INTERNATIONAL WORKSHOP AGREEMENT

IWA 14-2

First edition
2013-11-15

Corrected version
2014-01-15

Vehicle security barriers —

Part 2: Application

Barrières de sécurité de véhicule —

Partie 2: Applications

Reference number
IWA 14-2:2013(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

International Workshop Agreement IWA 14 was sponsored by UK Government's Centre for the Protection of National Infrastructure (CPNI) on behalf of the international community. The development of this IWA was facilitated by BSI Standards Limited. It came into effect on 15 November 2013.

IWA 14 consists of the following parts, under the general title *Vehicle security barriers*:

— *Part 1: Performance requirement, vehicle impact test method and performance rating*

— *Part 2: Application*

This corrected version of IWA 14-2:2013 incorporates editorial modifications.

Introduction

0.1 Workshop contributors

Acknowledgement is given to the following organizations that were involved in the development of this International Workshop Agreement:

— Allen Total Perimeter Security Limited

— APT Security Systems

— ATG Access Ltd

— BRE Global Limited

— Bristorm, Hill and Smith Ltd

— Centre for the Protection of National Infrastructure (CPNI)

— DELTA BLOC International GmbH

— GME Springs/Safetyflex Barriers

— Heald Limited

— HMS Nelson, Portsmouth Naval base

— Kirchdorfer Fertigteilholding GmbH

— L.I.E.R.

— Marshalls

— MFD International Limited

— Ministry of Commerce and Industry – Director General for Standards and Metrology (DGSM) (Sultanate of Oman)

— MIRA Ltd

— Norwegian Defence Estates Agency

— Perimeter Protection Group

— Perimeter Security Suppliers Association

— Rhino Engineering Ltd

— Royal Military Academy - Civil and Materials Engineering Department

— RSSI Barriers

— Sälzer GmbH

— Scorpion Arresting Systems LTD

— Ministry of Home Affairs (Singapore)

— Sudanese Standard and Metrology Organization (SSMO)

— Syrian Arab Organization for Standardization and Metrology (SASMO)

— Tallwang KVI PTY Ltd t/a AVS-elli

— Technical and Test Institute for Construction Prague

— Texas A&M Transportation Institute

— Transport Research Laboratory (TRL)

— US. Department of State

— US. Nuclear Regulatory Commission

— US. Army Corps of Engineers – Protective Design Center

0.2 Relationship with other publications

The following documents have been used to inform the development of this part of IWA 14:

— ASTM F 2656

— CWA 16221

— PAS 69

— PAS 68

Vehicle security barriers —

Part 2:
Application

1 Scope

This part of IWA 14 provides guidance for the selection, installation and use of vehicle security barriers (VSBs) and describes the process of producing operational requirements (ORs).

It also gives guidance on a design method for assessing the performance of a VSB.

2 Introduction to hostile vehicle mitigation

2.1 General

2.1.1 Vehicle-borne threats can range from the use of a vehicle for vandalism to determined attacks by adversaries (e.g. criminals and terrorists). The mobility and payload capacity of a vehicle can offer a tactical means to deliver a large explosive device and/or carry adversaries with attack tools. Hostile vehicles can be parked, manoeuvred or rammed in to or out of a site. Entry to, or exit from, a site can also involve surreptitious tampering with VSBs or their control apparatus, or the targeted placement of small explosive charges to breach the integrity of a barrier structure. Clear definition of the threat and the potential attack scenarios should be considered when deciding which methods of attack to defend against and consequently the most appropriate countermeasures.

2.1.2 The mitigation of all forms of vehicle-borne threat can be difficult while satisfying other business needs. The following should be considered as a minimum:

a) security:
   1) the level of residual risk is deemed acceptable by the organization;
   2) attack method to be mitigated;
   3) countermeasures;
   4) response to increased threat conditions;
   5) enforceable stand-off distance;

b) business needs:
   1) lifetime cost (training, manning levels, service, maintenance and replacement);
   2) traffic management;
   3) appearance;
   4) internal and external stakeholder requirements;

5) security risks induced by safety concerns or systems;

c) engineering constraints:

1) architectural;

2) foundations;

3) buried services;

4) land ownership and available space;

5) local authority planning restriction(s) (e.g. height/weight/noise restrictions of area of land, utilities).

2.1.3 It is important that a security operational requirement (OR) (see Clause 12) is developed in conjunction with a user requirement document (URD) and that all key stakeholders are involved from the outset.

2.1.4 The considered elements (i.e. security ORs, user requirements) can adversely influence each other. Therefore early consideration of acceptable compromises should be made, particularly with regard to the security and safety aspects of the VSBs.

2.1.5 There is likely to be a need to prevent unauthorized vehicle movement, to allow the safe, secure and timely transit of legitimate vehicles. Additionally, long-term security issues relating to system reliability and a change in threat level can also compromise the initial ORs. An unreliable VSB is unacceptable and has additional implications that may include costly compensatory measures to correct the condition. A change in threat can result in heightened security response levels and VSBs and procedures that cannot operate either safely or securely in that new environment.

NOTE See Clause 12 for further information on ORs.

2.1.6 Risk assessments should be conducted for safety and security early in the project design phase of project planning and after final installation to ensure the level of risk acceptable to the site is established and maintained. These assessments should be shared with or jointly produced by the stakeholders (e.g. site owner, security and safety representatives, project manager, staff association). The early engagement with the stakeholders can facilitate the development of business cases and can help identify potential issues, associated costs and constraints.

2.1.7 Often vehicular access has to be provided through the VSB line. The vehicles should be searched or be of known authenticity before arriving at the vehicle access control point (VACP). In this instance a single or multiple access point may be provided through the stand-off barrier line, e.g. rising, swing or sliding gate barriers. Where the stand-off measure forms the site boundary or site secure perimeter, the VACP then typically becomes the first point of challenge for all vehicles.

2.1.8 Regardless of the type of active VSB installed, a secondary access control point should be considered. This is to ensure that where the VSBs fail or there is an incident at the main VACP, traffic can easily be diverted to the secondary location. This location should be able to accommodate the traffic volumes typical to the main VACP while maintaining the same level of operational security.

2.1.9 Where an entrance has more than one VSB, for example a separate entry barrier and exit barrier, then each VSB should have independent drive and control systems. This is to prevent a cascade or nodal failure as a result of one VSB developing a fault. They may share the same user interface, hydraulic circuits and electrical systems, but should be designed so that its failure does not disable all VACPs. Provision of an uninterruptable power supply (UPS) or standby generator should also be considered.

2.2 Selection of a VSB

2.2.1 The selection of a VSB is dependent on a number of factors, including but not limited to:

a) the threat (Clause 3);

b) the assets to be protected (Clause 4);

c) the site (Clauses 5 and 6);

d) the required performance of the VSB (Clause 7);

e) the procurement strategy (Clause 8);

f) deployment and removal of the VSB (Clause 9);

g) the type of VSB required (Clauses 10 and 11).

2.2.2 The decision process for the selection of VSBs is illustrated in the flow diagrams in Clause 12, which covers ORs.

3 The threat

3.1 Identify and quantify the threat

3.1.1 Review any previous terrorist, criminal or malicious incidents and consider their relevance to your site regarding the target and attack methods used.

NOTE Contact your national, regional or local security force.

3.1.2 There are five main types of vehicle-borne threat. All can be deployed with or without the use of suicide operatives.

a) Parked vehicles – where unscreened vehicles are parked adjacent to a site, in underground parking facilities or overlooking a site.

b) Encroachment (exploiting gaps in defences) – where a hostile vehicle is negotiated through an incomplete line of barriers or an incorrectly spaced line of barriers without the need to impact. An alternative form of encroachment attack is exploitation of an active barrier system at a vehicle access control point (VACP) by a hostile vehicle "tailgating" a legitimate vehicle.

c) Penetrative attacks – where the front or rear of the hostile vehicle is used as a ram.

d) Deception techniques – a "Trojan" vehicle (one whose model, livery or registration is familiar to the site), or where hostile occupants negotiating their way through by pretence or by using stolen (or cloned) access control or ID passes. Alternative scenarios include an unwitting "mule", a driver unknowingly delivering an Improvised Explosive Device (IED) surreptitiously planted in their vehicle by an attacker, or an "insider" bringing an IED in to their own work site. Deception techniques prey on human and operational weaknesses.

e) Duress techniques – the driver of a legitimate vehicle is forced to carry an IED or where a guard controlling a VACP is forced to allow a vehicle entry. These are perhaps the most difficult forms of vehicle borne threat to defend against.

3.1.3 Site design can also accommodate countermeasures for layered attack scenarios using one or more of the threat types given in 3.1.2 a) to e), for instance, the use of a first hostile vehicle to create a gap by way of penetrative attack or blast which then allows a second to encroach through.

3.1.4 Potential threats to be considered:

a) whether the vehicle is parked outside or inside the security perimeter;

b) size of vehicle (both largest and smallest);

c) speed and direction of approach.

3.2 Duration of deployment

3.2.1 The period for which security measures is required (design life) should be defined.

3.2.2 Assess whether the security measures are to be operated continuously or occasionally. Decide whether a permanent, semi-permanent or temporary installation is required and identify the level of protection that the security measure is required to provide. Decide how and where the system is to be controlled from, i.e. controlled locally by guard, from a central control room or through the use of automatic access control systems (AACS).

3.2.3 A permanent installation is a physical measure, which may require significant civil engineering works and is expected to remain for the life of the asset.

3.2.4 A temporary installation is a physical measure that may be deployed on the basis that it remains *in situ* for a short period of time. The extent of the remedial measures required upon removal are kept to a minimum.

3.2.5 A semi-permanent installation is defined as a hybrid installation that incorporates some transitory elements that can be retracted or removed leaving any permanent foundation or anchorage *in situ*.

3.2.6 Assess and review at regular intervals whether the security measures need to be adapted to a change in the threat.

4 Assets

4.1 Identification of the critical assets

4.1.1 The assets to be protected should be identified, i.e. machinery, infrastructure, equipment, one or more buildings, an area, public event, or crowded place.

4.1.2 If more than one asset is identified, they should be prioritized.

4.1.3 It should be determined whether there is an existing defensible security perimeter and whether there is a need to establish a temporary or permanent perimeter security scheme.

4.1.4 The physical VSB strategy may be coordinated with adjacent interested parties.

4.2 Identification of stakeholders

The contact information should be obtained for all stakeholders who may be affected by the proposed security measures. These include but are not limited to staff, deliveries, local authorities, public transport, emergency services, utility companies, highway authorities, architects, neighbours and landlords.

4.3 Consideration of collateral damage

4.3.1 The consequences of a successful attack and the likely disruption in terms of loss of life, damage, delays, perception and business and financial impact should be assessed.

4.3.2 Locations or other assets which might suffer collateral damage, short- or long-term disruption to their operations from a successful attack should be identified. For example:

a) neighbouring buildings (e.g. government, military, residential, business, emergency services, schools, religious sites or other assets);

b) people;

c) major communication networks (above and below ground);

d) control rooms;

e) electricity, water and gas lines or storage facilities (above and below ground);

f) underground tunnels, basements and subways;

g) ventilation shafts;

h) bridges;

i) public transport infrastructure and airports.

4.3.3 Other locations/assets that might become alternative targets if the security strategy being employed at the principal asset is effective should be identified.

5 Site assessment

5.1 Review of existing security arrangements

Once the site security plans have been implemented that establish the acceptable level of security risk, a change control process should be adopted for any proposed site changes (e.g. site infrastructure, safety related, physical security related, VSB hardware and procedures) to ensure an acceptable level of risk is maintained. As part of the configuration control process, an analysis should be performed that ensures that acceptance of the proposed change does not reduce the effectiveness of the previous site security plans.

5.2 Site survey

5.2.1 All possible approach routes along which a hostile vehicle could challenge a VSB or secure perimeter should be determined. This includes all footpaths, footways, cycle paths, open spaces and gaps and also the likelihood of hostile vehicles travelling against the expected direction of traffic. The location and usability of drop kerbs/curbs and other adaptations for use by disabled persons should be considered.

5.2.2 Existing features should be identified that could be integrated into the vehicle mitigation scheme, such as resilient street furniture and traffic management measures. Consideration should be given to the effect on security of possible future changes to these features.

5.2.3 Any environmental conditions that might arise throughout the year that may be particular to the site should be identified, such as flooding, leaf mulch, frost, snow, ice, high wind speeds, sand storms, or extremes of temperature (see 7.5.4).

5.2.4 The existing road surface, kerbs and verges, gradients, camber or crossfall, at and in advance of, any proposed VSB location should be considered.

5.2.5 Any existing, or proposed road improvements or other works in the immediate area should be confirmed through the local planning office and highways department.

5.2.6 The need for a wider area traffic management plan should be reviewed and the impact of a perimeter security scheme on existing traffic movements should be considered.

5.2.7 If the potential threat exceeds the current security arrangements and any currently deployed VSBs' capability, additional protective measures should be considered.

5.2.8 The presence and location of all underground and overground services and utilities should be considered.

5.3 Civil works

5.3.1 Variations between VSB performance under vehicle impact test conditions and site conditions.

5.3.1.1 The performance of a VSB is likely to be affected by the site conditions.

5.3.1.2 When assessing the suitability of a VSB at a particular site, the performance of a VSB under site conditions should be assessed.

5.3.1.3 For example, the following site conditions could affect the performance of a VSB:

— urban areas, where utilities are frequently present;

— low temperature locations, i.e. frequently below –10 °C;

— high temperature locations, i.e. frequently above 40 °C;

— desert environments, where soil conditions are significantly different;

— wetland environments, where soil conditions are significantly different.

NOTE A suitably qualified engineer should determine how the VSB could be affected by non-standard conditions and should assess whether the VSB is fit for purpose under site conditions. The engineer should have experience in geotextiles, structural and mechanical work.

5.3.1.4 A process that should be followed to minimize the likelihood of performance variation is shown in Figure 1.

5.3.1.5 If a VSB is being evaluated for use at a specific site it could be beneficial to test the VSB in a site-specific construction.

NOTE A suitably qualified and experienced engineer could then evaluate the test result and adapt the installation for the specific site. NCHRP Report 350, "Recommended Procedures for the Safety Performance Evaluation of Highway Features", section 2.2.1, contains information about soil varieties.

5.3.1.6 It is known that varying the type of foundation (rigid/non-rigid) a VSB is installed in can affect the performance of the VSB. Further testing might be required if the tested conditions differ from the site conditions.

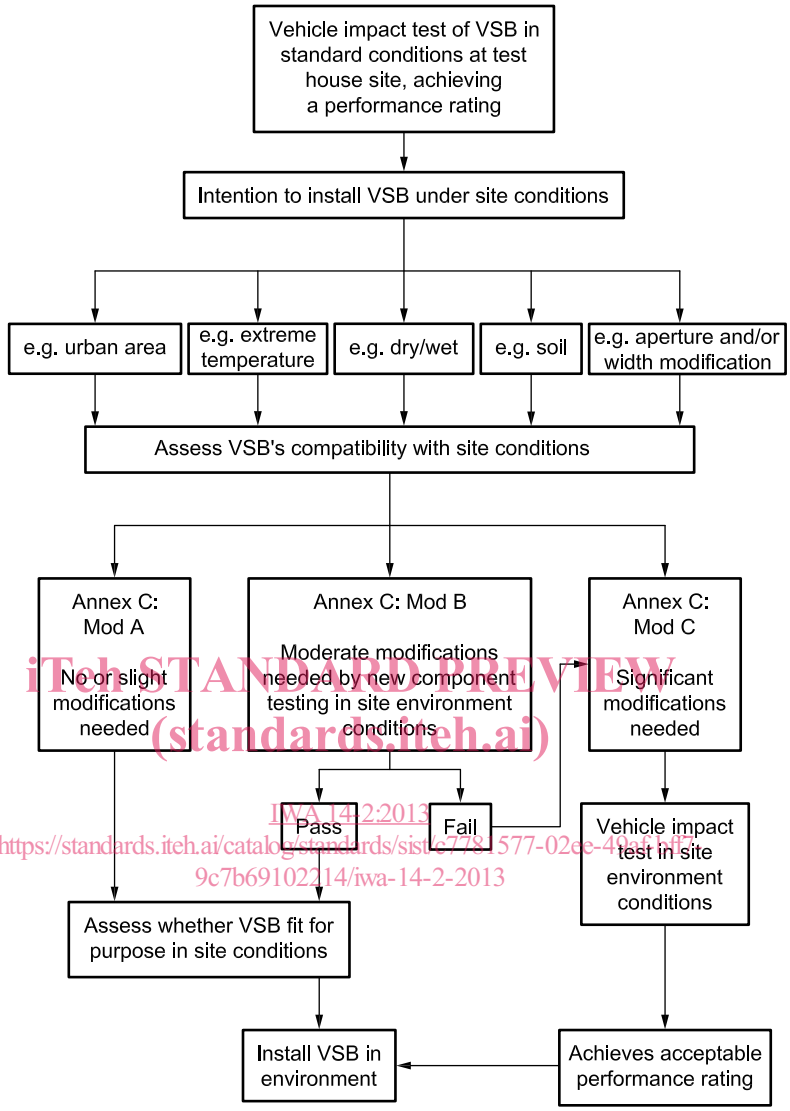

Figure 1 — Process for assessing a VSB for use under site conditions (informative)

5.3.2 Ground types

The ground should be assessed for its suitability for fixing to and supporting the selected VSBs.

NOTE This should be assessed by a suitably qualified and experienced civil/structural engineer and appropriate preparatory or remedial measures taken to ensure suitability. The engineer should have experience in structural and mechanical work.

5.3.3 Foundations

5.3.3.1 The depth required for foundations as well as the supporting ducting infrastructure for foul water drainage, sump pumps, soak aways, power and signal cables and contaminant (oil) collection should be assessed.

5.3.3.2 The ability of the concrete mix to flow in and around foundation steel (sections and reinforcement) should be considered to minimize voids and aggregate segregation.