INTERNATIONAL STANDARD

ISO 22343-2

First edition
2023-09

Security and resilience — Vehicle security barriers —

Part 2: Application

Sécurité et résilience — Barrières de sécurité pour véhicules —

Partie 2: Application

Reference number
ISO 22343-2:2023(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: 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 document 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).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents. ISO shall not be held responsible for identifying any or all such patent rights.

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

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 292, *Security and resilience*.

This first edition cancels and replaces IWA 14-2:2013, which has been technically revised.

The main changes are as follows:

— alignment with ISO 22343-1;

— updating of the document in light of changing threat and availability of tested vehicle security barriers (VSBs), i.e. surface-placed and shallow mount systems;

— re-organization of the document for international readability.

A list of all parts in the ISO 22343 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Security and resilience — Vehicle security barriers —

Part 2: Application

1 Scope

This document gives guidance on the selection, installation and use of vehicle security barrier (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.

This document is applicable to end users, such as site owners and specifiers, of VSBs, where they are used to protect people in any public or private location from vehicle attacks.

This document does not apply to the performance of a VSB or its control apparatus when subjected to:

— slow speed encroachment;

— slow speed nudging and ramming;

— blast explosion;

— ballistic impact;

— manual attack, with the aid of the vehicle (multiple impacts at slow speed);

— manual attack, with the aid of tools (excluding vehicles);

— electrical manipulation;

— attack on the control systems by any means.

NOTE 1 For manual attack, a variety of test methods exist. For assessing intruder resistance of building components, see LPS 1175[53].

NOTE 2 The VSB is designed and tested on the basis of:

a) vehicle type, mass and speed of the assessed vehicle-borne threat;

b) its geographical application (e.g. climate conditions);

c) intended site location (e.g. rigid or non-rigid soil/finished surface (paving, cobblestone, granite, asphalt).

It does not apply to guidance on design, the operational suitability of a VSB or other impact test methods.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 22343-1 , *Security and resilience — Vehicle security barriers — Part 1: Performance requirement, vehicle impact test method and performance rating*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 22343-1 apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

4 Introduction to hostile vehicle mitigation

4.1 General

4.1.1 Vehicle-borne threats

Vehicle-borne threats can range from the use of a vehicle for vandalism to determined attacks by adversaries (e.g. criminals and terrorists). The convenience, mobility and payload capacity of a vehicle offers a tactical means to deliver multiple adversaries and weapons (e.g. an explosive device, firearms or other hazardous payloads) closer to their target. Vehicles can also be used as a weapon: to drive into people to cause injury and/or ram into infrastructure to disrupt services.

To conduct such attacks, hostile vehicles can be parked, manoeuvred or rammed into or out of a site, or adversaries can use a deception or duress methodology.

Attacks on the VSB to enable access by the hostile vehicle without damaging the vehicle or occupants can include:

a) physical: forcing/tampering with the VSB or the use of an explosive device;

b) electronic: accessing and manipulation of the VSB control system or interfaced platforms (e.g. access control and building management systems).

A clear definition of the asset(s) (e.g. infrastructure and/or people) to be protected, the threat and how an attack can be manifested should be the foundation of a risk-based mitigation strategy.

4.1.2 Mitigation of vehicle-borne threats

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 deemed acceptable by the organization/interested parties;

   2) the asset(s) to be protected (see Clause 6):

      i) hard target (buildings and infrastructure);

      ii) soft target (people and crowded places);

   3) the attack method to be mitigated;

   4) security measures (their performance, deployment, operational and physical limitations);

   5) response to increased threat conditions;

   6) enforceable stand-off distance to the asset(s);

7) security risks induced by safety concerns or systems;

b) business needs:

1) lifetime cost (training, manning levels, service, maintenance and replacement, procurement options);

2) traffic management (vehicular and pedestrians);

3) appearance;

4) internal and external interested party requirements;

c) engineering constraints:

1) site topography;

2) architectural;

3) VSB technical and performance constraints;

4) foundations;

5) buried services;

6) land ownership and available space;

7) local authority planning restriction(s) (e.g. height/mass/noise, utilities).

It is important that a security OR (see Clause 16) is developed in conjunction with a user requirement document (URD) and that all key interested parties are involved from the outset.

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.

Risk assessments should be conducted for safety and security early in the design phase of project planning, during commissioning and after final installation to ensure the level of residual risk is identified and owned by the interested parties (e.g. site and or event owner, security and safety representatives, project manager(s), staff representatives).

These assessments should be shared with or jointly produced by the interested parties and regularly reviewed. Early engagement with the interested parties can facilitate the development of business cases and can help identify potential issues, associated costs and constraints.

There is likely to be a need to allow authorized 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.

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.

Often vehicular access has to be provided through the VSB line. The vehicles can be searched or be of known authenticity before allowing access through the vehicle access control point (VACP). In this instance, a single or multiple access point may be provided through the active security barriers. Where the stand-off measure forms the site boundary or security perimeter, the VACP then typically becomes the first point of challenge for all vehicles.

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.

Where an entrance has more than one VSB (e.g. 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 a failure does not disable all VACPs. Provision of an uninterruptable power supply (UPS) or standby generator should also be considered. An unreliable VSB is unacceptable and has additional implications that can include costly compensatory measures to correct the condition.

4.2 Selection of a VSB

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

a) the threat (see Clause 5);

b) the assets to be protected (see Clause 6);

c) the site (see Clauses 7 and 8);

d) the required performance of the VSB (see Clause 9);

e) the procurement strategy (see Clause 10);

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

g) the type of VSB required (see Clauses 12 and 13).

The decision process for the selection of VSBs is illustrated in the flow diagrams in Clause 16, which covers ORs.

5 The threat

5.1 Identify and quantify the threat

Previous and emerging terrorist, criminal or malicious incidents should be reviewed and their relevance to the site considered, regarding the target and attack methods used. Threats can evolve or change with time and it is recommended that periodic reviews of the threat and trends are undertaken, and the results recorded and documented, by the interested parties.

NOTE The national, regional or local security force can be contacted for threat level updates.

There are seven main methods a vehicle-borne threat (e.g. vehicle as a weapon (VAW) or a vehicle-borne improvised explosive device (VBIED)) can be deployed with or without the use of suicide operatives, as follows:

a) Parked vehicles: Unscreened vehicles are parked adjacent to a site, in underground parking facilities or overlooking a site.

b) Encroachment (exploiting gaps in defences): A hostile vehicle negotiates through/round 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 VACP by a hostile vehicle “tailgating” a legitimate vehicle.

c) Penetrative attacks: The front or rear of the hostile vehicle is used as a ram, either as a single or a repetitive impact, against the VSB.

d) Deception techniques: A “Trojan” vehicle (one whose model, livery or registration is familiar to the site) is used or where hostile occupants negotiate their way through by pretence or by using stolen (or cloned) access control or ID passes. Alternative scenarios include a driver unknowingly delivering an improvised explosive device (IED) or weapon(s) surreptitiously planted in their

vehicle by an attacker, or an "insider" bringing an IED/weapon(s) 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/weapon(s) 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.

f) Insider: A person with legitimate access willingly facilitates an attack by operating the security measures locally or remotely, managing or issuing access rights or tampering with the security measures.

g) Tamper/sabotage: With the intent of leaving no evidence, this attack facilitates hostile vehicle access at a later time. This can involve altering, weakening or disabling a barrier and/or associated security systems. This can be a physical or cyber-attack that occurs gradually over time or immediately before, in order to facilitate a fast-moving attack.

Consideration should be given to addressing the threat of layered attack scenarios using one or more of the threat types given in this subclause, and how physical and operational security measures should be introduced to counter that threat. 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.

5.2 Deployment considerations

5.2.1 General

The period for which security measures are required (design-life) should be defined.

The threat(s) should be assessed and an identification should be made of whether a permanent, semi-permanent or temporary installation is required as well as the level of protection that the security measure is required to provide.

5.2.2 Installation

For a new installation, the following types should be considered as part of the risk assessment and operating plans:

a) permanent installation, which can require significant civil engineering works and is expected to remain for the life of the asset;

b) semi-permanent installation, which is a hybrid that incorporates some transitory elements that can be retracted or removed leaving any permanent foundation or anchorage *in situ*;

c) temporary installation 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.

It is recommended that interested parties consider the advantages of choosing each of the above options where regular events are undertaken at the location, and whether there is a cost benefit to choosing option a) or b) rather than repeated deployment of option c).

It should be decided if, how and from where the system is to be controlled, e.g. controlled locally by guard, from a central control room or through the use of automatic access control systems (AACS).

An assessment and review should be made at regular intervals as to whether the security measures need to be adapted to a change in the threat.

6 Assets

6.1 Identification of the critical assets

The assets and their users to be protected should be identified as soft targets (e.g. people, an area, public event, crowded place) and hard targets (e.g. machinery, infrastructure, equipment, one or more buildings).

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

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.

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

6.2 Identification of interested parties

Interested parties should be identified and engaged at the start of the project and include both those who can deliver the solution as well as those affected by the proposed security measures. These include, but are not limited to, management, staff, security, local authorities, public transport, emergency services, utility companies, highway authorities, architects, security consultants, neighbours and landlords.

6.3 Consequence evaluation

The consequences of an attack and the likely disruption in terms of loss of life, damage, and business and financial impact and reputation should be assessed.

Locations or other assets which can suffer short- or long-term disruption to their operations from an attack should be identified. For example:

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

Threat displacement should be considered and communicated with all interested parties.

7 Site assessment

7.1 New locations

It should be recognized that the majority of measures to be installed will be retro-fitted to an existing asset, often in an urban environment, with challenges that come with working with existing services and structures, which can limit scope for innovation. When considering a new (green field) location, interested parties should introduce measures which can be specified for the site location, as well as the

design of the asset that can incorporate measures from the start of the build. This should minimize any compromise in security and will typically be more cost effective than installing a subsequent retrofit.

7.2 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.

The type of vehicles and their frequency of access and egress to the site should be established. The vehicles should also be assigned authorized and unauthorized pre-notified status and the means of access control defined for the different visitor types.

7.3 Site survey

All traversable routes along which a hostile vehicle can challenge a VSB or perimeter should be determined. This includes all carriageways, footways, cycle paths, open spaces and gaps. It should be recognized that there is likelihood that hostile vehicles can travel against the expected direction of traffic. The location and usability of drop kerbs and other adaptations in the streetscape should be considered.

A vehicle dynamics assessment (VDA) should be undertaken as part of the site survey. This provides a formalized evaluation of the speed that a threat vehicle, as identified in ISO 22343-1, can achieve at a specific location round the site. This enables the site to identify products including VSBs that have achieved a performance classification under ISO 22343-1 or an equivalent impact test standard for vehicle security barriers.

In many locations, it can be necessary to incorporate a vehicle swept path analysis to demonstrate the ability of the threat vehicle to access specific location or to ensure that authorized vehicles will not be compromised when accessing the site, by the location of the VSB.

The site survey should incorporate each of the site access locations such that the daily operation of the site is covered and that peak vehicle and pedestrian flow rates can be accounted for in the operation of the VACP and pedestrian barriers where appropriate.

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

Any environmental conditions that can arise throughout the year that can 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).

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

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

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.

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

The presence and location of all underground and above-ground services and utilities should be considered.

7.4 Traffic survey

Where appropriate, traffic surveys should be commissioned to identify traffic patterns and legitimate vehicle types at all proposed entry and exit points for representative periods. The peak traffic times and volumes and any special days/occasions which can create different traffic movements should also be identified.

The survey should consider the various categories of vehicle and their occupants that need to enter the proposed security zone legitimately, including public service vehicles, delivery vehicles, over-sized vehicles, taxis, very important people (VIPs), employees and emergency services. Site design should also accommodate infrequent over-sized vehicle access. Non-motorized vehicles and pedestrian movements should also be included in the survey. Contingency measures (e.g. movable elements of the VSB) can be used for infrequent over-sized vehicles and separate access points can be necessary to handle the volume of delivery vehicles determined by the traffic survey.

NOTE 1 See Clause 8 for additional site design considerations.

NOTE 2 Over-sized vehicles can include cranes, vehicle-mounted plant, multiple trailer vehicles, emergency equipment with extended wheelbase dimensions, etc.

7.5 Civil works

7.5.1 Variations between VSB performance under vehicle impact test conditions and site conditions

Having identified a VSB with a performance classification that meets the requirements of the specific location, it should be recognized that the impact test will be undertaken within specific parameters. Therefore, the site should ensure that the site conditions are recognized when installing the VSB in order that the performance rating is maintained and the VSB will operate reliably.

Factors that should be considered, include but are not limited to:

— 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.

It is recommended that a suitably qualified engineer determines how the VSB can be affected by non-standard conditions and assess whether the VSB is fit for purpose under site conditions. It is recommended that the engineer has experience in geotextiles, structural and mechanical work.

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

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

NOTE 1 A suitably qualified and experienced engineer can then evaluate the test result and adapt the installation for the specific site. See EN 1317-1 or Reference [49].

NOTE 2 Reference [51] contains information about soil varieties.

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

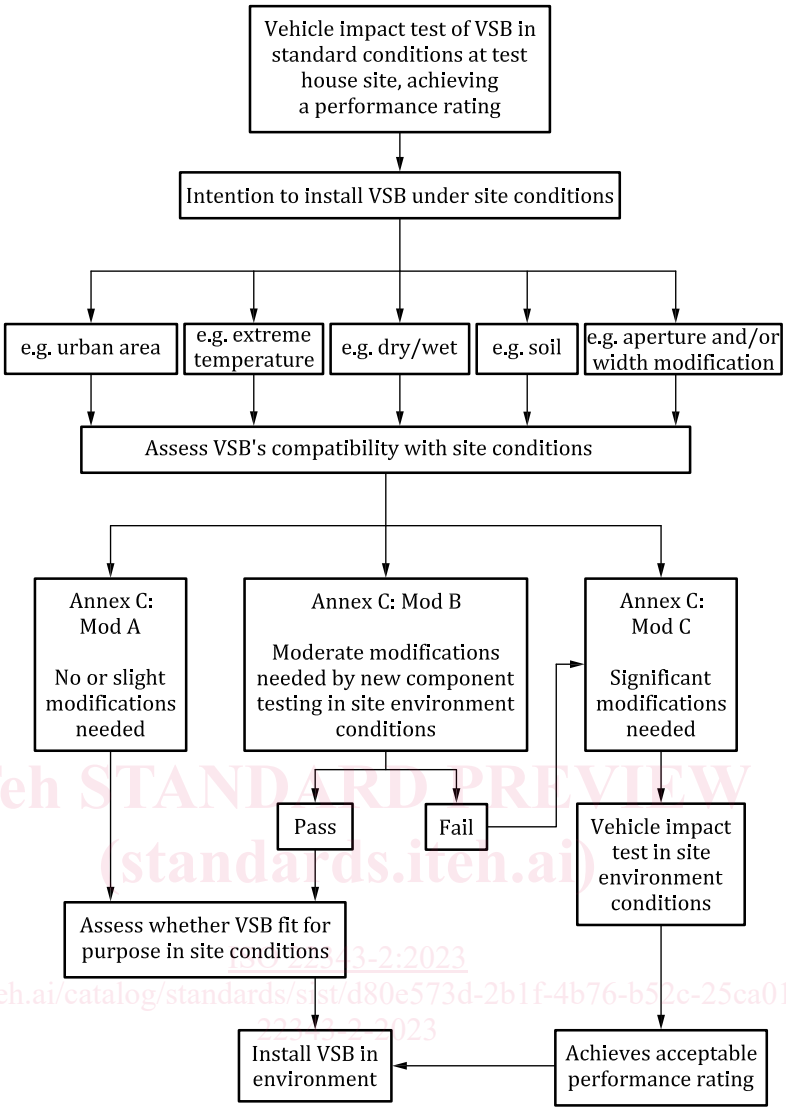

Figure 1 — Process for assessing a VSB for use under site conditions

7.5.2 Ground types

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

It is recommended that this be assessed by a suitably qualified and experienced civil/structural engineer and appropriate preparatory or remedial measures taken to ensure suitability. It is recommended that the engineer has experience in structural and mechanical work.

7.5.3 Foundations

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

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.

In many urban locations, underground services tend to be very close to the surface and often pass through gateways that are to be protected. In such locations, consideration should be given to