

PD CEN/TR 16705:2014



BSI Standards Publication

Perimeter protection — Performance classification methodology

bsi.

...making excellence a habit.™

National foreword

This Published Document is the UK implementation of CEN/TR 16705:2014.

The UK participation in its preparation was entrusted to Technical Committee B/201, Fences and gates.

A list of organizations represented on this committee can be obtained on request to its secretary.

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

© The British Standards Institution 2014. Published by BSI Standards Limited 2014

ISBN 978 0 580 85061 5

ICS 13.310

Compliance with a British Standard cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 30 April 2014.

Amendments issued since publication

Date	Text affected
------	---------------

ICS 13.310

English Version

Perimeter protection - Performance classification methodology

Protection périmétrique - Méthode de classification de
performance

Schutz von Grundstücksgrenzen - Methodologie für eine
Leistungsklassifizierung

This Technical Report was approved by CEN on 25 March 2014. It has been drawn up by the Technical Committee CEN/TC 388.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.



EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

Contents

Page

Foreword.....	5
0 Introduction	6
0.1 Purpose.....	6
0.2 Approach	6
0.3 Vital infrastructure	6
1 Scope	7
2 Normative references	7
3 Terms and definitions	7
4 Performance classification methodology	15
4.1 Outline of the approach	15
4.2 Determining the required the level of protection – picture of the methodology.....	16
4.3 Assumptions and starting point making the calculation model.....	18
4.4 The questionnaire of the calculation the model	20
4.4.1 Introduction to the questionnaire	20
4.4.2 Text of the questionnaire annex data entry sheet.....	21
5 Modus operandi	24
5.1 Introduction	24
5.2 Aggressor types.....	24
5.3 Scenarios	25
5.4 Toolsets	25
6 Risk assessment methodology	25
6.1 General.....	25
6.2 Risk – Target identification	26
6.3 Threats	26
6.4 Site characterization.....	26
6.4.1 General.....	26
6.4.2 Site and physical environment.....	26
6.4.3 Human and social factors of the environment	27
6.4.4 Use of the site	27
6.4.5 Type of access	27
7 Level of protection	27
8 Determining functional requirements.....	28
8.1 Introduction	28
8.2 Questions for establishing the functional requirement.....	28
9 Elements of possible solutions.....	29
9.1 Introduction	29
9.2 Elements of delay	29
9.2.1 Overview of elements of delay	29
9.2.2 Fences.....	30
9.2.3 Walls.....	31
9.2.4 Barriers	32
9.2.5 Gates	32
9.2.6 Roadblockers, Bollards.....	32
9.3 Elements of detection	32
9.3.1 Introduction	32
9.3.2 Overview of elements of detection	32

9.3.3	Detection	33
9.3.4	Exterior sensors PIDS	33
9.3.5	Lighting.....	33
9.3.6	Entry/exit control	33
9.4	External elements	34
9.5	Local law and regulations.....	34
10	Inventories	34
11	On testing.....	35
Annex A Security system operational requirements – Q and A		36
Annex B Framework for perimeter protection systems evaluation		39
Annex C An environmental and organizational checklist for perimeter protection		41
C.1	Introduction.....	41
C.2	Environmental checklist for perimeter protection	41
C.3	Organizational checklist for perimeter protection	45
Annex D A perimeter security technologies classification		49
D.1	Introduction.....	49
D.2	Four families for intrusion detection	49
D.2.1	Structure of the annex	49
D.2.2	Structure of the four main Tables D.3 to D.6	50
D.3	Stand-alone equipment.....	54
D.4	Fence-mounted sensors	58
D.5	Active Physical security	59
D.6	Underground sensors	62
Annex E Inventory of perimeter intruder detection systems (PIDs)		64
E.1	Introduction.....	64
E.2	Combination of two sensors	65
Annex F Matrix of current systems and (generic type) products		71
Annex G On Perimeter surveillance and burglary resistance		86
G.1	Introduction.....	86
G.2	Use of detection systems for perimeter protection	86
G.2.1	Basic requirements for perimeter surveillance systems	86
G.2.2	Basic principles of the detection systems.....	88
G.2.3	Comparison of detection systems.....	89
G.2.4	Summary	89
G.3	Classification for burglary resistance	90
G.3.1	Recommendations for the assessment of the resistance class.....	90
G.3.2	DIN-Standards for burglar resistance	91
Annex H Pictures of fences, gates and entrance barriers		92
H.1	Introduction.....	92
H.2	Different sorts of fences	92
H.2.1	Vegetable fences	92
H.2.2	Wood palisade	93
H.2.3	Walls	94
H.2.4	Metallic fences	96
H.2.5	Combinations of systems.....	99
H.3	Supplementary accessories	100
H.3.1	Razor wire.....	100
H.3.2	Sharp pins	100
H.4	Gates and entrance barriers.....	101
H.4.1	Gates.....	101
H.4.2	Road obstacles	102

Annex I CEN Workshop Agreement CWA 16221	104
I.1 Introduction	104
I.2 Scope of CWA 16221:2010	104
I.3 Table of Content of CWA 16221:2010	105
Bibliography	109

Foreword

This document (CEN/TR 16705:2014) has been prepared by Technical Committee CEN/TC 388 "Perimeter protection", the secretariat of which is held by NEN.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN [and/or CENELEC] shall not be held responsible for identifying any or all such patent rights.

The elaboration of this Technical Specification has been financially supported by the European Commission and the CIPS Programme (Grant Agreement N° HOME/2009/CIPS/FP/CEN-001).

0 Introduction

0.1 Purpose

The increasing need for customers to be able to select and purchase perimeter protection solutions that fit their needs calls for a generic and structured approach to the assessment of risks, to the identification of functional requirements, to the classification of perimeter protection solutions, including organizational measures, and to the design and test criteria for such perimeter protection solutions. This Technical Report is a step in the development of that approach.

The general goal that has been set is to make a European Standard that is applicable to a wide range of perimeter protection solutions, covering the needs for basic barriers and entrance solutions to more complex, high security solutions.

This Technical Report firstly describes the conceptual basis for further development of security performance requirements, technical specifications and test methods for use in perimeter protection systems in a European context. The report focusses on the performance classification methodology for the identification of the desired systems performance.

Secondly this Technical Report presents the results of inventories that have been made on current systems and (generic type) products that are available to the design engineer in both the public and private sector, relevant member states regulations, relevant documents from CEN, CEN/TC 325, ISO and other sources. The results are presented in annexes to this report.

This Technical Report therefore aims at providing information to be used for the design of future activities for making the 'perimeter protection standard'. It is not intended as a guidance for the actual development of perimeter protection systems. Nonetheless the information in this report may function as an aid to practitioners in their choice of appropriate measures in order to meet the diverse requirements.

0.2 Approach

Perimeter protection projects call for the interaction between suppliers of perimeter protection solutions, their customers and other relevant stakeholders. Only the proper interaction between these parties will lead to valid analyses and a certified perimeter protection solution.

A sequence of steps leading to the risk assessment, requested level of protection, functional requirements and basic selection of perimeter protection solution is proposed. The choice of the measure(s) to be taken depends upon a number of factors which include but are not restricted to: the local environment, the purpose of the measure(s), type property to be protected and environmental and organizational factors.

Perimeter protection systems or components may be used independently such as a perimeter fence or in combination with other measures in order to provide a more holistic solution such as a fence and gate. This approach may be extended to include Closed-Circuit TV systems (CCTV) and Perimeter Intruder Devices (PID).

To determine the risk involved for a site requiring perimeter protection is, for the most part, comparable to the analysis required for any given asset. Therefore this Technical Report builds on the work done for risk analysis by CEN/TC 325 'Crime prevention through building, facility and area design'.

0.3 Vital infrastructure

It is recognized that with regard to vital infrastructure and very high risk objects, the generic approach indicated in this Technical Report may not suffice and additional checklists and risk assessment tools may be required. There will be particular threats and modus operandi that should be considered when assessing vital infrastructure and very high risk objects that are outside the scope of this TR. For this reference can be made to documents from national authorities, etc.

1 Scope

This Technical Report aims at providing information to be used for the design of the future activities for making a 'perimeter protection standard'.

This CEN Technical Report describes a performance classification methodology for the identification of the desired systems performance for perimeter protection systems. It also gives a conceptual framework for matching the desired performance and the capabilities of a possible solution.

Furthermore this CEN Technical Report presents the results of inventories that have been made on current systems and (generic type) products, relevant member states regulations, relevant documents from CEN, CEN/TC 325, ISO and other sources. It should be noted that these inventories cannot be considered complete and any values given should be considered indicative values.

The following subjects are not covered by this Technical Report:

- threats approaching from the sea side;
- threats approaching through the air.

It is recognized that with regard to vital infrastructure and very high risk objects the generic system approach indicated in this Technical Report may not suffice and additional checklists and risk assessment tools may be required.

2 Normative references

Not applicable.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

NOTE The terms have been divided into three main perimeter related security categories: General, Electronic Security and Physical Security. The definitions are taken from existing documents as much as possible. Important sources are EN 14383-1:2006 [1], the term and definition standard from CEN/TC 325 "Crime prevention through building, facility and area design", and the Centre for Applied Science and Technology (CAST) [2].

3.1 General.

3.1.1

access control

set of techniques, means or procedures to control the passage of people and vehicles into and out of protected areas

[SOURCE: EN 14383-1:2006]

Note 1 to entry: Such systems allow levels of access rights and optionally the traceability of access, ranging from no entry to free traffic. The access control can be mechanical, human, electronic or a combination of these systems.

3.1.2

burglary

action of breaking into any premises with the purpose of theft

[SOURCE: EN 14383-1: 2006, modified]

3.1.3

neighbourhood

immediate surroundings of a secure site and their population

[SOURCE: EN 14383-1:2006]

3.1.4

operational requirement

statement of needs based upon a thorough and systematic assessment of the problems to be solved and the desired solutions

[SOURCE: PAS 68:2013]

3.1.5

perimetric space

space in close vicinity of the building (from the perimeter to the building envelope, including the accesses)

[SOURCE: EN 14383-1:2006]

3.1.6

peripheral space

land and neighbourhood around one or several sites

[SOURCE: EN 14383-1:2006]

3.1.7

risk analysis

identification and evaluation of threats

[SOURCE: EN 14383-1:2006, modified]

3.1.8

risk assessment

categorization of risks and measurement of their likelihood

[SOURCE: EN 14383-1:2006]

3.1.9

safety

freedom from unacceptable risk

[SOURCE: EN 14383-1:2006]

3.1.10

secure area

mechanically and/or electronically enclosed area protected for safety and/or security purposes [1]

3.1.11

security

freedom from an intended risk

[SOURCE: EN 14383-1:2006]

Note 1 to entry: Security is the condition of being protected against danger or loss. It is achieved through the mitigation of adverse consequences associated with the intentional or unwarranted actions of others. See [7].

3.1.12

standoff

distance that threat (e.g. vehicle, person, any potential explosive effect) may be allowed to encroach upon a perimeter or asset

[SOURCE: PAS 38:2013]

3.2 Electronic security.

3.2.1

active infrared

infrared beams transmitted between a transmitter and receiver which are broken when an intruder passes through

[SOURCE: PAS 38:2013]

Note 1 to entry: The receiver detects this as a drop in signal level.

3.2.2

alarm transmission

automatic transmission of alarm signals from an intrusion detection system to a monitoring centre or to a private individual

[SOURCE: EN 14383-1: 2006]

3.2.3

dead zone

area bounded by, or laying within the detection zone where a target cannot be detected

Note 1 to entry: That is either intrinsic to the detection system or due to some topographical feature within the detection zone (i.e. obstacle or hollow).

3.2.4

detection rate (DR)

measure of a system's capacity to detect an intrusion attempt (true alarm) through the zone protected by the system

[SOURCE: Centre for Applied Science and Technology (CAST)]

3.2.5

detection zone

area over which a detection system is configured to monitor for intruders

Note 1 to entry: The detection zone can also have upper and lower bounds: the detection ceiling and the detection floor.

3.2.6

doppler microwave

unit that emits a microwave field and monitors reflections

[SOURCE: Centre for Applied Science and Technology (CAST)]

Note 1 to entry: Motions from an intruder cause a change in the reflected signal received by the detector.

3.2.7

dual technology

combination of two separate technologies

[SOURCE: Centre for Applied Science and Technology (CAST)]

Note 1 to entry: For free-standing applications these technologies tend to be passive Infrared combined with doppler microwave, though other combinations exist.

3.2.8

environmental information / conditions

data pertaining to both weather and wildlife events in the vicinity of the perimeter

[SOURCE: Centre for Applied Science and Technology (CAST)]

3.2.9

electrified fence

detection system comprising horizontal electrical conductors which are energized approximately every 2 s with typically a 10,000 volt pulse

[SOURCE: Centre for Applied Science and Technology (CAST)]

Note 1 to entry: This pulse voltage will decrease if the fence is touched or is short circuited to ground and an alarm condition can be raised.

3.2.10

electrostatic field disturbance

arrays of wires create an electromagnetic field and sense either the current induced in neighbouring wires or the capacitance between the transmitter and the ground

[SOURCE: Centre for Applied Science and Technology (CAST)]

Note 1 to entry: The capacitance varies when an intruder approaches the barrier. Ported coax and leaky feeder systems come under this definition.

3.2.11

fabric-mounted PIDS

detection systems that are attached directly to the barrier material (as opposed to the fence posts)

[SOURCE: Centre for Applied Science and Technology (CAST)]

3.2.12

false alarm

alarm not caused by a human breaching the detection zone

[SOURCE: Centre for Applied Science and Technology (CAST)]

Note 1 to entry: Typically, false alarms are caused by animals, the effects of the weather or may have no obvious cause.

Note 2 to entry: Alternative definition:

alarm condition which has not resulted from:

- a) a criminal attack, or attempt at such, upon/to the supervised premises, the alarm equipment or the line carrying the alarm signal; or
- b) damage, or attempt at such, to the supervised premises, the alarm equipment or the line carrying the alarm signal; or
- c) actions by emergency services in the execution of their duties.

3.2.13

false alarm rate

FAR

measure of a system's capacity to avoid generating alarms which are not caused by human activity

[SOURCE: Centre for Applied Science and Technology (CAST)]

Note 1 to entry: False alarm rate (FAR) is expressed as the number of false alarms per day per kilometre (ADK).

3.2.14

fibre optic – interferometric

deformation of the detection cable causes a change in the path length in the fibre and hence the phase of laser light transmitted within the fibre

[SOURCE: Centre for Applied Science and Technology (CAST)]

3.2.15

fluid-filled tubes

parallel tubes typically filled with liquid are pressurized and connected via a piezoelectric membrane producing a balanced system

[SOURCE: Centre for Applied Science and Technology (CAST)]

Note 1 to entry: Differential pressure on the ground forces the fluid between the tubes and generates a voltage at the piezoelectric element. Requires access pits to pressurize the tubes and house the sensors.

3.2.16

geophone (point sensor)

series of low frequency microphones or accelerometers connected together and their outputs analyzed

[SOURCE: Centre for Applied Science and Technology (CAST)]

Note 1 to entry: Addressable point sensors can attribute alarms to a particular sensor.

3.2.17

height of detection zone

nominal maximum height of the detection zone relative to ground level

3.2.18

inductive cable

cable with conductive wires suspended in a magnetic field

[SOURCE: Centre for Applied Science and Technology (CAST)]

Note 1 to entry: Small currents are induced when the barrier and cable are disturbed.

3.2.19

maximum speed of crossing

maximum speed (metres per second) at which a target crossing the detection zone can travel and be successfully detected

3.2.20

microphonic

use of piezoelectric or triboelectric cables to detect audio frequency vibrations effectively acting as a microphone

[SOURCE: Centre for Applied Science and Technology (CAST)]

3.2.21

minimum target dimensions

minimum dimensions of a target that can cross the detection zone and be successfully detected

3.2.22

minimum target mass

minimum mass of a target that can cross or interact with the detection zone and be successfully detected

3.2.23

minimum speed of crossing

minimum speed (metres per second) at which a target crossing the detection zone can travel and be successfully detected

3.2.24

monitoring centre

private or public place staffed 24 h which takes action on receiving the remote alarm transmissions from automatic intrusion or fire detection systems

[SOURCE: EN 14383-1: 2006]

3.2.25

passive infrared

detectors sense the temperature contrast between an intruder and the background environment [2]

3.2.26

perimeter intruder detection system (PIDS)

external detection systems configured to detect a human target crossing from one side of a linear detection zone to the other

[SOURCE: Centre for Applied Science and Technology (CAST)]

3.2.27

post-mounted PID

wire or cable based perimeter intruder detection system mounted on posts attached to the barrier or mounted directly in front of or behind the barrier

[SOURCE: Centre for Applied Science and Technology (CAST)]

3.2.28

radar

antenna sends out a radio frequency pulse and detects the reflections from intruders and can determine their distance and speed

[SOURCE: Centre for Applied Science and Technology (CAST)]

Note 1 to entry: The antenna can either be static (linear) or rotating (wide area).

3.2.29

range (detection)

nominal maximum distance from a detector at which a detection system can be expected to generate an alarm in the event of a target crossing

3.2.30

tamper alarm

alarm generated by the system to indicate its integrity has been compromised

[SOURCE: Centre for Applied Science and Technology (CAST)]

Note 1 to entry: Typically this is a result of someone gaining access to the control circuitry or causing damage to the system.

3.2.31

target classification

capacity of a system to provide information pertaining to the target such as dimensions; or to categorize the likely intrusion type in addition to an alarm

3.2.32

target location

capacity of system to provide information as to the location of the target within the detection zone, in addition to an alarm

3.2.33

taut wire

wires under tension are monitored by mechanical sensors for changes in tension caused by intrusion events

[SOURCE: Centre for Applied Science and Technology (CAST)]

Note 1 to entry: Hybrid electrified taut wire systems are also available.

3.2.34

true alarm

any alarm or group of alarms caused by a human crossing the specified detection zone

[SOURCE: Centre for Applied Science and Technology (CAST)]

3.2.35

video-monitoring (CCTV)

technical means by which camera captured images are gathered, observed, stored, processed and transmitted (CCTV: Closed Circuit Television)

[SOURCE: EN 14383-1: 2006]

3.2.36

video motion detection

computer software that analyses video footage for motion or characteristics typical of an intrusion event by means of analyzing variations between video frames

[SOURCE: Centre for Applied Science and Technology (CAST)]

3.2.37

vulnerability to defeat

assessment of a system's vulnerability to disruption or sabotage by a knowledgeable attacker intent on disabling it

[SOURCE: Centre for Applied Science and Technology (CAST)]

3.2.38

width of detection

nominal maximum width of detection zone (for systems whose zone of detection is linear)

3.3 Physical security.

3.3.1

active system

security barrier which requires operation either by personnel or powered equipment

[SOURCE: PAS 38:2013]

Note 1 to entry: For example a manual dropping/ lifting-arm barrier or an automated retractable/rising bollard.

3.3.2

barrier

mechanical device to control the passage of vehicles (hand or power operated)

3.3.3

bollard

manufactured product which, once positioned, is a vertical device aimed at delimiting an area and hampering the access for vehicles

[SOURCE: EN 14383-1: 2006, modified]

3.3.4

folding gate

gate with two or more hinged leaves, guided and/or supported at the bottom and/or at the top

Note 1 to entry: The first leaf is hinged to the frame; leaves can be hinged only on one side of the frame or on both sides.

3.3.5

gate/door

device to close an opening in a boundary demarcation which is provided for the passage of vehicles and/or persons (hand or power operated)

3.3.6

hinged gate

gate with a leaf which is hinged or pivoted at one side which opens one way (single leaf or double leaf hinged gate)

3.3.7

locking system

equipment used to prevent an opening device from being opened without the use of a key or other mechanism designed for this purpose

[SOURCE: EN 14383-1: 2006]

3.3.8

planter

massive or well-anchored container (wood, concrete, steel, etc.) filled with soil and decorated with plants for the purpose of stopping vehicles

[SOURCE: EN 14383-1: 2006]

3.3.9

retractable bollards

device which can easily be lowered and secured in its position with a key (mechanical) or through a powered mechanism (automatic)

[SOURCE: EN 14383-1: 2006]

3.3.10

road blocks

device to stop vehicles, e.g. retractable ramps

[SOURCE: EN 14383-1: 2006]

3.3.11

sliding gate

gate with a leaf or leaves that moves horizontally in its guides (cantilever or moving on a roller rail)

Note 1 to entry: There are single leaf or bi-parting or telescopic sliding gates (gate leaf consisting of two or more parts).

3.3.12

speed gate

folding or sliding gates with one or more leaf (leaves) designed for rapid operation (> 0,5 m/s)

3.3.13

sterile zone

defined controlled area, normally clear of obstructions and undergrowth, incorporating measures to preclude larger wildlife and accidental incursion from personnel

[SOURCE: Centre for Applied Science and Technology (CAST)]

3.3.14

turnstile

form of gate which allows one person to pass at a time (and or power operated)

Note 1 to entry: Full-height turnstiles are similar in operation to a revolving door.

3.3.15

traffic calming

use of self enforcing physical measures to produce road alignments that require a reduction in vehicle speed in order to be successfully negotiated

[SOURCE: PAS 38:2013]

3.3.16

vehicle airlock system

system created by using two active barriers of any type across the vehicle path of approach, with a secure sterile area between the barrier

[SOURCE: PAS 38:2013]

3.3.17

vehicle security barrier

system designed and installed to bring to rest or redirect an impacting vehicle

[SOURCE: PAS 38:2013]

4 Performance classification methodology

4.1 Outline of the approach

Unprotected perimeters mean unprotected assets, unprotected people and inevitably security breaches. The consequences of these breaches can be catastrophic so the threat of intrusion remains a prime concern at all major facilities.

The approach presented in this report starts with a calculation model that generates a score indicating the required level of protection.

Important key questions for the client are:

- What are my assets I should be protecting?
- Against what threats?
- What are my vulnerabilities and risks?

Once the required level of protection has been established, the basic performance requirement, the required time of delay, has to be determined or chosen.

It is possible that other more general functional requirements have been identified during the process. The complete set of functional requirements and performance defines the overall set of requirements the perimeter security (system) solution has to meet.

Given the available elements for a perimeter security solution and their individual performance characteristics, most likely various security systems can be generated that meet the overall set of requirements. A schematic view of this approach is given in Annex B, 'Framework for perimeter protection systems evaluation'.

4.2 Determining the required the level of protection – picture of the methodology

The assessment of the desired performance of the perimeter protection system is based on two variables:

The first variable is related to risks, threats and vulnerability. By filling out a questionnaire regarding risks and threats the user of the method can get a clear understanding of his current situation. For such an analysis, the scenarios to be expected have to be defined along with the toolset the intended aggressor may use (together forming the Modus operandi). The outcome is a number for the Potential risk. Based on the Potential risk the desired Level of protection is chosen.

The second variable is related to the site. In the second part of the questionnaire site characteristics are evaluated such as surroundings roads and practical conditions of use. The outcome is a number for the site characterization.

NOTE This number is similar to 'Potential significance' as used by CEN/TC 325.

The Potential risk and the Site characterization combined define the Level of protection, which is the starting point to identify the necessary Functional requirements.

The methodology described above is implemented in a calculation model. Figure 1 presents an overview of the elements of the method.

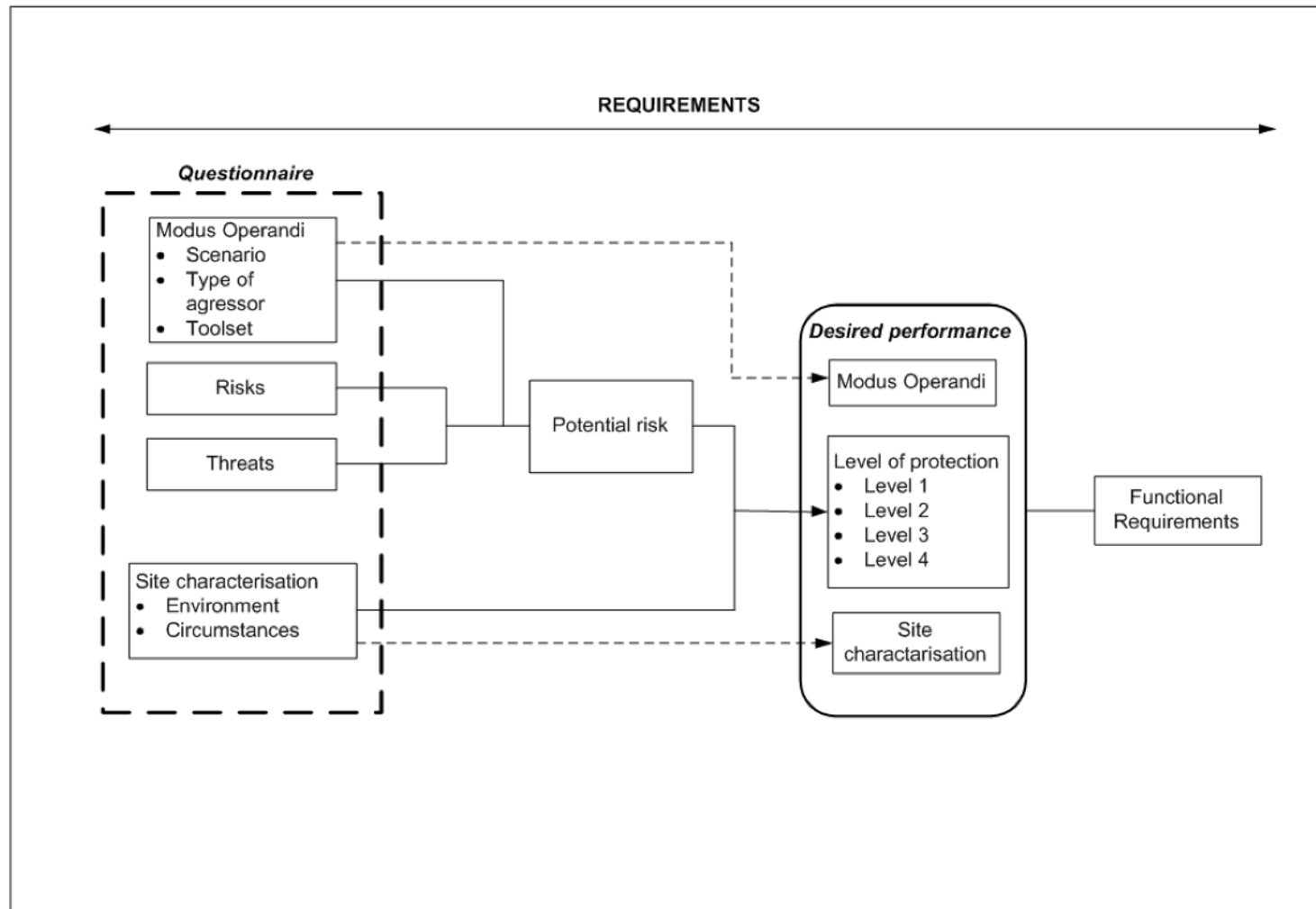


Figure 1 —Subsequent steps in the assessment model

The description of the elements shown in Figure 1 is given in the following subclauses on the calculation model.

4.3 Assumptions and starting point making the calculation model

The following assumptions and starting points have been used to compose the questionnaire and the calculation model to determine the numbers for the Potential risk and the Site characterization.

a) Relevant aggressor types:

Four aggressor types should be sufficient to cover the Modus operandi with intended breach of the perimeter. More detail will not add relevant information on the ways the attack will take place, nor will it differentiate better in the perseverance of the potential attacker. The four aggressor types reflect mainly the level of know-how, preparation and motivation.

b) Terrorist attack:

In case the Modus operandi involves the potential threat of a terrorist attack, the perimeter protection shall always involve extensive (organizational) measures.

c) Multiple Modus operandi:

In case several risks are involved with different Modus operandi, the model requires the highest risk be chosen.

- 1) It can be the case that different risks require different security measures. For instance if an activist is likely to pass over a fence (to make a statement) and a thief is likely to penetrate the fence to be able to transport the stolen goods.
- 2) The model identifies the highest risk, but compartments (a lay-out of the site in different zones) can apply to select areas with lower required levels of security. However, this requires that the user knows what the highest risk (factor) is.

NOTE An option would be to add the risks (combine the scores), but this complicates the model with little to gain. Alternatively, one could compare the scores before continuing in the questionnaire to the section on Site characterization.

d) Inside and outside:

All valuables on the site are applicable to the risk assessment, both inside as well as outside the buildings.

NOTE CEN/TC 388 and CEN/TC 325 have a different perspective as illustrated in Figure 2.

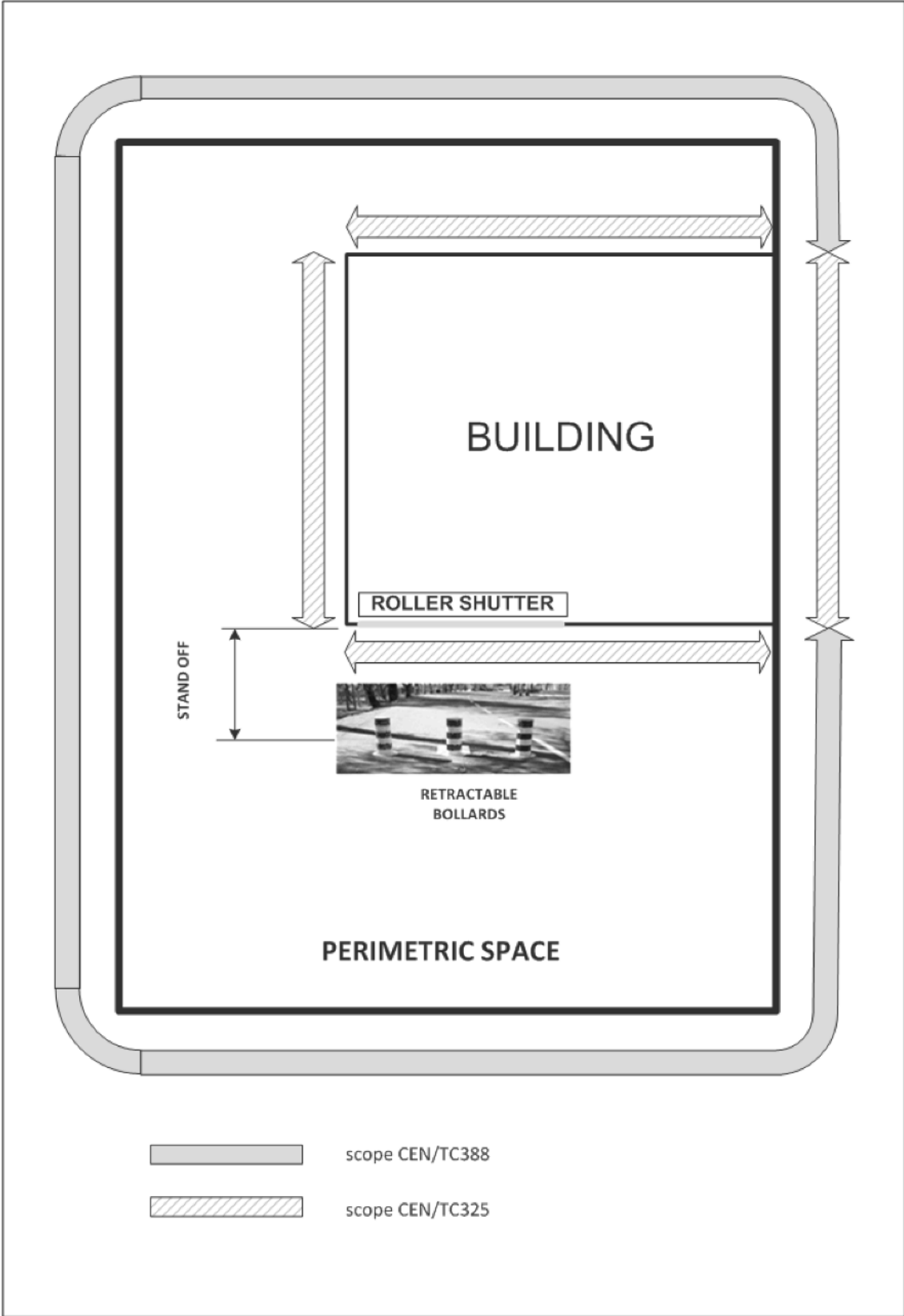


Figure 2 — Different perspectives of CEN/TC 388 and CEN/TC 325

- e) First choose the relevant Modus operandi, and then fill in the model.

If the scenario is an attack by an activist, and there is no risk of taking any valuables (there are no valuables), then MO 1 should be chosen. Multiplication with a risk factor would make no sense for this threat.

If the scenario is an attack by an activist, and there is a medium threat for business continuity, then MO 2 should be chosen. Multiplication with the risk factor 1,5 would be appropriate.

NOTE For most Modus operandi only the impact on one or two risk in the calculation model (out of 1.1., 1.2, 1.3) are relevant. The total maximum score of 90 requires a terrorist threat on all three items.

- f) Consider geographic spread of occupancy

This parameter measures to what extent the site/buildings are monitored by personnel during operating hours through their presence at the site.

NOTE At a highly monitored site every part is in use and monitored at least each 30 min.

- g) Access requirements influence the risk for a site

The access requirements regarding vehicles, people and goods require suitable security measures. A site which is visited by external parties, at irregular times including the nights, has a greater security risk than a site which is used only by personnel at regular time frames.

NOTE Access requirements have influence on the quality of the gates, the number of entrance points, time that a gate can remain open, or the way people are monitored at a site and have authorization to access the site at different timeframes.

4.4 The questionnaire of the calculation the model

4.4.1 Introduction to the questionnaire

Answers to relevant questions regarding risks and site characterization should be given in the form of a score selected from the range of factors and the subtotals expressed as a percentage of the maximum value.

Figure 3 gives a partial picture of the first part of the data entry sheet of the calculation model. The risk level value is multiplied by the MO-dependent risk factor. Both the MO-dependent risk factor and the risk level value (for risk 1.1 Importance of goods) are marked in light grey.

Potential risk	Value	Factor				Score	Max
		MO 1	MO 2	MO 3	MO 4		
		1	1,5	2	3		
1.1 Importance of goods (Market value of goods)						%	18
Low	1	1	1,5	2	3		
Medium	4	4	6	8	12		
High	6	6	9	12	18		

Figure 3 — Data entry sheet calculation model (partial)

NOTE 1 The wording 'potential risk' is used here instead of simply 'risk' since CEN/TC 325 uses this terminology. As for 'potential significance' the present document does not follow CEN/TC 325. The wording 'site characterization' is used for that part of the classification methodology.

Both the MO-dependent risk factor and the risk level values (see 4.4.2) are to be considered as preliminary values still to be discussed further. In fact that holds for the whole of the questionnaire.

NOTE 2 The question of the types of risks is a good example for this. In the questionnaire three risks are mentioned. Yet it has been noted that the 'human aspect' is missing. It is possible therefore that risks like 'Trauma to people', 'Image damage' and 'Damage to society/public' will be considered a future version.





4.4.2 Text of the questionnaire annex data entry sheet

More detailed information on the key elements of the questionnaire can be found in Clause 5 'Modus operandi' and Clause 6 'Risk assessment methodology'. Below the full text of the (present version of the) questionnaire is given:




Potential risk	Value	Factor				Score	Max
		MO 1	MO 2	MO 3	MO 4		
		1	1,5	2	3		
1. Importance of goods (Market value of goods)							18
low	1	1	1,5	2	3		
medium	4	4	6	8	12		
high	6	6	9	12	18		
2. Operational and environmental safety							45
low	1	1	1,5	2	3		
medium	10	10	15	20	30		
high	15	15	22,5	30	45		
3. Business Continuity (Confidential documents, prototypes, machinery etc.)							27
low	1	1	1,5	2	3		
medium	6	6	9	12	18		
high	9	9	13,5	18	27		
Total of potential risk (assets)							90
Total score potential risk							%

Site characterization

1. Site and physical environment	Value	Factor	Score	Max
1.1 Density of the area		3		9
low density	3	9		
medium density	2	6		
high density	1	3		
1.2 Access and road network		2		6

multiple accesses from several roads, close to an intersection	3	6		
two-way road	2	4		
single track road or cul de sac	1	1		
1.3 Type of access road		2		6
Public road	3	6		
Semi-public road	2	4		
Private road	1	1		
1.4 Presence of landscaping giving visual obstructions		3		9
low (attacker cannot hide)	3	9		
medium (some visual obstruction)	2	6		
high (easy to hide during attack)	1	3		
1.5 Level of noise		1		3
low	1	1		
medium	2	2		
high	3	3		
1.6 Site adjoins railway line or river or wooded area		1		5
yes	5	5		
no	0	0		
Subtotal 1 Site and Physical environment				38
Subtotal 1 Score				%

2. Human and social factors of the environment

2.1 Crime history		1		20
No major incidents	1	1		
Incident in last three years	10	10		
Incident in last year	20	20		
2.2 Visitor impression of tidiness/level of organization		1		12
poor	12	12		
average	6	6		
good	1	1		
2.4 Crime rate in neighbourhood compared to national average		1		10
low	1	1		
medium	5	5		

high	10	10		
Subtotal 2 Human and social factors				42
Subtotal 2 Score				%
3. Use of the site (occupancy)				
3.1 Periods of occupancy (during operating hours some parts of the site are not monitored (for over 30 min)		concentrated	non-concentrated	15
24/7	–	1	5	
daytime	–	5	10	
seasonal	–	10	15	
Subtotal 3 Use of the site				15
Subtotal 3 Score				%
4. Access				
4.1 Do you have a need of access for employees? Select highest category		1		10
Pedestrians	1	1		
Cars	3	3		
Trucks	7	7		
Boat or train	10	10		
4.2 Does the site require access by external parties? Select highest category		1		20
Pedestrians	2	2		
Cars	6	6		
Trucks	14	14		
Boat or train	20	20		
4.3 Type of access		regular	irregular	10
daytime	–	1	5	
night	–	5	10	
4.4 Access intensity Intensity (use)		regular	irregular	15
low	–	1	3	
medium	–	5	8	
high	–	10	15	
Subtotal 4 Access				55

Subtotal 4 Score

%

Total of potential significance		155
Total score potential significance		%

155

Total score potential significance

%

5 Modus operandi

5.1 Introduction

Most breaches of perimeter security on a site are committed because aggressors enjoy opportunities: easy access, hiding places, absence of demarcation of the site, poor lighting and/or favourable landscaping. It is important to analyse and identify in order to understand the motivation of potential aggressors.

Modus operandi should cover all combinations of:

- aggressor type (5.2);
- scenario to breach the perimeter (5.3);
- toolset (5.4).

The aggressor type is the most important 'constituent' of the Modus operandi. Four Modus operandi (MO 1 to MO 4) should cover all possible situations with intended breach of the perimeter. Further detailed descriptions are deemed irrelevant, as it does not add to the ways the attack will take place, nor will it differentiate in the perseverance of the potential attacker.

5.2 Aggressor types

Four aggressor type are distinguished:

- 1) Opportunist – vandalism and theft;
- 2) Activist;
- 3) Organized crime (creating opportunity, experienced);
- 4) Terrorist.

The types reflect the level of know-how, preparation and motivation of the attacker. For example, opportunists are those who will commit an offence if the opportunity presents itself. They are interested in sites with easy access, a low level of surveillance and ready escape routes.

A more experienced aggressor will, prior to carrying out an offence, conduct an important phase of gathering information. It is also probable that he will have a specific target in mind and may be prepared to use more effective tools to gain entry to the site. He very often has expertise in bypassing or sabotaging mechanical, electronic or CCTV and electronic detection devices.

5.3 Scenarios

The most likely methods to breach the perimeter are:

- walk in;
- reach over;
- climb over;
- go underneath;
- swim/sail over inland water;
- intrusion with hand tools;
- intrusion with electric/pneumatic toolset;
- intrusion with hydraulic tools;
- vehicle intrusion/attack.

5.4 Toolsets

To be able to choose the proper Modus operandi, the tools the attacker may be expected to use have to be determined or chosen.

The user of the present classification methodology might want to choose his own list. A list distinguishing between three toolsets is given here as an example:

- a) manual, easily-portable tooling crowbar, handsaw, hammer and pliers;
- b) intermediate tooling including battery-operated tools, car jack;
- c) power operated tools including petrol-driven tools.

NOTE If a fixed list of pre-defined toolsets is considered necessary, the development such list will be part of the future activities.

6 Risk assessment methodology

6.1 General

Although the methods for risk assessment for perimeter protection can be generic, a risk assessment itself shall be conducted specifically for each site. It should take into account the perimeter and its location, the assets on the site, their value and their function and the threats and their probability.

Completing the risk assessment itself is a task performed by people. It is a task that is highly influenced by a number of (subjective) factors such as: moment in time, past experiences, interaction of stakeholders, skills and competences of the people involved and complexity of the situation. The validity of a risk assessment therefore depends on the availability of a comprehensive structure and the minimization of interpretation.

The risk assessment has to be conducted from the customer/user point of view and not from the product point of view. Considering the purpose of the risk assessment itself, it is of importance that all relevant stakeholders are involved in the assessment and that the assessment is formally accepted by the customer. Stakeholders are everyone who has an interest in the security of the site including site owner, site users, budget holders and security managers.

6.2 Risk – Target identification

Risk is defined by the probability of an event multiplied by its impact. For a site owner or user of a site, the risks to analyse can be (see Questionnaires 1.1 to 1.3):

- 1.1. Financial loss;
- 1.2. Operational and environmental safety;
- 1.3. Business Continuity (Confidential documents, prototypes, machinery).

NOTE It has been noted that the 'human aspect' is missing. It is possible therefore that risks like 'Trauma to people', 'Image damage' and 'Damage to society/public' will be considered in the future.

6.3 Threats

Threats can be:

- a) burglary - thefts of goods, thefts of information, thefts of data;
- b) vandalism;
- c) aggression to people;
- d) sabotage;
- e) damage by arson;
- f) product contamination;
- g) espionage;
- h) escape;
- i) non complying / breach of health and safety regulations.

The threats enter the questionnaire through the choice of the risk level (risk value) taken into account.

6.4 Site characterization

6.4.1 General

Site characterization with regard to e.g. surroundings, access and use should be reviewed in order to determine vulnerability and necessary resistance methods.

6.4.2 Site and physical environment

See Questionnaires 1.1 to 1.6:

- 1.1. Density of the area;
- 1.2. Access and road network;
- 1.3. Type of access road;
- 1.4. Presence of landscaping giving visual obstruction;

- 1.5 Level of noise;
- 1.6. Site adjoins railway track, river, wooded area.

6.4.3 Human and social factors of the environment

See Questionnaires 2.1 to 2.3:

- 2.1. Crime history;
- 2.2. Visitor impression of tidiness level of organization;
- 2.3. Crime rate in neighbourhood compared to national average level.

6.4.4 Use of the site

See Questionnaire 3.1:

3.1 Periods of occupancy – human presence:

- Daytime;
- Full time 24/7;
- Seasonal.

6.4.5 Type of access

See Questionnaires 4.1 to 4.4:

- 4.1. Need for access employees;
- 4.2. Access by external parties;
- 4.3. Type of access regular, irregular, daytime, 24/7;
- 4.4. Access intensity.

7 Level of protection

Once the value for 'Potential risk' and 'Site characterization' have been established, the required level of protection has to be determined. This step is rather intuitive and subjective, since clear procedures for this are not (yet) available.

However, by assessing the sensitivity of use of the calculation model for various situations, which the user may have select himself, the user can tune in on the following classification:

Table 1 — Nature of the problem and Level of protection

Combination of 'Potential risk' and 'Site characterization'	Desired 'Level of protection'
No problem	1
Medium problem	2
Serious problem	3
Very serious problem	4

8 Determining functional requirements

8.1 Introduction

The aggregation of Level of Protection, Modus Operandi and Site Characterization will define, as a result, a Desired Performance as required by the site owner or user regarding the perimeter protection system. With the criteria described in the Desired performance the functional requirements need to be determined.

The desired Level of protection is the main determining factor. Data about the Modus operandi and from the Site characterization are more or less 'boundary conditions'.

A preliminary, indicative first impression of possible solutions given a desired Level of protection, may be as follows:

Table 2 — Level of protection and indicative solution

Level of protection	Objective	Possible solution (indicative)
1	Deter and delay	Mechanical solution
2	Deter, detect and delay	Mechanical solution plus single intrusion detection
3	Deter, detect, delay and intervention	Mechanical solution plus multiple detection, including alarm and verification
4	Deter, detect, delay and intervention	Multiple mechanical solutions (zoning) plus multiple detection including alarm and verification

8.2 Questions for establishing the functional requirement

In the process of actually formulating the functional requirement the following three main questions have to be answered:

- What should the system do?
- How well / to what degree should the system do that?
- Why?

While identifying the actual objectives/requirements the following (non-exhaustive) list can be used:

- a) restrict area perimeter – demarcation;
- b) secure site assets - protecting assets and persons;
- c) regulate flow of persons and vehicles;

- d) control flow persons and vehicles;
- e) creating time to respond:
 - 1) deter;
 - 2) detect;
 - 3) delay;
 - 4) deny.

9 Elements of possible solutions

9.1 Introduction

Perimeter protection is all about deterrence, detection, assessment and delaying of the intrusion for a intervention and response is initiated. Every solution needs to match the criteria set in the functional requirements of the site to be protected.

Operating environment, perimeter protection construction, security history, site layouts, surrounding environment, activity in and around the site, local weather conditions are all factors to be considered when planning a perimeter protection system solution. These influence the detection technologies selected and as a consequence the overall performance of the system.

Often the final perimeter protection solution will consist of several different but complementary technologies to form layers of protection.

In this clause a quick survey is given regarding possible solutions to meet the functional requirements providing an adequate match. In Clause 10 'Inventories' an overview is given of all the annexes with the Inventories that have been made.

Distinction is made between the following elements of a possible solution:

- elements of delay;
- elements of detection;
- external elements;
- local law and regulations.

A combination of the above measures is needed to provide a level of delay commensurate to the maximum response time from detection of intruder to interception; and to facilitate intervention.

9.2 Elements of delay

9.2.1 Overview of elements of delay

- Fence;
- wall;
- topping;
- traffic barrier;

- gate: swing, sliding, cantilever, speedgate, folding;
- turnstile;
- bollard: retractable, fixed;
- road block, wedge barrier;
- standoff;
- distance between fence lines;
- water (ponds etc.);
- vegetation.

9.2.2 Fences

Perimeter fencing should be installed to provide enhanced protection:

- To provide a clear demarcation between the site and the surrounding area;
- To act as a deterrent to unauthorized access into the site;
- To delay unauthorized entry to and exit from site by climbing, cutting or burrowing;

A fence should be over 1,8 m in height (indicative) below which there is considered to be no delay.

- To assist in the control of access to and egress from the site;
- To assist in deterring and preventing vehicle intrusion through adoption of hostile vehicle impact mitigation measures;
- (optional) To lend itself to support a vibration-based detection system.

In line with Table 2 with a first impression of possible solutions given a desired Level of protection, Table 3 illustrates a possible set-up for a classification for fences. It should be clear that this set-up is only indicative, both with respect to the number of classes and the description of those classes.

Table 3 — Tentative classes for fences

Level of protection	Fence class TENTATIVE	Description
1	1	A physical barrier that whilst not being designed to meet any particular security requirements, provides a minimum legal barrier to mark the boundary of the site. The barrier would, however, provide a deterrent to prevent unauthorized access.
2	2	A physical barrier to deter intruders offering a degree of resistance to climbing and breaching by an opportunist not having particular skills and using materials and breaching items that are readily to hand. The barrier also acts as boundary demarcation preventing accidental egress without drawing attention.
3	3	An intermediate security barrier that will deter and delay a resourceful and experienced intruder who has access to a limited range of tools and equipment. The design will offer resistance to attempts at climbing and breaching and will delay access for persons intent on unauthorized access.
4	4	A high security barrier that is designed to offer maximum deterrence and delay to both climb and penetration to the most determined and experienced intruder who is well resourced with tools that may not be readily available on the street. A Class 4 fence will need to be supported by [PIDS, lighting].

Protection from vehicle-based attacks may be a requirement. In that case any of the following functions may be required:

- maintain blast stand-off;
- prevent encroachment;
- stop penetrative attack;
- control vehicle access;
- enforce speed management measures.

Besides requirements directly related to perimeter protection, other requirements will also have to be considered, like the following:

- windloads shall not cause an unacceptable level of loading or deflection to the fence panels that would negatively affect operations or safety;
- changes in direction of a welded mesh fences line shall not affect the mesh deflection;
- the rattle or vibration to the fence panels shall be minimal.

9.2.3 Walls

Instead of using a fence as physical barrier at the perimeter of a site, a concrete or masonry wall can be in place. Take into consideration that potential intruders do not like to be seen on the site.

9.2.4 Barriers

Traffic barriers are used to offer limited protection against unauthorized vehicular access to the site.

9.2.5 Gates

The height, design and construction of gates should have a similar protection according to the adjoining fence. Hinges should be constructed in such a way as to prevent lifting and should be shielded, in order to prevent their use as ladders or climbing frames. It should not be possible to gain access under the gate. The locking device of a gate should be securely mounted and protected.

9.2.6 Roadblockers, Bollards

Road blockers and Bollards provide a physical barrier against unauthorized entry of a vehicle into a site at defined access and egress points.

The physical protection of a site against the use of vehicles for a criminal purpose will in most cases not be limited to the sole application of access control through physical obstacles.

9.3 Elements of detection

9.3.1 Introduction

Where automated detection of an intruder is required, an integrated security system comprising a Perimeter Intruder Detection System (PIDS) is needed. It is necessary to define minimum intruder criteria height of X m or more and a mass of X kg or more, crossing the detection zone at a rate of X m/s to Ym/s.

The types of attack styles (Modus operandi) which the PIDS are required to detect, are to be defined, such as detection of climb or cutting of, or approach to a barrier. The PIDS shall detect and annunciate an alarm for tampering with system enclosures and/or cutting of signal cables.

The PIDS shall cater for a range of host medium / site features, gates, secluded areas, exposed areas with public access to the outside of the barrier. Where multiple PIDS are used, they should not interfere with each other.

A method of validating the alarm should be considered to separate false alarms from true alarms, which require a guard force response. Validation can be achieved through assessment of CCTV, footage, although it may also be carried out manually by guard force.

When providing CCTV footage to validate an alarm, the following measures can increase the effectiveness of validation:

- appropriate picture quality to verify the cause of alarm;
- matching the CCTV zones with the PIDS zones to make it easier for alarm validation to be performed; and
- collecting footage immediately before, during and after the alarm.

9.3.2 Overview of elements of detection

- Detection;
- Exterior sensors PIDS;
- Lighting;

- Entry/exit control.

9.3.3 Detection

Perimeter intrusion detection systems are based on the core principle of establishing a steady background state and continuously monitoring to detect any change above or below a predetermined threshold which indicates that an intrusion event has occurred.

Like all technologies, these systems are constantly evolving. Although new improved equipment is being developed and introduced into the marketplace, the fundamental detection principles and applications rarely change.

9.3.4 Exterior sensors PIDS

There is a large and diverse range of sensing technologies available for perimeter security, varying in their effectiveness, affordability and accuracy. When evaluating any of the available technologies, the major requirements are:

- system durability/reliability;
- minimal nuisance alarms;
- maximum detection capability;
- minimal maintenance;
- ability to accurately pinpoint the location of intrusion;
- ability to function with other existing or complementary technologies.

Regardless of the selected system, the need for adequate warning and a response mechanism for unwanted intrusion is crucial. It is not sufficient only to know that a breach of the perimeter has occurred.

9.3.5 Lighting

Security lighting should be designed in such a way as to avoid shadow areas that favour aggressors by enabling them to operate without being seen.

Security lighting can be used to:

- lighten a vehicle/pedestrian access point;
- aid visual observation by patrolling guards;
- support CCTV surveillance or Video Based Detection;
- offer concealment of guards and/or activity;
- deter entry into the area.

9.3.6 Entry/exit control

The entrance is the first means of controlling access to any site. Gates and barriers should only be opened for persons and vehicles.

The entrance forms an integral part of the perimeter protection solution in order to control access to the site. Admission of vehicles should be through controlled gates, the control being exercised by an attendant or electronic access systems.

9.4 External elements

The following external elements are distinguished:

- alarm communication;
- response;
- response force;
- response force communication.

9.5 Local law and regulations

Local law and regulations might influence the perimeter security solution. As safety on a site is a prime importance there are regulations regarding escape routes, access of emergency vehicles.

10 Inventories

Inventories of current systems and (generic type) product, relevant member states regulations, relevant documents from CEN, CEN/TC 325, ISO and other sources have been made. The results are presented in annexes to this report.

Annex A 'Security system operational requirements – Q and A' intends to convey a general understanding of a the operational requirement for a security system through a format of questions and answers.

Annex C 'An environmental and organizational checklist for perimeter protection' consists of two lists of questions to be asked when assessing the need for security measures. The first list is about 'What are the environmental factors that will influence the solution?'(C.2). The second list is about 'What are the organizational factors that will influence the solution? (C.3).

In Annex D 'A perimeter security technologies classification' a subdivision of the technologies of intrusion detection is proposed into four main families (clusters). A table for each family resumes exhaustively the technologies that have been identified. For each family, a list of technical and functional features details the possibilities and the limits of each technology.

Annex E 'Inventory of perimeter intruder detection systems (PIDs)' consists of a list of information regarding perimeter intruder detection systems (PIDs). Information is given on some typical characteristics and fields of application. An indication is also given whether or not European or National standardization has taken place.

Annex F 'Matrix of current systems and (generic type) products' consists of a matrix of current perimeter protection systems and products. The generic product types are subdivided into the following categories: Permanent, Redeployable, Perimeter access, Gates and Barriers etc. The matrix gives the information in the following columns: Application, Standards/Guidance, Security - Application dependent, CEN/ Cenelec (1) and CEN/ Cenelec (2).

Annex G 'On Perimeter surveillance and burglary resistance' deals with the following two subjects: Use of detection systems for perimeter protection and Classification for burglary resistance.

In Annex H 'Pictures of fences, gates and entrance barriers' a non-exhaustive list is given of the different sorts of fences, supplementary accessories and gates and entrance barriers that can be found around private, commercial, industrial, military sites or installations.

It should be noted that these inventories cannot be considered complete; by nature they will be dated at some stage. The reader should be aware that any values given in these annexes are indicative values.

11 On testing

In the general conceptual framework for perimeter protection systems evaluation as presented in Annex B, 'Testing' is a way of verifying the (proposed) perimeter protection solution against the functional requirements.

Besides that, there is the testing of individual systems or components for Technical Specifications. An example of this kind of testing is described in CEN Workshop Agreement CWA 16221:2010 'Vehicle security barriers – Performance requirements, test methods and guidance on application'; see also Annex I.

Both kinds of testing are beyond the scope of the present Technical Report.

Annex A

Security system operational requirements – Q and A

This annex intends to convey a general understanding of a the operational requirement for a security system through a format of questions and answers.

The first draft of this annex originated from the United Kingdom.

Detection

What are you trying to detect?

- People (general public, criminals, deadly and determined, specific individuals);
- Vehicles (cars, boats, planes, bicycles, specific vehicles, other);
- Objects (thrown packages, stationary packages, weapons).

Where are you trying to detect them?

- Immediately outside but adjacent to a secure area (no man's land);
- Attempting to breach a cordoned secure area;
- Within a secure area.

Define the secure area – Map detail required showing public areas, no man's land and cordoned secure area?

Can the area be divided into zones – define zones?

What is likely outcome of a breach of the secure area (zone)?

- Theft;
- Threat to Protected Persons;
- Damage to property;
- Compromise of Information;
- Personal Injury.

Notification

Who is to be notified of all alarms generated?

- Anyone within range of secure area (Alarm Bells, Sirens);
- Covertly anyone within range (covert search team);
- Dedicated control room for alarm verification;

- Assigned personnel remote from secure area.

What timescale?

- Within 10 s;
- Within a minute;
- Within 10 min;
- Post event.

What information is required?

- Breach of secure area (single zone);
- Breach of specific zone.

How will they be notified?

- Mobile personnel notification equipment (radio, local pager, pager, mobile call, SMS);
- Global notification equipment (bells, sirens, triggered lighting);
- Control room notification (radio, local pager, pager, mobile call, SMS, email, GUI, mimic panel).

Verification

Who will perform verification of alarm?

- Site security team;
- Dedicated control room (requires pre/live/post video and/or audio);
- Assigned personnel remote from secure area;
- Offsite response deployed to verify alarm.

What are actions on known false alarm (wildlife, environment)?

- Log and investigate;
- Log and investigate and take action.

What are actions on unknown false alarm?

- Log and investigate;
- Log and investigate and take action.

What are actions on verification of intruder detection?

- Log and investigate;
- Notify on-site active security team;
- Log and notify dedicated onsite security team (how);

- Log and notify dedicated remote intervention team (how).

What is acceptable timescale between detection and verification?

- Less than 1 min;
- Up to 10 min;
- Up to 1 h.

Who makes final decision?

Further notification (Alarm distribution)

Who will be notified of verification of intruder detection?

- Site security team;
- Dedicated onsite intervention team;
- Dedicated offsite intervention team;
- Assigned personnel remote from secure area.

What information is required?

- Type of breach, number of attackers, etc.;
- Verification of breach of specific zone.

How will they be notified?

- Personnel notification equipment (radio, local pager, pager, mobile call, SMS, email, GUI, mimic panel);
- Other.

Annex B

Framework for perimeter protection systems evaluation

Figure B.1 illustrates the general conceptual framework for perimeter protection systems evaluation. It includes the sequence of steps in the performance classification methodology as presented in this Technical Report.

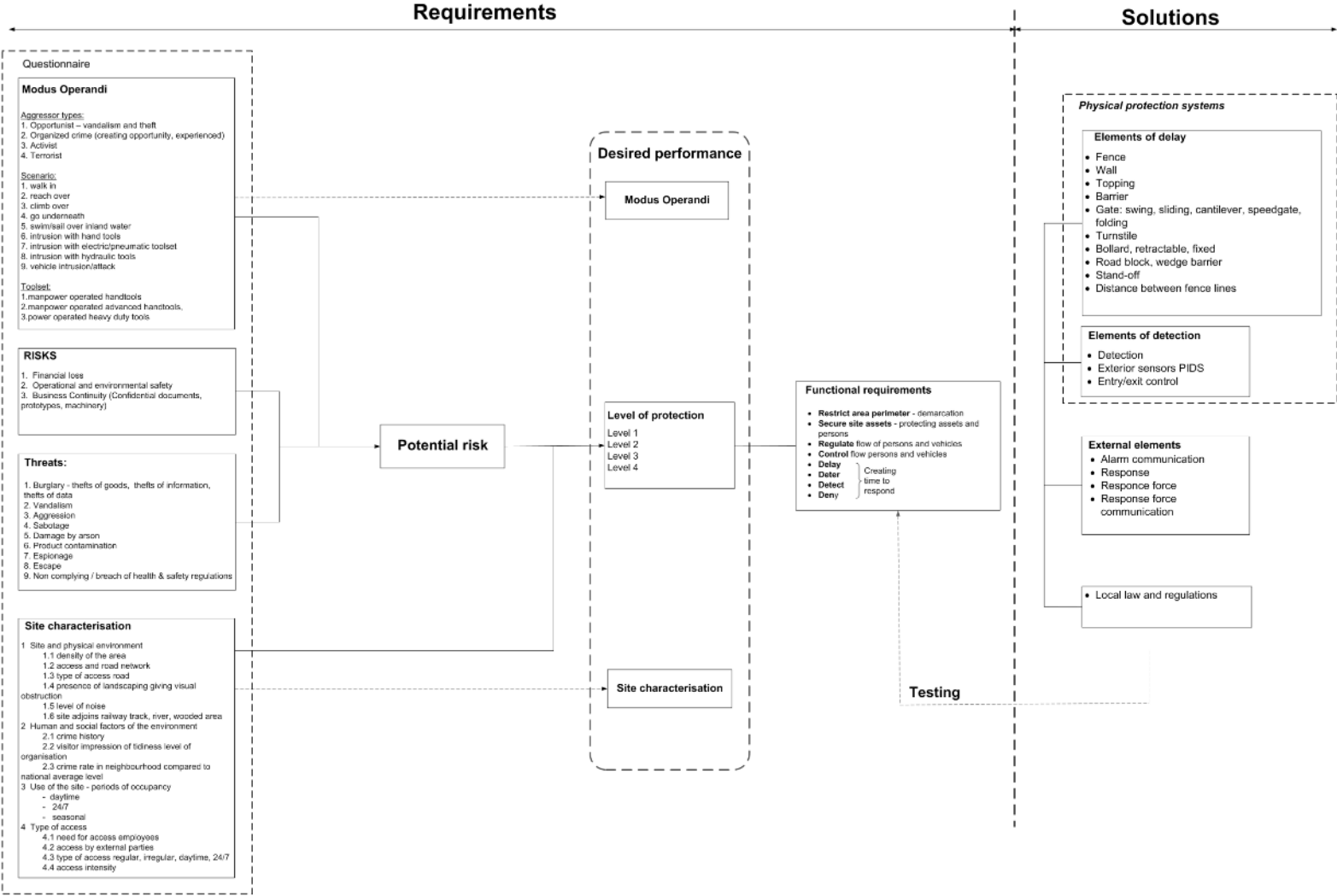


Figure B.1 — Framework for perimeter protection systems evaluation

Annex C

An environmental and organizational checklist for perimeter protection

C.1 Introduction

WARNING: Any values given in this annex are indicative values and can vary according to the product.

This annex consists of two lists of questions to be asked when assessing the need for security measures.

The first list helps to answer the question 'What are the environmental factors that will influence the solution?'(C.2). The second list helps to answer the question 'What are the organizational factors that will influence the solution?' (C.3).

The first draft of this annex originates from Belgium.

C.2 Environmental checklist for perimeter protection

What are the environmental factors that will influence the solution?

Table C.1 — Environmental checklist for perimeter protection

Topic	Question	Comment
E.1. General	What can define the secure area?	Map detail required showing public areas, no man's land and cordoned secure area
	Can the area be divided into zones – define zones?	
	Are there any developments in the surrounding area?	Surrounding developments may also mean that a risk analysis has to be carried out again. For example, if a residential neighbourhood is created in the vicinity, any emissions may have a more significant impact; or if new neighbouring companies with safety policies that differ from those of their predecessors are being established (with possible effects on the security of our organization).
E.2. Surroundings	Are there dwellings in the immediate vicinity?	Are these low-rise or high-rise?
	Is it a mono-site (a site just for the organization concerned) or is it an industrial estate?	Are the adjoining industrial sites and neighbouring companies protected or not?
	Are there any undeveloped sites in the immediate vicinity?	Are these open or wooded? Are they accessible?
	Are there parking spaces outside the company gates that are publicly accessible (from which people could make undisturbed observations)?	Is this parking area monitored or not?
E.3. Accessibility		

Topic	Question	Comment
E.3.1. Road	Define legitimate pedestrian / vehicular access points. For which mode of transport are they suitable: pedestrian, bike, car? Are these monitored or not?	When using PIDS, these access points may require certain zones to be switched off at particular times of day, for instance.
	Are there vehicular traffic routes adjacent to the perimeter?	Vehicular traffic can cause vibrations which, if in close proximity to certain PIDS types, could cause false alarms. Furthermore, passive infrared systems are sensitive to distance hot objects, i.e. vehicles. If they are not angled correctly, they could be triggered by the hot engines of vehicles passing by.
E.3.2. Rail	Does the railway line and the train enter into the industrial site?	
	Is the loading point inside or outside the gateway?	
	Is the access gate monitored?	
	Is there a continuing rail connection on which trains for other organizations can pass (multi-usage)?	
E.3.3. Air	Define the type of facilities that run over the industrial site.	High-voltage lines? Flight routes? Bridges and viaducts? Aircraft can cause vibrations in the air, which could be transferred to the PIDS.
E.3.4. Water	Define rivers and streams in adjacent to the site.	Moving water within the detection field of microwave systems could cause them to false alarm.
	Are there areas with standing water following heavy rainfall?	
	Does the organization use a supply via the water (port, river)?	
	Is the port private? Is the quayside for ships private?	
	Can fishing boats, leisure craft and other ships enter the area at their will?	
E.4. Weather	What is the temperature that can be expected?	Range to be defined: -20 °C to +55 °C (outdoor equipment) ; 0 °C to 40 °C (indoor equipment) Temperature differentials (e.g. caused by clouds moving across the sun) and rapid temperature change can have an impact on the occurrence of false alarms for some systems. Air temperature can vary considerably with respect to ground surface temperature.
	What is the humidity that can be expected?	Range to be defined: 0 % to 95 % non-condensing (outdoor equipment); 10 % to 90 %

Topic	Question	Comment
		<p>non-condensing (indoor equipment). Humidity could affect the processor electronics by causing corrosion. This can be minimized by ensuring processor boxes or other housings have the correct IP rating for the environment in which they will be used.</p>
	<p>What is the exposure to direct sunlight that can be expected?</p>	<p>Solar radiation can affect the performance of some PIDS. Rapid changes in the exposure to solar radiation (e.g. caused by clouds moving across the sun) can impact the occurrence of false alarms.</p>
	<p>What is the wind speed that can be expected?</p>	<p>Range to be defined: up to 65 km/h High winds can cause sensor mountings to vibrate. Where units are positioned at either end of a zone, this can affect alignment of the units. The direction of the wind and how quickly it is changing can influence the number of false alarms. Objects may also be blown through the detection zone by high winds.</p>
	<p>What is the rainfall / rain rate that can be expected?</p>	<p>Range to be defined: up to 25 mm/hour Rainfall may cause false alarms; reduce the detection performance along the entire zone; or reduce the effective range of the detection zone.</p>
	<p>What is the fog that can be expected?</p>	<p>The effectiveness of infrared systems can be reduced in mist or fog. Fog may cause false alarms or alternatively reduce the detection performance by reducing the size of the detection zone. Fog can reduce the ease of alarm verification using CCTV.</p>
	<p>What is the snowfall that can be expected?</p>	<p>Range to be defined: up to 30 cm/hour Snowfall may cause false alarms or alternatively reduce the detection performance by reducing the size of the detection zone.</p>
	<p>What are the freezing conditions (ground frost, ice) that can be expected?</p>	<p>Freezing conditions can cause ice to build up on the surface of the sensors, reducing their detection performance. For some buried systems, a seasonal adjustment may be required.</p>
	<p>What about the lightning strikes?</p>	<p>Inside a radius of 1 km Lightning strikes can damage system electronics.</p>
<p>E.5. Wildlife</p>	<p>Define possible wildlife in the near of the perimeter.</p>	<p>Wildlife such as rabbits, foxes, dogs or birds often cause false alarms. Systems which are immune to false alarms from a few animals may still false alarm in the presence of large numbers of animals.</p>
<p>E.6. Public</p>	<p>Define possible pedestrian access adjacent to the perimeter.</p>	<p>Where people have access to the perimeter (e.g. a public footpath alongside the perimeter fence), radiating field systems (e.g. microwave systems) may detect them.</p>
	<p>Are there many or few residents</p>	

Topic	Question	Comment
	adjacent to the perimeter?	
	Are there, e.g., stadiums, amusement parks, schools and sporting facilities in the immediate vicinity?	
	Or are there events in the surrounding area that attract a great many people? (e.g. a large, annual pop festival)	
E.7. Vegetation	Define existing trees and vegetation near of the perimeter.	Trees and vegetation encroaching into a detection field could cause false alarms when blown by winds. They may also produce fruit or organic debris which can fall into the detection zone. Grass, if left unmentioned, may cause false alarms when blown by the wind. Trees/vegetation can also be used to conceal an attacker.
	Do trees and foliage obstruct visibility of the site?	
E.8. Other indirect impact	Define existing machinery near of the perimeter.	Heavy machinery in the vicinity may cause vibrations and vibrate sensors out of alignment and cause false alarms.
	Define existing underground and overhead power cables / supplies.	Power cables, transformers etc. can result in electrical interference which may affect some PIDS. The presence of any power cables or supplies in or around the detection zone should be declared in the specification. Electrical shielding may be required to prevent these giving rise to false alarms.
	Define existing drainage problems.	A propensity for flooding or water saturation in any part of the detection zone may have significant impact on the suitability of some systems. For example, moving bodies of water can cause microwave systems to false alarm. Drainage may be installed to alleviate the problem.

C.3 Organizational checklist for perimeter protection

What are the organizational factors that will influence the solution?

Table C.2 — Organizational checklist for perimeter protection

Topic	Question	Comment
O.1. General	Are there developments in terms of the organization's activities?	New or other activities may give rise to new risks; further investigating needed.
	Are there developments in terms of the level of threat?	The threat level is subject to change, for example if a malicious event involving a similar organization has taken place, if a reorganization has taken place that may lead to dissatisfied employees or if the organization is in the public spotlight and therefore is attracting the attention of potential perpetrators. There may also be a case of an increased alert level.
O.2. Staff	Who will be responsible for the system?	
	Who will monitor the PIDS?	
	What other duties will these staff have?	
	Who will have access to the system and what permissions should they have?	<ul style="list-style-type: none"> - Administrators: full access with the ability to change settings - Supervisors: ability to view, edit, delete alarm information, create reports - Users / Guards: ability to view, classify and reset alarms only
	Who will be responsible for external investigation of alarms and detention of any intruders?	
	Who is to be notified of all alarms generated	<ul style="list-style-type: none"> - Anyone within range of secure area (Alarm Bells, Sirens) - Covertly anyone within range (covert search team) - Dedicated control room for alarm verification - Assigned personnel remote from secure area
	Who will perform verification of alarm?	<ul style="list-style-type: none"> - Overt onsite search team - Covert onsite search team - Dedicated control room (requires pre/live/post video and/or audio) - Assigned personnel remote from secure area - Offsite response deployed to verify alarm
	Who makes final decision?	
	Who will be notified of verification of intruder detection?	<ul style="list-style-type: none"> - Overt onsite search team - Covert onsite search team - Dedicated onsite intervention team - Dedicated offsite intervention team

Topic	Question	Comment
		- Assigned personnel remote from secure area
O.3. Facilities	Is a dedicated control room to be provided?	
	Will the PIDS be integrated into an existing security infrastructure?	
	How will be notified responsible staff for external investigation of alarms and detection of any intruders?	<ul style="list-style-type: none"> - Mobile personnel notification equipment (radio, local pager, pager, mobile call, SMS) - Global notification equipment (bells, sirens, triggered lighting) - Control room notification (radio, local pager, pager, mobile call, SMS, email, GUI, mimic panel)
	How will be notified responsible staff to perform verification of alarms?	<ul style="list-style-type: none"> - Personnel notification equipment (radio, local pager, pager, mobile call, SMS, email, GUI, mimic panel) - Other
	What form will the display take?	<p>Alarms can be displayed as a simple text-based list of alarms. Mimic panels can be used although these are becoming outdated and replaced with more sophisticated graphical user interfaces (GUIs).</p> <p>GUIs typically contain maps of the site with alarm locations overlaid to help operators quickly identify where the alarm originated. Alternatively the PIDS alarms could be integrated into a single GUI with other components of the security system, for example the CCTV system.</p> <p>Where screens are used to display information it is important that they are uncluttered and easy to view with the information presented in a clear, concise and easy to understand manner. The size of screen required to achieve this, relative to the viewing distance should also be considered.</p>
O.4. Procedures		
	Are there procedures, training, and resources in place?	<p>If yes, are procedures clear and practiced regularly?</p> <p>Are there sufficient resources to carry out the procedures?</p>
	Are audits undertaken?	<p>If yes, how many times a year?</p> <p>Are there controls in place?</p>
	Is confirmation of alarms required?	<p>This can be in the form of audio or visual confirmation (this could be provided by CCTV cameras which on alarm are triggered to store footage from before, during and after the alarm) which is made available following an alarm activation.</p> <p>If the PIDS is to be supplied with a digital video recording system for the purpose of confirming alarms, the length of footage</p>

Topic	Question	Comment
		<p>recorded pre- and post-alarm should be specified as well as any requirement for redundant data storage (e.g. a RAID array) to reduce the likelihood of video data loss in the event of a hard-drive failing.</p> <p>It is recommended that where CCTV confirmation of alarms is to be used, the cameras be fixed to match the zones of the PIDS. This saves valuable time being lost aligning a PTZ camera to find any intruders following an alarm and may prevent recorded evidence from being lost.</p> <p>Audio confirmation of alarms can provide a cheaper alternative but relies on a skilled operator to interpret the audio recordings obtained. It is inherently less accurate than using video footage.</p>
	<p>What information about the secure is required?</p>	<ul style="list-style-type: none"> - Breach of secure area (single zone) - Breach of specific zone
	<p>How will the alarms be evaluated and what would the operator be required to do?</p>	<p>Alarm logs can be created automatically or manually by the operator. If logs are created manually this can provide the operator with a lot of extra work and could lead to some alarms being missed out by mistake. Logs created automatically on a computer system can be saved electronically or printed out to provide a permanent record of events.</p> <p>Actions which operators might be expected to perform are to 'accept' the alarm event (silence any audible signal); 'verify' the cause of the alarm event; deploy the required 'response' to the alarm event; add any extra details to the alarm log (e.g. observed cause); and then to reset the alarm event.</p> <p>Operators should be provided with clear instructions on how to determine the cause of alarms and what response is required for different types of alarm.</p> <p>Weather data could be used to help decide the likely cause of an alarm, however using it as the sole means of determining the cause of an alarm should be avoided wherever possible.</p> <p>Using complementary sources of information, like CCTV, to help determine the cause of an alarm will provide greater confidence that the correct cause of the alarm has been identified.</p>
	<p>How will multiple alarms be processed?</p>	<p>While multiple alarms on PIDS could be caused for example by heavy rain, the operators should be warned that multiple alarms may also be a deliberate diversion caused by a potential intruder. Consideration should be given to how multiple alarms will be stacked or queued by the entire system, or for an individual zone, and whether alarms from particular zones should be given higher priority.</p> <p>All tamper alarms should be investigated</p>

Topic	Question	Comment
		<p>promptly as they could indicate deliberate sabotage or a fault within the sensor.</p> <p>It is important to ensure that control room operator(s) are not overloaded and that the workload designated is realistically achievable.</p>
	<p>What are actions on known false alarm (wildlife, environment)?</p>	<ul style="list-style-type: none"> - Log and do nothing - Log and call off further search (how) - Other
	<p>What are actions on unknown false alarm?</p>	<ul style="list-style-type: none"> - Log and do nothing - Log and call off further search (how) - Other
	<p>What are actions on verification of intruder detection?</p>	<ul style="list-style-type: none"> - Log and do nothing - Notify on-site active search team - Log and notify dedicated onsite intervention team (how) - Log and notify dedicated remote intervention team (how)
	<p>What happens in the event of power failure to the alarm enunciation / monitoring system?</p>	<p>Should the system shut down non-essential services to maintain operation for as long as possible under UPS power?</p> <p>Should a controlled shutdown be initiated automatically on switching to UPS power?</p> <p>This can ensure a smooth start-up once the power supply is resumed.</p>
	<p>How will system malfunctions and breakdowns be processed?</p>	<p>It would be useful to have a comprehensive maintenance contract which specifies expected response times for repairing the PIDS should there be a fault as well as the acceptable limits on downtime as described in section 4.6. Further information on maintenance is provided in section 7 'Maintenance'</p>
	<p>What is acceptable timescale between alarm generation and information being processed?</p>	<ul style="list-style-type: none"> - Immediately (within 10 s) - Immediately (within a minute) - Immediately (within 10 min) - Post event
	<p>What is acceptable timescale between detection and verification?</p>	<ul style="list-style-type: none"> - Less than 1 min - Up to 10 min - Up to 1 h - No time limit

Annex D

A perimeter security technologies classification

D.1 Introduction

WARNING: Any values given in this annex are indicative values and can vary according to the product or the regulation of sensibility.

The first draft of this annex originated from France.

One can rationally think that a device is designed for a use fitted for almost all situations and thus able to detect the more or less fast crossing of a target which can be a person or a vehicle.

However, some events have to be analysed and recognized as “no events of security” by the system in order to avoid a bad ratio between events of real insecurity and events connected to the operational environment. Sometimes, detection could be caused by small targets such as small animals or leaves; or detection could be caused by weather disturbances due to natural phenomena or movements situated outside the system detection zone. The characterization of a minimal security target (for example a person) can be considered as having minimal dimensions (25 × 40 × 120) or a minimum weight or a thermal mass.

Some criteria of characterization of the capacity of detection or no detection could be thus given with regards to a typical human target, having minimal values. This target shall generate an alarm with certainty when it evolves within the sensitive zone as defined by the system.

D.2 Four families for intrusion detection

D.2.1 Structure of the annex

In this annex a subdivision of the technologies of intrusion detection is proposed into four main families (clusters):

- technologies of detection by means of stand-alone sensor and which analyses the variation of signals resulting from the crossing of a sensitive area situated above the ground (D.3);
- technologies of detection by means of sensor (Integral) and intrusion detection signal being captured on the fence (D.4);
- technologies of detection by means of sensor which is inseparable and is an integral part of the physical protection system (wall or fence) (D.5);
- technologies of intrusion detection integrated in the ground (D.6).

A table for each family resumes exhaustively the technologies that have been identified: see Tables D.2 to D.5.

For each family, a list of technical and functional features details the possibilities and the limits of each technology, in the range of conditions of functioning in which the system in operational condition of detection can be operated.

D.2.2 Structure of the four main Tables D.3 to D.6

The following table gives the list of technical features and their subdivision as used in the tables for the four families of technologies of intrusion detection. This table also gives a brief explanation of the principles of functioning of each technology and the definition of every feature, offered or not, by each technology of detection.

Table D.1 — List of technical features and their subdivision

Technical Features		Explanation
Detection zone features	Range	It is the nominal distance of detection starting from which the detector has the sensibility allowing the detection and the alarm triggering to operate in the event of a target crossing.
	Width: volume or curtain	For the systems whose zone of detection is linear, it indicates the typical necessary and/or sufficient detection width to the technology. For the volumetric detectors, the feature is the one of the volume of detection defined by the minimal and the maximal width according to the distance.
	Height	Indicates the maximal of the nominal height of detection with respect to the ground.
	Dead zone	Indicates if a target of the size of a person cannot be detected on its smallest dimension (30 cm) on all or part of the nominal reach of the technology.
	Detection on concave areas	A ground which is not flat can generate shadow areas and cause detection failure. This criterion characterizes the possibility of being able to detect a target of 30 cm on all or part of the system reach representing a bump of xx cm.
	Detection on convex areas	Characterizes the possibility of detecting a crossing of a target of 30 cm with a hollow representing xx cm.
	Disqualification/Masking	The introduction of an obstacle in the field of detection can enable the system to detect all or part of the zone of nominal detection. This feature allows to inform if the technology is capable of detecting a partial or total masking caused by any kind of obstacles which would be added anywhere in the zone of detection.
	Configuration of the width or sensitivity of the detection zone	Allows indication if the zone of detection is limited, in order to avoid detecting a crossing beyond the zone defined by the range, the width and the height wished particularly those which have been determined and tested at the time of the initial parameter setting.
Technology	Optical, radiofrequency, thermal, seismic	Characterizes one or several physical signals making the technology
Detection features	Vertical detection	Allows the determination of capacity of detection of a target having the height of a man crawling (30 cm) over all the nominal reach of the system (except dead angle already characterized later) to be determined.
	Ground-level detection	Allows the determination of the capacity of detection of an object having a dimension of xx cm when it crosses the sensitive zone beyond a certain height, for example, a 1 m height (jumping).
	Minimum intrusion speed	Allows characterization of the minimal speed that a target of 30 cm height evolving in the ground will have to be completely detected by the nominal reach of the system (expressed in cm/second). Remark: We can rationally think that a person cannot evolve slowly other than with support taken in the ground.
	Maximum intrusion speed	Allows characterization of the maximal speed that a target having a minimal dimension of xx cm height shall not exceed in order to be detected in a sure way by the system on the totality of its range of detection.

Technical Features		Explanation
	Resolution of detection	Allows characterization of the minimal dimension that a target will have to be completely detected. The step of resolution determines the differentiation of perceptible dimension by the system between 2 targets of nearby size. Allows a keen adjustment of the sensibility between 2 targets.
Discrimination capacity	Maximum of non-intruder object	
	Minimum detected mass without alarm	Characterizes the minimal mass that the system can detect entirely at the range of detection. The step of resolution determines the differentiation of perceptible mass by the system between two targets of nearby size. Allows a keen adjustment of sensibility between two targets. The measure of the mass can be temperature, weight, radiofrequency absorption.
Intrusion qualification	<i>This family of characteristics allows a more exact qualification of a crossing on various geographical or dimensional criteria.</i>	
	Intrusion location: video-confirmation	Characterizes the capacity of the detector to indicate the location of the target more precisely than the nominal range. In complement, it indicates the resolution of location between two close but different targets (expressed in metres).
	Target dimension	Indicates the capacity to supply as a supplement to the alarm, the dimension or the range of dimension detected with a step of resolution between two targets of a nearby size. The dimension is expressed in the measure corresponding to the one used by the technology.
	Target height	Characterizes the capacity to supply as a supplement to the alarm the vertical dimension of the target which has crossed the zone of detection.
Immunity to weather variations	<i>Climatic conditions can disturb the performance of detection or decrease the reliability of the system by generating false alarms. For every meteorological condition, the system indicates the losses of performance connected to the technology.</i>	
	Immunity to sun glare	The measure of the loss of performance connected to the sun dazzle is rather difficult to measure. It is simply indicated that an average appreciation of loss of performance of the technology which could be made with the position of sunrise, at the zenith, sunset, by adding the number of luxes measured in the direction of the sun.
	Maximum range in fog (in % of the Weather Optical range)	The meteorological international standard norms define the meteorological visibility as the distance or the meteorological optical reach which corresponds to 95 % of attenuation of a light source. In cases where the technology (mainly optical) is altered by a loss of visibility, the maximal reach of detection is expressed in percentage of the optical reach .
	Rain	According to Météo France, there would be no statement on the type of rain or snow. The weather report measures the result (height of precipitation) associated with the other parameters (visibility, humidity, temperature).
	Snow	According to Météo France, there would be no statement on the type of rain or snow. The weather report measures the result (height of precipitation) associated with the other parameters (visibility, humidity, temperature).
	Wind	
Immunity to other disturbances	Electro-magnetic	
	Underground vibrations	
	Underground fluids	
	Main false alarms causes	

Technical Features		Explanation
Wiring / installation (Cabling / communication)	<i>Allows defining one or several means of communication that a technology or a system can offer to communicate with central equipment.</i>	
	NO/NC output	
	Serial output	
	Native IP communication	
	Connection between active equipment	
Other criteria	Non-detection causes	
	False alarms causes	
	Identification (video confirmation)	
	Dissuasion	
	Intrusion delayed	
Maintenance and breakdown/repair rate	<i>These characteristics are specific with each equipment and their integration in a standard is not adapted.</i>	

The following table gives the list of technical features and their subdivision as used in the tabled for the four families of technologies of intrusion detection.

Table D.2 — Definition of the technologies considered in Tables D.3 to D.6

Technology	Description
Infrared barrier	A system made of one or several couples of emission and reception cells of an infrared radiation, which analyzes the emitted beams to detect their cut by a target. It triggers an alarm according to the number of beams cut during a certain time.
Hyper frequency barrier	A system made of a couple of microwave emitter and receiver. The receiver analyzes the variation of the received signal when a target moves in the lobe of transmission and absorbs a part of the emitted signal. It triggers an alarm beyond the threshold of variations.
Video motion detection	A system which analyzes the video signal transmitted by different types of cameras (visible, near infrared, thermal infrared) in order to detect any variation in the analyzed images. The more or less sophisticated algorithms differentiate the true target in motion from a variation of images resulting from the natural environment.
Video analysis of an infrared contrast pattern	A system which analyzes the image of an infrared contrast pattern implanted at a distance. Thanks to a camera and a mirror effect, the infrared pattern is seen several times due to various heights of filming. The passage of a target between the pattern and the column of analysis generates a partial cut in every image of pattern, and in a different way according to the height of filming. An algorithm calculates the dimension and the location of the target by triangulation in order to trigger or not an alarm.
Passive infrared	A system which analyzes any thermal motion perceived by pyro elements which receive the average thermal flow of a scene of variable dimension according to the optical device (lens) situated between the scene and the sensor. Some of the systems are equipped with several sensors, in order to differentiate the type of target or to locate the intruder in the scene and analyze its movement in

Technology	Description
	space.
Detection by Doppler effect	A system which emits a microwave signal which is reflected by slightly modifying or not its frequency according to the speed of reflecting objects (Doppler effect); the system analyzes the power of the signals whose frequency has been modified and triggers or not an alarm according to the chosen parameters of sensibility.
Rotating Laser	A system which emits a laser signal which make a quick rotation on an axis. It analyzes the distance measured by the time needed for the trip and round trip of the beam for every angular position. The comparison of the distances cartography measured cyclically at every rotation of the laser enables the detection of the target intrusion in the field of measurement and triggers or not an alarm according to its dimension and to its spatial evolution.
Combination of technology	All those systems which, by combining complementary technologies (such as barrier infrared and hyper frequency, passive infrared and Doppler), allow false alarms to be avoided by making a logical combination AND alarms resulting from each technology, or to strengthen the certainty of detection by making a logical combination OR, every technology can generate an alarm.
Perimeter surveillance radar	High resolution radar that accurately detects personnel and vehicles up to 2 500 m range. It operates in virtually any climate, weather or lighting condition to provide 24/7 security, scanning 360° every second. Scan a full 360 degrees covering over 6 km ² (2,3 square miles).
Liquid Tube	A tube with a fluid is buried along the perimeter. The passage of the target provokes a pressure variation in the tube (increment (support) or redaction (leakage)). The analysis of the pressure variations allows an alarm release.
Underground coaxial	A system of underground coaxial cables based on the coaxial cables technology (radiant). The detection field is shaped by signals of radio electrical frequency transported by the buried coaxial cables along the perimeter. The radio frequency signals make a field of an invisible electromagnetic detection around the sensor cables. The passage of a target varies the electromagnetic field which releases an alarm.
Seismic	A geophone which is a device that converts ground movement (displacement) into voltage, which may be recorded at a recording station. The deviation of this measured voltage from the base line is called the seismic response and is analyzed for structure of the earth.
Optical fibre	The optical fibre is fixed on the fence or integrated in the ground. The passage of a person provokes vibrations which are transmitted to the optical fibre. These vibrations make the luminous fluxes which cross the fibre vary. The analysis of the signal allows or not an alarm release according to the frequency and variation of the analysed signal.

D.3 Stand-alone equipment

Table D.3 — Stand-alone equipment

Technical Features		Active beams	IR	Microwave	Dual-tech barriers	Video Motion Detection	Active Video Detection	Passive IR	PIR doppler +	Rotating Laser	Radar
Detection zone features	Range	Up to 200 m		Up to 200 m	Up to 200 m	30 m to 100 m	Up to 200 m	From 35 m (curtain) to 150 m (linear)		50 m to 200 m according to set-up	Up to 2 500 m
	Width: volume or curtain	50 mm		From 2 m to 10 m	Combination	NA	Some centimetres	Volumetric	Volumetric	Several millimetres	Volumetric
	Height	Many metres depends on column		Up to 3 m	Up to 3 m	Several metres	Up to 3 m	Typically 2,5 m to 3 m	Typically 2,5 m to 3 m		
	Dead zone	No		Near the column		Near the camera	No	Depending on the lens	Depending on the beams	Yes under the beam	No
	Detection on concave areas			No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Detection on convex areas	No		Yes if low hollow	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Disqualification/ Masking	Yes		No	No	No	Yes	No	No	Yes	No
	Configuration of the width or sensitivity of the detection zone	Yes		Yes for the range, difficult for the width	Yes with "AND" function of the technologies	No	Yes	No	No		
Technology	Optical, radiofrequency, thermal, seismic	Optical		Radio frequency	Combination	Optical	Optical	Thermal	Thermal and radio frequency		Radar
Detection	Vertical										Yes

Technical Features		Active beams	IR	Microwave	Dual-tech barriers	Video Motion Detection	Active Video Detection	Passive IR	PIR doppler +	Rotating Laser	Radar
features	detection										
	Ground-level detection										Yes
	Minimum intrusion speed										
	Maximum intrusion speed										
	Resolution of detection	Very variable depends on space between units 25 cm to 80 cm	Very variable depends on the nature of the subject	Very variable depends on space between units 25 cm to 80 cm	Depends on the distance between the target and the camera	Up to 1 cm					From 0,6 m to 1,2 m
Discrimination capacity	Maximum of non-intruder object	Very low (some centimetres) Except by coupling the beams	Medium depending on the target		Low near of the camera	10 cm					
	Minimum detected mass without alarm										
Intrusion qualification	Intrusion location: video-confirmation	Zoning on a model top of the line	No	No	Possible	Yes	Possible about 4° depending of the lens and the technology	No	Yes about 1°		
	Target dimension	Yes, when number of disrupted beams is counted	No	No	Yes possible depending on the 3 D analysis	Yes	No	No	Yes		

Technical Features		Active beams	IR	Microwave	Dual-tech barriers	Video Motion Detection	Active Video Detection	Passive IR	PIR doppler +	Rotating Laser	Radar
	Target height			No	No		Yes				
Immunity to weather variations	Immunity to sun glare	Typically low on sunset / sunrise (xx lux) yy lux in a zenith point		No sensitive to the light		Low	No sensitive to the light	Low	Depends on the technology		No sensitive to the light
	Maximum range in fog (in % of the Weather Optical range)	Limited to the optical reach meteorological		Good	Good without IR	Low 50 % to 80 % of the visibility	Good 3 times the visibility	Good if small range	Good if small range		Good
	Rain	Good		Good	Good	Medium	Medium	Good if small range	Good if small range		Good
	Snow										Good
	Wind										Good
Immunity to other disturbances	Electro-magnetic										
	Underground vibrations										
	Underground fluids										
	Main false alarms causes										
Wiring / installation	NO/NC output	Yes		Yes	Yes	Yes	Yes	Yes	Yes	Yes	
	Serial output	Yes		Yes	Yes	Yes	Yes	Yes	Yes	Yes	
	Native IP communication			No	No	Yes possible	Yes	No	No	Yes	Yes
	Connection between active equipment	Yes		No need	Yes	No need	No need	No need	No need	No need	No need
Other criteria	Non-detection										

Technical Features		Active beams	IR	Microwave	Dual-tech barriers	Video Motion Detection	Active Video Detection	Passive IR	PIR doppler +	Rotating Laser	Radar
	causes										
	False alarms causes										
	Identification (video confirmation)			No	No	Yes	No	No	No	No	No
	Dissuasion	Little		Little	Little	Little	Little	Little	Little	Little	Little
	Intrusion delayed			No	No	No	No	No	No	No	No

D.4 Fence-mounted sensors

Table D.4 — Fence-mounted equipment

Functional features		Microphonic sensitive cable	Fibre optics sensitive cable	Vibration sensor	Copper cable
Detection zone features	Range	100 m up to 300 m	Up to 80 km	100 m up to 300 m	100 m up to 300 m
	Width: volume or curtain	NA	NA	NA	NA
	Height	Depends	Depends	Depends	Depends
	Dead zone	No	No	No	No
	Detection performance on non-even grounds	Yes (depends on fence)	Yes (depends on fence)		NA
	Detection on ground with no hollow plan	Yes (depends on fence)	Yes (depends on fence)		
	Disqualification	Yes (sabotage)	Yes (sabotage)	Yes (sabotage)	Yes (sabotage)
	Configuration of the width or sensitivity of the detection zone	Yes	Yes	Yes	No
Technology	Optical, radiofrequency, thermal, seismic	Piezoelectric	Fiber Optics + laser		
					Seismic
		Passive	Passive		Passive
Detection features	Vertical detection	Yes (depends on fence)	Yes (depends on fence)		No
	Ground-level detection	Yes	Yes	Yes	Yes
	Minimum intrusion speed	Depends on fence	Depends on fence		
	Maximum intrusion speed	Depends on fence	Depends on fence		Easy
	Resolution of detection	5 m to 25 m	5 m to 25 m		Not possible
Discrimination capacity	Maximum of non-intruder object	NA	NA		
	Minimum detected mass without alarm	NA	NA		
Intrusion qualification	Intrusion location: video-confirmation	5 m up to 10,0m	No		5 m
	Target dimension	?	?		Yes 5 m with certain models (according to

Functional features		Microphonic sensitive cable	Fibre optics sensitive cable	Vibration sensor	Copper cable (size)
	Target height	?	?		No
Immunity to weather variations	Immunity to sun glare	NA	NA	NA	NA
	Maximum range in fog (in % of the Weather Optical range)	Insensitive	Insensitive	Insensitive	Insensitive
	Rain	Insensitive	Insensitive	Insensitive	Insensitive
	Snow	Insensitive	Insensitive	Insensitive	Insensitive
	Wind	Insensitive	Insensitive	Insensitive	Insensitive
Immunity to other disturbances	Electro-magnetic	Insensitive	Insensitive	Insensitive	Insensitive
	Underground vibrations	Insensitive	Insensitive	Insensitive	Insensitive
	Underground fluids	Insensitive	Insensitive	Insensitive	Insensitive
	Main causes of false alarms	Storm, strong EMI	Storm		
Wiring installation /	NO/NC output	Yes	Yes		
	Serial output	Yes	Yes		
	Native IP communication	Yes	Yes		
	connection between active equipment	No	No		
Other criteria	Non-detection causes				
	Causes of false alarms				
	Identification (video confirmation)	No	No		
	Dissuasion	No	No		
	Intrusion delayed				

D.5 Active Physical security

Table D.5 — Comparative of perimetric detection technologies

Functional features		Taut wire	Electric fence	Sensitive barbed wire	Active fence	Sensitive net	Sensitive outriggers
Detection zone features	Range	20 m up to 50 m	Variable from 20 m to 1 500 m	20 m up to 500 m	20 m up to 50 m	20 m up to 50 m	20 m up to 50 m
	Width: volume or curtain	NA	NA	NA	NA	NA	NA

Functional features		Taut wire	Electric fence	Sensitive barbed wire	Active fence	Sensitive net	Sensitive outriggers
	Height	according to need	according to need	according to need	according to need	according to need	according to need
	Dead zone	No	No	No	No	No	No
	Detection performance on non-even grounds	Yes	Yes	Yes	Yes	Yes	Yes
	Detection of concave areas	Yes	Yes	Yes	Yes	Yes	Yes
	Disqualification	NA	NA	NA	NA	NA	NA
	Configuration of the width or sensitivity of the detection zone	Yes	Yes	Yes	Yes	Yes	Yes
Technology	Optical, radiofrequency, thermal, seismic	Electric or electro-mechanic or piezo-electric or pressure tube	Electric	Electric	Electric or optic	Electric or optic	Electric
Detection features	Vertical detection	Yes	Yes	Yes	Yes	Yes	Yes
	Ground-level detection	Yes	Yes	Yes	Yes	Yes	Yes
	Minimum intrusion speed	With or without destruction	With or without destruction	With or without destruction	With or without destruction	With or without destruction	With or without destruction
	Maximum intrusion speed	With or without destruction	With or without destruction	With or without destruction	With or without destruction	With or without destruction	With or without destruction
	Resolution of detection	NA	NA	NA	NA	NA	NA
Discrimination capacity	Maximum of non-intruder object	NA	NA	NA	NA	NA	NA
	Minimum detected mass without alarm	20 kg	NA	NA	20 kg	20 kg	20 kg
Intrusion qualification	Intrusion location: video-confirmation	20 m up to 50 m	20 m up to 200 m by zone of detection	20 m up to 500 m by zone of detection	20 m up to 100 m by zone of detection	20 m up to 50 m	20 m up to 50 m
	Target dimension	NA	NA	NA	NA	NA	NA
	Target height	NA	NA	NA	NA	NA	NA
Immunity to	Immunity to sun	No	Not	Not	Not	No	No

Functional features		Taut wire	Electric fence	Sensitive barbed wire	Active fence	Sensitive net	Sensitive outriggers
weather variations	glare		sensitive to light	sensitive to light	sensitive to light		
	Maximum range in fog (in % of the Weather Optical range)	No	Not sensitive to fog	Not sensitive to fog	Not sensitive to fog	No	No
	Rain	No	No	Not sensitive to rain	Not sensitive to rain	No	No
	Snow	No	No	No	No	No	No
	Wind	No	No	No	No	No	No
Immunity to other disturbances	Electro-magnetic	Slightly sensitive	Slightly sensitive	Slightly sensitive	Slightly sensitive	Slightly sensitive	Slightly sensitive
	Underground vibrations	No	Not sensitive	Not sensitive	Not sensitive	No	No
	Underground fluids	No	not sensitive	not sensitive	not sensitive	No	No
	Main causes of false alarms						
Wiring installation /	NO/NC output	Yes	Yes	Yes	Yes	Yes	Yes
	Serial output	Yes	Yes	Yes	Yes	Yes	Yes
	Native IP communication	Yes	Yes	Yes	Yes	Yes	Yes
	Connection between active equipment	No	Yes	Yes	Yes	No	No
Other criteria	Causes of non-detection						
	Causes of false alarms						
	Identification (video confirmation)	No	No	No	No	No	No
	Dissuasion	Average because obstacle and presence are visible	Very dissuasive thanks to unpleasant effect and visible presence	Very dissuasive because hurtful	Average because obstacle and presence visible	Average because obstacle and presence visible	Average because obstacle and presence visible and trapping effect
	Intrusion delayed	Yes	Yes	Yes	Yes	Yes	Yes

D.6 Underground sensors

Table D.6 — Buried Sensors

Functional features		Fibre Optics	Leaky-coax cables	Coax	Geophone	Microphonic
Detection zone features	Range	50 m up to 40 000 m	100 m	100 m	7 m up to 30 m	20 m up to 100 m
	Width: volume or curtain	NA	NA	NA	NA	NA
	Height	No	No	No	No	No
	Dead zone	No	No	No	No	No
	Detection performance on non-even grounds	Yes	Yes	Yes	Yes	Yes
	Detection on ground with no hollow plan	Yes	Yes	Yes	Yes	Yes
	Disqualification	Yes	Yes	Yes	Yes	Yes
	Configuration of the width or sensitivity of the detection zone	Yes	Yes	Yes	Yes	Yes
Technology	Optical, radiofrequency, thermal, seismic	Optic laser with	Pressure Tube	Pressure Tube	Seismic	Piezo-electric
Detection features	Vertical detection	No	No	No	No	No
	Ground-level detection	No	No	No	No	No
	Minimum intrusion speed					
	Maximum intrusion speed					
	Resolution of detection	10 m up to 300 m according to model	10 m upto100 m according to model	10 m up to 100 m according to model	7 m up to 30 m	20 m up to 100 m
Discrimination capacity	Maximal of non-intruder object	NA	NA	NA	NA	NA
	Minimal detected mass without alarm	50 kg	50 kg	50 kg	50 kg	50 kg
Intrusion qualification	Intrusion location: video-confirmation	10 m up to 300 m according to model	10 m up to 100 m according to model	10 m up to 100 m according to model	7 m up to 30 m	20 m up to 100 m
	Target dimension	NA	NA	NA	NA	NA
	Target height	NA	NA	NA	NA	NA
Immunity to	Immunity to sun	No	No	No	No	No

Functional features		Fibre Optics	Leaky-coax cables	Coax	Geophone	Microphonic
weather variations	glare					
	Maximum range in fog (in % of the Weather Optical range)	No	No	No	No	No
	Rain	No	No	No	No	No
	Snow	No	No	No	No	No
	Wind	No	No	No	No	No
Immunity to other disturbances	Electro-magnetic	No	No	No	No	No
	Underground vibrations	Yes	Yes	Yes	Yes	Yes
	Underground fluids	Yes	Yes	Yes	Yes	Yes
	Main causes of false alarms					
Wiring installation /	NO/NC output	Yes	Yes	Yes	Yes	Yes
	Serial output	Yes	Yes	Yes	Yes	Yes
	Native IP communication	Yes	Yes	Yes	Yes	Yes
	connection between active equipment					
Other criteria	Non-detection causes					
	Causes of false alarms					
	Identification (video confirmation)	No	No	No	No	No
	Dissuasion	No	No	No	No	No
	Intrusion delayed	No	No	No	No	No

Annex E

Inventory of perimeter intruder detection systems (PIDs)

E.1 Introduction

WARNING: The tables in this annex are a work in progress. Any values given in this annex are indicative values. The contents of the tables in this annex should not be considered to be 'objective' and should be used with due diligence.

The first draft of this annex originated from the United Kingdom.

This annex consists of a list of information regarding perimeter intruder detection systems (PIDs), see Table E.1. Information is given on some typical characteristics and fields of application. An indication is also given whether or not European or National standardization has taken place.

Table E.1 also provides 'other information' in the following form:

Other information				
VD	PD	NAR	FAR	MTTR

The abbreviations have the following meanings:

VD	Vulnerability to Defeat	likelihood that a sensor could be beaten
	<i>Vulnérabilité à la casse</i>	<i>probabilité qu'un senseur puisse être détruit, cassé ?</i>
FAR	False Alarm Rate	rate of invalid alarms caused by unknown sources
	<i>Degré de fausse alarme</i>	<i>degré d'alarme non fondée causée par des sources inconnues</i>
NAR	Nuisance Alarm Rate	rate of invalid alarms caused by identifiable non-threat sources
MTTR ^a	Mean Time To Repair	average time that a device will take to recover from any failure
	<i>Temps moyen de remise en état</i>	
MTBF	Mean Time Between Failures	
	<i>Temps moyen de bon fonctionnement</i>	<i>temps moyen arithmétique entre deux pannes</i>
^a RSPL Recommended Spare Part List - list of tender parts. This list is always in combination with the MTTR.		

NOTE From a user perspective, it might be useful to combine FAR and NAR into one single quantity. It is possible that this will be considered in the future.

E.2 Combination of two sensors

Combinations of PIDs can also be used. Depending on their relation, they behave like an “OR” system or an “AND” system.

If the detector system is switch in a “OR “situation the security level goes up.

If the detector system is switch in a “AND “situation the security level goes down.

In low risk times “AND ” can be acceptable, in high risk times switch to “OR”.

<u>Used as:</u>	<u>“OR”</u> ^a	<u>“AND”</u> ^b
VD	down	up
PD	up	down
NAR	up	down
FAR	up	down
^a “OR” means both detectors shall generate an alarm. ^b “AND” means one of the detectors shall generate an alarm.		

Table E.1 — Information on perimeter intruder detection systems (PIDs)

Product type (generic)	Type	Application	Protection system	Protection system	CEN/ Cenelec	National ISO +	CEN/ Cenelec	Other information							
								Classification	General risk level	Passive/ Active	Visible/ Invisible	Standard applicable	Standard applicable	TC active on product	VD
General PIDS Technologies															
Barrier Mounted PIDS															
							TC 79								without traveling
Electrified fence	Line detection	Low/ middle	Active	Visible	EN 60335–2-76	EN 60335–2-76		high	low	high	high	high	< 4 h		
Electrostatic Field Disturbance	Line detection	middle/ high	Active	Visible	EN 50130–4	EN 50130–4		middle	high	high	high	high	< 4 h		
Fibre Optic	Line detection	Low/ middle	Passive	Visible		C 48–431 / C 48–465 / NF C 48–211 / NF C 48–225		high	low	low	high	high	> 4 h		
Geophone or Point Sensor	Point detection	Low/ middle	Passive	Visible				middle	middle	middle	low	low	> 4 h		
Vibration	Point detection	high	Passive	Visible				middle	middle	middle	middle	middle	> 4 h		
Magnetic Strain-Sensitive Cable	Line detection	Low/ middle	Passive	Visible				middle	middle	middle	middle	middle	> 4 h		
Microphonic cable	Line detection	low	Passive	Visible				high	low	middle	low	low	< 4 h		
Reflected wave	Line detection	low/middle	Active	Visible		NF C 48–229		middle	middle	high	low	low	< 4 h		
Taut wire	Line detection	middle/high	Passive	Visible				low	middle	low	middle	middle	< 4 h		
Ground Based PIDS															

Product type (generic)	Type	Applica-tion	Protection system	Protection system	CEN/ Cenelec	National + ISO	CEN/ Cenelec	Other information				
								Classificati on	General risk level	Passive/ Active	Visible/ Invisible	Standard applicable
Fibre Optic	Terrain following	low	Passive	Invisible		C 48-431 / C 48-465 / NF C 48-211 / NF C 48-225		middle	middle	middle	middle	> 4 h
Fluid Filled Tubes	Terrain following	high	Passive	Invisible				low	high	low	low	> 4 h
Ported Coaxial	Terrain following	high	Active	Invisible				low	high	high	low	> 4 h
Microphonic	Terrain following	low	Passive	Invisible				high	middle	high	low	> 4 h
Free standing PIDS												
Active Infrared	Line of Sight	low/middle	Active	Visible		NF C 48-226		high	low	high	high	> 4 h
Bistatic Microwave Barrier	Line of Sight	high	Active	Visible				low	high	low	low	< 4 h
Doppler/monostatic Microwave	Line of Sight	middle	Active	Visible		NF C 48-229		low	middle	high	low	< 4 h
Passive Infrared	Line of Sight	low	Passive	Visible				middle	low	high	low	< 4 h
Intelligent Video analysis	Line of Sight	low	Passive	Visible				middle	middle	middle	low	< 4 h
Volumetric PIDS												
LIDAR	Volumetric	low/middle	Active	Visible				middle	middle	high	middle	< 4 h
RADAR	Volumetric	middle/high	Active	Visible		NF C 48-229		low	middle	middle	middle	< 4 h

Product type (generic)	Type	Applica- tion	Protection system	Protection system	CEN/ Cenelec	National + ISO	CEN/ Cenelec	Other information									
								Classificati on	General risk level	Passive/ Active	Visible/ Invisible	Standard applicable	Standard applicable	TC active on product	VD	PD	NAR
Vegetable fences																	
Wooden palisades						Local rules											
Wall type perimeter protection																	
Concrete wall						Local rules											
Natural stone wall						Local rules											
Building materials (constructed) wall						Local rules		Ballistic requirement s or anti- overclimbing measures possible									
Metallic fences																	
Chainlink fences								TC 30	EPPA Whitebook								
Welded mesh fences								TC 30	EPPA Whitebook								
Pallisade fences								TC 30	EPPA Whitebook								

Product type (generic)	Type	Applica- tion	Protection system	Protection system	CEN/ Cenelec	National + ISO	CEN/ Cenelec	Other information					
								Classificati on	General risk level	Passive/ Active	Visible/ Invisible	Standard applicable	Standard applicable
Barbed wire								Used on top of permanent solution					
Razorblade wire								Used on top of permanent solution					
Access Control					EN standards	-		EPPA Whitebook					
Swing gates					EN standards	-		TC33 EPPA Whitebook					
Sliding gates on Rail					EN standards	-		TC33 EPPA Whitebook					
Cantilever sliding gates					EN standards	-		TC33 EPPA Whitebook					
Turnstiles					EN standards	-							
Boom barriers					EN standards	-							
Speed gates (Bi-fold)					EN standards	-		EPPA Whitebook					
								EPPA Whitebook					
Road blocking systems													

CEN/TR 16705:2014 (E)

Product type (generic)	Type	Applica- tion	Protection system	Protection system	CEN/ Cenelec	National + ISO	CEN/ Cenelec	Other information							
								Classificati on	General risk level	Passive/ Active	Visible/ Invisible	Standard applicable	Standard applicable	TC active on product	VD
Crash gates						PAS 68 [3] / ISO IWA 14 [5]									
Road Barriers						PAS 68 [3] / ISO IWA 14 [5]									
Bollards						PAS 68 [3] / ISO IWA 14 [5]									
V-gates						PAS 68 [3] / ISO IWA 14 [5]									
Defence barriers						PAS 68 [3] / ISO IWA 14 [5]									
Tyre killer															

Annex F

Matrix of current systems and (generic type) products

WARNING: The matrix in this annex is a work in progress and therefore not necessarily entirely correct. Its content may not be consistent with Annex E on PIDs. Any values given in this annex are indicative values.

The first draft of this annex originated from the United Kingdom.

This annex consists of a matrix of current perimeter protection systems and products. The generic product type are subdivided into the following categories:

- Permanent,
- Redeployable,
- Perimeter access,
- Gates,
- Barriers etc.

Table F.1 gives the information in the following format:

Application 1)	Standards/Guidance 2)	Security - Application dependent 3)	CEN/ Cenelec (1) 4)	CEN/ Cenelec (2) 5)
-------------------	--------------------------	---	---------------------------	---------------------------

The notes indicate:

- 1) Other may include Security.
- 2) Internal government standards/guidance may include testing which builds on current published documents but the results of which are not for public release.
- 3) Security products might be anti ram, anti cut and climb and the level of security which is assigned is generally based upon the time taken to get over, get under or push through with or without a vehicle.
- 4) Further information being sought.
- 5) Technical Committee which may, by the nature of their scope of activities, have an influence on the product. For example: TC 7 conventional designation of steel and material being used in bollard section.

Table F.1 — Information on systems and products for perimeter protection

Product type (generic)	Application (1)				Standards/Guidance (2)							Security - Application dependent (3)			CEN/ Cenelec (1) (4)	CEN/ Cenelec (2) (5)
	Domestic	Highway	Industrial	Other	CEN	National country	ISO	Trade Association	Local Authority	Other	Internal Government	Low	Med	High	TC active on product	TC Linked activities
Permanent																
Vegetation - shrubs	X								X			X				
Vegetation - trees	X								X			X				
Geotextile - soil/material filled units	X	X			X							X		X	WG 45	
Post and wire- plain	X		X						X			X				
Post and wire - barbed	X		X						X			X				
Post and rail- Wooden	X		X						X			X				

Product type (generic)	Application (1)				Standards/Guidance (2)							Security - Application dependent (3)			CEN/ Cenelec (1) (4)	CEN/ Cenelec (2) (5)
	Domestic	Highway	Industrial	Other	CEN	National country	ISO	Trade Association	Local Authority	Other	Internal Government	Low	Med	High	TC active on product	TC Linked activities
Post and rail-Metal	X	X	X						X			X				
									X							
Post and panel - wooden (1 m to 1,86 m)	X					BS 17 022			X			X				
Post and panel - wooden (≥ 1,86m)			X			BS 17 022			X			X				
Concrete post - wooden panel (1 m to 1,86 m)	X					BS 17 022			X			X				
Concrete post - wooden panel (≥ 1,86 m)	X	X	X			BS 17 022			X			X				
Concrete post - concrete panel (1 m to 1,86 m)	X					BS 17 022			X			X				

CEN/TR 16705:2014 (E)

Product type (generic)	Application (1)				Standards/Guidance (2)							Security - Application dependent (3)			CEN/ Cenelec (1) (4)	CEN/ Cenelec (2) (5)
	Domestic	Highway	Industrial	Other	CEN	National country	ISO	Trade Association	Local Authority	Other	Internal Government	Low	Med	High	TC active on product	TC Linked activities
Concrete post - concrete panel (≥ 1,86 m)		X		X		BS 17 022			X			X				
Highway safety fence - multistrand Cable		X			EN 1317 series	CHRP 350						X			TC 226	
Security fence - Multistrand					CEN CWA 16221 [4]	PAS 68 [3]	ISO IWA 14 [5]						X	X		
Chain link - plain (1 m to 1,86 m)	X		X			BS 17 022		European Perimeter Protection Association (EPPA)	X	LPS 1175		X			TC 30	
Chain link - plain (≥ 1,86 m)	X		X			BS 17 022		“	X	“	X	X			“	

Product type (generic)	Application (1)				Standards/Guidance (2)							Security - Application dependent (3)			CEN/ Cenelec (1) (4)	CEN/ Cenelec (2) (5)
	Domestic	Highway	Industrial	Other	CEN	National country	ISO	Trade Association	Local Authority	Other	Internal Government	Low	Med	High	TC active on product	TC Linked activities
Chain link - anti climb top barbed wire strands (≥ 1,86 m)			X	X								X				
Welded mesh - Plain (1 m to 1,86 m)	X		X			BS 17 022		EPPA	X	LPS 1175		X			TC 30	
Welded mesh - with topping (1,86 m to 3,4 m)			X	X		BS 17 022		“	X	“	X	X	X		“	
Welded mesh - with topping (≥ 3,4 m)			X	X					X	“	X	X	X		“	
Welded mesh - size of mesh						BS 41 02										

Product type (generic)	Application (1)				Standards/Guidance (2)							Security - Application dependent (3)			CEN/ Cenelec (1) (4)	CEN/ Cenelec (2) (5)
	Domestic	Highway	Industrial	Other	CEN	National country	ISO	Trade Association	Local Authority	Other	Internal Government	Low	Med	High	TC active on product	TC Linked activities
Welded mesh - mesh materials						BS 4102										
Palisade - plain (1 m to 1,86 m)	X		X				EPPA			LPS 1175		X			TC 30	
Palisade - with topping (1,86 m to 3,4 m)			X	X			"			"		X	X		"	
Palisade - with topping (≥ 3,4 m)			X	X						"		X	X		"	
Constructed Wall - Dry stone	X		X						X			X	X			
Constructed Wall - Brick/Block work	X		X						X		X	X	X			

Product type (generic)	Application (1)				Standards/Guidance (2)							Security - Application dependent (3)			CEN/ Cenelec (1) (4)	CEN/ Cenelec (2) (5)
	Domestic	Highway	Industrial	Other	CEN	National country	ISO	Trade Association	Local Authority	Other	Internal Government	Low	Med	High	TC active on product	TC Linked activities
Constructed Wall - Reinforced concrete		X	X	X		BS 14 992							X	X		
Constructed Wall - Steel with concrete fill			X	X	CEN CWA 16221 [4]	PAS 6 8 [3]	ISO IWA 14 [5]				X			X		
Concrete slipform wall -		X	X	X	CEN CWA 16221 [4]	PAS 6 8 [3]	ISO IWA 14 [5]						X	X		
Passive Bollards - steel			X	X		TC-E054 TC A05							X	X		TC 11/TC 6/ TC 7
Passive Bollards - concrete			X	X									X			
Retractable bollards - Steel			X	X	CEN CWA 16221 [4]	PAS 6 8 [3]	ISO IWA 14 [5]						X	X		TC 11/TC 6/ TC 7

Product type (generic)	Application (1)				Standards/Guidance (2)							Security - Application dependent (3)			CEN/ Cenelec (1) (4)	CEN/ Cenelec (2) (5)
	Domestic	Highway	Industrial	Other	CEN	National country	ISO	Trade Association	Local Authority	Other	Internal Government	Low	Med	High	TC active on product	TC Linked activities
Redeployable																
Barbed wire picket				X								X				
Passive bollards		X									X	X				
Passive traffic cones		X									X	X				
Site fencing - Metal mesh (1 m)	X		X									X				
Site fencing - Metal mesh (≥ 1,86 m)			X									X				

Product type (generic)	Application (1)				Standards/Guidance (2)							Security - Application dependent (3)			CEN/ Cenelec (1) (4)	CEN/ Cenelec (2) (5)
	Domestic	Highway	Industrial	Other	CEN	National country	ISO	Trade Association	Local Authority	Other	Internal Government	Low	Med	High	TC active on product	TC Linked activities
Site fencing - Wooden sheet (≥ 1,86 m)			X									X				
Site fencing - Metal panel (≥ 1,86 m)			X	X								X	X			
Plastic demarcation containers - Water/soil filled		X	X		EN 1317 series	CHRP 350					X	X			TC 226	
Security fence - Multistrand WIRE				X	CEN CWA 16221 [4]	PAS 68 [3]	ISO IWA 14 [5]						X	X		

Product type (generic)	Application (1)				Standards/Guidance (2)							Security - Application dependent (3)			CEN/ Cenelec (1) (4)	CEN/ Cenelec (2) (5)
	Domestic	Highway	Industrial	Other	CEN	National country	ISO	Trade Association	Local Authority	Other	Internal Government	Low	Med	High	TC active on product	TC Linked activities
Highway safety fence - Metal - Protection at temporary works		X	X	X	EN 1317 series	CHRP 350							X		TC 226	
Highway safety fence - Linked Concrete blocks - Protection at temporary works		X	X	X	EN 1317 series	CHRP 350							X		TC 226	
Non Highway - Linked stone/concrete blocks	X		X	X									X			
Non Highway - Stone/concrete blocks	X			X									X			

Product type (generic)	Application (1)				Standards/Guidance (2)							Security - Application dependent (3)			CEN/ Cenelec (1) (4)	CEN/ Cenelec (2) (5)
	Domestic	Highway	Industrial	Other	CEN	National country	ISO	Trade Association	Local Authority	Other	Internal Government	Low	Med	High	TC active on product	TC Linked activities
Wire baskets (Gabions)		X	X	X	CEN CWA 16221 [4]	PAS 68 [3]	ISO IWA 14 [5]						X	X		
Planters - surface placed				X	CEN CWA 16221 [4]	PAS 68 [3]	ISO IWA 14 [5]						X			
Planters - Fixed to surface				X	CEN CWA 16221 [4]	PAS 68 [3]	ISO IWA 14							X		
Seating units - Concrete/ other materials			X										X			
Linked steel casement filled with soil/concrete			X	X									X	X		

CEN/TR 16705:2014 (E)

Product type (generic)	Application (1)				Standards/Guidance (2)							Security - Application dependent (3)			CEN/ Cenelec (1) (4)	CEN/ Cenelec (2) (5)
	Domestic	Highway	Industrial	Other	CEN	National country	ISO	Trade Association	Local Authority	Other	Internal Government	Low	Med	High	TC active on product	TC Linked activities
Perimeter access																
Doors - Steel/Wood/ other	X		X		EN 1324 1-1					LPS 1175	X		X			
Roller Shutter - Steel/other	X		X		EN 1324 1-1 / CEN CWA 16221 [4]	PAS 68 [3]	ISO IWA 14 [5]			LPS 1175	X		X			
Portals				X	CEN CWA 16221 [4]	PAS 68 [3]	ISO IWA 14 [5]					X				
Turnstiles			X	X						LPS 1175	X	X				
Tube locks				X						LPS 1175	X		X			

Product type (generic)	Application (1)				Standards/Guidance (2)							Security - Application dependent (3)			CEN/ Cenelec (1) (4)	CEN/ Cenelec (2) (5)
	Domestic	Highway	Industrial	Other	CEN	National country	ISO	Trade Association	Local Authority	Other	Internal Government	Low	Med	High	TC active on product	TC Linked activities
Gates																
Swing gates - Wood	X				EN 1324 1-1			EPPA				X			TC 33	
Swing gates Steel	X		X	X	EN 1324 1-1			EPPA				X			TC 33	
Steel - solid panel /mesh			X	X				EPPA				X			TC 33	
Crash Gates - Steel mesh			X					EPPA				X				
V-gates			X	X				EPPA								
Bi-Fold (Speed gates) - Non-metal panel			X	X	EN 1324 1-1			EPPA			X	X				

Product type (generic)	Application (1)				Standards/Guidance (2)							Security - Application dependent (3)			CEN/ Cenelec (1) (4)	CEN/ Cenelec (2) (5)
	Domestic	Highway	Industrial	Other	CEN	National country	ISO	Trade Association	Local Authority	Other	Internal Government	Low	Med	High	TC active on product	TC Linked activities
Bi-Fold (Speed gates) - Steel mesh			X	X	EN 1324 1-1			EPPA			X	X				
Bi-Fold (Speed gates) - Steel panel			X	X	EN 1324 1-1			EPPA			X		X			
Sliding gates - Rail			X	X	EN 1324 1-1 / CEN CWA 16221 [4]	PAS 68 [3]	ISO IWA 14 [5]	EPPA				X		X		
Sliding gates - Cantilever			X	X	EN 1324 1-1 / CEN CWA 16221 [4]	PAS 68 [3]	ISO IWA 14 [5]	EPPA				X		X		
Barriers etc.																
Rising arm barriers - Plastic (GRP)			X		CEN CWA 16221 [4]	PAS 68 [3]	ISO IWA 14 [5]	EPPA				X	X			

Product type (generic)	Application (1)				Standards/Guidance (2)							Security - Application dependent (3)			CEN/ Cenelec (1) (4)	CEN/ Cenelec (2) (5)
	Domestic	Highway	Industrial	Other	CEN	National country	ISO	Trade Association	Local Authority	Other	Internal Government	Low	Med	High	TC active on product	TC Linked activities
Rising arm barriers - Steel			X	X	CEN CWA 16221 [4]	PAS 68 [3]	ISO IWA 14 [5]	EPPA				X	X			TC 11/TC 6/ TC 7
Rising beam steel			X	X	CEN CWA 16221 [4]	PAS 68 [3]	ISO IWA 14 [5]	EPPA				X		X		TC 11/TC 6/ TC 7
Road blockers - Steel			X	X	CEN CWA 16221 [4]	PAS 68 [3]	ISO IWA 14 [5]						X	X		TC 11/TC 6/ TC 7
Tyre Blades etc.			X	X								X				
Vehicle Catch nets				X								X				

Annex G

On Perimeter surveillance and burglary resistance

G.1 Introduction

This annex deals with the following two subjects:

- use of detection systems for perimeter protection (F2);
- classification for burglary resistance (F3).

On the one hand, this annex is part of the inventory (which is one of the main goals of the present document). On the other hand the subjects covered in this annex illustrate some of the crucial ideas that the present document has been built upon.

Subclause G.2 on detection systems is in fact part of the brochure "Anwendungsbereiche Freigeländeüberwachung" of the Bundesverband der Hersteller- und Errichterfirmen von Sicherheitssystemen (BHE). [6]

Subclause G.3 on burglary resistance classification is taken from: http://www.baulexikon.de/Bautechnik/Begriffe_Bautechnik/e/einbruchmelder/baulexikon_einbruchhemmunggw.htm.

Both G.2 and G.3 are based on information from Germany. It is emphasized here that similar concepts and approaches have been developed in many countries. The texts in the English language are non-authorized translations from the original text in German.

G.2 Use of detection systems for perimeter protection

G.2.1 Basic requirements for perimeter surveillance systems

The protection of a perimeter starts with a project-specific security and a subsequent security concept. These should be developed by competent companies (planners and installers), in close cooperation with the operator, and will be elaborated specifically for each object. At least the following points should be considered:

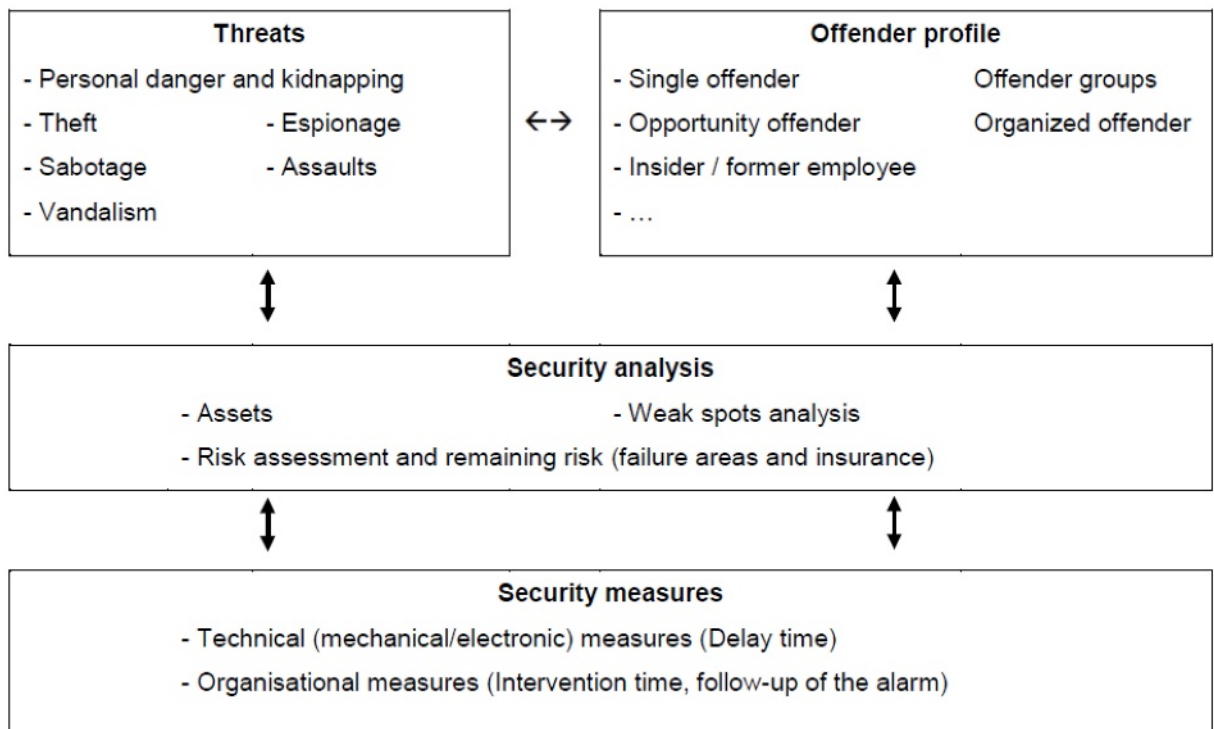


Figure G.1 — Elements of a security analysis

Practice shows that, when detection systems are used in outdoor areas, it is necessary in most cases to inspect the local circumstances and, if necessary, to perform test trials once a system has been selected. In order to protect an object effectively, the resistance time should be equal to or greater than the time required by the security personnel from the time of the alarm until the arrival at the security post.

The formula for the safety factor is:

$$SF = WZ / RZ$$

SF is the Security factor (Sicherheitsfaktor);

WZ is the Delay time of the perimeter system (Widerstandszeit der Umschließung);

RZ is the Reaction time of the security personnel (Reaktionszeit des Sicherheitspersonals).

For an effective outdoor security system, the safety factor should be more than 1. The resistance time depends among others things on the tools that are used to breach the barrier.

G.2.2 Basic principles of the detection systems

Table G.1

System	Definition and detection principle
Field change detector	Volumetric field detection, which operates on the principle of field change. Changes in the field (persons, etc.) are identified and evaluated.
Open area sensors	Interruptions between transmitter and receiver are detected.
Buried detection systems	Installed sensors hidden in the ground. Detects field changes, by movements or pressure changes.
Fence mounted detection systems – without destruction	Attached to physical barriers such as fences, bars, etc. or integrated into them. Noise, inclination and deformation of the system are recognized and valued.
Fence mounted detection systems – with destruction	Attached to physical barriers such as fences, bars, etc. or integrated into them. Cutting of the signal wires is detected.
Electro-mechanical detection system	The detection element is mechanically and triggers the electronics. Can be used in addition to mechanical barriers.
Video motion detector / -sensor	Evaluation of video signals from cameras. Changes in the picture pattern are detected and assessed.

G.2.3 Comparison of detection systems

	Walk / run	Climb	Cut	Step-ladder	Go underneath	Breach by car
Field change detector - Microwave barrier - Electrostatic field - HF cable systems - Passive infrared detector	●	--	--	○	--	●
Open area sensors - Infrared beam - Laser beam	●	--	--	○	--	●
Buried detection systems - Pressure systems (tubes, mats, cable, etc.) - HF cable systems - Magnetic field	●	--	--	○	●	●
Fence detection systems – without destruction - Noise sensor - Tilt sensor - Vacuum system - Fibre optic (FO) - Pressure / weight systems	--	●	●	○	--	●
Fence detection systems – with destruction - Current monitoring - Fibre optic (FO)	--	--	●	--	--	●
Electro-mechanical detection systems - Tension wire and electric fence - Switch systems	--	○	●	○	--	●
Video motion detector/sensor	●	--	--	○	--	●
Remark: Combinations of various systems may be appropriate. The overview is not necessarily complete. Please also consider the BHE-brochure 'False alarm or false notification'. Legend: ● good suitability; ○ average suitability; -- not suitable.						

Figure G.2 — Comparison of detection systems

G.2.4 Summary

Good analyses and demand oriented planning with users, installers and security personnel ensure the optimization of various systems in closed security concepts. For all applications competent specialist companies are available to provide assistance regarding the following points:

- Threat and vulnerability analysis;
- Safety concept;

- Taking into account the topography, weather conditions at the location;
- Organizational design of the security department;
- Consideration of relevant regulations, rules and standards;
- Appropriate and proper decision making about the perimeter surveillance systems;
- Interaction of different site systems;
- Appropriate or proper distribution of reporting lines/alarm sectors, e.g. overlap;
- Description/explanation of technical requirements;
- Appropriate or proper technology;
- Documentation of taken measures;
- Maintenance and repair.

G.3 Classification for burglary resistance

G.3.1 Recommendations for the assessment of the resistance class

The following table can be used for decision making regarding the resistance class to be selected for building elements (windows and doors). The sum of the points of the individual evaluation of the object to be protected and secured results in the classification in a recommended resistance class as listed in the Table G.4.

Table G.3

Aspects		Points
What type of location is the building to be protected situated on?	Busy road	10
	Lower frequented road	20
	Secluded location	30
Can the window to be protected or the doorstep viewed by people passing by?	Is clearly visible	20
	Is restricted visible	30
	Not visible at all	40
How is the window to be protected or the front door if a potential burglar can reach it?	Relatively easy	40
	With little effort	30
	Only with very great effort	10
In which time after an alarm could help be on site?	Within 2 min	10
	Within 5 min	20
	Within 10 min	30
Total Score		

Given the score, which represents the assessed risk, it is recommended to use windows or doors with the following resistance class:

Table G.4

Total score	Resistance class
Less than 70 points	No measures
80 to 110 points	WK 1
120 to 150 points	WK 2
More than 150 points	WK 3

G.3.2 DIN-Standards for burglar resistance

The European Standards ENV 1627:1999, ENV 1628:1999, ENV 1629:1999 and ENV 1630:1999, describe a classification of hazards and the associated technical requirements.

NOTE This group of standards have been superseded by EN 1627:2011, EN 1628:2011, EN 1629:2011 and EN 1630:2011 respectively.

The application and selection of a resistance class is the responsibility of the client.

As possible decision support, the requirements of the score table can be used, from which the users get information on which resistance class should be selected.

In addition, for special cases, the police should also be consulted to assess the relevant risk.

Furthermore, the installation of a burglar-resistant component requires special qualification. Depending on the resistance class, certificates are required, in which the check of the complete building component is guaranteed.

Table G.5

Resistance class	Expected offender type	Cylinders for locks DIN 18252	Security hardware DIN 18257	Security glazing DIN 52290	Test certificate required
WK 1	Basic protection against attempts with physical violence such as counter stand, counter jump, shoulder throw (mainly vandalism), low protection against the use of levering tools	P2BZ	ES 1	Not prescribed	No
WK 2	The opportunity offender tries, in addition with simple tools such as a large screwdriver, pliers and wedges, to break open the locked and bolted building components.	P2BZ	ES 1	A3	Yes
WK 3	The offender tries, in addition with a second screwdriver and a crowbar, to break open the locked and bolted building components.	P2BZ	ES 2	B1	Yes
WK 4	The experienced offender in addition with sawing tools and tools such as strike axe, a chisel and hammer and a battery operated drill.	P2BZ	ES 3	B1	Yes
WK 5	The experienced offender in addition with power operated tools, such as drill or a reciprocating saw and grinder.	Special test	Special test	B2	Yes
WK 6	The experienced offender in addition with powerful electric tools, such as drill, jigsaw or reciprocating saw and an angle grinder.	Special test	Special test	B3	Yes

Annex H

Pictures of fences, gates and entrance barriers

H.1 Introduction

WARNING: The information shown is partly based on the information from the USA. The European vehicle fleet is not compatible with the American fleet.

This annex is a non-exhaustive list of the different sorts of fences, supplementary accessories and gates and entrance barriers that can be found around f.i. private, commercial, industrial, military sites or installations.

The first draft of this annex originated from France.

The first sort of fence is more psychological than material: **white line** (for example in the middle of the road).

H.2 Different sorts of fences

H.2.1 Vegetable fences

Vegetable fences with thorns more or less effective or dangerous (Pyracanta, Berberis, etc.). The principle is to obtain a very dense edge with thorns.



a)



b)

Figure H.1 — Vegetable fences

H.2.2 Wood palisade

Wood palisade can be made from wood of different qualities; it is on the market in complete panels and posts or as panels to be assembled (planks, beams, etc.) and posts.



a)



b)

Figure H.2 — Wood palisade

H.2.3 Walls

Concrete reinforced



a)



b)



c)

Figure H.3 — Concrete reinforced

Stone



a)



b)

Figure H.4 — Stone

Breezeblock

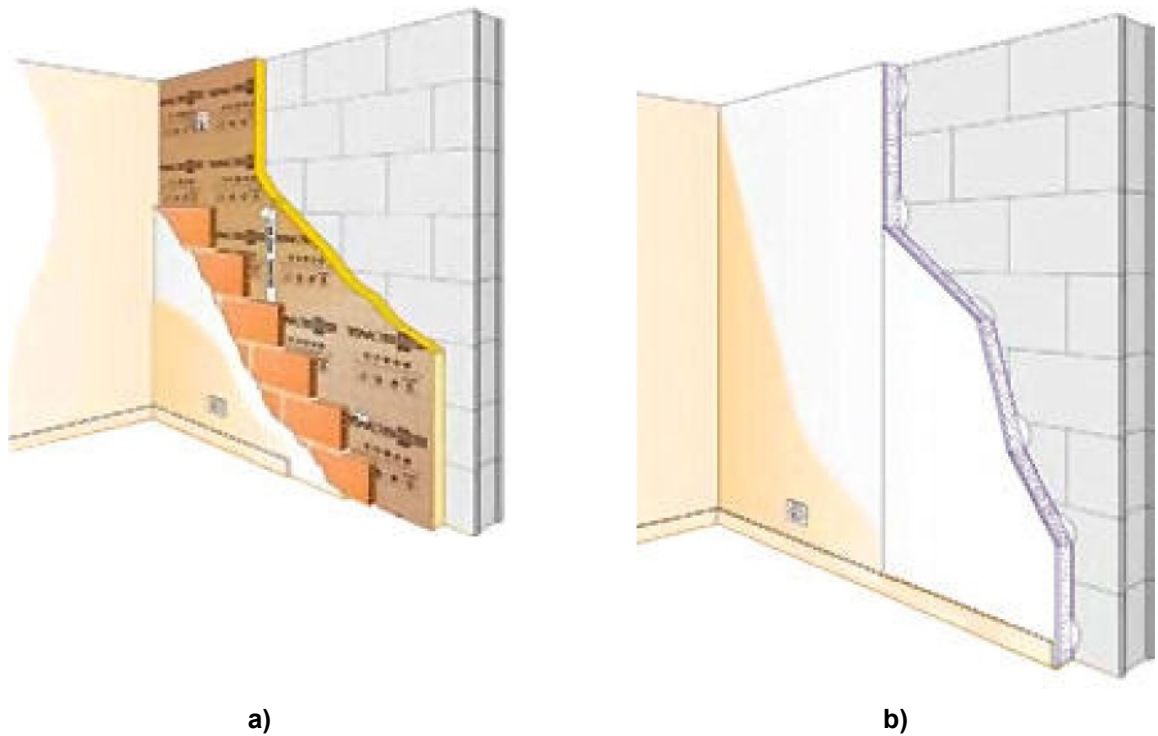


Figure H.5 — Breezeblock

Some of the breezeblocks have more technical features, such as being bulletproof or shockproof to vehicles.

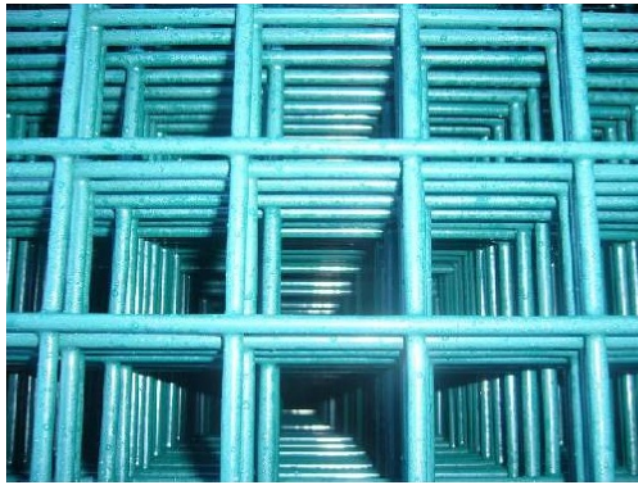
They can be provided with features such as a system on top to avoid somebody to throw a grapnel to climb over the wall (for example in a prison).

H.2.4 Metallic fences

Chainlink fences



a)



b)

Figure H.6 — Chainlink fences

By roll (25 m to 50 m) with diamond or rectangular mesh. They can be welded or not welded. Different diameter of wires are used.

Welded mesh fences



a)



b)



c)



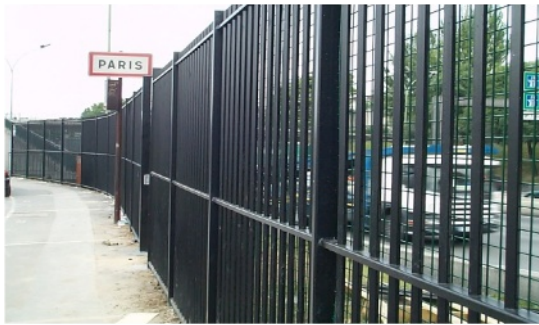
d)

Figure H.7 — Welded mesh fences

Various wires diameters are used. More important is the fact that it is a welded mesh panel. Different sizes of mesh aperture are used.

Palisades

Panels of fences with bars in place of wire. They can be tubes or full bars.



a)



b)



c)



d)

Figure H.8 — Palisades

H.2.5 Combinations of systems

There are some case where the fence is the result of the combination of two or more different systems.

Vegetable Fence + Razor wire



a)



b)

Vegetable Fence + metallic fence



c)

Figure H.9 — Combinations of systems that include a vegetable fence

H.3 Supplementary accessories

H.3.1 Razor wire



a)



b)

Figure H.10 — Razor wire

H.3.2 Sharp pins



a)



b)

Figure H.11 — Sharp pins

H.4 Gates and entrance barriers

H.4.1 Gates

Swing Gates



Figure H.12 — Swing Gates

Sliding Gate



a)



b)

Figure H.13 — Sliding Gate

Cantilever Gate



a)



b)

Figure H.14 — Cantilever Gate

H.4.2 Road obstacles

Bollard

A bollard enables pedestrians to pass through unobstructed while effectively stopping heavy vehicles at high speed.



Figure H.15 — Bollard

Road Block

A road block blocks the road within 2 s to 4 s and is designed to remain functional after a collision.



Figure H.16 — Road Block

Wedge barrier

A wedge barrier effectively blocks the road within 3 s, decreasing to 1 s with the assistance of an accumulator. Wedge barriers are also installed in city centres as the foundation is only 40 cm deep.



Figure H.17 — Wedge barrier

Crash gate

A crash gate is a solid gate that closes the site and effectively stops heavy vehicles travelling at high speeds.



Figure H.18 — Crash gate

Barriers lift system

A barriers lift system consists of a boom barrier that quickly rises out of the ground and blocks the entire width of the road within 4 s. The barrier completely destroys the chassis of a vehicle that tries to gain access by force. Lowered into the ground, it fulfils class 60 bridge security requirements to withstand extremely heavy vehicles.



Figure H.19 — Barriers lift system

Defence barrier

A defence barrier is a boom barrier that effectively stops heavy vehicles travelling at very high speeds.



Figure H.20 — Defence barrier

Tyre killer

A tyre killer consists of pointed barriers that effectively block a road within 2 s. These barriers completely destroy the tyres, axles and suspension of a vehicle that tries to gain access by force.



Figure H.21 — Tyre killer

Annex I

CEN Workshop Agreement CWA 16221

I.1 Introduction

This annex gives the Scope and the Table of Contents of CWA 16221:2010 'Vehicle security barriers – Performance requirements, test methods and guidance on application' [4].

This CEN Workshop Agreement has been drafted and approved by a Workshop of representatives of interested parties, the constitution of which is indicated in the foreword of this Workshop Agreement.

The formal process followed by the Workshop in the development of this Workshop Agreement has been endorsed by the National Members of CEN but neither the National Members of CEN nor the CEN Management Centre can be held accountable for the technical content of this CEN Workshop Agreement or possible conflicts with standards or legislation.

This CEN Workshop Agreement can in no way be held as being an official standard developed by CEN and its Members.

This CEN Workshop Agreement is publicly available as a reference document from the CEN Members National Standard Bodies.

I.2 Scope of CWA 16221:2010

Scope

This CWA specifies a classification system for the performance of a vehicle security barrier (VSB) when subjected to a single horizontal impact.

This CWA specifies two methods for determining the performance classification of a VSB:

- the vehicle impact method for all types of VSBs using a test vehicle classified in accordance with EC Directive 2007/46/EC [15] and registered for use in Europe;
- the design method for all types of VSBs.

This CWA refers to alternative test methods for determining the performance classification of a VSB (see Annex A).

This CWA also provides guidance for the selection, installation and use of VSBs (see Annexes D to M).

This CWA also describes the process of producing “operational requirements” (see Annex N).

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

- blast explosion;
- ballistic impact;
- manual attack, with the aid of tools (excluding vehicles).

NOTE For manual attack, attention is drawn to LPS 1175 which covers test methods for assessing burglary resistance of building components, such as doors, windows, shutters, grilles, strongpoints and security enclosures.

I.3 Table of Content of CWA 16221:2010

Contents	Page
Foreword	5
1 Scope	8
2 Normative references	8
3 Terms and definitions	8
4 General	11
4.1 Selection of test method	11
4.2 Documentation	11
4.3 Profile	11
4.4 Test conditions	11
4.4.1 General	11
4.4.2 Conformity between test item and documentation	11
4.4.3 Impact point	12
4.4.4 System operation	12
5 Vehicle impact method	13
5.1 Classification	13
5.2 Test vehicle specification	14
5.3 Test impact criteria	16
5.4 Performance requirements	16
5.5 Test method	17
5.5.1 Principle	17
5.5.2 Apparatus	17
5.5.3 Pedestrian intruder access	20
5.5.4 Test facility	20
5.5.5 Test item preparation	21
5.5.6 Test vehicle preparation	21
5.5.7 Occupant severity indices (optional)	22
5.6 Test procedure	23
5.6.1 Pre-impact data	23
5.6.2 Impact	23
5.6.3 Impact data	23
5.6.4 Post-impact data	24
5.6.5 Post-impact vehicle encroachment data	28
5.6.6 Post-impact person access data	28
5.6.7 Further impact tests	28
5.7 Test report	28
6 Design method	29

6.1 Classification	29
6.2 Design criteria	29
6.3 Design procedure	30
6.4 Design data	30
Annex A (informative) Alternative methods of testing single bollards at low impact energy	31
Annex B (normative) Modifications	32
Annex C (normative) Generic rigid test foundation for a single fixed bollard for vehicle impact tests	34
Annex D (informative) Introduction to hostile vehicle mitigation	37
D.1 General	37
D.2 Selection of a VSB	38
Annex E (informative) The threat	39
E.1 Identify and quantify the threat	39
E.2 Duration of deployment	39
Annex F (informative) The assets	41
F.1 Identification of the critical assets	41
F.2 Identification of stakeholders	41
F.3 Consideration of collateral damage	41
Annex G (informative) Site assessment	42
G.1 Review of existing security arrangements	42
G.2 Site survey	42
G.3 Civil works	42
G.3.1 Ground types	42
G.3.2 Foundations	42
G.3.3 Surface mounted VSB	43
G.4 Traffic survey	43
Annex H (informative) Site design	44
H.1 Traffic management	44
H.2 Aesthetics	45
Annex I (informative) VSB performance	46
I.1 Impact performance	46
I.1.1 General	46
I.1.2 Vehicle type	46
I.1.3 Vehicle speed	46
I.1.4 Impact angle	47
I.1.5 Vehicle penetration and dispersion	47
I.2 Operational performance	48
I.2.1 Vehicle access control	48
I.2.2 Speed of legitimate access	48

I.2.3 Power requirement	48
I.2.4 Durability and reliability	49
I.2.5 Environmental considerations	49
I.2.6 VSB integrity	49
I.2.7 Staff, skills and availability	50
Annex J (informative) Procurement strategy	51
J.1 General	51
J.2 Availability and maintenance of the VSB	51
J.3 Quality	51
J.4 Cost	51
J.5 Commissioning and handover	52
Annex K (informative) Deployment and removal	53
K.1 Highway/local authority approval	53
K.2 Logistics of deployment	53
K.3 Setting out	53
K.4 Lifting and placement issues	53
K.5 Removal considerations	53
Annex L (informative) Types of VSBs	54
L.1 General	54
L.1.1 Passive VSBs	54
L.1.2 Active VSBs	54
L.2 Examples of passive VSBs	55
L.2.1 Fixed bollards	55
L.2.2 Planters	55
L.3 Examples of active VSBs	56
L.3.1 General	56
L.3.2 Rising bollards	56
L.3.3 Road blockers	57
L.3.4 Rising arm barriers	58
L.3.5 Sliding and swing gates	59
Annex M (informative) Active VSBs	61
M.1 General	61
M.2 Categories of active VSBs	62
M.2.1 General	62
M.2.2 VACP	62
M.2.3 Anti-ram VSB	62
M.2.4 Counter-terrorist VSB	62
M.3 Layout of active VSBs at VACPs	62
M.3.1 General	62

M.3.2 Single line of VSBs	63
M.3.3 Interlocked VSBs	64
M.3.4 Final denial VSB	65
M.3.5 Traffic throughput	66
M.4 Safety issues	66
M.5 Training	68
M.6 Maintenance, service and inspection	68
M.7 Control system	68
Annex N (informative) Operational requirements	70
N.1 General	70
N.1.1 Introduction	70
N.1.2 Level 1 OR	70
N.1.3 Level 2 OR	72
N.2 Level 2 OR proforma	73
N.2.1 Document references	73
N.2.2 Level 1 OR references	73
N.2.3 Level 2 OR references	74
N.2.4 Area of concern	74
N.2.5 Period of Concern	75
N.2.6 Vulnerabilities	75
N.2.7 HVM measure(s) function	80
N.2.8 Performance requirements - Modus Operandi (MO)	81
N.2.9 Impact and performance requirement (hostile vehicle)	82
N.2.10 Performance requirement (normal operation)	83
N.2.11 Physical constraints	85
N.2.12 Environment constraints	86
N.2.13 Rules and regulations	87
N.2.14 Success criteria	88
N.2.15 Integration	89
N.2.16 Management	90
N.2.17 Service and maintenance	91
Annex O (Informative) Proforma test report	93
O.1 Impact test report	93
O.2 Contents of report	93
Bibliography	94

Bibliography

- [1] EN 14383-1: 2006, *Prevention of crime — Urban planning and building design — Part 1: Definition of specific terms*
- [2] Centre for Applied Science and Technology (CAST)
<https://www.gov.uk/government/collections/centre-for-applied-science-and-technology-information>
- [3] PAS 68:2013, *Impact test specifications for vehicle security barrier systems*
- [4] CWA 16221:2010, *Vehicle security barriers — Performance requirements, test methods and guidance on application*; CEN
- [5] ISO IWA 14¹⁾, *Vehicle security barriers*
- [6] *Freigeländeüberwachung - Anwendungsbereiche und Aufbau von Freigeländeüberwachungssystemen*; BHE, 09/2009 - Überarbeitet 06/2013.
<http://www.bhe.de/die-fachbereiche/freigelaende/anwendungsbereiche-und-aufbau-von--freigelaendeueberwachungssystemen.html>
- [7] TALBOT J., JAKEMAN M. *Security risk management body of knowledge*. RMIA, Carlton South, 2009
- [8] CEN/TR 14383-2:2007, *Prevention of crime — Urban planning and building design — Part 2: Urban planning*
- [9] CEN/TS 14383-3:2005, *Prevention of crime — Urban planning and building design — Part 3: Dwellings*
- [10] CEN/TS 14383-4:2006, *Prevention of crime — Urban planning and design — Part 4: Shops and offices*
- [11] CEN/TR 14383-5:2010, *Prevention of crime — Urban planning and building design — Part 5: Petrol stations*
- [12] prCEN/TR 14383-6:2013, *Prevention of crime — Urban planning and building design — Part 6: Schools*
- [13] CEN/TR 14383-7:2009, *Prevention of crime — Urban planning and building design — Part 7: Design and management of public transport facilities*
- [14] CEN/TR 14383-8:2009, *Prevention of crime — Urban planning and building design — Part 8: Protection of buildings and sites against criminal attacks with vehicles*
- [15] EC Directive 2007/46/EC of the European Parliament and of the Council of 5 September 2007 establishing a framework for the approval of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles (Framework Directive)

1) Under development. The reference is therefore preliminary and subject to further discussions. Once ISO IWA 14 is published, a true comparison can be made with CEN CWA 16221 and PAS 68.

The IWA is comprised of two parts: Part 1: Performance requirement, vehicle impact test method and performance rating; Part 2: Application. It also incorporates ASTM 2656-07, Standard Test Method for Vehicle Crash Testing of Perimeter Barriers.

- [16] EN 60335-2-76, *Household and similar electrical appliances — Safety — Part 2-76: Particular requirements for electric fence energizers (IEC 60335-2-76)*
- [17] EN 50130-4, *Alarm systems — Part 4: Electromagnetic compatibility — Product family standard: Immunity requirements for components of fire, intruder, hold up, CCTV, access control and social alarm systems*
- [18] NF C 48-211, *Détection d'intrusion — Centrales d'alarme — Règles*
- [19] NF C 48-225, *Détection d'intrusion — Détecteurs d'intrusion — Règles générales*
- [20] NF C 48-226, *Détection d'intrusion — Détecteurs à infrarouge actif — Norme spécifique*
- [21] EN 1317 (all parts), *Road restraint systems*
- [22] BS 4102, *Specification for steel wire for general fencing purposes*
- [23] EN 13241-1, *Industrial, commercial and garage doors and gates — Product standard — Part 1: Products without fire resistance or smoke control characteristics*
- [24] ENV 1627:1999, *Windows, doors, shutters — Burglar resistance — Requirements and classification*
- [25] ENV 1628:1999, *Windows, doors, shutters — Burglar resistance — Test method for the determination of resistance under static loading*
- [26] ENV 1629:1999, *Windows, doors, shutters — Burglar resistance — Test method for the determination of resistance under dynamic loading*
- [27] ENV 1630:1999, *Windows, doors, shutters — Burglar resistance — Test method for the determination of resistance to manual burglary attempts*

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

All the data, software and documentation set out in all British Standards and other BSI publications are the property of and copyrighted by BSI, or some person or entity that owns copyright in the information used (such as the international standardization bodies) and has formally licensed such information to BSI for commercial publication and use. Except as permitted under the Copyright, Designs and Patents Act 1988 no extract may be reproduced, stored in a retrieval system or transmitted in any form or by any means – electronic, photocopying, recording or otherwise – without prior written permission from BSI. Details and advice can be obtained from the Copyright & Licensing Department.

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



...making excellence a habit.™