PAS 69:2013

BSI Standards Publication

Guidance for the selection, installation and use of vehicle security barrier systems

bsi.

...making excellence a habit.™

Publishing and copyright information
The BSI copyright notice displayed in this document indicates when the document was last issued.

ISBN 978 0 580 81203 3

ICS 93.080.30

Publication history
First published December 2006
Second (current) edition August 2013

Amendments issued since publication

Date	Text affected

Contents

Summary of pages
This document comprises a front cover, an inside front cover, pages i to iv, pages 1 to 39, an inside back cover and a back cover.

This page deliberately left blank

Foreword

This PAS was sponsored by the UK Government's Centre for the Protection of National Infrastructure (CPNI). Its development was facilitated by BSI Standards Limited and published under licence from the British Standards Institution. It came into effect on 31 August 2013.

Acknowledgement is given to the following organizations that were involved in the development of this guide as members of the steering group.

- Allen Fencing Limited
- ATG Access
- Bavak Security Group
- Building Research Establishment (BRE)
- Centre for the Protection of National Infrastructure (CPNI)
- D.J. Goode and Associates Limited
- MFD International Limited
- MIRA Limited
- Perimeter Security Suppliers Association (PSSA)
- Transport Research Laboratory (TRL).

Acknowledgement is also given to the valuable contribution made by those organizations that reviewed the working drafts of PAS 69 and who submitted comments for consideration.

Supersession

This PAS supersedes PAS 69:2006, which will be withdrawn on publication of this PAS.

Information about this document

PAS 69 has been updated and extended in the light of recent industry developments and changes to good practice for the installation, selection and use of vehicle security barriers.

This PAS is not to be regarded as a British Standard. It will be withdrawn upon publication of its content in, or as, a British Standard.

The PAS process enables a document to be rapidly developed in order to fulfil an immediate need in industry. A PAS may be considered for further development as a British Standard, or constitute part of the UK input into the development of a European or International Standard.

Relationship with other publications

PAS 68 was originally developed alongside PAS 69 and is an impact test specification for vehicle security barriers.

An international workshop agreement (IWA) is currently in development for the International Organization for Standardization (ISO) that covers similar content to PAS 68 and PAS 69. However, both PAS 68 and PAS 69 are well-established in the UK and they are being revised to meet immediate industry requirements and developments in the vehicle secure barrier (VSB) industry since their last publication.

Presentational conventions

The guidance in this standard is presented in roman (i.e. upright) type. Any recommendations are expressed in sentences in which the principal auxiliary verb is "should".

Commentary, explanation and general informative material is presented in smaller italic type, and does not constitute a normative element.

Contractual and legal considerations

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

Compliance with a PAS cannot confer immunity from legal obligations.

Particular attention is drawn to the following specific Acts:

- The Data Protection Act 1998 [1];
- The Equality Act 2010 [2].

Introduction

The purpose of PAS 69 is to provide guidance on the effective specification and implementation of vehicle security barrier (VSB) systems. It has been developed with the intention of being used by security practitioners such as project managers, planners, architects, civil engineers, VSB designers, installers, security managers and facilities managers within the public and private sectors.

PAS 69 has been developed to complement PAS 68, *Impact test specifications for vehicle security barriers*, which addresses the needs of organizations requiring VSB systems with a specific level of resistance to hostile vehicle impact.

PAS 69 highlights the numerous issues to be addressed when considering the implementation of VSB systems as part of a holistic security system. The topics considered are by no means exhaustive, and the practitioner is encouraged to consider additional questions and responses to cater for specific requirements.

A holistic security system is likely to require integration of a VSB system with one or more security features including: pedestrian perimeter barriers, building fabrics, perimeter intruder detection systems (PIDS), intruder detection systems (IDS), access control, CCTV and security lighting. All of these features require appropriate management throughout their life cycle and are directed by clearly defined security procedures.

The mitigation of all vehicle-borne threats whilst maintaining all other needs can be difficult, especially when numerous project constraints are applied. Competing needs and the requirement to ensure fully integrated security can compromise the effectiveness of individual elements. In order to achieve an integrated system it is imperative from the outset to define the requirements of the site in terms of security and operational performance. This is where careful thought and production of an operational requirements document (OR) can add significant value to the whole process, from specification through to installation, commissioning, implementation and planning for future threats.

This edition of PAS 69 introduces the concept of a VSB system scoping document, based on the OR, which can be used by security practitioners to analyse and compare the precise design and functionality of each proposed VSB system.

1 Scope

PAS 69 provides information and guidance for the selection, installation and use of vehicle security barrier (VSB) systems deployed to mitigate threats from vehicle-borne attack as part of a holistic security system.

NOTE The detailed process of producing operational requirements is given in the CPNI documents, Guide to producing operational requirements for security measures *[3] and* Level 2 operational requirements for hostile vehicle mitigation measures *[4]. A VSB scoping document that can be used by security practitioners to compare and contrast proposed VSB solutions from suppliers is given in the CPNI document,* Vehicle security barrier scoping document *[5].*

2 Normative references

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

PAS 68, *Impact test specifications for vehicle security barrier systems*

3 Terms and definitions, and abbreviations

3.1 Terms and definitions

For the purposes of this PAS, the terms and definitions given in PAS 68 and the following apply.

3.1.1 operational requirements document (OR)
statement of needs based upon a thorough and systematic assessment of the problems to be solved and the desired solutions

3.1.2 blast stand-off distance
defined distance between a critical asset and the enforceable secure perimeter

3.1.3 secure area
area surrounded by a secure perimeter

3.1.4 secure perimeter
boundary consisting of one or more physical security features (e.g. pedestrian perimeter barrier combined with one or more VSB systems)

*Note See also **11.2**.*

3.1.5 site
location within which a secure area could be situated

3.1.6 traffic calming
intelligent highway design or deployment of physical measures on the highway such that vehicles are encouraged to reduce speed

3.1.7 traffic management
segregation, guidance and diversion of vehicles to help mitigate potential hazards, reduce congestion and enhance the safety of road users and personnel working close to, or on, the highway

3.1.8 vehicle

3.1.8.1 hostile vehicle
vehicle used with malicious intent to access a secure area or deliver an explosive device

3.1.8.2 legitimate vehicle
vehicle which has been permitted access to a secure area not being directly used with malicious intent to access a secure area

3.1.9 vehicle security barrier (VSB) system
physical vehicle barrier, operating mechanism, power source and associated controls used to prevent or control vehicle access

3.2 Abbreviations

For the purposes of this PAS, the abbreviations given in PAS 68 and the following apply.

AACS	automatic access control system
ANPR	automatic number plate recognition
CAD	computer aided design
CCTV	close-circuit television
GPR	ground penetrating radar
HVM	hostile vehicle mitigation

IDS	intruder detection system
IED	improvised explosive device
MO	modus operandi
O and M	operation and maintenance
OR	operational requirements document
PC	personal computer
PCB	printed circuit board
PIDS	perimeter intruder detection system
PLC	programmable logic controller
UPS	uninterruptible power supply
VACP	vehicle access control point
VBIED	vehicle borne improvised explosive device
VDA	vehicle dynamics assessment
VRM	vehicle restraint measure
VSB	vehicle security barrier

4 Vehicle restraint measure (VRM)

4.1 General

Vehicle restraint measure (VRM) is a term used to describe any physical feature or system that is employed to influence driver behaviour or affect their vehicle movement, such as:

- horizontal deflections (e.g. corners or chicanes);
- traffic control barriers (e.g. for car park control);
- road kerbs;
- earthworks (e.g. ditches and bunds).

A VRM could have a minor effect on vehicle speed or direction if struck, but should be considered ineffective against determined encroachment or penetrative vehicle attack.

Security threats have encouraged the rapid development of VSB systems. Under the umbrella term VRM, VSB systems can also be split into three categories (see **4.2** to **4.4**).

4.2 Access control

Access control VSB systems are used to control the movement of vehicles and are typically used as revenue control systems, e.g. at a public car park. These types of barrier tend not to have any structural resilience for prevention of unauthorized vehicle access, tamper or vandalism.

4.3 Anti-ram

Anti-ram VSB systems are often used at sites where it is necessary to control the movement of vehicles and also to deter and provide delay to vehicle-borne attack at the site perimeter. These types of barrier typically appear structurally robust though they might or might not have been tested against vehicle impact. These systems typically take the form of bollards, road blockers or heavy duty gates.

4.4 Counter-terrorist

Counter-terrorist VSB systems aim to mitigate both terrorist and criminal threats from vehicle-borne attack. The majority of these VSB systems are designed to be structurally resilient to vehicle impact and aim to provide enforcement to traffic calming as well as deterrence and delay to determined hostile vehicle attack. These VSB systems are typically deployed at sites deemed to be critical to national infrastructure. They are increasingly used in crowded places, transport interchanges, military and foreign locations.

NOTE Further information regarding protection against terrorism and business continuity can be found in the following publications: Pursue, prevent, protect, prepare – The United Kingdom's strategy for countering international terrorism *[6],* Protecting against terrorism *[7],* Secure in the knowledge – Building a secure business *[8]*, Expecting the unexpected – Business continuity in an uncertain world *[9].*

5 Types of VSB system

5.1 General

A VSB system stops encroachment and penetrative vehicle-borne attack. A VSB system is structural in nature and can be passive (static, fixed, not operable, but can be moved or removed manually; see **5.2**) or active (moving, operable either manually or powered; see **5.3**). VSB system designs are continually being developed, resulting in the availability of a wide range of products with different specifications.

For new build developments in the public realm, VSB system selection should be incorporated at the initial design stage so that the VSB systems can be fully integrated from the outset. A balance should be struck between proportionate security measures, and, for example, the needs of the local businesses and functionality of public space.

NOTE Further information regarding VSB system design can be found in the CPNI publication, Integrated security – A public realm design guide for hostile vehicle mitigation *[10],* Vehicle security barriers within the streetscape *[11]. See also the CPNI and DfT traffic advisory leaflet,* Bollards and pedestrian movement *[14].*

Bespoke VSB systems can be integrated into public sites, and often they can be developed to be multi-functional. Examples include:

1) integrated street furniture;
2) decorative, structural or energy-absorbing planters;
3) strengthened light-weight structures;
4) shrouded or cosmetically clad bollards;
5) landscaping features.

If practicable, a design that includes only passive VSB systems that restrict all vehicle access is preferable as it automatically removes threats to the site from deception, duress, tailgating or tampering with control apparatus. There are also other operational benefits, including: reduced maintenance costs, fewer operators and a lower risk of accidental misuse.

5.2 Passive VSB systems

5.2.1 General

Passive VSB systems include the following:

a) earthworks (e.g. ditches or bunds);
b) bollards (e.g. fixed or removable);

c) planters;

d) integrated streetscape elements (e.g. seating, walls, balustrades);

e) wire-rope fencing;

f) re-deployable barriers (e.g. modular units that can be built up to the required dimensions).

Some of these passive VSB systems are discussed in more depth in **5.2.2** to **5.2.6**.

5.2.2 Earthworks

There might be naturally formed barriers located around a site that could be used as part of a secure perimeter. Natural barriers include: rivers, ponds, lakes, densely-wooded areas, steep slopes or changes in ground level that either divert attack or that preclude vehicle passage.

Where these features do not naturally occur, it might be feasible to engineer them. The recommended solutions are to construct a ditch or a bund, or a combination of the two. These are often preferred solutions due to:

- cost (simple designs reduce costs for long perimeters);
- availability of local materials or lack of production facilities (e.g. in remote locations);
- ground conditions (e.g. underground services preclude excavation for VSB system foundation construction); and
- architectural advantage (e.g. to blend in with the landscape).

5.2.3 Ditches

A ditch can prevent or delay a hostile vehicle from gaining access to a secure area. Assuming that the ground level is equal on either side of the ditch, the speed required for a vehicle to successfully traverse the ditch increases in proportion to the ditch width.

The approach to a ditch should be rendered smooth and, wherever practicable, include a downhill slope leading to the ditch. If the approach to the ditch is uneven, there is potential for the vehicle suspension to compress on approach and then rebound. If this happens just before reaching the front edge of the ditch, launching of the vehicle occurs, taking the vehicle up and across the ditch.

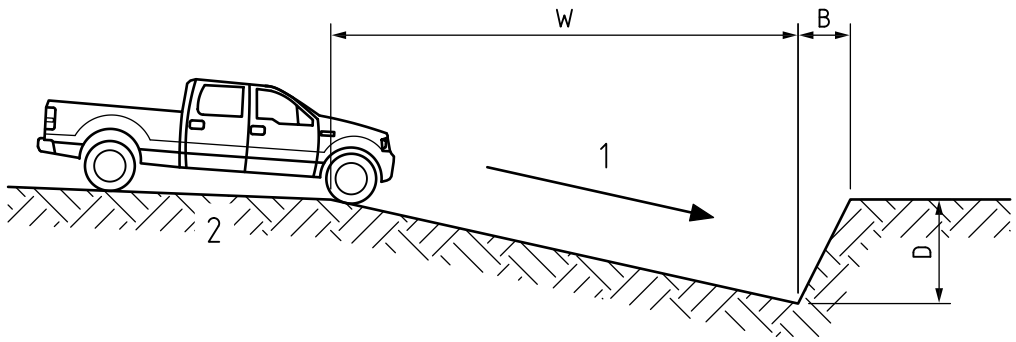
If the ditch is too narrow, on approach, the suspension and wheels might drop down into the ditch but the main vehicle body would not have time to react and fall. As the vehicle traverses, the dropped suspension could allow the wheels to contact the back face of the ditch and compress, allowing the vehicle to cross the ditch without effect or restraint.

NOTE 1 The suspension characteristics of 4x4 vehicles play an important role in the vehicle's ability to traverse a ditch. A shallow entry "V" ditch, as shown in Figure 1, offers the optimum ditch protection against an attack from a 4x4 hostile vehicle.

A ditch is specified by the following dimensions (see Figure 1 and Figure 2):

- *ditch width (*W*)*. This should be measured from the front edge of the ditch where the down-slope begins, to the bottom of the back face;
- *back face (*B*)*. This should be sufficiently steep angled at a minimum of 50°, as measured at a horizontal from the lowest point of the ditch. such that a vehicle cannot continue to drive up and out of the ditch;
- *ditch depth (*D*)*. This should be measured as the depth of ditch below ground level and should be a minimum of 1.25 m.

Figure 1 **"V" ditch profile**



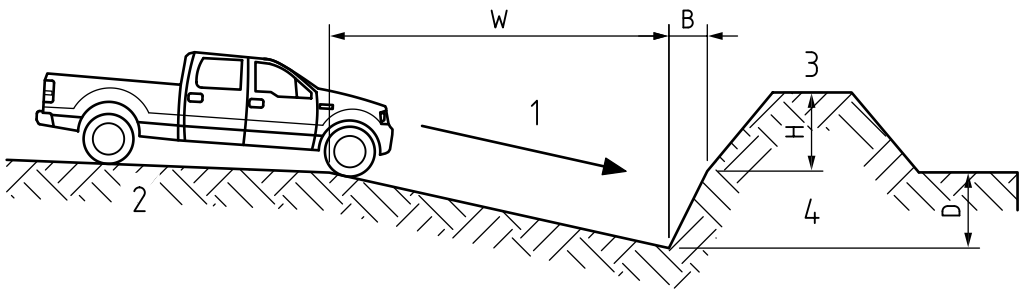
Key

1 Vehicle path
2 Graded negative slope
W Ditch width
B Back face
D Ditch depth

The ability of the ditch design to mitigate against hostile vehicle attacks can be further improved by introducing a graded negative slope and a bund of appropriate dimensions (see **5.2.4**). Constructing a graded negative slope on the approach side introduces a shallow slope, which helps to draw the hostile vehicle down into the ditch. Constructing a bund of appropriate dimensions to the defence side (see Figure 2) presents a raised level to a hostile vehicle on the approach side of the ditch. The bund increases the chance of vehicle impact, minimizing penetration and preventing encroachment.

NOTE 2 A bund can be constructed using material excavated from a ditch, therefore minimizing the need to ship material to or from the site.

Figure 2 **"V" ditch with bund**



Key

1 Vehicle path
2 Graded negative slope
3 Berm
4 Bund
W Ditch width
B Back face
H Height of berm from ground level
D Ditch depth

The ditch profile dimensions should be determined by an assessment of the following:

a) *hostile vehicle type:* this would determine the hostile vehicle's ability to drive across rough terrain, steep gradients and traverse ditches;

b) *surface characteristics:* these affect a hostile vehicle's ability to traverse the terrain approaching the ditch (especially larger hostile vehicles);

c) *approach speed:* a hostile vehicle might have little space in which to manoeuvre or accelerate on approach to the ditch. The maximum approach speed for each hostile vehicle should be assessed by undertaking a vehicle dynamics assessment (VDA);

d) *soil characteristics:* local soil characteristics might also affect the practicability of constructing the ditch to the recommended dimensions;

NOTE 3 Ditch *profiles with steep faces might also require fortification or stabilization.*

e) *site space:* the physical footprint and space required to construct a ditch is relatively large in comparison with other VSB systems.

5.2.4 Bunds

By itself, a well-designed bund can prevent hostile vehicle encroachment by presenting a raised, steep-angled profile. This causes an encroaching vehicle to:

a) engage the front overhang of the vehicle body with the bund front face;

b) engage the rear overhang of the vehicle body with the ground level;

c) lose traction when attempting to climb up the front face; and

d) ground the underside of the chassis when surmounting the top of the bund.

A minimum front face angle of 50° should be maintained. The height of the berm from ground level (see Figure 2, H) should be a minimum of 1.25 m. Bund designs should be selected that take into account the following local material (soil) properties and environmental conditions:

1) *compaction:* consolidation of soil (under its own weight) over time;

2) *erosion:* removal or displacement of solids through weathering, vegetation or the activity of local wildlife; and

3) *slump:* gravity causing the sliding of materials down the front face of a bund.

The use of cellular geo-textile materials can be employed to support and stabilize the main body of the bund.

5.2.5 Trees

The use of individual trees as a VSB is not generally recommended. This is because full-scale impact testing has shown that even mature trees of similar dimensions to a VSB system do not perform well against a determined hostile vehicle impact.

Where an existing tree cannot be moved and forms part of the physical perimeter (thereby acting as a VSB system), an acceptable level of the following elements should be determined and regularly checked:

a) the health of the tree (including inspection for evidence of deliberate tamper such as pre-cutting that could aid a penetrative vehicle attack);

b) the stability of local ground conditions around the tree roots;

c) the length of the branches;

NOTE Long branches can act as climbing aids (e.g. over a perimeter fence) and therefore the frequent trimming and cutting of branches is important.

d) the clear lines of sight for security guards and CCTV surveillance.

Where areas of forest or other densely-packed trees are present, then the combined resistance is likely to be more effective against determined hostile vehicle impact. Furthermore, any gaps between trees might only need infill VSB systems to prevent a slow speed encroachment attack.

5.2.6 Pedestrian perimeter barriers

Pedestrian perimeter barriers (e.g. security fences) provide a physical demarcation for a secure area and provide a measure of deterrence and delay to criminal activity. They can also be used as the means of supporting perimeter intruder detection systems (PIDS) such as motion sensors.

NOTE Conventional security fences (designed to deter or to delay climb or cut attack) provide very limited protection against penetrative vehicle-borne attack.

A 4x4 pick-up is able to breach a variety of security fences (performance rated for climb or cut attack) with ease, and at relatively low speeds [security fences have been breached by vehicle impact at speeds lower than 16 kph (10 mph)] in comparison to VSB systems that have typically been designed to mitigate against a penetrative vehicle impact at 48 kph (30 mph) or more.

Pedestrian perimeter barriers should not be relied on as the only HVM measure and other means of preventing or delaying hostile vehicle access should also be considered and implemented. However, where there is limited space for vehicles to accelerate up to a fence boundary or where the terrain restricts maximum vehicle speed, an assessment might indicate that a conventional pedestrian perimeter barrier is an appropriate HVM measure.

5.3 Active VSB systems

In order to control vehicle access, an active VSB system should be selected and installed.

NOTE 1 The term "active" refers to the system's ability to operate from closed access (secure) to open access. See also PAS 68 for definitions of active and passive VSB systems.

Active VSB systems can include:

a) retractable bollards;

b) retractable blockers;

c) folding, sliding, swinging, rising-arm gates.

NOTE 2 Further information regarding retractable VSB systems can be found in the CPNI publication, Retractable vehicle security barriers – Maintaining road surface friction *[12].*

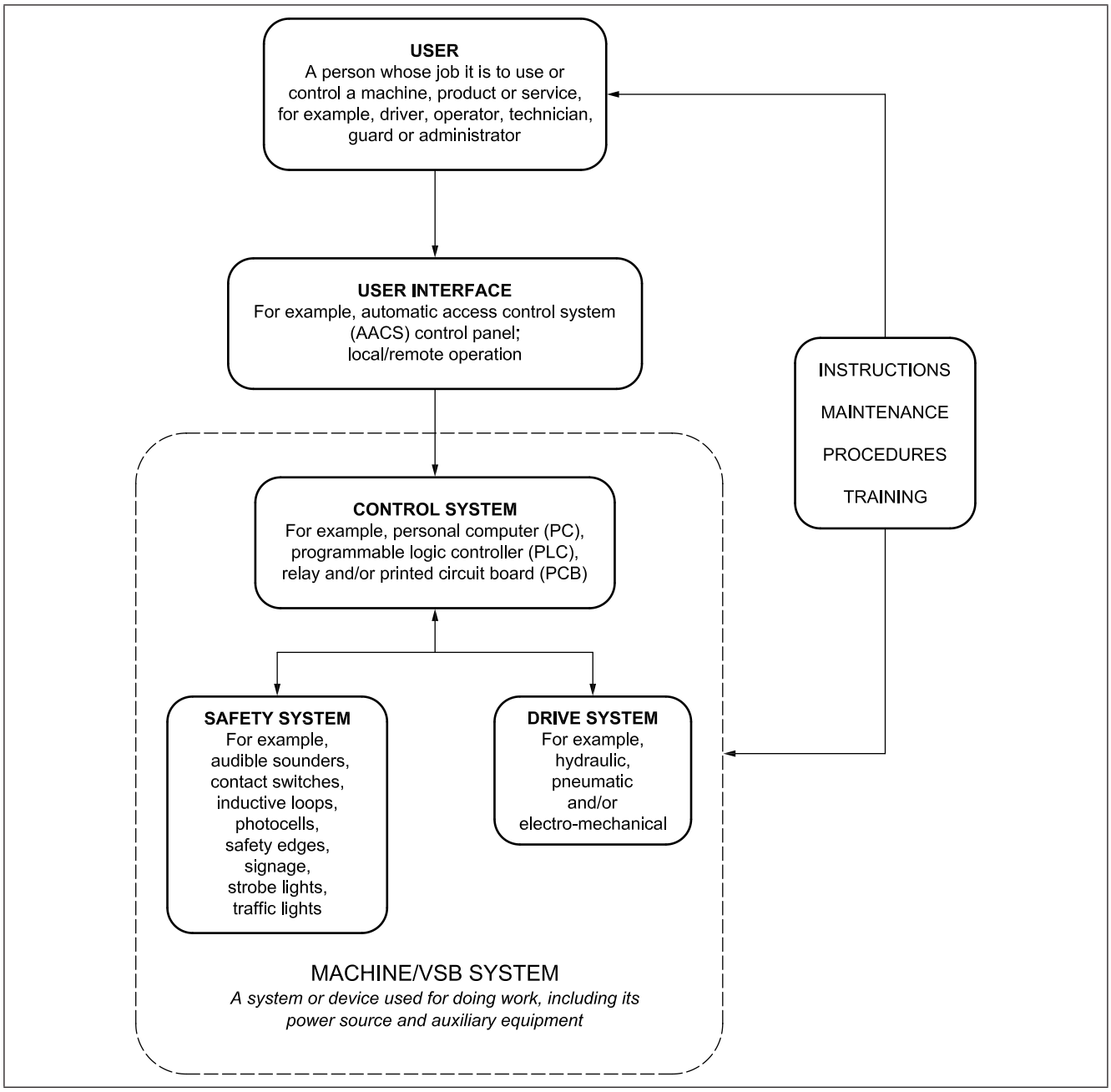
An active VSB system can be either manually operated or powered by an external source (hydraulic, pneumatic, electric). Although manual and powered VSB systems might look very similar and perform equally well under vehicle impact, there are often significant differences in their respective whole life costs. Such whole-life costs take into consideration installation, set up, operation and on-going maintenance.

A powered VSB system, by the nature of its design, should be considered to be machinery and therefore should be designed, maintained and operated accordingly. Figure 3 highlights the common elements of an active VSB system and machinery.

Drainage from a retractable VSB system might be required to maintain its operation and prevent blockage due to detritus. It is important to be aware of the drainage discharge point to prevent contaminants from having a negative impact on the environment.

When the controls cannot be located within a secure area, it is important to check the security of the VSB system control box. Increased distance between the control pumps and a VSB system might impact on the design of the control mechanisms and might offer tamper opportunities.

Figure 3 **Commonalities between an active VSB system and machinery**



As with machinery, a VSB system should be selected not only on the basis of performance or operational requirements (see **6.1**), but also cost. An analysis of the full cost of a VSB system should be made during, or prior to, the selection process. The cost analysis should include post-installation costs and the cost of long-term requirements such as:

1) training;
2) service requirements;
3) maintenance and repairs; and
4) spare parts.

6 Selection and installation of VSB systems for HVM

6.1 General

The selection and implementation of a VSB system that can be used effectively as part of an HVM scheme is dependent on, but not limited to, the following factors:

a) a critical asset assessment (see Clause **7**);

b) a threat assessment, including the predicted effects of explosions and blast (see Clause **8**);

c) a site assessment (see Clause **9**);

d) the design and management of the vehicle access control point (VACP) (see Clause **10**);

e) the required performance of the VSB system (see **10.9**);

f) the deployment and removal of the VSB system (see Clause **11**); and

g) the procurement strategy (see Clause **12**).

The OR can also be used to facilitate the development of a business case to justify the need to deploy a VSB system.

It can be difficult to mitigate all forms of vehicle-borne threat whilst satisfying all other requirements. When selecting a VSB system, the requirements and constraints given in **6.2** to **6.4** should be assessed as a minimum, in the form of an OR. The OR should be produced with input from key stakeholders (e.g. site owner, site operator, security and safety representative, project manager) early on in the design process. It should be reviewed at regular intervals as defined by the site owner or operator, or when a change in threat has been identified.

NOTE The detailed process of producing operational requirements is given in the CPNI documents, Guide to producing operational requirements for security measures *[3] and* Level 2 operational requirements for hostile vehicle mitigation measures *[4]. A VSB scoping document that can be used by security practitioners to compare and contrast proposed VSB solutions from suppliers is given in the CPNI document,* Vehicle security barrier scoping document *[5].*

6.2 Security requirements

The following should be assessed:

- attack method(s) to be mitigated;
- enforceable blast stand-off distance;
- procedural controls (e.g. vehicle searches or identity checking);
- proportionate HVM measures;
- potential response to increased threat; and
- level of residual risk deemed acceptable by the organization.

6.3 Engineering constraints

The following should be assessed:

- foundation-related constraints;
- buried services (e.g. water utilities, power utilities, communications services);
- planning restrictions;
- architectural constraints;
- ownership (i.e. of the land or buried services);
- space available.

6.4 Management and control

The following should be assessed:

- lifecycle cost (e.g. training, manning levels, service, maintenance and replacement);
- VSB system reliability (e.g. the potential for components to fail or malfunction and associated maintenance of these components);
- access controls;
- traffic management;
- safe use of the VSB system (e.g. the potential for deactivation as a result of accident).

7 Critical asset assessment

7.1 General

The critical assets within the site should be identified and located (see **7.2**). These critical assets should be prioritized based on each element's contribution, as defined by the relevant stakeholder (see **7.3**), to the continuing operation of the business and the consequences of damage or loss (see **7.4**). Such information can be used to inform the selection and positioning of a VSB system.

7.2 Critical assets

The critical asset(s) to be protected should be identified and ranked in order of priority, based on business needs. Critical assets can include, but are not limited to:

- people (e.g. staff, visitors, contractors, customers);
- physical assets (e.g. buildings, contents, equipment, machinery);
- information (e.g. IT systems, transactions systems, paper/electronic data);
- processes (e.g. supply chains, critical procedure or production cycles).

NOTE It might be necessary to identify other locations or critical assets that could become alternative targets as a result of a successful security strategy.

7.3 Stakeholders

Contact information for all stakeholders who might be affected by the proposed security measures should be identified and obtained. These might include, but are not limited to:

- staff;
- deliveries;
- local authorities;
- private and public transport providers;
- emergency services and responders;
- utility companies;
- neighbours;
- landlords.

NOTE 1 Early identification of and coordination with stakeholders is critical to understanding the broader security picture. It can also influence decision-making and increase support for any significant physical or operational changes to the local surroundings.

NOTE 2 Attention is drawn to the Data Protection Act [1].

7.4 Consequences of damage or loss

The likely consequences of a successful hostile vehicle attack can be measured using a number of parameters:

- personal injury and loss of life;
- financial cost to repair or replace critical assets;
- service delays, reductions or stoppages;
- reputational damage and loss of stakeholder confidence.

In addition to the direct consequences of vehicle-borne attack, security practitioners should also consider collateral physical damage and the long-term consequences to their business. These have the potential to extend beyond the immediately apparent short term consequences. To deal with this, the following actions may be undertaken:

a) the point of challenge (of a hostile vehicle) may be positioned away from critical assets (see **7.2**) or key components of the wider security scheme;

b) vulnerable areas may be protected from blast or vehicle attack;

c) a contingency plan, including the accessibility of spares and an alternative site designed to enable the business to continue to operate. Such a plan should take into account interconnected organizations and the resultant effect on their business or operation.

8 Threat assessment

8.1 General

In order to ascertain the performance required from a VSB system, a thorough assessment of the perceived threat to a secure perimeter should be undertaken.

This threat assessment should include the following:

a) research of previous threats (see **8.2**);

b) likely forms of attack [modus operandi (MO)] (see **8.3**);

c) perceived hostile vehicle(s) (see **8.4**);

d) duration of deployment, potential changes in threat and subsequent response (see **8.5**); and

e) explosions and blast effects (see **8.6**).

8.2 Research of previous threats

Any recent terrorist, criminal or malicious activities should be researched. This research should be used when assessing the relevance of such threats, the reasons for targeting a specific location and the methods used.

NOTE Further information regarding terrorist, criminal or malicious activities can be obtained from the local police or the National Counter Terrorism Security Office (NaCTSO) (http://www.nactso.gov.uk/). Such organizations can refer security practitioners to the appropriate adviser, such as a counter terrorism security adviser (CTSA).

8.3 Hostile vehicle modus operandi (MO)

8.3.1 Main methods of vehicle-borne attack

Vehicle-borne threats range from vandalism to sophisticated or aggressive attacks by criminals and terrorists. The mobility and payload capacity of a hostile vehicle can offer a convenient delivery mechanism for an explosive device. Hostile vehicles can be parked, manoeuvred or rammed into or out of a target site.

Hostile vehicle entry to, or exit from, a site can involve surreptitious tampering with a VSB system or its control apparatus, or the targeted placement of small explosive charges to breach the integrity of a VSB system. There are five main methods of vehicle-borne attack that could be attempted with, or without, suicide operatives. These are detailed in **8.3.2** to **8.3.6**.

8.3.2 Parked vehicle-borne improvised explosive device (VBIED)

This is where a VBIED is parked as close to its intended target as is practicable, in order to cause the maximum damage when detonated.

Parking for unscreened vehicles in close proximity to, or in underground parking facilities beneath, a critical asset can pose significant problems; as these areas are often outside of the secure perimeter.

It is important for guard surveillance and patrols to be equally attentive towards all vehicles, including those familiar to the site and any that have been seen repeatedly in close proximity to the secure perimeter.

8.3.3 Encroachment

Encroachment is where a hostile vehicle negotiates through an incomplete perimeter without the need for impact.

A dilemma exists in the design of a VSB system where pedestrian access is also required. This is because gaps wide enough to cater for pedestrians, including those with mobility and disability needs can also allow clear access for narrow hostile vehicles such as bicycles or motorbikes. Site designers can employ procedural and vehicle access policies that help to identify and mitigate threats of this form.

An alternative form of encroachment is a hostile vehicle tailgating a legitimate vehicle through an active barrier at a VACP. The only effective way of countering this MO is by the use of an interlock VACP (see **10.4.3**), which uses two consecutive lines of VSB systems.

8.3.4 Penetrative attack

Penetrative attacks use the front or rear of a vehicle to ram a secure site and gain entry. They have been used for criminal activity and in terrorist attacks to breach building facades or a VSB system at targeted critical assets. The analysis of likely hostile vehicle type in terms of their structure, mass, velocity, manoeuvrability and load-carrying capacity can directly affect the VSB system selection and design of a VSB system.

8.3.5 Deception

The choice of vehicle and driver by those with hostile intent can prevent it from being challenged. Deception techniques rely on the erroneous human perception of a hostile situation. Such techniques can include the use of a Trojan vehicle to gain access (i.e. the use of a vehicle whose model, livery or registration is familiar to the site and is therefore assumed to be legitimate, while in reality it is being

used with malicious intent), or by hostile occupants gaining access beyond a VACP by pretence or by using stolen (or cloned) access control or ID passes.

Other deception scenarios can include using a driver as a mule to unknowingly deliver an improvised explosive device (IED) planted in their vehicle, or an insider bringing an IED in to the secure area.

8.3.6 Duress

Duress against the driver of a legitimate vehicle who is forced to carry a hostile person or device, or duress against a security guard controlling a VACP are perhaps the most difficult forms of vehicle-borne attack MO to mitigate.

Risk management strategies include removing control of an active VSB system from a security guard at the VACP, and instead relying on remote access control via a secure control room that has CCTV oversight of the VACP. Or excluding all vehicle access to a secure area by installing only passive VSB systems. Vehicle searches and confirmation of occupant identity may also be used to mitigate duress against drivers of authorized vehicles.

8.3.7 Other attack methods

Other attack methods can include the following.

a) *Layered attacks*. These use two or more hostile vehicle attack MOs. For instance, one vehicle might be used to create a gap in defences by way of penetrative attack, which subsequently enables a second VBIED to encroach beyond the defence line.

b) *Person-borne, surreptitious or forced attack*. This might be surreptitious tampering (physically or electronically) with an active VSB system or its control apparatus in order to open a VSB or to compromise its ability to resist penetrative attack. Forced attack is through the use of tools (e.g. levers, cutting tools) to cause physical damage in order to weaken or disable the VSB system.

c) *Explosive charges*. Targeted placement of explosive charges might be used against VSB systems (passive or active) to damage or remove structural elements. Explosive charges might be placed to specifically damage a locking mechanism, hydraulics or power supply of an active VSB system, or to breach the integrity of any VSB system.

8.4 Hostile vehicle

8.4.1 Identifying the hostile vehicle

Determining the qualities of the anticipated hostile vehicle can affect the choice of a VSB system or its implementation. Once perceived attack method(s) have been identified, the hostile vehicle should be classified in terms of:

- type or class;
- dimensions; and
- performance.

8.4.2 Modified vehicles

8.4.2.1 General

Hostile vehicles might be modified to aid an attack. Modifications vary and might include those given in **8.4.2.2** to **8.4.2.4**. The result of such hostile vehicle

modifications might influence the design and/or selection and implementation of a VSB system.

NOTE A detailed vehicle inspection might be required to confirm suspicion of a hostile vehicle. Security guard capabilities and the time needed to perform a detailed investigation might need to be considered when designing and/or selecting a VSB system.

8.4.2.2 Cosmetic modifications

Cosmetic modifications might include:

- modifying a vehicle body or container to hide an IED or weaponry so that items cannot be seen by passers-by or security guards;
- concealing a hostile payload within a legitimate vehicle, thereby using an unwitting legitimate driver and their vehicle as a mule to transport the hidden payload;
- altering the livery, design or registration of a hostile vehicle to match that of a legitimate vehicle, i.e. a Trojan vehicle.

8.4.2.3 Component modifications

Component modifications might include:

- load-bed or suspension modification to prevent a vehicle riding low on its suspension, if carrying an IED in addition to a normal load;
- presentation of a vehicle so that it appears empty but is actually carrying a cosmetically hidden IED;
- enhanced performance or manoeuvrability of a vehicle.

8.4.2.4 Structural modifications

Structural modifications might include:

- strengthening the chassis and vehicle components;
- modifying the occupant cell or cab.

8.5 Duration of VSB system deployment

The duration for which a VSB system is required is dependent on the following:

a) duration of event or length of occupancy of the site;

b) threat (e.g. the need to deploy additional VSB system measures at times of increased threat); and

c) budget constraints.

Security measures should be reviewed and assessed at regular intervals, which should be defined by the responsible organization, to establish whether a HVM scheme needs to be adapted to a change in threat.

8.6 Explosions and blast effects

8.6.1 General

The key aim of most security schemes is to maximize the blast stand-off distance between a critical asset and a potential explosive. A VSB system can be designed to mitigate against blast but where it is not, it can add to secondary fragmentation created by an explosion. Security practitioners should identify acceptable levels of risk.

When an explosion occurs there are several effects that can cause damage and injury. The severity of these effects is dependent on the power, quality and quantity of explosive material and reduces rapidly with distance.

Explosions and blast effects can include the following:

- blast wave;
- fire ball;
- brisance (a shattering effect created in material in contact with the explosive);
- cratering and ground shock;
- primary fragments;
- secondary fragments.

8.6.2 Blast effects on buildings and infrastructure

If the first point of challenge is considered to be the point of VBIED detonation, then the potential for collateral damage to people, buildings and utilities above and below ground should also be assessed.

An explosion within, under (e.g. in an underground car park), or very close to a building can have catastrophic effects, destroying or causing severe damage to the building's external and internal structural framework, collapsing walls, blowing windows in/out and disabling critical systems such as fire detection or fire suppression systems and building utilities.

Loss of life and injuries to occupants can occur from building collapse, flying glass and other debris, direct blast effects, fireball, projectile impact, smoke and fire. Indirect effects (local damage or collapse) can prevent swift evacuation of a building, potentially leading to further injuries and additional casualties.

The security practitioner should assess the following:

- the minimum required blast stand-off distance;
- the potential to install a secure perimeter beyond the minimum blast stand-off distance;
- the structural robustness of nearby building(s) and infrastructure, and the need for additional protection;
- the need for, and use of, bomb shelters and/or spaces protected from blast;
- any requirement for blast-resistant glazing.

NOTE Further information regarding the blast effects on buildings can be found in the Thomas Telford publication, Blast effects on buildings *[13].*

8.6.3 Balancing blast stand-off distance with building resilience

Blast stand-off distance has traditionally been defined on the assumption that a detonation occurs at a set distance from the target, e.g. at the site boundary (when typically delineated by a perimeter fence) or at the edge of the kerb in a city centre location. However, previous experience of vehicle-borne attacks has shown that those with hostile intent are likely to attempt to deliver a VBIED as close to the intended target as possible, demonstrating intelligent surreptitious techniques or use of overt aggressive attack.

Therefore, it cannot be assumed that a site having a perimeter that is secure from pedestrian intruders will necessarily provide suitable protection against the full range of vehicle-borne threats. As part of the OR process (see **6.1**), the first requirement for the assessment or design of any site required to resist a VBIED is to define the optimum blast stand-off distance and then to ascertain and

implement the most appropriate method for preventing hostile vehicles from coming closer than the defined distance.

In the majority of new-build developments, it might be possible to accommodate either:

- adequate blast stand-off distance (through management of the site layout); or
- enhanced robustness to the building construction (based on the achievable blast stand-off distance).

However, for many existing locations, and in some new-build designs, there are likely to be constraints that limit design and that can compromise the effectiveness of HVM measures, such as:

a) business needs (e.g. budget, health and safety);

b) site management (e.g. traffic management, access control); and

c) construction (e.g. appearance, planning consent).

As a result, it is important to carry out a risk assessment to identify and manage vulnerabilities. Management of vulnerabilities can often be conducted through the use of enhanced security measures that have been fitted retrospectively to meet the current OR, in conjunction with traffic-screening procedures to check the legitimacy of staff and site visitors.

It is essential that the specified blast stand-off distance is practicable to enforce and can prevent hostile vehicle access. Where the blast stand-off distance can be increased, this might reduce the need to strengthen critical assets or building structures against blast.

The reduction of blast mitigation measures can also reduce associated costs and it is to be noted that the cost of protecting a critical asset from blast due to an insufficient blast stand-off distance can be significantly greater than installing HVM measures at an adequate distance.

There is no single solution and each scenario should be assessed on an individual basis, as there are likely to be numerous stakeholder and operational requirements to consider that affect the balance between blast stand-off distance, blast strengthening of critical assets and buildings and business needs.

9 Site assessment

9.1 General

In order to select the most appropriate VSB system for a site and to complete the OR (see **6.1**), information should be collected regarding the physical landscape and its environmental conditions in order to highlight any engineering constraints and identify vulnerabilities for hostile vehicle attack.

The security practitioner should take a methodical and layered approach to the site assessment, so that: they have an understanding of the daily operation of the site, they have identified the full extent of the areas to be made secure and the location of the secure perimeter, and they are aware of how the physical and procedural traffic management controls on- and off-site can integrate with the overall HVM scheme. Subclauses **9.2** to **9.4** provide common considerations that should be covered as part of a practical VSB system assessment. However, every site has its own specific security challenges and the VSB system assessment should be tailored accordingly.

Changes to the site might necessitate a complete review of the OR. For example, the demolition of a neighbouring building could expose one side of the site or open up a vehicle approach that might exceed the capabilities of an existing VSB system.

The security practitioner should also consider how the deployment of a VSB system could re-direct a hostile vehicle to another part of the site, or to a different site, and whether the HVM scheme at that location can mitigate the perceived threat.

9.2 Local environment

The local environment that encompasses the land beyond the enforceable blast stand-off distance perimeter should also be evaluated during the site assessment.

The following should be included in the assessment:

a) geography including:
   1) topography (e.g. gradient, level changes);
   2) ground conditions (e.g. bearing capacity, water table);
   3) traversable terrain (e.g. grass, rough ground);
   4) water features (e.g. rivers, lakes);
   5) weather conditions;
   6) plant, wildlife and protected species;
   7) subterranean features;

b) architecture including:
   1) aesthetics (e.g. design, materials, colour);
   2) buildings and structures;
   3) public realm;
   4) streetscape;
   5) integrated security;

c) transport network including:
   1) traffic analysis (volumes and flow at different times);
   2) public transport interchanges;
   3) parking, legitimate or otherwise;
   4) planned network developments;
   5) traffic regulation orders;
   6) accident hot spots.

NOTE See also the joint CPNI and DfT publication, Bollards and pedestrian movement *[14] and the CPNI and DfT traffic advisory leaflet,* Vehicle security barriers within the streetscape *[11].*

9.3 Secure perimeter

*NOTE See also **8.6.***

The secure perimeter should be assessed during the site assessment [see **6.1**c)]. The assessment should encompass the existing or proposed secure perimeter surrounding the critical asset (see **7.2**) and include the:

a) composition (identifying the boundary components), covering the:
   1) boundary;
   2) natural landscape;
   3) buildings and large structures;
   4) access points;
   5) existing VSB systems;

b) neighbours (investigating operations, security, plans and requirements), covering:
   1) residential, commercial, industrial;
   2) land ownership;
   3) those overlooking critical asset, perimeter or access routes;
   4) operations and traffic patterns;
   5) security management (especially HVM);
   6) development plans;

c) VSB system deployment (identifying existing VSB systems in place and their suitability for the intended purpose), covering:
   1) existing VSB systems;
   2) new VSB systems;
   3) enforceable blast stand-off distance;
   4) passive or active functionality;
   5) purpose of the VSB system;
   6) vehicle dynamics assessment (VDA);
   7) whether the impact performance has been tested;
   8) whether the VSB systems are integrated with other security measures.

9.4 Traffic management, vehicle access control and parking

9.4.1 General

Traffic management, vehicle access control and parking cover designated areas where vehicles can legitimately access, or park, inside or outside the secure perimeter. An assessment of these aspects should be made prior to selecting and installing a VSB system.

The assessment should include:

a) legitimate vehicles (to determine who, or which vehicles, require access and why), covering:
   1) purpose of entry or exit;
   2) vehicle types (e.g. size and mass);
   3) drivers (e.g. staff, contractor, visitor);
   4) special loads (e.g. very wide or long loads);
   5) emergency services;
   6) traffic volumes;
   7) other road users;

   NOTE *See also* ***10.9.2****.*

b) access control (to analyse the operational requirements and integration with other systems), covering:
   1) location and layout of the VACP(s);
   2) existing or proposed VSB systems;
   3) capacity or throughput requirements;
   4) method of access control (e.g. security guard, staff ID);

5) integration with other site security measures;
6) security guard manning;

c) parking (to identify parking location and operation), covering:
1) location on- or off-site;
2) underground or overground;
3) drop-off or pick-up zones;
4) unauthorized parking;

d) protocols and planning (to consider VACP management and procedures), covering:
1) management of legitimate vehicles;
2) rejection of unauthorized vehicles;
3) search procedures;
4) VSB system fail safe (open) or secure (closed and locked);
5) emergency plans in the event of a site lockdown;
6) breakdown contingency procedures and maintenance.

A good HVM strategy aims to minimize the number of vehicles requiring site access and create an enforceable blast stand-off distance from the critical asset. The use of passive VSB systems can remove vulnerability to deception, duress, tailgating or tamper attack methods.

The way in which traffic management is to be dealt with in and around a site should be used to inform the positioning of the secure perimeter and the selection of an appropriate VSB system(s). Four different traffic management options are given in **9.4.2** to **9.4.5**.

9.4.2 Total vehicle exclusion

Total vehicle exclusion providing a secure cordon at a substantial and enforceable blast stand-off distance should be the starting point for a high level of effective critical asset protection.

This method can use remote car parking, for both visitors and staff, outside of the enforceable blast stand-off perimeter. Covered walkways or a park and ride system could be implemented to transport staff to their workplace. However, the exclusion of traffic from a wide area can cause increased traffic volumes and congestion in the surrounding local transport network, thus creating a need for wider traffic management plans.

The routine and emergency servicing requirements of the critical asset can also have an impact on access requirements and therefore should be considered before this type of traffic management system is implemented. For example, a plan should be formulated regarding how deliveries or waste disposal can be dealt with if no vehicles are allowed on site.

9.4.3 Vehicle exclusion coupled with screening and/or searching

Only vehicles that have been screened and/or searched by security guards should be granted access beyond the secure cordon. To minimize risk, the security guards would be required to screen and/or search 100% of vehicles entering, even if they are known or regular visitors.

The use of off-site consolidation and screening facilities (with bonded vehicles servicing the site) can offer multiple security benefits, by reducing the number of vehicles requiring access to the site and moving the first point of challenge to a remote location.

Although vehicles are screened, this method of vehicle access control still provides opportunities for duress to be used against the security guards. A diligent security guard given the authority to turn away those that do not meet access control requirements can also reduce the risk of being deceived.

9.4.4 Vehicle inclusion coupled with VSB systems around individual critical assets

Vehicle inclusion on an existing road network around a critical asset is an option, but would normally necessitate the protection of the individual critical asset at reduced blast stand-off distance relative to the options given in **9.4.2** and **9.4.3**.

Use of this option might lead to multiple (disjointed) smaller perimeters and potentially more complex site security management, where the site is large and consists of more than one critical asset that needs to be protected.

9.4.5 Contingency measures or re-deployable VSB systems

Contingency measures can be permanently pre-installed for use at times of heightened threat, or temporary re-deployable measures installed for a specific event or as a prelude to a permanent VSB system installation. Whilst these measures can offer flexibility, they can also include a number of drawbacks.

These include the following:

a) deployment is intelligence-based or uses an incomplete intelligence picture;

b) intelligence-based deployment indicates to adversaries that their hostile plans have been identified and could be compromised;

c) deployment could be too late in the case of a first attack; and

d) visual deterrent to hostile vehicle attack is lost when re-deployable VSB systems are removed.

In addition, re-deployable VSB systems can also have further operational drawbacks, which are that:

1) such measures often require greater blast stand-off distances than permanent alternatives due to the use of freestanding or surface mounted VSB systems that rely on the absorption of energy from hostile vehicle impact over a greater distance;

2) transport and specialist equipment is required for delivery and installation;

3) modular and wall-like systems cannot always be deployed effectively on undulating or uneven ground;

4) their appearance might prevent their use in attractive public environments;

5) their mass can prevent their use on certain ground conditions or elevated slabs;

6) few re-deployable VSB systems incorporate integrated powered active measures;

7) VSB systems might be difficult to implement on sites where desired pedestrian routes are not clearly defined.

9.5 Vehicle speed management

9.5.1 General

Managing the maximum possible speed of a vehicle limits its ability to undertake penetrative hostile vehicle attack. This can also manage the speed of drivers with non-hostile vehicles on approach to, and within, a secure area and can be used for the purpose of security guard recognition and traffic safety.

Traffic calming solutions do not provide an impenetrable hard stop, but complement a VSB system by seeking to reduce the speed of a hostile vehicle approaching a particular critical asset. This speed reduction can have the added benefit of allowing the security practitioner to select a VSB system that is proportionate to the lower speed hostile vehicle impact. Such VSB systems are often simpler to integrate and more visually acceptable.

Common traffic calming methods can take the form of:

- horizontal deflections (e.g. bends, chicanes);
- vertical deflections (e.g. road humps);
- road signs (e.g. speed limit, access control signs).

9.5.2 Horizontal deflections

9.5.2.1 General

Horizontal deflections are often employed in urban or residential areas to encourage drivers to slow to make the required horizontal direction change. This results in reducing vehicle speed in order to maintain driver and passenger comfort and improve road user safety.

Horizontal deflections such as bends or chicanes can also be deployed as a traffic calming measure to limit the maximum speed of a vehicle operated by a hostile driver. Speed reduction can only be assured when a chicane is enforced by a VSB system.

NOTE Only horizontal deflections that are enforced by a VSB system are considered to be a suitable HVM measure.

Key chicane dimensions that can be altered to limit the maximum exit speed of a hostile vehicle are as follows:

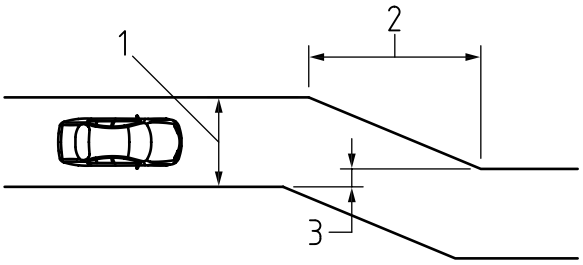
- lane width (maximum width of traversable terrain);
- stagger length [distance between chicane turns in the direction of vehicle travel; see Figure 4];
- free view width (offside and nearside kerb offset as viewed on approach, might be positive (gap) or negative (overlap); see Figure 4).

9.5.2.2 Parameters required before designing a chicane

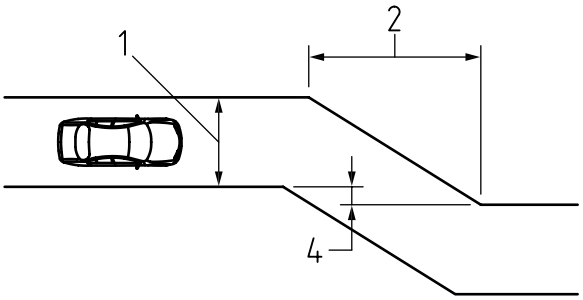
The parameters that should be ascertained before designing a chicane for HVM include the:

- perceived hostile vehicle(s);
- desired hostile vehicle exit speed; and
- legitimate vehicle access requirements.

Figure 4 **Key chicane dimensions**



a) Positive free view width



b) Negative free view width

Key

1	Lane width	3	Positive free view width
2	Stagger length	4	Negative free view width

9.5.2.3 Factors to consider for chicane integration within a road layout

Factors that should be assessed for chicane integration within a road layout include the:

- maximum road width required (for legitimate vehicles);
- number of lanes required (for legitimate vehicles);
- swept path of legitimate vehicles;
- traversable terrain (e.g. footpath or verge); and
- method for providing access to, or rejection of, large vehicles.

A double chicane has a larger longitudinal footprint than a single chicane but can provide greater reduction in the maximum possible hostile vehicle speed. This is due to it forcing two directional changes, increasing instability in an attacking vehicle.

It might be necessary to design a chicane that allows occasional access for larger vehicles or vehicles with a poor turning circle. This is achievable with the use of a removable or retractable VSB system, which can provide a greater useable road width.

9.5.2.4 Hostile vehicle impact velocity

The impact velocity of a hostile vehicle exiting a chicane should be assessed. This impact velocity is dependent on the:

- exit speed (from the chicane);
- vehicle type and specification;

- acceleration distance from chicane exit to the critical asset; and
- traversability of terrain leading to the critical asset.

9.5.2.5 Other horizontal deflections

There are other horizontal deflections which can be enforced by a VSB system. These include:

- bends on the road, especially sharp bends and compound curves;
- pinch points (i.e. where a road narrows to restrict or prevent vehicle access);
- roundabouts.

9.5.3 Vertical deflections

Vertical deflections such as road humps (sleeping policemen) and rumble strips are often employed on the highway as a visual deterrent and to disrupt ride comfort, encouraging road users to reduce speed. In reality, vertical deflections provide negligible deterrent or speed reduction against a determined vehicle-borne attack.

9.5.4 Gradient

Uphill gradient can affect a hostile vehicle's ability to maintain speed or to accelerate towards a critical asset (especially for larger, heavier vehicles). However, the physical space required to create a suitable gradient is likely to preclude this option unless there is natural gradient available in the site's surrounding topography.

9.5.5 Road signs

A well-designed system of road signage and markings increases drivers' awareness when approaching a VACP or when moving inside a secure area. However, road signs cannot prevent any form of vehicle-borne attack and the implementation of a VSB system is a more effective solution.

NOTE Non-compliance to the system of traffic control might be an indicator to security guards that a vehicle is a security threat.

10 Vehicle access control, VSB system implementation and usage

10.1 General

Vehicle access control is designed to provide an area in which the flow and access of traffic is controlled by a VSB system and to provide security guards with an area in which they can safely identify and inspect a vehicle, its driver, any occupants and any vehicle load before granting access through an enforced blast stand-off perimeter.

Often vehicular access is provided through a secure perimeter. In this instance, the vehicles might be searched or be certified to be of known authenticity before arriving at the VACP. In this instance a single or multiple VACP might be provided through a secure perimeter (e.g. rising, swing or sliding barriers). Where the blast stand-off distance forms the site boundary or secure perimeter, the VACP typically becomes the first point of challenge for all vehicles.

Regardless of the type of active VSB system installed, an independent secondary VACP should be created, wherever practicable. This is so that vehicles can be diverted to the secondary location in instances where a VSB system fails or where

there is an incident at the main VACP. This secondary location should be designed to accommodate the same traffic volumes as the main VACP and also to maintain the same level of operational security.

Where a VSB system is provided separately at both entry and exit points at a VACP, then it is recommended that each VSB system has an independent drive and control system. This is to prevent a nodal or cascade failure as a result of one VSB system developing a fault. The VSB systems might share the same user interface, hydraulic circuits and electrical systems, but they should be designed so that the failure of one does not result in the failure of both. Provision of an uninterruptable power supply (UPS) or standby generator should also be considered, and, if practicable, implemented.

10.2 VACP components

A VACP is made up of a number of components. When planning, selecting and installing a VSB system, each of the following components should be considered in order to ascertain that all of the necessary requirements for the VSB systems are fulfilled and that the different components do not conflict in any way.

a) *Entry lane(s)*. This provides vehicle access from a public highway to the correct part of a VACP. It might also incorporate a waiting area or parking and needs to have sufficient queuing space to accommodate the anticipated traffic flow at peak times.

b) *Communication point.* This provides a means of verbal communication to the security guards. It is typically located before the VACP barrier. It can be used for emergency communications to VACP operators.

c) *Vehicle access control.* This provides a means for identifying legitimate vehicles or drivers. The access control method used depends on the operational requirements of the site.

d) *Guardhouse.* This provides protection for security guards from weather, and has good visibility over the VACP and surrounding area. It might be designed to provide blast and ballistics protection. The guardhouse might (if not controlled remotely) contain control systems for active VSB systems and other integrated security systems (e.g. CCTV or detection systems).

e) *Traffic control barrier.* This controls the movement of traffic through the VACP. Typically this measure is a lightweight traffic control barrier that has not been impact tested in accordance with PAS 68, or an equivalent standard. (See also Clause **4**.)

f) *VSB system.* This provides proportionate physical protection against the perceived vehicle-borne threat. See also Clause **5**.

g) *Search or waiting area.* This is a controlled area where a vehicle, its occupant(s) or its load can be screened, searched or held for further investigation. It is generally located before the VACP. It is important that the search or waiting area is not located beyond the VACP or inside a secure perimeter.

h) *Rejection route.* This provides a means for a vehicle to be rejected from a VACP without being allowed through an active VSB system. It typically comprises a separate rejection lane and space for vehicles to manoeuvre, without impeding other vehicles. Unauthorized vehicles should not be able to pass beyond a VSB system if rejected.

i) *CCTV or ANPR*. This can be used to identify legitimate vehicles and/or watch over specific areas of the VACP (e.g. search areas or VSB system controls).

Automatic number plate recognition (ANPR) technology can be susceptible to deception techniques and therefore should not be considered effective (when used in isolation) for legitimate vehicle or hostile vehicle identification.

10.3 Typical considerations for VSB system implementation and usage

10.3.1 Signage and road markings

Clear signage and road markings should be implemented to guide users to the correct location and advise them as to the required driving behaviour in proximity to a VSB system.

NOTE The PAS user is advised that there might be applicable legislation regarding signage and road markings.

10.3.2 Traffic control signals

Red or green traffic control signals may be implemented to instruct drivers regarding what is expected of them at an active VSB system. Traffic control signals should not become obscured and lights should not be affected by direct sunlight. Traffic control signals should be located such that they do not give conflicting advice on a public highway.

10.3.3 Segregating traffic

Separating pedestrians from vehicular traffic can improve VACP management procedures and help maintain local health and safety requirements. Segregating staff access from visitor access can further improve VACP control and throughput.

10.3.4 Surveillance and lines of sight

Security guard lines of sight and CCTV cameras' field of view should be free from obstructions such as street furniture and vegetation. CCTV cameras may be used for monitoring and for the enforcement of correct VSB system usage when a VACP is unmanned or outside of normal operating hours.

NOTE Further information regarding CCTV can be found in BS 7958 and BS 8418. CCTV footage can be used to record events to provide evidence for accidents or health and safety investigations.

10.3.5 VSB system installation

An active VSB system should not present foot and hand traps or trip hazards in the road surface when installed. The maximum recommended gap around the opening segment of a blocker or bollard when fully open should not exceed 5 mm.

It might also be advisable to minimize or protect the gaps around the edges of an active VSB system as this could reduce the amount of water and debris from getting into an active VSB system mechanism.

10.3.6 Road surface

Where a retractable VSB system forms part of the road surface, grip levels should be even and consistent.

Where there is an existing VSB system with uneven and/or inconsistent grip levels, a surface enhancement treatment should be retrospectively applied to it to rectify the problem. This is particularly important in weather conditions where surfaces could become wet or icy. Application of a surface enhancement treatment should also be considered where a VSB system has been positioned so that it is more

likely to attain uneven grip levels (e.g. on a gradient, on a sharp bend, close to a junction stop line or where the road is used by two-wheeled vehicles). Further consideration should be given to the axle load and frequency of vehicle traffic, as these can accelerate the polishing or rutting of the running surfaces of the road blockers and rising bollards.

NOTE Pedestrians and two-wheeled vehicles can be particularly susceptible to falling or slipping. See also the CPNI publication on retractable vehicle security barriers [12].

10.3.7 Safety sensors

Safety sensors should be incorporated into the VSB system when it is installed in order to minimize the potential for accidents. The type of safety sensor should be selected based on the risks affecting the relevant VSB system. The safety sensor should be positioned to cover the vulnerable areas around the VSB system.

NOTE 1 Various types of safety sensor are available, such as induction loops and photocells.

NOTE 2 Safety features might also contain vulnerabilities which could mean that they can be overridden to compromise VSB system user safety or site security. Checks of the correct implementation of safety features can prevent security issues from occurring.

10.4 Vehicle access control methods

10.4.1 General

Active VSB systems may be controlled in a number of ways, with or without surveillance. Examples of these methods of control are through:

a) free access;

b) automatic access control systems (AACS); or

c) security guard control.

Table 1 gives examples of access control methods.

Table 1 **Vehicle access control methods**

Free access	AACS	Security guard
Induction loops	Keypad	Driver/vehicle
Photocells	Card reader	Vehicle inspection
Ticket system	Token	Communications device
	VHF transmitter	Surveillance systems
	Vehicle recognition	Push button console

The strengths and weaknesses of each of the methods given in Table 1 should be assessed in terms of their:

1) security;

2) safety (for users and operators);

3) traffic management;

4) traffic throughput; and

5) costs (short- and long-term).

It is often advisable to implement a combination of access control solutions together, to take into account security or throughput requirements that change during daily traffic cycles or on-site activities. For example, additional security

systems (e.g. an access card reader) might be turned on at night to replace site access normally authorized by security guards.

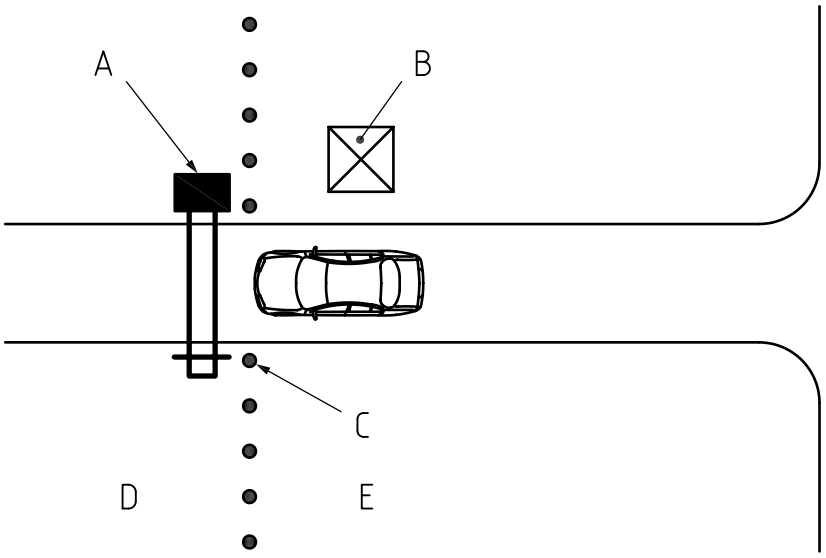
The security of the access control method should be assessed for its effectiveness in mitigating deception and duress attack methods. Operating equipment and control systems should be protected against deliberate tamper or accidental damage in order to maintain the security of the whole VACP.

Different types of VACP layouts are given in **10.4.2** to **10.4.4**.

10.4.2 Single line VACP

A single line VACP, as shown in Figure 5, is the most basic access control layout, having a line of VSB system measures (e.g. fixed bollards). The single line VACP has a smaller footprint and is generally a lower cost than other VACP layouts to implement.

Figure 5 **Single line perimeter with VSB system control gate**



Key

A Active VSB system (e.g. rising arm barrier)

B Security kiosk

C Passive VSB system (e.g. fixed bollard)

D Secure area

E Unprotected area

NOTE For simplicity, approach road layouts, traffic calming, search/screening facilities and/or rejection lanes, etc. are not shown. The layout given in Figure 5 illustrates a right-hand drive configuration (i.e. the security kiosk appears on the driver's side).

10.4.3 Interlock VACP

The interlock VACP layout, as shown in Figure 6, employs two rows of active VSB systems supported by additional HVM measures to create a contained secure zone that a vehicle cannot enter or leave until authorized by the security guard or AACS.

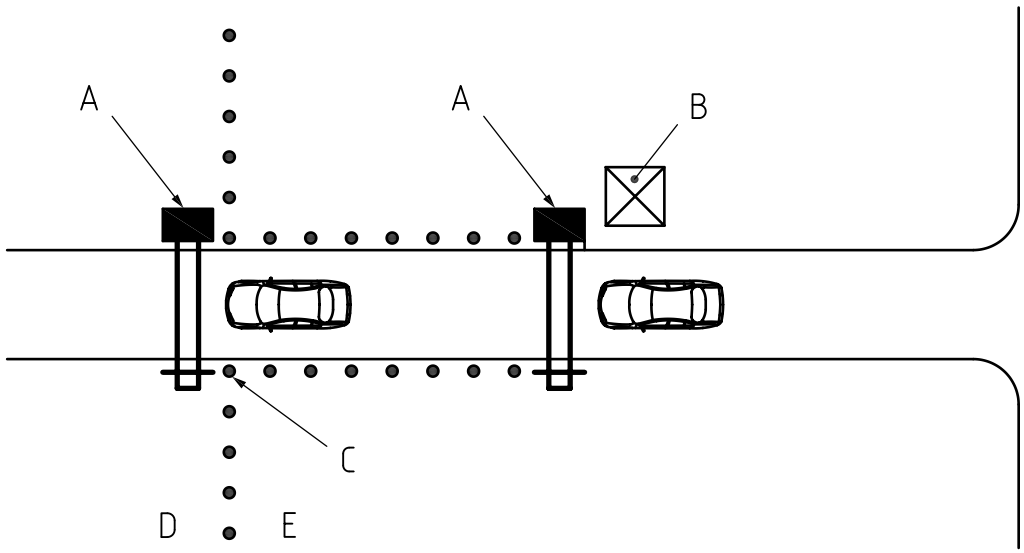
In this layout, each vehicle is securely contained between the two active VSB systems, segregating individual vehicles and therefore reducing the likelihood of tailgating. At no point are both VSB systems open at the same time, thus

preventing access from being compromised if one of the VSB systems were to fail (remaining in the open position).

Transit through the first VSB system allows a controlled zone in which security guards can check the identity of the driver and/or the vehicle. Upon successful identification of the driver and/or vehicle, and with the outer VSB system fully closed, the inner VSB system gate can be controlled to open and allow legitimate vehicle access.

This solution is significantly more secure than a single line VACP method, but requires a larger footprint, is comparatively more expensive to purchase and maintain, and significantly slows legitimate traffic throughput.

Figure 6 **Interlock VSB control enforced by VSB systems**



Key

A Active VSB system (e.g. rising arm barrier)

B Security kiosk

C Passive VSB system (e.g. fixed bollard)

D Secure area

E Unprotected area

NOTE For simplicity, no rejection lanes, search bays or parking facilities are shown in Figure 6.

10.4.4 Final denial VACP

In the final denial VACP layout, as shown in Figure 7, the inner impact-rated VSB system remains in the open position during normal operation. Where the security guard suspects or identifies a potential vehicle-borne threat, there is sufficient time for them to react and close (secure) the inner VSB system in time to prevent hostile vehicle entry.

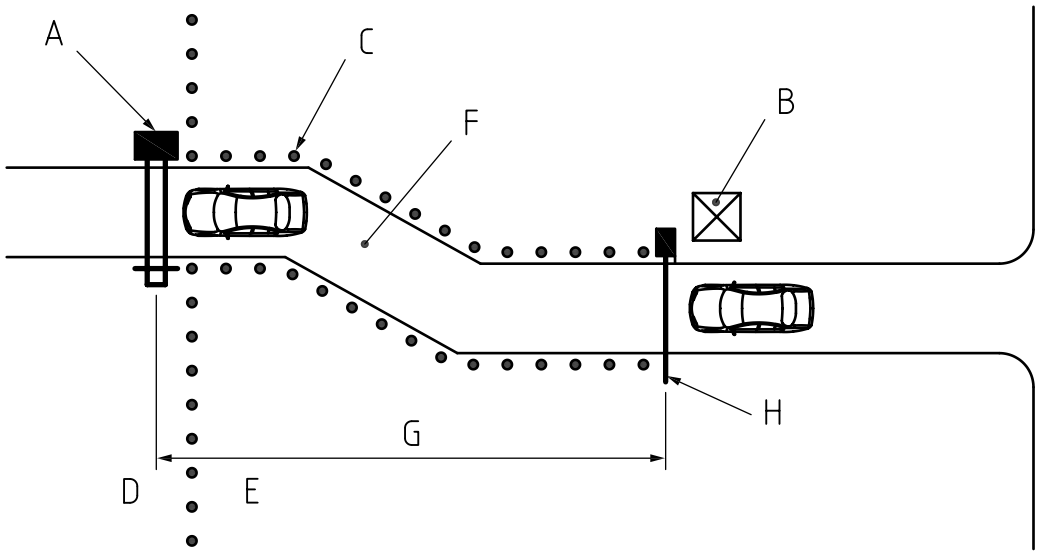
The final denial VACP is typically adopted where available room and blast stand-off distance are not a design constraint. In theory, this method can be considered to provide a high level of security, but it relies heavily on security guard training and procedures. In this layout, security guards are required to identify, interpret hostility and react proportionately to threats in time to close the final denial VSB system.

It is advisable to carry out a risk assessment regarding the vulnerability of the security kiosk and the controls located within in order to implement procedures to

prevent the active VSB system from being overridden if the security staff become overpowered and prevented from securing the site perimeter.

NOTE Generally this format VACP is remotely operated and the guard does not have access to VSB system controls at the point of challenge.

Figure 7 **Final denial vehicle access control solution**



Key

A Active VSB system (e.g. rising-arm barrier)
B Security kiosk
C Passive VSB system (e.g. fixed bollard)
D Secure area
E Unprotected area
F Chicane
G Variable distance*
H VACP

* Distance between the VACP and active VSB system is dependent on the predicted hostile vehicle transit time and the time it takes to activate and close the active VSB system.

NOTE For simplicity, no rejection lanes, search bays or parking facilities are shown in Figure 7.

10.5 Protocols and planning

Good management procedures and forward thinking can help control the daily operations surrounding a VSB system at a VACP and can prepare security guards to deal with unexpected events or a vehicle-borne attack. As good practice, where access is allowed into a site, more than one VSB system should be provided. This is to take account of:

- planned maintenance;
- breakdown and reactive unplanned repairs;
- damage caused by hostile vehicle attack; and
- emergency access.

When selecting a VACP layout to implement, the flexible solutions and contingency plans that each design offers should be assessed.

10.6 Training

Where security guards are used in conjunction with a VACP, they should be provided with training covering the following:

- maintaining site security;
- managing and controlling VACP operations;
- operating active VSB systems correctly;
- using integrated security systems (e.g. CCTV or vehicle access control);
- reacting appropriately to emergency scenarios, security threats or periods of heightened security;
- understanding contingency plans and response procedures;
- reporting faulty equipment or operational issues;
- following health and safety standards.

Proper training is especially important if relying on a final denial VACP concept where a security guard is expected to identify a threat and react quickly to potential vehicle-borne attack.

10.7 VSB system operations management

In order to maintain the effective daily function of a VACP and operation of the VSB system(s), it is essential that procedures and protocols regarding the management of VSB system operations are planned, documented and communicated to the relevant individuals (see also **10.6**).

Operations management procedures and protocols covering the following should be implemented.

- *Traffic management.* How is the flow of traffic and the processing of pedestrians, vehicles, staff, deliveries, visitors, contractors, etc. to be maintained? What are the requirements for each site user and how should the security guards deal with them in order to maintain security? How should the security guards deal with an emergency situation?
- *Identification procedures.* By what means are legitimate site users correctly identified and granted access? How are security guards or vehicle access control systems required to deal with those that are denied access?
- *Search procedures*. On what basis and frequency are vehicles searched? How are vehicles, drivers, passengers, loads searched? Where do searches take place and by whom? How are the security guards expected to react in the event of a suspicious vehicle, person or item?
- *Maintenance*. How is the active VSB system equipment, other integrated systems, communications, road surface condition, etc. to be maintained? Is maintenance preventative (i.e. planned based on time or operational cycles) or reactive?

10.8 Emergency procedures

The action undertaken by the security guards at the VSB system as the result of an emergency should be determined in the documented procedures and protocols detailed for each scenario (see **10.7**) and the training given (see **10.6**). The provision of access for emergency vehicles (e.g. fire or ambulance) and business continuity should be determined whilst also maintaining site or critical asset security against vehicle-borne threat.

NOTE Further information regarding business continuity can be found in the publications, Secure in the knowledge – Building a secure business *[8],* Expecting the unexpected – Business continuity in an uncertain world *[9].*

10.9 Technical assessments

10.9.1 General

Technical assessments and analyses might also be necessary in order to provide additional detail to the site assessment and to help quantify the perceived vehicle-borne threat. These should be undertaken in collaboration with security consultants or technical experts. Three examples of technical assessment that may be undertaken are given in **10.9.2** to **10.9.4**.

10.9.2 Traffic analysis

Traffic analysis may be used to investigate the type, intensity and movement patterns of traffic to determine the typical daily operation of the site. It can be used to check that proposals for HVM meet site operational requirements in terms of the:

a) composition of authorized vehicles, covering:
   1) cars;
   2) 4x4 or off-road vehicles;
   3) vans;
   4) rigid vehicles;
   5) articulated vehicles;
   6) emergency vehicle;
   7) special loads;
   8) two-wheeled vehicles (e.g. cycle, motorcycle);

b) regular visitors, covering:
   1) contractors;
   2) deliveries;
   3) waste disposal or utilities;

c) traffic, covering:
   1) volumes;
   2) routes;
   3) peak periods;
   4) ingress and egress;
   5) vehicle queuing;

d) timings covering:
   1) queuing;
   2) vehicle search; and
   3) waiting.

10.9.3 Swept path analysis

A swept path analysis may be used to check that legitimate vehicles using a site have adequate space to safely manoeuvre. Typical applications include the design of:

- VACPs;
- rejection lanes;
- chicanes;
- pinch points;
- delivery areas;
- car parking zones.

10.9.4 Vehicle dynamics assessment (VDA)

A vehicle dynamics assessment (VDA) is the process of investigating the existing or proposed road (public highway or private land) layout and off-road terrain to identify all possible hostile vehicle attack routes leading to a critical asset, VACP or secure perimeter and to determine the maximum possible hostile vehicle approach speed along these routes.

It can be relatively easy to engineer a clear hostile vehicle approach path (e.g. using accomplices to hold up traffic). There would be no hesitation for a determined driver with hostile intent to drive against the normal direction of traffic flow (e.g. the wrong way along a one-way street) or to cross pedestrian areas. All normal road rules and behaviour (e.g. road signs and markings) can be ignored as it is only necessary to assess a vehicle's ability to traverse the terrain.

NOTE 1 A hostile vehicle might not abide by the typical rules of the road.

The output of the VDA includes the final impact speed and angle of all identified hostile vehicles for each identified approach route. This information can be used to select an appropriate VSB system.

NOTE 2 The hostile vehicle approach angle can significantly affect the result of the hostile vehicle impact speed. VSB system performance can also vary depending on the impact angle.

The main VDA techniques are a 2D manual assessment or 3D computer simulation, both of which require the provision of dimensionally and descriptively accurate survey data. The supply of accurate and informative site details often produce VDA results which are of a better quality and are more reliable.

The following information should be included in a VDA:

a) details, covering:
    1) site background and critical asset(s);
    2) perceived hostile vehicle(s);
    3) location of existing or proposed VSB systems;
b) terrain details, covering:
    1) surface type (e.g. soil, gravel, concrete);
    2) gradient and level changes;
    3) lines of sight to or from target or asset;
    4) kerb lines and heights;

5) street furniture;
6) large or immovable objects or structures;

c) visual media, covering:
1) CAD drawings (e.g. site or road network plans);
2) satellite imagery;
3) photographic images.

11 VSB system construction and removal

11.1 General

A key part of successful implementation of deployable HVM schemes is the deployment of VSB systems in accordance with their design plans. Incorrect deployment can leave gaps large enough to allow vehicle encroachment or could weaken the overall secure perimeter, particularly for re-deployable installations.

NOTE 1 Security practitioners might wish to discuss deployment and removal activities with the highways and local authorities at the planning stages as part of the stakeholder liaison process.

The installation of a VSB system should prevent or control vehicle access whilst integrating as seamlessly as possible with the surrounding environment.

NOTE 2 For VSB systems integrated in the public realm, attention is drawn to the Equality Act 2010 [2]. It is important to be aware that their installation might be subject to local authority, highway and transport guidelines.

11.2 Positioning

The air gap between structural elements of adjacent VSB systems or any other rigid or fixed physical feature forming the secure perimeter should be no greater than 1 200 mm. Where a VSB system is narrower at the top than at its base, this gap should be measured at 600 mm above the finished ground level.

NOTE For VSB systems located along a highway, it is advisable to consult the local authorities for any relevant requirements. A VSB system on a highway is usually required to be positioned at least 450 mm from the road kerb edge in order to prevent handlebars of two-wheeled vehicles from striking the street furniture. However, some local authorities have permitted this dimension be reduced to 300 mm. Some local authorities also require a minimum pavement width (for example, 1 200 mm) to be maintained to allow for disabled access.

11.3 Foundations

11.3.1 General

The foundation design is extremely important as its purpose is to provide adequate support for the VSB system and prevent the VSB system from overturning when impacted. VSB systems generally require either an underground foundation, or a plinth onto which they can be fixed (e.g. with bolts or pins).

Where a VSB system impact tested to PAS 68 is selected, the foundation design as tested as part of the VSB system should be obtained from the manufacturer along with evidence of testing. However, it is important to note that such tests are

usually conducted on test-site ground conditions which might differ from those local ground conditions in which the VSB system is to be placed.

11.3.2 Underground obstructions

The selection of a VSB system might be dependant on the presence of underground obstructions (e.g. utilities or infrastructure), and the security practitioner should check for such obstructions at the site assessment stage.

A full underground survey map can be generated from engineering drawings supplied by the site owner and utilities companies, ground penetrating radar (GPR) surveys and the digging of trials pits. Critical assets situated on the public highway are generally registered on the highway authority's asset management database.

Where such underground obstructions exist, the following questions should be asked, and the answers used to inform the selection of a VSB system for installation.

a) Is it practicable, or desirable, to move or divert the underground obstructions to accommodate a VSB system with deep foundations?

b) Can a VSB system with a shallow foundation provide the required level of performance?

c) Can a surface-mounted VSB system provide the required level of performance?

NOTE It is inadvisable to install VSB systems above or near critical underground services, due to potential installation problems and subsequent collateral damage to those services in the event of a vehicle-borne attack.

11.3.3 Design and modification of VSB system foundations

VSB system foundation designs should conform to the following.

a) Ground conditions for VSB system foundations should provide a minimum soil-bearing capacity of 75 kN/m².

b) The foundation design of the VSB system should be developed when the perceived hostile vehicle threat and the calculated impact loading have been assessed.

c) Design and re-engineering of the as-tested foundation might be required so that the foundation can accommodate any below ground obstruction or services that might exist while maintaining the original impact test performance.

d) Where there are underground services in close proximity to VSB system foundations, as indicated in the site assessment, see **11.3.2**, the site should be assessed for VSB system suitability and appropriate protection should be given to the underground services as a precautionary measure, such as:

   1) shielding the underground services from the VSB system foundations or ground movement caused by vehicle impact;

   2) protecting the underground services against blast effects;

   3) maintaining access to underground services.

e) Modifications might need to be made to an impact-tested VSB system foundation design where the VSB system is required to fit within the physical constraints of the site whilst retaining its as-tested performance.

NOTE It is advisable that modifications are undertaken by an appropriately qualified engineer.

11.4 Logistics

There is potential for deployment and removal of a VSB system to cause disruption to the local area in terms of traffic delay and noise. The security practitioner should plan for this, and should carry out discussions with stakeholders beforehand to minimize the period of disruption. In many cases works can be carried out during quieter periods of the day (even at night), although this might require staff to work unsociable hours.

An assessment of the practicability of using specialist transport, tooling or lifting equipment to expedite logistical processes should be undertaken. An awareness of site accessibility is critical to enable deployment vehicles or equipment (in terms of their mass, width, height and turning circle) to reach the desired location(s).

11.5 Installation phase

11.5.1 General

An assessment of the time required for setting out, the need for checking and controlling the quality and the additional expenditure this could generate, should be undertaken. The ease with which a VSB system can be implemented should be factored into the selection process so that it can be rapidly assembled without undue complication. Subsequent access to services in chambers, cabinets or overhead should also be considered.

11.5.2 Lifting and placement

Before lifting and placement, a pre-deployment and engineering assessment of the site should be conducted to investigate potential placement issues. These issues include the following:

- overhead lifting, which could have health and safety implications and the potential for damaging street furniture or overhead utilities;
- heavy lifting equipment or re-deployable VSB systems, which might sink into soft or weak ground/road surfaces;
- local services or utilities, which could be damaged (e.g. underground services, drains access covers);
- hydraulic oil, which might require containment when relocating or moving systems. Sites that require double bunding of oil reservoirs and oil spills from hose disconnections should be avoided.

11.5.3 Removal

Upon removal of a VSB system (temporary or permanent), any deformed or damaged ground should be reinstated to its pre-deployment condition before removal works can be considered complete.

12 Procurement strategy

12.1 General

VSB systems may be purchased or hired based on an OR (see **6.1**). A number of factors should be used to influence the procurement strategy. Security practitioners should take the following factors into account when devising their procurement strategy: the VSB system availability, manufacturing quality, service and maintenance

contracts, costs (short term and whole life) of the equipment and all peripherals, including associated staffing, as given in **12.2** to **12.6**.

12.2 Availability

The availability of certain types of VSB systems and any spare parts might have an effect on the viability of implementing a particular design layout. The following should therefore be considered:

- the lead time for site design, manufacture, delivery and deployment of measures (it might be necessary to implement a temporary measure prior to implementation of the final solution); and
- the whole life availability of spares or complete units in the event of damage or failure.

12.3 Quality

VSB systems should conform to PAS 68.

NOTE Users of this PAS are advised to consider the desirability of quality system assessment and registration against the appropriate standard in the BS EN ISO 9000 series by an accredited third-party certification body.

12.4 Costs

When assessing the costs of VSB systems, security practitioners should consider the full life-cycle of the HVM scheme and include any associated costs from sources of expenditure such as:

- liaison with stakeholders;
- planning consent;
- design (e.g. VSB system and HVM scheme design);
- integration with other security systems;
- manning requirements (especially for VACPs);
- project management;
- training (initial and ongoing);
- warranty and exclusions;
- maintenance and service plans;
- spare parts and upgrades (i.e. to hardware and software); and
- decommissioning, removal and disposal.

12.5 Commissioning and handover

The means of evaluating the operational performance of a VSB system should be considered from the outset and specified within the OR (see **6.1**); the detail of which should then be developed into a performance/tender specification and given to VSB system suppliers.

Security practitioners should request evidence of VSB system's conformity to PAS 68 and the details and results of any testing undertaken to indicate that the VSB system meets the operational requirements.

NOTE 1 It is important that VSB systems meet operational needs, especially if a particular VSB system is bespoke or the first of a new design.

A VSB system should be supplied, where applicable, with installation drawings, cable and circuit diagrams, foundation drawings, programmable logic controller (PLC) ladder diagrams, control console diagrams and operation and maintenance (O and M) manuals.

The O and M manuals should be site-specific and include the following:

- description of the VSB system;
- list of recommended spare parts;
- training logs and procedures;
- procedures for operating the VSB system, fault finding, system isolation and overriding functionality;
- planned preventative maintenance procedures, schedules and logs;
- service and breakdown logs;
- contact details;
- relevant drawings;
- log of drawings;
- design and technical specifications;
- health and safety, risk registers;
- emergency response plans; and
- test and commissioning procedures and reports.

A training programme covering the safe and correct operation of the relevant VSB systems should also be developed and implemented for those members of staff responsible for operating the VSB system equipment. Staff names should be documented in writing and retained as a record of those who have attended training and been deemed competent to operate the VSB system equipment safely and according to the manufacturer/supplier/site owner instructions.

NOTE 2 Attention is drawn to the Data Protection Act [1].

12.6 Routine inspections and maintenance

The owner of the VSB system should create and implement a plan for its routine inspections, maintenance and repairs. Regular reviews of the VSB system operation should be undertaken and any changes in threat used to inform revisions and improvements to the processes and procedures.

NOTE Whilst the owner of the VSB system is ultimately responsible for the routine inspections and maintenance of the VSB system(s), they might elect to delegate the tasks to a third party. Further information regarding the lifetime operation of VSB systems can be found in the CPNI documents, Guide to producing operational requirements for security measures *[3] and* Level 2 operational requirements for hostile vehicle mitigation measures *[4].*

Bibliography

Standards publications

For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

BS 7958, *Closed circuit television (CCTV) – Management and operation – Code of practice*

BS 8418, *Installation and remote monitoring of detector-activated CCTV systems – Code of practice*

BS EN ISO 9000 (series), *Quality management systems*

Other references

[1] UNITED KINGDOM. The Data Protection Act 1998. London: The Stationery Office.

[2] UNITED KINGDOM. The Equality Act 2010. London: The Stationery Office.

[3] CENTRE FOR THE PROTECTION OF NATIONAL INFRASTRUCTURE. *Guide to producing operational requirements for security measures*. London: CPNI, 2010.

[4] CENTRE FOR THE PROTECTION OF NATIONAL INFRASTRUCTURE. *Level 2 operational requirements for hostile vehicle mitigation measures*. London: CPNI, 2010.

[5] CENTRE FOR THE PROTECTION OF NATIONAL INFRASTRUCTURE. *Vehicle security barrier scoping document*. London: CPNI, 2010.

[6] HM GOVERNMENT. *Pursue, prevent, protect, prepare – The United Kingdom's strategy for countering international terrorism*. London: The Stationery Office, 2009.

[7] CENTRE FOR THE PROTECTION OF NATIONAL INFRASTRUCTURE. *Protecting against terrorism*, third edition. London: CPNI, 2010.

[8] NATIONAL COUNTER TERRORISM SECURITY OFFICE. *Secure in the knowledge – Building a secure business*. London: London First, 2010.

[9] NATIONAL COUNTER TERRORISM SECURITY OFFICE. *Expecting the unexpected – Business continuity in an uncertain world*. London: London First, 2010.

[10] CENTRE FOR THE PROTECTION OF NATIONAL INFRASTRUCTURE. *Integrated security – A public realm design guide for hostile vehicle mitigation*, version 1.0. London: CPNI, 2011.

[11] CENTRE FOR THE PROTECTION OF NATIONAL INFRASTRUCTURE/DEPARTMENT FOR TRANSPORT. *Traffic advisory leaflet 1/11 – Vehicle security barriers within the streetscape*. London: CPNI/DfT, 2011.

[12] CENTRE FOR THE PROTECTION OF NATIONAL INFRASTRUCTURE. *Retractable vehicle security barriers – Maintaining road surface friction*. London: CPNI, 2012.

[13] CORMIE, D., MAYS, G., SMITH, P. *Blast effects on buildings*, second edition. London: Thomas Telford, 2009.

[14] CENTRE FOR THE PROTECTION OF NATIONAL INFRASTRUCTURE/DEPARTMENT FOR TRANSPORT. *Traffic advisory leaflet 2/13 – Bollards and pedestrian movement*. London: CPNI/DfT, 2013.

This page deliberately left blank

This page deliberately left blank

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email bsmusales@bsigroup.com.

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Copyright

Useful Contacts:

Customer Services
Tel: +44 845 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 845 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

bsi.

...making excellence a habit.™