SLOVENSKI STANDARD
SIST-TP CEN/TR 16705:2014

01-julij-2014

Perimetrijska zaščita - Metodologija razvrščanja zmogljivosti

Perimeter protection - Performance classification methodology

Schutz von Grundstücksgrenzen - Methodologie für eine Leistungsklassifizierung

Protection périmétrique - Méthode de classification de performance

Ta slovenski standard je istoveten z: **CEN/TR 16705:2014**

ICS:

13.310	Varstvo pred kriminalom	Protection against crime

SIST-TP CEN/TR 16705:2014 **en,fr,de**

TECHNICAL REPORT

RAPPORT TECHNIQUE

TECHNISCHER BERICHT

CEN/TR 16705

April 2014

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

Ref. No. CEN/TR 16705:2014 E

Contents

Page

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 capacitancy 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)