of CCTV will have to be discussed and agreed with the CPDA.

32.2.4 The provision of windows above ground floor level can provide surveillance over publicly accessible areas, but it is recognised that this may be impractical. Likewise the absence of windows on the ground floor elevations may be a security advantage in some circumstances as these would otherwise have to be protected to prevent burglary.

### **33 Automatic opening window systems and vents**

33.1 Many sustainable industrial and warehouse buildings being proposed require an automatic building management control system in order to ventilate the building and regulate the temperature, including at night to pre-cool the building during hot weather. This can cause security problems and the following issues may need to be addressed:

33.1.1 Automatic opening window systems, vents and pressure relief panels that operate when the building is unoccupied should be designed in such a way that they do not pose a security risk.

33.1.2 Care should be taken to ensure that any bars or grilles that are used to secure a building aperture associated with one of the mechanisms in 33.1.1 do not interfere with their operation.

33.1.3 The fitting of grilles to protect the building apertures associated with one of the mechanisms in 33.1.1 may affect the airflow requirements and advice should be sought from the relevant experts.

33.1.4 It is recommended that an automatic opening window or vent system incorporates a fail safe mechanism to notify building management that a window or vent has failed to close.

## **34 Walls – facades, apertures and graffiti**

34.1 Facades of buildings should minimise the opportunity for hiding and climbing up to windows or onto roofs. An unobstructed building line should be used to provide enhanced protection to the perimeter space as accessible ledges, parapets, indentations and protrusions may provide means of assisting unlawful entry.

34.2 The potential for unauthorised entry by misuse of facilities for essential services i.e. goods lifts, fuel delivery points or



ventilation ducts should be considered. Where possible such services should be concealed and/or located in locked compartments. Grilles, air ventilation apertures and shutters should be fitted so that they cannot be removed to permit unauthorised access. Reinforced mounting and fixing points for internal and external grilles, shutters and shutter roller boxes may be necessary as part of the building structure.

- 34.3 As graffiti tends to attract further graffiti, police will always advise that it is removed as soon as possible. Designers should therefore consider wall finishes that make this task easier to perform, particularly when the risk of graffiti is high. Surfaces should be coated with either an anti-graffiti glaze or sacrificial coating, or alternatively be designed for ease of maintenance e.g. painted in the event of a graffiti attack. Alternative measures for reducing or eradicating graffiti may also be considered such as growing an appropriate non-invasive climbing plant up the wall.

## 35 Roof design and access and aids to climbing

- 35.1 Preventing easy access to roofs should be considered at the design stage of the building. External rainwater pipes can be used for climbing and should be either square or rectangular in section, flush fitted against the wall or contained within a wall cavity or covered recess. Bends in pipes and horizontal runs should be minimized. They should be of fire resistant material. Physical barriers should be used to prevent access to an existing roof.
- 35.2 Flat roofs, particularly those at a low level, may be more easily accessed and depending on materials may be more vulnerable to intrusion either by cutting through the deck or forcing open roof lights and other openings (*See Section 2 paragraphs 54 for roof construction and paragraphs 55.1 to 55.3 for roof lights security standards*) (Note 35.2).

*Note 35.2: Attention is drawn to*

*relevant legislation (including the Occupier's Liability Act) concerning the responsibilities and liabilities of building owners / occupiers for the safe use of roof areas and relevant signage.*

- 35.3 Designers should take care not to inadvertently create climbing aids to upper windows and flat roofs via structures such as boundary walls, external buildings handrails and external staircases. It is hoped that external staircases for new industrial units and warehouses will be avoided.

## Internal layout issues

### 36 Entrances into the building

#### Main public/visitor entrance

- 36.1 Unless a commercial development is specifically intended to allow large numbers of the public into the building/s, public access to commercial units should be restricted to one main public/visitor entrance into the building. For industrial and high risk premises, the entrance should be electronically access controlled from a reception desk or office. Audio and or visual link back to the reception will be determined by local crime risks.
- 36.2 The space on the outside and inside of the entrance doors should be well illuminated during dark hours.
- 36.3 Reception staff should have a clear view of the approaches to the entrance. If the lighting levels directly outside the building reception are too low after dark, a reflection of the reception area will be seen on the inside of the glazing, which will hamper the receptionist's ability to look outside the building. It is therefore important that levels of illumination both inside and outside of the reception area are well balanced to avoid this inconvenience.
- 36.4 Where a separate automatically opening door is deemed more desirable for disabled access, the door opening system should be operated utilising



suitably located vandal resistant proximity reader (See Section 2 paragraphs 61).

- 36.5 In some circumstances it may be appropriate to use an 'airlock' door system whereby two sets of automatic doors are used, the first opening upon the detection of a visitor and the second set, either opening upon closure of the first, or controlled from the reception desk. This can be combined with a draft lobby/unheated transition space for energy conservation.

### **Staff or additional entrances**

- 36.6 There may be instances, especially with multiple buildings, where further entrance doors will be required for the convenient movement of staff. The crime opportunity risks that this arrangement might create will be minimised if access onto the site beyond the entrance forecourt and car park is restricted.
- 36.7 Electric door lock solutions for these additional external doorsets are available, which can be operated in numerous ways. Such operations might include the use of card swipes and proximity read fobs. Such arrangements should not prevent people from exiting the buildings in the event of emergency (See Section 2 paragraphs 61).
- 36.8 Some businesses use ID cards that incorporate a metallic strip or chip that provides them with access through selected doors. An integrated access

control system installed throughout the building using vandal resistant proximity readers (the SBD preferred technology) can also help to maintain a record of attendance and where necessary can selectively bar access to certain areas of the building or bar ex staff members who have ceased to be employed by the company. Biometric access control and voice recognition systems are also now available, which can be used in conjunction with other forms of access control into sensitive areas of the building. It is recommended that these various forms of access control are not used in isolation and should be discussed with the CPDA at the earliest opportunity.

- 36.9 Doorsets that are fitted with electric locks or electric release staples must form part of the manufacturer's certificated range of doorsets. (See Section 2 paragraphs 56 and 61.3 and 61.4)

## **37 Reception area and visitor control**

- 37.1 For business operations expecting large numbers of visitors it is recommended that the reception is staffed or supervised at all times. Access beyond the reception area should be controlled using automatic locking doors or barriers controlled by the receptionist or by proximity reader technology with fobs/ID cards issued to staff. Such doors or barriers must allow emergency exit and be integrated into the fire/

smoke alarm system for automatic release in an emergency when the building is occupied, however when the building is unoccupied the doors or barriers should fail safe i.e. secure (the relevant fire authority should be consulted on this arrangement).

- 37.2 Reception desks should provide the receptionist with a clear view of the waiting area, the approach to the entrance door and have restricted access from the public side.
- 37.3 Reception desks should be high and deep enough to afford protection for the receptionist, but the design should consider the needs of a wheelchair user. The floor level behind the reception desk can be raised if deemed appropriate.
- 37.6 Where the nature of the business or local crime problems result in higher risks of assault to reception staff, an escape route to a place of safety, such as an office located behind the reception area, should be provided. A 'slam to lock' door between the reception desk and the place of safety should include a door viewer or secure vision panel to allow a view of the reception area from the place of safety. (See Section 2 paragraph 58.5 for secure vision panels)
- 37.7 Where the risks of assault are high an audible personal attack alarm should be located at the reception desk so that the receptionist can use it to summon assistance from trained staff if confronted by an aggressive visitor. Consideration should be given to an additional alarm sounder located in nearby offices where other members of staff can be alerted. In some areas, where this type of incident is not uncommon, automatic response to this type of alarm by the police or contracted security service may be necessary. Staff training in the use of this deliberately-operated device will be required. False activations may result in limited provision or complete withdrawal of police response. (See Section 2 paragraphs 64)



## 38 Internal doorsets

- 38.1 As a general rule all internal doorsets should be fitted with locking furniture so that they can be locked when the room is left unoccupied. Very large buildings may incorporate electronic access control systems to all or most of the internal doorsets.
- 38.2 Rooms storing high risk/value equipment, such as IT servers, and materials or security systems/utilities services will require more robust doorsets and locking systems. Early discussions with the occupier of the building may also indicate the level of access control required for each room and floor and possibly the lifts. (See also Section 2 Paragraph 66)



## Security lighting

### 39 External lighting

- 39.1 The need for lighting will be determined by local circumstances. For example, in an inner city environment the lighting of a footpath is generally only effective in reducing crime levels if it is matched with a high degree of natural surveillance from surrounding buildings, where reaction to an identified incident can be expected. The lighting of an underused footpath may give the user a false sense of security and should be avoided. If there is a history of crime along an existing footpath, or where the additional connectivity due to the development could attract criminal or anti-social behaviour, consideration should be given to closing the path at night rather than lighting it. It is accepted that this would only be an option in exceptional circumstances.
- 39.2 In terms of security, the objective of lighting commercial units after dark is to deter or detect an intruder (*See Section 2 paragraphs 48 for standards and values*).
- 39.3 Lighting design should be co-ordinated with a CCTV installation (when specified) and the landscape designed to avoid any conflicts and to ensure that the lighting is sufficient to support a CCTV system. Light fittings should be protected where vulnerable to vandalism.

- 39.4 A lighting scheme should provide uniformed lighting levels with good colour rendition and be sufficient to cater for lawful after dark activity around the industrial or warehouse unit and site. It should not cause glare or light pollution and should support both formal and informal surveillance of the site.
- 39.5 External illumination when the building is unoccupied is recommended for entrance gates and routes to the main entrance and doors, car parks (if occupied by vehicles) and observable building elevations.
- 39.6 In some circumstances, and especially where security guards are monitoring the building from outside, it may be useful to direct lighting at the building to aid intruder detection.
- 39.7 The use of bollard lights may be useful for way finding, however bollard lights fail to properly model the facial features of pedestrians and are vulnerable to vandalism and vehicle collision. Therefore, their use for security purposes is discouraged.

### 40 Internal lighting

- 40.1 It is recommended that most internal office lighting is operated by detection devices which will automatically switch lights on and off due to movement activity or the lack of it in each room. Apart from being a considerably more efficient method for reducing energy consumption (does not require a

deliberate and remembered action by the user) such a system will identify the presence and progress of intruders in the building when it is closed. It therefore follows that the controlling mechanisms for the system should be contained securely.

- 40.2 In critical movement areas, such as corridors and staircases, the use of two stage lighting (a constant low level lighting level supplemented by activity switched lighting mode) may be utilised. This provides both safety and security.



## **SECTION 2:** PHYSICAL SECURITY – SPECIFICATIONS

## Introduction

### 41 Levels of security standards

- 41.1 It is important that an effective and realistic level of physical security, commensurate with the risk, is incorporated into building construction.
- 41.2 The CPDA will justify a requirement for higher levels of security with the provision of supporting crime analysis and other police vulnerability assessment advice that indicates heightened levels of risk based primarily on the location and anticipated use of the premises to be developed.

### 42 Unknown occupiers and risk

- 42.1 Due to the way in which many industrial developments evolve from inception to completion, and the fact that in many instances the intended occupier, and the nature of their business is unknown even beyond completion, it is often not possible to prescribe the completely appropriate security standard for the assessed crime risk. This document therefore details the minimum acceptable level of security for industrial and warehouse units and also offers relevant guidance for premises that may attract higher security risks. As soon as the end user and their business type are known, the CPDA should be consulted for further guidance.
- 42.2 Adherence to the SBD security standards will normally exceed minimum insurance requirements. Where there is a known higher risk, in terms of value or business continuity, then early liaison with the insurers is advised.

## Perimeter and external areas

### 43 Fencing

- 43.1 The demarcation between public space and industrial or warehouse premises is important. However, in many circumstances, there is also a need for fencing that offers greater security in order to protect a particular risk. It is

therefore important that the boundary treatment is discussed in detail with the CPDA at the earliest possible opportunity.

- 43.2 The five main reasons for providing a perimeter boundary fence are to:
- Mark a boundary to make obvious what is private and what is public property
  - Provide safety for employers and employees
  - Prevent casual intrusion by trespassers
  - Prevent intrusion onto the site by criminals
  - Reduce the wholesale removal of property from the site by thieves
- 43.3 The height of the fence will be determined by local circumstances, crime risk and the system chosen. In most circumstances heights between 1.2m (demarcation) and 2.4m (higher security) will be appropriate. Lower heights of fencing (1.2m to 1.6m) are suitable for boundary demarcation and controlling movement only and not for security, the height of security fencing will generally start at 1.8m and above. It is normally preferable that the perimeter fencing allows clear views over the commercial buildings and the grounds from the surrounding land and buildings. Dark colour finish to fencing reduces the reflection of light and therefore makes it easier for passersby to observe activity within the grounds/premises.
- 43.4 SBD requirements for fencing will be determined by risk:
- Normal crime risks require the use of the timber or steel security fencing specification listed in paragraphs 43.5 to 43.15 below
  - Higher crime risks require adherence to the requirements listed in paragraph 43.16 below



Photo: Jacksons Fencing

### Specification for timber or steel security fencing for normal crime risks

- 43.5 Where the fence panel is of a pale/slat design, they should be oriented vertically to avoid step-up points for climbing and able to resist being pried off/away and should be no less than 25mm thick timber or tubular steel with a wall thickness no less than 1.5mm and securely affixed to the frame/rails.
- 43.6 Where a fence panel is constructed of welded mesh the gaps between the mesh strands must be small enough to resist climbing.
- 43.7 The method of fixing between panel/rails and posts should create a secure mechanical bond so that panels/slats cannot be easily removed and in addition should provide a chain linking effect where each panel and post acts in concert with the next to resist attack by pushing and pulling.
- 43.8 The fixings employed in the panel/pale to rail construction should be of galvanized steel or stainless steel with a design life to match the fence or gate.
- 43.9 Posts should allow the construction of an unbroken panel to post chain and be of a non-brittle material.
- 43.10 Fence heights should be of a minimum 1.8m overall and be capable of raking or stepping to maintain height over different ground levels without creating gaps underneath
- 43.11 Pedestrian gates should be of a framed design and employ galvanized adjustable hinges and fixings mounted behind the attack face. On outward opening gates, where the hinges/brace is mounted on the attack face, fixings should be of a galvanized coach bolt design. Gates should be fitted with locks as agreed with the CPDA. The gate design and fixing features should match that of the fence (*See also paragraph 44.1*).
- 43.12 Entrance gates should be inward opening, of substantial framed construction and employ galvanized adjustable hinges and fixings mounted behind the attack face. Gates should be fitted with galvanized drop bolts and a facility for padlocking (manual gates) or electro-mechanical locking (automated gates) and employ mechanical/electro-mechanical devices as applicable to hold gate leaves in the open position. The locking method must be agreed with the CPDA. The gate design and fixing features should match that of the fence (*See also paragraph 44.1*).
- 43.13 The tops of timber fences should finish flush with the neighbouring posts and a securely fixed capping rail should run across the fence and posts to create a continuous chain. The tops/top rail/capping of fencing and gates should be of a design able to accommodate



a security topping to deter attempts to scale over the perimeter.

43.14 All timber employed in the manufacture of the fencing should be fit for purpose, from FSC certified sustainable sources and be treated to provide protection against all types of rot and insect infestation for a minimum of 15 years.

43.15 All steel used in manufacture should be galvanized to BS EN ISO 1461:2009 and/or stainless steel with a service life in excess of 25 years.

### Standard for security fencing for higher security risks

43.16 In circumstances where there is a higher risk of crime, a fence that is resistant to intrusion will be required. The minimum standard for such a fencing system is one that is certified to LPS 1175: Issue 7, Security Rating 1 (*Note 43.16*) or Sold Secure Gold standard (*See Glossary of terms*) or higher, depending upon risk. In order to meet this security standard the fence may not be aesthetically acceptable in some settings. Should this be an issue the applicant must discuss the matter with the CPDA and an alternative fencing system may be recommended. Higher standards for fencing are available, such as systems tested for use around government property.

*Note 43.16: The above LPS standard relates to both the height and penetrative resistance of the fence i.e. SR 3 is substantially more resistant to penetration than SR1. Such penetrative resistance may not always be required even though a height of 2.4m is necessary. In such circumstances, SBD will allow the extension in height of a certificated SR 1 fence.*

43.17 All fencing systems and gates as described in paragraphs 43 and 44 must be installed by the manufacturer or to the exact installation specifications provided by the manufacturer. BS 1722 offers installation advice. Consideration must be given to the provision of a strip foundation if there is a perceived

risk of the fence being bypassed or undermined by the removal of substrate, guidance is also provided in BS 1722.

43.18 Secured by Design currently accredits a number of fencing manufacturers and installers who between them can provide fencing solutions for all circumstances. They can be found in the Members and Products section of the SBD website [www.securedbydesign.com](http://www.securedbydesign.com)

## 44 Gates

44.1 All gates installed within a secure fencing system as described above must be suitable for the fencing specification or certified to the same standard as the adjoining certified fencing and be of the same height and similar style. It should not be possible to lift the gate from its hinges, and the hinges and lock cylinder should be protected in such a way as to prevent their use as climbing aids. Care should also be taken in the design to ensure that cross sections do not inadvertently aid climbing. It should not be possible to pass under the gate when in the closed position. If gates are installed with locks that are remotely operated, they must form part of the manufacturer's certified range. (*See paragraphs 57.1 for lock and cylinder standards and see also paragraphs 43.11 and 43.12*)

44.2 Gates used for the purpose of preventing access into a 'fire path' to the side and rear of an industrial or warehouse unit (particularly where the path runs between two units) should be certificated to either of the following standards:

- LPS 1175: Issue 7, SR 2
- STS 202: Issue, BR2

The gates should be of a design that allows for a line of sight along the side wall of the unit. If the gate requires an emergency release mechanism, i.e. release without the use of a key, it should be protected to prevent operation from the outside of the gate. Anti-climb measures above the gate should be included.



Photo: Frontier Pitts

44.3 Gates that are certificated to the standards described above or are otherwise suitable for use within fencing systems can be found in the Members and Products section on the Secured by Design website at this link: [Perimeter Security](#).

## 45 Security bollards (including those intended for Hostile Vehicle Mitigation)

45.1 Where crime risks dictate that there is a realistic chance of a ram raid type attack, with the intent to aide theft of the contents, or a vehicular borne attack to enter the premises or penetrate the shell of the building, ,to carry out an act of terrorism, the following standards for secure bollards that will prevent such an attack should be specified:

- Fixed bollards should have been successfully tested to PAS 68-1:2013 *Performance specifications for vehicle security barriers – fixed bollards* (Note 45.1)
- Rising Bollards should have been successfully tested to PAS 68-2:2013 *Performance Specification for vehicle security barriers – rise and fall bollards* (Note 45.1)
- Bollards providing passive protection to areas of a development or building that either are not required to have protection against an attack by a vehicle e.g. to keep a fire door (opening outwards) clear of obstruction, or where there is no

means by which a vehicle may have access but a substantial barrier is still required may be tested to BS 170-1.

*Note 45.1: The International Organization for Standardization (ISO) has produced an International Workshop Agreement (IWA) for vehicle security barriers. This new agreement has been supported by the UK and therefore Bollards meeting the requirement of IWA 14-1 (Vehicle Security Barriers) will be deemed acceptable for SBD Commercial Developments.*

45.2 PAS 69: 2013 provides guidance on the appropriate selection, installation and use of such bollards and should be referenced in the first instance (Note 54.2).

*Note 45.2: The International Organization for Standardization (ISO) has produced an International Workshop Agreement (IWA) issuing greater advice on site assessment and bollard installation. This new agreement has been supported by the UK and therefore bollards meeting the requirements of paragraph 45.1 and installed to the requirements within IWA 14-2 (Advice on site assessment and installation) will be deemed acceptable for SBD Commercial Developments.*

45.3 Other measures may be considered to address a possible vehicle borne attack as an alternative to bollards e.g. substantial planting boxes or raised kerb. These should be discussed with



Photo: Jacksons Fenning

the Crime Prevention Design Advisor at the earliest possible opportunity.

## 46 Vehicle parking

46.1 The design criteria for car parks should follow the principles laid down in the police owned 'ParkMark' initiative. Full registration to 'ParkMark' is not a requirement of this document. The CPDA will be able to offer additional advice. Further information can be found at [www.parkmark.co.uk](http://www.parkmark.co.uk) (See also Section 1 paragraphs 20 above).

### Underground car parking

46.2 Should a development have an element of underground car parking then the developer should note that the following requirements are necessary:

46.2.1 Every effort must be made to prevent unauthorised access into the car park. Therefore an access control system must be applied to all pedestrian and vehicular entrances. Where terrorism is a consideration access should be controlled with a PAS 68 rated measure.

46.2.2 Inward opening automatic gates, roller shutters or grilles should be located as close to the building line as possible to avoid the creation of a recess. Such products must be certificated to one of the following standards:

- LPS 1175: Issue 7, SR2
- STS 202: Issue 3, BR2
- Sold Secure Gold
- PAS 68:2013

They must be capable of being operated remotely by the driver whilst sitting within the vehicle. All motorized grilles or shutters must be installed with appropriate safety detection systems to avoid personal injury or damage to vehicles. Such systems may afford easy access to disabled drivers, and will satisfy the requirements of the Highways Agency who, under normal circumstances, do not permit vehicles to obstruct a pedestrian footway or highway whilst the driver is unlocking a gate.

46.2.3 The lighting standard required is BS 5489-1:2013. The CPDA may request to be provided with an IsoLux Diagram (Lux Plan) in order that the lighting system can be assessed (Note 46.2.3)

*Note 46.2.3: The details on the diagram must include the maximum, minimum and average lux levels proposed. The diagram must also show the Uo and Ra values for the scheme).*

46.2.4 The lighting system can be activated either by a passive infra red switch, or similar. Alternatively a timed system may be utilised based on a predetermined timed period following activation of the main vehicular or pedestrian doorset. Specifiers and lighting engineers should take due regard to the need for instant requirement for light levels to immediately meet the needs of the user, therefore luminaires that have a slow 'strike up' will not be acceptable for use.



Photo: Cyclepods

- 46.2.5 It is advised that walls and ceilings have light colour finishes to maximise the effectiveness of the lighting. This will reduce the luminaires required to achieve an acceptable light level.
- 46.2.6 Any internal door that allows access to the industrial unit or office floors above must have an access control system and meet the physical requirements as advised by the CPDA and described in paragraphs 56 to 58. Due regard must be taken of the requirement of the Building Regulations (Fire and Means of Escape).
- 46.2.8 In larger developments closed circuit television may be required. The car park must therefore be capable of being monitored from each individual unit if no formal monitoring agreement is planned. Developers are reminded that if images of public space are visible and recorded then there may be a legal responsibility to register the system with the Information Commissioner. Such a system would only be practical if there is a planned management service for the development.

### Bicycles

- 46.3 The securing of cycles left unattended must be considered within the design of any new commercial premises. The cycle stand must facilitate the locking of both wheels and the crossbar.

- 46.4 Minimum requirements for such equipment are:
  - Galvanised steel bar construction (minimum thickness 3mm) filled with concrete
  - Minimum foundation depth of 300mm with welded 'anchor bar'
- 46.5 External and preferably roofed bicycle stores with individual stands for securing bicycles are best located close to supervised areas of the main building. The 'walls' of such buildings should be open to surveillance and therefore constructed of materials such as welded mesh, grilles or bars, polycarbonate or other secure glazing such as glass composites. When in use the store must be lit after dark using vandal resistant, dedicated energy efficient light fittings and energy efficient lamps, such as compact fluorescent (*Note 46.5*).  
*Note 46.5: SBD prefers roofed bicycle stores to keep bicycles dry and encourage cycling*
- 46.6 External containers specifically designed for the secure storage of 2 or 3 bicycles and certificated to LPS 1175:Issue 7, SR1/2 or Sold Secure SS314 Bronze are available. These may be suitable for the use of members of staff.
- 46.7 Ventilated, bicycle stores within the main building must either have no windows or windows with security grilles and be fitted with a secure doorset that meets the standard as required by the CPDA.

The locking system must be operable from the inner face by use of a thumb turn to ensure that persons are not accidentally locked in by another user. The lighting in such a building must be automatically activated by a device, such as passive infra-red detector. The store should contain cycle stands as described in 46.4 above.

- 46.8 Further information about secure cycle parking can be found at the following resource section on the 'Bikeoff' website: [www.bikeoff.org/design\\_resource](http://www.bikeoff.org/design_resource)

### Two-wheeled motor vehicle parking

- 46.9 External parking stores for motorcycles, mopeds and scooters should be covered and located close to and in view of the main building and be provided with secure anchor points certified to Sold Secure Silver Standard. Secure containers for crash helmets and waterproof clothing are recommended.
- 46.10 Similar requirements as in paragraph 46.7 are required for ventilated stores within the main building for two-wheeled motor vehicles. Secure anchor points certificated to Sold Secure Silver Standard must be provided. Secure containers for crash helmets and waterproof clothing are recommended.

### 47 Telecommunications and utility access covers

- 47.1 Telecommunication lines and cables should enter buildings below ground and be protected by secure access covers certificated to a minimum of LPS 1175 Security Rating 2 or STS 202:Issue 3, Burglary Resistance 2 and be positioned in highly visible locations. For high risk areas or vulnerable businesses, access to other utilities should also be secured to LPS 1175 Security Rating 3 or STS 202 Burglary Resistance 3 or above. This will help to delay or prevent the occurrence of burglaries where the perpetrators cut the CCTV or alarm signalling wiring prior to undertaking the offence. (See also 30.1 to 30.2)

### 48 External lighting standard requirements

- 48.1 All street lighting for both adopted highways and footpaths, private estate roads and footpaths and car parks must comply with BS 5489-1:2013. Where conflict with other statutory provisions occurs, such as developments within conservation areas, requirements should be discussed with the CPDA and the local authority lighting engineer (Note 48.1).

*Note 48.1: It is recognised that some local authorities have 'dark sky' policies and deliberately light some of their rural, low crime areas to very low levels of illumination and that others are currently experimenting with switching off street lamps in low crime areas between certain hours of the night in order to save energy costs and reduce CO2 emissions. If such policies exist then these must be brought to the attention of the CPDA at the time of application.*

- 48.2 Landscaping, tree planting and lighting schemes shall not be in conflict with each other.
- 48.3 The Overall Uniformity of light for an SBD development is expected to achieve a rating of 0.4Uo and should never fall below 0.25Uo (Note 48.3).

*Note 48.3: The evenness of light distribution is almost always more important than the levels of illumination being achieved by the system (the levels are determined by BS 5489) The British Standards Institute have issued an advisory note stating that they recommend that Uo be at least 0.25 or 25%. A 0.4 Uo value is the ideal standard for an SBD lighting system, but where technical reasons prevent this we will still require the very best levels possible and under no circumstances may the rating fall below 0.25Uo.*

- 48.4 The Colour Rendering qualities of lamps used in an SBD development should achieve a minimum of at least 60Ra (60%) on the Colour Rendering Index (Note 48.4).

*Note 48.4: The Colour Rendering Index, scaled from 0 to 100 indicates the colour rendering qualities of lamps. 0 is a non-existent ability to render colour under illumination, such as low pressure sodium lamps, and 100 is the colour rendering qualities of daylight. The 'whiter' the light the better the colour rendition qualities. Properly controlled white light will illuminate an area to higher satisfaction levels for people whilst actually delivering less light than would be required for similar levels of satisfaction if non-white light sources were used.*

- 48.5 The CPDA must be provided with a 'Lux Plan' in order that the lighting system can be assessed (*Note 48.5*).

*Note 48.5: The details on the plan must include the maximum, minimum and average lux levels proposed. The plan must also show the Uo and Ra values for the scheme.*

- 48.6 Light Pollution must be minimised (*Note 48.6*)

*Note 48.6: All living things adjust their behaviour according to natural light. The application of artificial light has done much to improve our experience of the night-time environment, but if this light is not properly controlled both physiological and ecological problems may occur. Minimising light emitted in directions where it is neither necessary nor desirable is extremely important. Obtrusive lighting is a statutory nuisance and illuminating areas unintentionally is wasteful. SBD requires that only luminaires with suitable photometry serving to reduce light spill and direct light only to where it is required may be used.*

*In terms of sustainability consideration must be given to the consequences of turning off street lights. Such a measure may be counterproductive in terms of CO2 emissions and lead to the greater use of motor vehicles because residents are too afraid to use unlit streets. Crime levels, and in particular fear of crime levels, must also be carefully monitored*

*to see what impact such an action has made to the community. There are other possible technical alternatives to simply 'switching off' including the use of street lights that are sensitive to levels of moonlight, those that are switched on through the detection of pedestrians or vehicles and emerging LED technology which is 80% more efficient than contemporary street lighting.*

## **49 Closed circuit television (CCTV)**

49.1

CCTV is not a universal solution to security problems. It can help deter vandalism or burglary and assist with the identification of offenders once a crime has been committed, but unless it is monitored continuously and appropriately recorded, CCTV will be of limited value in relation to the personal security of staff and visitors. That being said, the provision and effective use of CCTV fits well within the overall framework of security management and is most effective when it forms *part* of an overall security plan.

49.2

Developers of new commercial premises and managers of existing premises that are considering the use of CCTV must be very clear about the objectives they wish to meet and establish a policy for its use and operation before it is installed. It is important to seek independent advice before approaching an installer and to develop a comprehensive operational requirement for the system, which can be supplied to installers during the tendering process. An operational requirement will be used for the design, performance specification and functionality of the CCTV system. In effect, it is a statement of problems, not solutions and will highlight the areas that must be observed by the system and the times and description of activities giving cause for concern. A useful reference to help achieve this goal is the *CCTV Operational Requirements Manual 2009 ISBN 978-1-84726-902-7 Published April 2009 by the Home Office Scientific Development Branch*



- 49.3 The CCTV system must have a recording capability, using a format that is acceptable to the local police. The recorded images must be of evidential quality if intended for prosecution. Normally this would require a full 'body shot' image of a suspect. It is recommended that fixed cameras are deployed at specific locations for the purpose of obtaining such identification shots. An operational requirement must take account of this fact and decisions made as to what locations around the building are suitable for obtaining this detail of image. The recording of vehicle licence plates may also be practical and useful.
- 49.4 Whilst the location of cameras is a site specific matter it would be normal practice to observe the main entrance to the premises and the reception area. Early discussions with an independent expert and potential installers can resolve a number of matters including:
- monitoring and recording requirements
  - activation in association with the intruder alarm
  - requirements for observation and facial recognition/identification
  - areas to be monitored and field of view
  - activities to be monitored
  - the use of recorded images
  - maintenance of equipment and the management of recording
  - subsequent ongoing training of operatives
- 49.5 CCTV systems must be installed to BS EN 50132-7: 2012+A1:2013 *CCTV surveillance systems for use in security applications*
- 49.6 The design of a CCTV system should be co-ordinated with the existing or planned lighting system for the buildings and the external grounds, to ensure that the quality of the lighting is sufficient to support the CCTV.
- 49.7 In high crime areas CCTV cameras may need protection within a vandal-resistant housing.
- 49.8 CCTV systems may have to be registered with the Information Commissioner's Office (ICO) and be compliant with guidelines in respect to Data Protection and Human Rights legislation. Further information is available at this website: [www.ico.gov.uk](http://www.ico.gov.uk)
- 49.9 For guidance on the use of CCTV images as legal evidence see also BS 7958: 2009 *Closed circuit television (CCTV). Management and operation. Code of practice*. This document provides guidance and recommendations for the operation and management of CCTV within a controlled environment where data that may be offered as evidence is received, stored, reviewed or analysed. It assists owners of CCTV systems to follow best practices in gaining reliable information that may be used as evidence.
- 49.10 Remotely monitored detector activated CCTV systems must be installed



in accordance with BS 8418: 2015  
*Installation and remote monitoring of  
detector operated CCTV systems -  
Code of practice*

## Building shell security

### 50 Wall construction

- 50.1 Due to the remoteness of some industrial and warehouse units and or reduced activity at night and over the weekends on industrial sites some buildings become prone to criminal attack through the wall, bypassing security doors and shutters. The walls should therefore be designed to withstand such attacks and materials resistant to manual attack or damage should be used to ensure the initial provision of security.
- 50.2 Where lightweight construction is being considered, for example the use of insulated sheet cladding, a reinforced lining such as welded steel mesh can enhance the security of the building fabric.

### 51 Glazed curtain walling and window walls

- 51.1 SBD recognises four distinct types of glazed wall systems. These are:
- i. Large glazed units connected by a 'spider clamp' system
  - ii. Glazed units directly retained within a framing system (usually aluminium)

- iii. Framed windows installed within a separate framing system
  - iv. Framed windows connected to other framed windows to create a 'window wall'
- 51.2 Glazed curtain walling (i & ii above) must be installed using a secure glazing retention system. The method of retaining the glass must include one or more of the following:
- Security glazing tape
  - Dedicated security sealant or gasket
  - A secure mechanical fixing system (Evidence will be required to prove the system is secure. This may be achieved by utilising the specific glazing retention test within PAS 24:2012 or by an indicative test on the retention system to LPS 1175: Issue 7, SR1 or STS 202: Issue 3, BR1)
- 51.3 Framed windows (iii & iv above) used within the construction of a 'window wall' must meet the requirements as required in paragraphs 62 below
- 51.4 Attack resistant glazing as defined by paragraph 60.1 below is required where the glazing is easily accessible. (See *Glossary of terms*)
- 51.5 For information only the following British Standard 'Codes of Practice' are relevant:
- BS 5516-1: 2004 *Patent glazing and sloping glazing for buildings. Code of*



# STORE

*practice for design and installation of sloping and vertical patent glazing*

- BS 5516-2: 2004 *Patent glazing and sloping glazing for buildings. Code of practice for sloping glazing*

## 52 Roller shutters and grilles

- 52.1 Grilles and shutters can provide additional protection to both internal and external doors and windows. The minimum standard for such products, when required, is certification to
- LPS 1175: Issue 7 Security Rating 1 or
  - STS 202: Issue 3, Burglary Rating 1
- 52.2 For roller shutters, the above minimum security ratings are generally sufficient where:
- a shutter is required to prevent minor criminal damage and glass breakage or
  - the shutter is alarmed and the building is located within a secure development with access control and security patrols or
  - the shutter or grille is intended to prevent access into a recess or
  - the door or window to be protected is of a high security standard in its own right.
- 52.3 Security ratings higher than the minimum may be required and will be dictated by one or more of the following security considerations
- Type of crime risk
  - Level of crime risk

- Location of the building
- Security level of the door or window being protected

Such a requirement will be justified and communicated to the applicant by the CPDA in writing.

- 1.4 In new build developments roller shutters should be integrated into the fabric of the building

## 53 Roller shutter doors providing vehicular access

- 53.1 Roller shutter doors providing access for deliveries and other apertures where no other door is present must be certificated to a minimum of:
- LPS 1175 Issue 7, Security Rating 2 or
  - STS 202 Burglary Resistance 2
  - Sold Secure Gold
- 53.2 A higher level of security will be determined by similar factors as in paragraph 52.3 above and a requirement for such will be justified and communicated to the applicant by the CPDA in writing at the earliest opportunity following receipt of the application.
- 53.3 In new build developments roller shutter doors must be integrated into the fabric of the building.

## 54 Roof construction

- 54.1 Roofs are vulnerable to criminal intrusion and damage through vandalism, therefore careful



consideration must be given to their construction.

54.2 Lightweight roofing systems must be certified to a minimum of:

- LPS 1175: Issue 5 or above, SR 1
- STS 202: Issue 1 or above, BR1

54.3 The standards above tests the product and its fixings, therefore lightweight roofing systems must be installed utilising the manufacturer's approved fixing system.

54.4 Where traditional roofing systems are being used, the CPDA must be consulted to discuss alternative security measures e.g. the introduction of additional security features to address criminal penetration via the roof such as expanded metal.

54.5 Vulnerable ceiling voids should be protected by a monitored intruder alarm system.

54.6 Due regard must be taken to ensure full compliance with the 'duty of care' obligations under Occupiers' Liability Act 1984.

## 55 Roof lights and sun tubes

### Roof lights

55.1 Based on a site specific risk assessment which will be communicated in writing to the applicant (by the CPDA) and which will take into account contributing factors such as the accessibility (See *Glossary of terms*) and visibility e.g.

whether activity can be seen from the street or a nearby occupied building, a roof light aperture must be protected by either one, or a combination of the following:

55.1.1 In low crime, low risk applications a roof light aperture must be protected by roof lights certificated to LPS 1175: Issue 5 or above, Security Rating 1 or STS 202: Issue 1 or above, Burglary Resistance 1.

55.1.2 In higher crime, higher risk applications a roof light aperture must be protected by roof lights certificated to LPS 1175: Issue 5 or above, Security Rating 2 or 3, or STS 202: Issue 1 or above, Burglary Resistance 2 or 3.

55.1.3 Alternatively, a roof light meeting the requirements in 55.1.1 above may be used in conjunction with an internal grille certificated to LPS 1175: Issue 5 or above, Security Rating 1 or 2, or STS 202: Issue 1 or above, Burglary Resistance 1 or 2.

55.2 The CPDA must be supplied with proof of certification including the technical schedule, prior to the SBD certificate being awarded, unless the supplier is a member of the Secured by Design Licensing Scheme and the roof light can be identified on the SBD website (see *also paragraph 62.10*).

55.3 Roof lights must be securely fixed in accordance with the manufacturer's specifications. The CPDA may request a copy of the manufacturer's fitting specifications.

## Sun tubes/tunnels

55.4 To prevent a sun tube being used as an access point into a commercial building the maximum diameter allowed is 350mm. In rare occurrences where larger diameters are required the CPDA should be contacted to discuss alternative means of protection.

## 56 External doorset apertures

56.1 It is important that the doorset aperture is protected. Due to the nature of some commercial building uses and locations there is an expectation that the security will be required to meet the following minimum standards when the building is unoccupied:

- PAS 24:2012
- LPS 1175: Issue 7, SR2
- STS 201 or STS 202: Issue 3, BR2

Additional security may be gained by utilising additional protection such as a certified roller shutter or grille as described in paragraphs 52 or through the use of a doorset certified to higher security standards in paragraph 56.3.

56.2 It is expected that all doorset products are fit for purpose and therefore certification to the following material specific standards is also required:

- BS 6510:2010 (Steel)
- BS 7412:2007 (PVCu)
- BS 644:2012 (Timber)
- BS 8529:2010 (Composite)
- BS 4873:2009 (Aluminium)

56.3 In some circumstances it is highly likely that neither the CPDA nor the developer will know who the occupier of an industrial unit will be or the nature of the business therein. In such circumstances the CPDA will normally require the minimum level of security described in paragraph 56.1 above. If, however, the occupier is known then it is essential that the occupier's insurers are advised in order that the correct level of security can be specified.

56.4 A requirement for external doorsets to be certified to a higher standard of security will be supported by crime analysis provided by the CPDA or specific insurance requirements.

56.5 See paragraphs 52 for the SBD requirements for roller shutters and grilles.

56.6 Doorsets must be certificated by one of the following UKAS accredited certification bodies (*Note 56.5*):

- BM Trada Certification
- British Board of Agrément
- British Standards Institute
- Loss Prevention Certification Board (part of the Building Research Establishment)
- Exova Certisecure Scheme
- ER Certification
- UL Certification
- Buildcheck

*Note 56.6: Certificated products undergo continuous assessment to ensure that product standards are maintained. Any documentation submitted as proof of compliance should clearly show the certification body name and the manufacturer/fabricator of the product installed within the development. Documentation that is provided bearing the name of a component or system manufacturer will not be deemed acceptable.*

56.7 Alternative compliance is acceptable only from SBD member companies that have alternative compliance testing or reached an advanced stage of the certification process with one of the above bodies. Such cases must be verified with SBD, the managing body that oversees the Secured by Design initiatives

56.8 Alternatively, third party accreditation to the above standards via a Notified Certification Body that has signed the EA MLA (European cooperation for accreditation multi-lateral agreement) may be acceptable if this body is also specifically accredited to conduct such activities. The CPDA may refer such cases to SBD for verification.



56.9 Outward opening doorsets must specifically form part of the manufacturer's certificated product range.

56.10 The CPDA must be provided with proof of certification through one of the above bodies, including the scope of certification, prior to the SBD certificate being awarded, unless the supplier is a member of the Secured by Design licensing scheme and the doorset can be identified on the SBD website.

### Avoiding door recesses

56.11 Recessed doorways should, where possible, be avoided as they provide opportunities for crime and anti-social behavior i.e. graffiti, arson and burglary. In the event that the building design or location requires such recesses efforts should be made minimize such negative consequences. This may include a requirement for higher security rated doorsets, doorsets and surrounding building material to be fire retardant and anti-graffiti surface treatments to be applied to both.

## 57 Locking systems for doorset upgrade and gates

57.1 Doorsets in new developments or replacement doorsets within refurbished premises should comply with section 56. Doorsets subject to an upgraded i.e. the door and frame are not being changed, or external gate systems utilising a single or multipoint locking system should comply with paragraph 56.

57.2 Locking mechanisms incorporating cylinders (Euro or oval profile) must include an assessment to BS EN 1303:2005 (minimum requirements key security Grade 5, attack resistance Grade 0 and drill attack resistance Grade 2). In addition to the above requirement, the cylinder certification scheme must include cylinder 'snapping' and 'anti-bump' assessments, for this reason all cylinders must be certificated to DHF TS 007 1 star (if the cylinder is protected by DHF TS 007 2-star external hardware) or DHF TS 007 3-star if no external protective hardware is being provided.

The following certification schemes for lock cylinders are currently recognised for use in SBD developments

- British Standard Institute 'Kitemark'
- Loss Prevention Certification Board LPS 1242: Issue 2:2010

57.3 A single point locking system certificated to BS 3621: 2007+A2:2012, BS 8621: 2007+A2:2012 or BS 10621: 2007+A2:2012 (*Note 57.3.1*). Alternatively a multipoint locking system certificated to PAS 3621:2011, PAS 8621:2011 or PAS 10621:2011 (*Note 57.3.2*)

*Note 57.3.1: These British Standard (BS) references have been developed from BS EN 12209, which is the European standard for single point locking devices and BS EN 1303, which is the European standard for lock cylinders and which incorporates an additional General Vulnerability Assessment, which is unique*

to the UK. These British Standards reflect the elements of BS EN 12209 and BS EN 1303 that are considered to be the minimum level required for insurance cover with the UK.

The only difference between these British Standards is the level of security offered from the internal face of the door:

- BS 3621 offers the same level of security to the internal and external face of the lock
- BS 8621 allows the use of a non-key operated release mechanism (e.g thumb turn)
- BS 10621 offers the same functionality at BS 8621, but has an external override facility, which disables the internal operated release mechanism (e.g thumb turn). This type of lock must only be specified for use within buildings that have alternative means of escape.

Locksets certificated to the above standards will not require any further protection for the cylinder as this is catered for within the test standards.

Note 57.3.2: The UK multipoint standards have been developed to be equal to or exceed the equivalent single point variations. The operational characteristics echo those of the single point variants i.e. The only difference between these British Standards is the level of security offered from the internal face of the door:

- PAS 3621 offers the same level of security to the internal and external face of the lock
- PAS 8621 allows the use of a non-key operated release mechanism (e.g. thumb turn)
- PAS 10621 offers the same functionality at PAS 8621, but has an external override facility, which disables the internal operated release mechanism (e.g. thumb turn). This type of lock must only be specified for use

within buildings that have alternative means of escape.

Locksets certificated to the above standards will not require any further protection for the cylinder as this is catered for within the test standards.

57.3 In addition to the above requirements, doorsets designated as 'emergency' or 'panic' exits must be fitted with the hardware appropriate to the specific use:

- BS EN 179: 2008 *Emergency exit devices*
- BS EN 1125: 2008 *Panic exit devices*

57.4 Doorsets must be supplied with a suitable (easily removed) label outlining the operational instructions for the locking system. The label shall be applied to the internal face of the door at the time of installation and remain in place until handover to the end user. A separate instruction leaflet for the locking system shall also be supplied to the end user.

## 58 Glazing within doorsets and secure vision panels

58.1 All glazing in and adjacent to doors must include one pane of attack resistant glass (See paragraph 60.1) that is securely fixed in accordance with the manufacturer's instructions.

58.2 If glazed panels are installed adjacent to the doorset and are an integral part of the doorframe then they should be tested as part of the manufacturer's certificated range of door assemblies. Alternatively, where they are manufactured separately from the doorframe, they shall be certificated to either:

- PAS24: 2012 or STS 204
- LPS 1175: Issue 7, at a Security Rating to match the doorset or
- STS 202: Issue 3, at a Burglary Rating to match the doorset

Such windows must be securely fixed to the door assembly in accordance with the manufacturer's instructions.

58.3 Care should be taken to ensure that access for the disabled does not conflict

with the requirements of the Equality Act 2010. Doorset attributes which may require closer attention include opening mechanisms, glazing, level access and door width.

- 58.4 In some circumstances, such as in a remote building with no surveillance over an external, unglazed door, it is recommended that a door viewer is installed between 1200mm and 1500mm from floor level (see also paragraph 58.5).

### Secure vision panels

- 58.5 Where privacy is required, together with a degree of security, both external and internal doorsets can be fitted with a secure vision panel. Secure vision panels allow for the control of vision into a private area or room or for views of an outside area for the purpose of manual visual access control. They can be supplied to various security levels dependent upon the door in which they are installed.

## 59 Door installation

- 59.1 Doorsets must be securely fixed into the fabric of the building in accordance with the manufacturer's instructions. The CPDA may require a copy of the manufacturer's installation specification.

## 60 Security glazing

- 60.1 All ground floor and easily accessible glazing must incorporate one pane of laminated glass to a minimum thickness of 6.4mm (See *Glossary of terms*) or glass successfully tested to BS EN 356:2000 *Glass in building. Security glazing - resistance to manual attack* to category P1A unless it is protected by a roller shutter or grille as described in paragraphs 52 above. With effect from 1<sup>st</sup> January 2014 the Secured by Design requirement for all laminated glass in commercial premises will be certification to BS EN 356 2000 rating P1A unless it is protected by a roller shutter or grille as described in paragraphs 52 above.
- 60.2 Occasionally, when large laminated glazed panels are used on south

facing elevations, there have been incidents of glazing failure (cracking) due to thermal stress. Whilst the use of toughened glass would seem to be a simple solution to the problem of thermal stress, ordinary toughened glass offers no security resistance. It is therefore recommended that the inner pane of glass used in a double glazed unit is 'laminated toughened'. This combination of the two sheets of toughened glass and the interlayer offers both resistance to intrusion and thermal stress associated with large glazed areas. Specifiers are reminded that the minimum requirement for SBD is BS EN 356: 2000 category P1A.

- 60.3 When premises are assessed as being at significant risk to the effects of blast from a terrorist attack, blast resistant glazing or anti shatter film may be required to mitigate the risk of death or injury from the effects of flying glass. Refer to the Home Office glazing document.

## Electronic access control

### 61 Electronic access control systems

- 61.1 Electronic access control is likely to be required at the main entrance to a warehouse or industrial unit and may also be required on some internal doorsets, such as those that lead from an entrance lobby or reception into offices and production and warehouse floors. The requirement for electronic access control will be influenced by some of the following factors:
- The need to protect a lone worker or vulnerable persons working in a reception area
  - To prevent access into parts of the building beyond the reception to prevent crime and maintain health and safety
  - To prevent trespass onto the production or warehouse floors, especially where the offices and the reception are located on an upper floor



- Type of business or business practices
- Local crime risk factors
- Where two or more businesses are served by a common entrance

61.2 In all such cases the doors must incorporate an electronic access control system, with an electronic lock release and (for the main entrance) an audio link to the individual businesses' offices or receptions. In some cases visual verification by CCTV camera incorporated into the call panel or separately located may be required. Specifiers are reminded that changing the lock specification of a certificated security doorset will require further testing. It is therefore important to discuss such changes with the manufacturer and the CPDA.

### Electronic access control standards

61.3 Specifiers are advised to make reference to guidance published by the British Security Industry Association (BSIA) 'A specifiers guide to the Security classification of access control systems'.

### Electronic Access control and security staff

61.4 Where security officers are to be employed at the entrance electronic access control will still be required. See paragraph 69 for further information about security staff and manned guarding and guard houses.

## Protection of window apertures

### 62 Protection of window apertures

62.1 It is important that the window aperture is protected. Due to the nature of some commercial building uses and locations there is an expectation that the security will need to exceed the following standards when the building is unoccupied:

Certification to

- PAS 24:2012 or
- STS 204 Issue 3: 2012, or
- LPS 1175 Issue 7:2010 Security Rating 1 or
- LPS 2081 Issue 1:2014 Security Rating A

Additional security may be gained by utilising additional protection such as a certified roller shutter or grille as described in paragraphs 52 or through the use of a doorset certified to higher security standards in paragraph 56.3.

62.2 In some circumstances it is highly likely that neither the CPDA nor the developer will know who the occupier of an industrial unit will be or the nature of the business therein. In such circumstances the CPDA will normally require the minimum level of security described in paragraph 62.1. If, however, the occupier is known then it is essential that the occupier's insurers are advised



in order that the correct level of security can be specified.

62.3 A requirement for external windows to be certified to a higher standard of security will be supported by crime analysis provided by the CPDA or specific insurance requirements.

- LPS 1175: Issue 6, Security Rating 2 or higher
- STS 202 Burglary Rating 2 or higher (Note 62.3.1)

*Note 62.3.1; STS 202 is the equivalent standard to LPS 1175 and is published by Warrington Certification Laboratories*

62.4 See paragraphs 52 for the SBD requirements for roller shutters and grilles

62.5 Windows must be certified by one of the following UKAS accredited certification bodies (Note 62.5):

- BM Trada Certification
- British Board of Agrément
- British Standards Institute
- Loss Prevention Certification Board (part of the Building Research Establishment)
- Exova Certisecure
- ER Certification
- UL Certification

*Note 62.5: Certificated products undergo continuous assessment to ensure that product standards are maintained. Any documentation submitted as proof of compliance should clearly show the certification body name and the manufacturer/fabricator of the product*

*installed within the development. Documentation that is provided bearing the name of a component or system manufacturer will not be deemed acceptable.*

62.6 Alternatively, third party accreditation to the above standards via a Notified Certification Body that has signed the EA MLA (European cooperation for accreditation multi-lateral agreement) may be acceptable if this body is also accredited to conduct such activities. The CPDA may refer such cases to SBD for verification.

62.7 All glazing in windows that are easily accessible (See *Glossary of terms*) must include one pane of attack resistant glass (See *paragraph 60.1*) that is securely fixed in accordance with the manufacturer's instructions.

62.8 Windows must also be fit for purpose and must be certificated to the relevant material standard i.e.:

- BS 6510:2010 (Steel)
- BS 7412:2007 (PVCu)
- BS 644:2012 (Timber)
- BS 8529:2010 (Composite)
- BS 4873:2009 (Aluminium)

62.9 The CPDA must be provided with proof of certification through one of the above bodies, including the scope of certification, prior to the SBD certificate being awarded, unless the supplier is a member of the Secured by Design licensing scheme and the window can be identified on the SBD website.



62.10 Windows must be securely fixed and installed in accordance with the manufacturer's specifications. The CPDA may require a copy of the manufacturer's installation specification.

62.11 Windows must meet the requirements of the local Building Regulations with regard to safety glazing and emergency egress. The following additional specific SBD requirements must be complied with:

- Security glazing as required in paragraph 60.1 in windows below 800mm (from floor level) or 1500mm if within 300mm of a doorframe.
- Non-key locking hardware on designated emergency egress windows together with security glazing as required in paragraph 60.1.

### Secondary glazing

62.12 Security of the minimum standard windows can also be improved through the use of secondary glazing systems to the standards as shown in paragraphs 62.1 and 62.3.

## Mail Delivery

### 63 Mail Delivery

63.1 Letter plates and letter boxes must meet one of the following requirements:

- A robust external letter box securely fixed to the external face of the building in accordance with the manufacturer's specifications with fire retardation and anti-fishing attributes Letter boxes complying with DHF TS 009 have been found to meet the above requirements
- A letter plate located within the wall, providing 'through the wall' delivery via a sloping chute into a secure internal letter box with fire retardation and anti-fishing attributes.

63.2 Letter plates for the above must comply with BS EN 13724: 2002 and must have a maximum aperture size of 260mm x 40mm . Letter plates complying with DHF TS 008 have been found to meet the above requirement and provide

additional security against anti-fishing characteristics and are especially recommended where thumb-turn release mechanisms are installed.

## Internal security considerations

### 64 Intruder alarms systems

64.1 A suitably designed, fit for purpose, monitored intruder alarm system must be installed. For police response, the system must comply with the requirements of the Security Systems policy, which can be found at [www.securedbydesign.com](http://www.securedbydesign.com)

64.2 System designers may wish to specify component products certificated to the following standards:

- LPS 1602 Issue 1.0: 2005  
*Requirements for LPCB Approval and Listing of Intruder Alarm Movement Detectors*
- LPS 1603 Issue 1.0: 2005  
*Requirements for LPCB Approval and Listing of Alarm Control Indicating Equipment*

64.3 Security fogging devices can be incorporated within the intruder alarm system to disorientate the intruder when the alarm system is activated. They must conform to BS EN 50131-8:2009 Security device fog systems.

### 65 Public address systems

65.1 In large commercial buildings a public address system is recommended to provide instant, effective communication to all staff members particularly in emergency situations where a prearranged and rehearsed response to particular situations can be initiated.

### 66 Physical security standards for computers and server rooms

66.1 Consideration must be given to the structure of the internal walls, floors and ceilings of computer server rooms to provide appropriate security and to prevent damage by fire, smoke or fire extinguishment (water) from other



parts of the building. Due to varying construction methods and materials it is not possible to be prescriptive, however combinations of different materials, such as high impact gypsum boards, expanded metal sheets, plywood, and masonry have proved to be effective.

66.2 Where it is impractical to secure a room housing a computer server, there are two alternative solutions i.e. secure cabinets for individual computers, or small server units, and security caging for large or multiple servers. In both cases the SBD requirement is for full product certification. The following standards apply:

- LPS 1214: Issue 2.1, Category 1 (small server units)
- LPS 1175: Issue 7, SR2 (for large or multiple servers)
- LPS 1175: Issue 7, SR3 (for high risk or value servers)
- STS 202: Issue 3, BR 3
- LPS 2083: Issue 1

## 67 Secure internal doorsets

67.1 There is no specific SBD requirement for secure internal doorsets unless there is an identified security risk. Specifiers should contact the CPDA if there are any internal doorsets that may require additional security e.g. computer server room. The standards applicable will vary dependent upon the risk but the minimum recommended standards are as follows:

- PAS 24: 2012 or
- STS 201

High risk doorsets should be certificated to the following standards:

- LPS 1175: Issue 7, SR 2 or above, or
- STS 202: Issue 3, BR 2 or above

## 68 Safes and strongrooms

68.1 SBD recommends commercial safes and strongrooms are certificated to:

- LPS 1183: Issue 4.2, or
- BS EN 1143-1:2012 (*Note 68.1*).

The required resistance grade for a safe is determined by the value of the contents of the safe. The ratings in the table below should only be used as a guide as insurers will define their own ratings depending on the performance of the safes and the situation in which the safes and strongrooms are to be used. It is therefore very important that specifiers talk to insurers prior to selecting a safe or strongroom.

*Note 68.1 There are reported variations in some safes certificated to BS EN 1143-1:2012, however testing quality and consistency by VDS (Germany), SBSC (Sweden), CNPP (France) and LPCB (UK) is generally recognised by the UK insurance industry.*



Standard	Resistance grade	Typical overnight cash rating (£k)	Typical overnight jewellery rating (£k)
LPS 1183 & BS EN1143-1	0	6	60
	I	10	100
	II	17.5	175
	III	35	350
	IV	60	600
	V	100	1000
	VI	150	1500
	VII-XIII	-	-

Reproduced with the kind permission of the Loss Prevention Certification Board

## Other design security considerations

### 69 Security staff manned guarding and guard houses

- 69.1 Where security staff are to be employed the following information should prove useful for designers where such a service is to be employed.
- 69.2 The provision of manned guarding may require additional design features to be built into the buildings and grounds at the outset in order to reduce overall costs.
- 69.3 In order to ensure a comprehensive patrolling regime is maintained an

electronic patrol monitoring system is recommended.

- 69.4 BS 7499: 2013 *Static site guarding and mobile patrol services. Code of practice* offers guidance for the operation of a security control room.
- 69.5 Should the security control room (or guard house) act as a key holding facility and first response to an activated alarm system consideration should be given to BS 7984.
- 69.6 Doors, windows and glazing in masonry built guard houses must meet the same requirements as shown in the above relevant paragraphs.
- 69.7 It is recommended that purpose built modular build guard houses or other prefabricated buildings used for the purpose are certificated to LPS 1175: Issue 7, SR 1 or STS 202: Issue 3, BR 1 or higher depending on local risks.

### 70 Arson and fire protection

- 70.1 If arson is identified as one of the potential risk factors in an area the new industrial units or warehouses should be designed with arson prevention in mind. Architects should consult with the fire service and insurance specialists and it is deemed appropriate a sprinkler system should be installed.
- 70.2 Measures that the designer should consider to prevent arson include:
- Deterring unauthorised entry onto the site

- Preventing unauthorised entry into the building
- Reducing the opportunity for the potential offender to start a fire
- Reducing the scope for potential fire damage

70.3 Measures that the building occupier should consider to prevent arson include:

- Ensuring the designer's in-built measures are put into practice
- Reducing subsequent losses and disruption to business resulting from a fire by preparing a disaster recovery plan

70.4 The following places of special fire hazard have been identified as such either because of the activities in these places could provide opportunity for a fire or the place is or contains a valuable resource

- Boiler rooms
- Storage space for fuel or other highly flammable substances or chemicals
- Laboratories
- Other rooms with open heat sources
- Kitchens
- Oil filled transformer and switch gear rooms
- Rooms housing a fixed internal combustion engine

## 80 ARGUS: Professional

Project ARGUS Professional is aimed at encouraging architects, designers and planners to consider counter terrorism protective security measures within the built environment at the concept design stage. It encourages debate and demonstrates that counter terrorism measures can be designed into structures and spaces to create safer crowded places. It is fully supported by the various organizations associated with these professions.

## Undercrofts

### 90 Buildings with Undercrofts – recommended protective measures

90.1 Depending upon the nature of the building, its location and use, under-croft car parking can assist in the commission of a terrorist attack. It is therefore of paramount importance that the police Crime Prevention Design Advisor is notified at the earliest possible opportunity if there are plans to incorporate such a feature within a new development. It is probable that if the building is deemed to be 'at risk' that the CPDA will inform the Police Counter Terrorism Security Advisor (CTSA).

90.2 **In an ideal world the preferred advice would be not to construct buildings on top of under-croft parking areas;** however it is acknowledged that the availability of land and the increased expense of purchasing larger plots are not particularly viable options in the world of business. Where space is at a premium then consideration should be given to placing any parking in a single storey open environment above the main building structure. The blast effect would have less impact than with an under-croft design. However, if under-croft or 'stilts' design is to be pursued then the two points below **should be implemented as a matter of course if the CTSA has assessed the build as a Medium High/ High risk** and will assist to make these buildings safer:

90.2.1 It is recommended that the structure is enhanced to withstand a 100kg (TNT Equivalent) explosive device (VBIED) such that it has adequate resistance to disproportionate and progressive collapse and maintains lateral stability at all times all in accordance with the Approved Document part A, BS 5950 Structural Use of Steel in Buildings, and SCI report P244 Protection of Buildings against Explosions. The

flooring system should be designed such that it will resist the effects of blast uplift and is fully restrained to the horizontal structure in the event of load reversal including the provision of suitable peripheral and internal ties and maintains horizontal continuity across all lines of support. The location of the 'design basis device' should be noted as appropriate to the configuration of the building – i.e. inside the structural envelope for a situation where vehicle parking is below the retail space.

90.2.2 As recommended by the CPNI, where the primary means of pedestrian access and egress is through or near the parking area, the transit route should be designed in such a way as to provide a minimum of two routes all in accordance with the Approved Document Part B and BS9999; 2008 Code of Practice for Fire Safety in the Design, Management and Use of Buildings. The physical resilience of these two routes should be constructed so that following the design basis event at least one route will remain fully functional and accessible. This is to allow for emergency response to and evacuation of the retail/office area. It should be noted that the desired physical resilience of the access routes relates to the generated blast effects and not just the effects of fire.

The following points are offered as best practice and will enhance the recommendations above:

- The use of laminated glazing to all public areas adjacent to the car park area or within any potential blast area. Where there is existing glazing then the use of Anti-Fragmentation Film (AFF) should be installed.
- If the under-croft area is used for deliveries then the access point should have Access Control - consider deployment of active Vehicle Security Barrier solutions, procedures, long term operations management and emergency access.

- In addition, all staff should receive counter terrorism awareness briefings such as Project Argus and Project Griffin. Whilst this is not directly linked to the planning process

it will improve staff awareness and resilience of the site.

Where space allows within a new build design or an existing build then the recommendations below should also be considered:

- Traffic exclusion is the ideal in terms of ambitious and effective protection. On larger self-contained sites, car parking for both visitors and staff further away from a protected building can bring extra confidence through natural stand-off (*Note 90.2.2*). Covered walkways which are not typically provided in car park designs, or a park and ride facility depending on relative distances, may reduce any staff/public concerns.
- Traffic exclusion but with screening of any vehicles that are allowed in to the secure area is the next best option. Less than 100% screening or a random screening strategy increases risk. Off-site consolidation and screening facilities can offer multiple security benefits by reducing the number of vehicles that need to access a secure site and/or underground delivery and parking facilities within a development. This increases the confidence in any vehicle that does arrive at a site following security checks and releases valuable space inside the development. If screening is to be conducted on site then the ability to reject a vehicle without allowing it access to secure areas must be built into the design.
- Traffic inclusion into a large perimeter site is an option but typically would need to be coupled with individual protection around critical and/or vulnerable assets to provide some standoff.

*Note 90.2.2: Blast stand-off is used to keep a potential VBIED away from a protected asset thus limiting the damage caused by blast effects. Adequate blast stand-off distance can be enforced through the use of physical barriers and effective traffic management. See the link on the NaCTSO website under Threats/ VBIED for more information: <http://www.nactso.gov.uk/threats>.*



# GLOSSARY OF TERMS

## Architectural Liaison Officer

Specially trained police officers or police staff, employed by police forces to administer the Secured by Design initiative on behalf of the Police Service. This is the same role as Crime Prevention Design Adviser (CPDA). The term CPDA is used throughout the SBD guides.

## Easily Accessible

Easily accessible windows (or doorsets) are those that can be accessed via a flat roof, balcony or other similar structure e.g. external supporting or decorative balcony detail. Also means that access can be gained by two persons (one climbing, one assisting) without the use of a climbing aid, such as a ladder.

## Certification (of products)

Independent, ongoing third party surveillance of the manufacturing process of security tested products, such as doors, windows and shutters, which includes periodic sample re-testing and factory audits to ensure consistency in manufacture. Independent certification by an accredited organisation is a vital requirement of the SBD project.

## Crime Prevention Design Adviser (CPDA)

Specially trained police officers or police staff, employed by police forces who administer the Secured by Design initiative on behalf of the Police Service. This is the same role as Architectural Liaison Officer (ALO). The term CPDA is used throughout the SBD guides.

## Defensible Space

An environment where the physical characteristics allow the legitimate occupiers to assert influence and control to ensure their security. Secured by Design recognises the benefit of spaces that are recognisably private in nature, as such spaces promote a sense of ownership and responsibility by the people who live and work in them. *Further reading: Design Guidelines for Creating Defensible Space. Oscar Newman*

## Natural Surveillance

An architectural design that limits the opportunity for crime by enhancing the chance that a potential offender might be or will be seen. The effectiveness of such measures relies on witnesses reacting to and or reporting what they have seen to others to enforce the law and the potential offender's expectation of such a reaction.

## ParkMark®

Safer parking status, ParkMark®, is awarded to parking facilities that have met the requirements of a risk assessment conducted by the police. These requirements mean that the parking operator has put in place measures that can help deter criminal activity and anti-social behaviour. The scheme is managed by the British Parking Association. Further information is available at [www.britishparking.co.uk](http://www.britishparking.co.uk)

## Secured Environments

Secured Environments is a police certification scheme. It is awarded to organisations that are able to show that they have adopted key principles for protecting themselves against crime. The scheme is administered by Perpetuity Research and Consultancy International Ltd on behalf of Secured by Design. Further information is available at [www.securedenvironments.com](http://www.securedenvironments.com)

## Sold Secure

A test and certification body, owned by the Master Locksmiths Association, which accredits security products. Typically, products are graded bronze, silver or gold.

## Terrorism

The use or threat of a specified action where the use or threat is designed to influence the government or to intimidate the public or a section of the public, and the use or threat is made for the purpose of advancing a political, religious or ideological cause. The action is a specified action if it involves serious violence against person; involves serious damage to property; endangers a person's life, other than



the person committing the action; creates a serious risk to the health or safety of the public; or is designed seriously to interfere with or disrupt an electronic system *Section 1 The Terrorism Act 2000*

## **UKAS**

The United Kingdom Accreditation Service. The sole national accreditation body recognised by government to assess, against internationally agreed standards, organisations that provide certification, testing, inspection and calibration services.

The authors of the SBD guidance documents are always ready to receive and respond to constructive criticism and if necessary make alterations to the guidance providing this is based upon evidence. Should you wish to contribute towards this or any of the Secured by Design guides please contact our head office by email to [guides@acpo-sbd.co.uk](mailto:guides@acpo-sbd.co.uk)

# References

## Publications

BREEAM UK New Construction: Non-domestic Buildings  
Technical Manual: SD5076: 2.1

CCTV Operational Requirements Manual

Design and access statements

Guidance on changes to the development control system

National Planning Policy Framework

National Planning Practice Guidance

PAN 77 Designing safer places

TAN12 Design 2009

Safer places: a counter-terrorism supplement

## Published by:

2014 BRE Global Ltd

2009 HOSDB

2012 DCLG

2012 DCLG

2012 Home office

2014 Home office

2006 Scottish Executive

Welsh Assembly Government

2009 Home Office

## Legislation

Equality Act 2010

Countryside and Rights of Way Act 2000

## Changes made in Version 2:

Page 33: Note 1.17 changed to 43.17

Page 40: Note 1.5 changed to 51.5

Page 43: Note 56.5 changed to 56.6

Page 43: New text added to Note 56.6: “Any documentation submitted as proof of compliance should clearly show the certification body name and the manufacturer/fabricator of the product installed within the development. Documentation that is provided bearing the name of a component or system manufacturer will not be deemed acceptable.”

Page 48: New text added to Note 62.5: “Any documentation submitted as proof of compliance should clearly show the certification body name and the manufacturer/fabricator of the product installed within the development. Documentation that is provided bearing the name of a component or system manufacturer will not be deemed acceptable.”

**Secured by Design**



**Official Police Security Initiative**

**Secured by Design**

First Floor, 10 Victoria Street

London SW1H 0NN

**Telephone:** 0207 084 8962

**Email:** [generalenquiries@acpo-sbd.co.uk](mailto:generalenquiries@acpo-sbd.co.uk)

[www.securedbydesign.com](http://www.securedbydesign.com)