SLOVENSKI STANDARD
SIST-TP CLC/TR 50515:2009

01-marec-2009

Seznam interpretacij izdanih standardov za alarmne sisteme

List of interpretations on published standards on Alarm Systems

Liste von Interpretationen auf herausgegebenen Standards auf Alarmanlagen

Liste d'interprétations sur les normes publiées sur les Systèmes d'alarme

Ta slovenski standard je istoveten z: **CLC/TR 50515:2008**

ICS:

13.320 Alarmni in opozorilni sistemi Alarm and warning systems

SIST-TP CLC/TR 50515:2009 **en**

TECHNICAL REPORT

RAPPORT TECHNIQUE

TECHNISCHER BERICHT

CLC/TR 50515

December 2008

ICS 11.040.40

English version

List of interpretations on published standards on "Alarm Systems"

Liste d'interprétations sur les normes publiées sur les "Systèmes d'alarme"

Liste von Interpretationen auf herausgegebenen Standards auf "Alarmanlagen"

This Technical Report was approved by CENELEC on 2008-07-04.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and the United Kingdom.

CENELEC

European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

Central Secretariat: rue de Stassart 35, B - 1050 Brussels

Ref. No. CLC/TR 50515:2008 E

Foreword

This Technical Report was prepared by the Technical Committee CENELEC TC 79, Alarm systems.

The text of the draft was submitted to vote in accordance with the Internal Regulations, Part 2, Subclause 11.4.3.3 (simple majority) and was approved by CENELEC as CLC/TR 50515 on 2008-07-24.

Contents

1 Scope

This is a list of interpretations to currently published standards.

2 List of interpretations

2.1 EN 50131-1:1997 “Alarm systems – Intrusion systems – Part 1: General requirements”

2.1.1 Subclause 8.7.1

2.1.1.1 Question

In the 1st paragraph of 8.7.1, it is expressed that the system components shall provide means to prevent access to internal elements in general and that tamper protection depends on the grade of IAS and whether the system components are located within or outside the supervised area.

In the 2nd paragraph of 8.7.1, it is stated that system components of IAS located external to the supervised premises shall have means of tamper protection and detection. The question is, if (all) the system components within the supervised area need a certain tamper protection?

2.1.1.2 CLC/TC 79 response

The 4th paragraph of 8.7.1 requires housings (of all systems components as no limitations or grading requirements are included) to be “sufficiently to prevent undetected access without visible damage”. Individual component standards should include requirements appropriate to the type of equipment.

2.1.2 Subclause 8.7.2, Table 7

2.1.2.1 Question

In contradiction to the requirements of the 2nd paragraph of 8.7.1, in Table 7 in all grades tamper protection is required mandatory without any dependability on the situation of the components.

2.1.2.2 CLC/TC 79 response

The reference to “detection” in the 2nd paragraph of 8.7.1 is an error. The reference should be deleted as requirements for “Tamper detection” are specified in 8.7.2.

2.1.3 Subclause 8.3.1, level 3

2.1.3.1 Question

Not only devices, which are generally, termed control and indicating equipment (CIE) but also detectors contain configurable elements, which are matched to the system (Table 1, penultimate row).

It can be concluded that, at the least, all movements detectors with configurable sensitivity or a variable angle of detection must be provided with access restrictions. Is this correct ?

2.1.3.2 CLC/TC 79 response

The requirements included in 8.3.1, level 3 were intended to apply to access to functions/controls as specified in Table 1. When a system component includes the facilities described in Table 1 the requirements of 8.3.1 shall be achieved. Access to configurable adjustable elements of system components e.g. detectors, are addressed by the requirements relating to tamper security (EN 50131-1, 8.7). Normal access to these elements would require the tamper detection function to be inhibited/isolated, which would require authorisation as specified in 8.3.6 and 8.3.7.

2.1.4 Subclause 8.3.1, level 4

2.1.4.1 Question

In conjunction with 8.3.2 it is required that an alteration to or a substitution of the main program is subject to a logical or physical access restriction exceeding level 3.

The operating program of control panels in common use is typically located in a socketed PROM or a PROM which is able to be programmed in situ. Either way it is easy to manipulate as far as access level 3 is concerned. A socketed PROM can simply be exchanged. A fixed PROM can be easily reprogrammed, with commercially available equipment by directly connecting to the hardware.

The conclusion in the future will be that all devices with PROMs must have a further level of security. This could be for example padlocks protecting the socketed PROMs. For consistency soldered PROMs must be secured against desoldering so as to comply with the requirements of Table 2. One must not forget that a soldering iron is normally a usual tool whereas a key, even a simple one, represents a higher level of security. Is this correct?

2.1.4.2 CLC/TC 79 response

The requirements included in 8.3.1, level 4 were intended to apply to access to functions/controls as specified in Table 1 only when changes to equipment design are possible without access to the internal elements of the system components, i.e. without accessing the equipment by normal means.

NOTE The requirements included in EN 50131-1 apply to “installed systems”. When the requirements were developed it was assumed that a manufacturer wishing to “change equipment design” would have two choices:

a) change/replace hardware;

b) change/replace software.

In the event of hardware being replaced it would be necessary for the manufacturer to be authorised to access the CIE to isolate/inhibit the system component tamper detection function.

When the hardware being replaced was the CIE (or part of a CIE) authorisation, at access level 4, would be required to isolate/inhibit the tamper detection function of the CIE.

In the event of software being replaced, if access to the internal elements of the systems component were required, the same requirements apply as for replacing hardware.

When software can be replaced without accessing the internal elements of a system component, e.g. remotely by a modem or a local external connection, authorisation would be required at access level 4 to permit such changes.

Any attempt to change hardware or software without authorisation at access level 4 to isolate/inhibit the tamper detection function or permit software changes would result in the generation of a tamper signal or message.

In the event of a change to equipment design by either hardware or software means the system would require re-commissioning and that issue will be addressed in CLC/TS 50131-7 “Alarm systems – Intrusion systems – Part 7: Application guidelines”.

2.1.5 Subclause 8.3.1 contradict with Clause 6

Classes 1 and 2 are based upon an intruder who has very little or no technical knowledge (Clause 6). From the operator's point of view it is therefore incomprehensible that locks are required on class 1 and 2 housings. It is out of question that in these classes the owner/user would be the intruder.

This ambiguity in the standard may be a source for very differing conformance statements made by the various testing laboratories all over Europe, which cannot be accepted.

Subclause 8.3.1 specifies that access, to the functions specified in Table 1, at levels 2, 3 and 4 must be restricted by “means of a key or code operated switch or lock or other equivalent means”.

Requirements for authorisation are included in 8.3.2, which makes reference to Table 2, which uses the terms “logical or physical key”. Therefore “access” may be restricted by logical or physical key or any equivalent means.

Requirements relating to “housings” are included in 8.7.1 “Tamper Protection” which specifies requirements relating to access to internal elements of system components.

2.2 EN 50131-6:1997 inconsistencies with EN 50131-1:1997

2.2.1 Subclause 4.2.1

2.2.1.1 Question

The text under Table 1 about fault signal within 10 s is an unnecessary requirement. Vds regulations require 1 h. We will quote national remark about its non necessity.

2.2.1.2 CLC/TC 79 response

10 s is adequate for the generation of an EPS fault signal, delays in the annunciation of this signal would then be a “System requirement”. However, we agree that, depending on how the document is interpreted, 10 s for the generation of an APS fault signal could be regarded as incorrect. CLC/TC 79/WG 3 recommends that the two paragraphs under Table 1 in EN 50131-6 are changed to:

An APS fault signal shall be generated within 10 s of the completion of the internal APS test, if one of the following conditions occurs (according Table 1):

2.2.2 Table 2 and Note on page 9

2.2.2.1 Question

Compliance with the relevant chapters of EN 50131-1: is there meant Table 16 and why are multiple differences ?

2.2.2.2 CLC/TC 79 response

Agree. Table 2 in EN 50131-6 should be changed to be the same as Table 16 of EN 50131-1 and the subsequent note should be deleted.

2.2.3 Table 2 and Note on page 9

2.2.3.1 Question

Instead of i, ii, iii, iv, it should be I, II, III, IV. Will it be changed ?

2.2.3.2 CLC/TC 79 response

CLC/TC 79 agrees with the comment and recommends that the document is checked to ensure that it complies with PNE rules.

2.2.4 Table 4

2.2.4.1 Question

Severity level in grade 3: do not correspond to EN 50103.

2.2.4.2 CLC/TC 79 response

In order to correct the mistake, Table 4 in EN 50131-6 should be updated as follows:

Table 4 – Tamper protection

	Grade 1	Grade 2	Grade 3	Grade 4
Severity level (IK code)	07	07	07	08
Impact energy (Joule)	2	2	2	5

However, reviewing the document, CLC/TC 79 recommends modifying Table 4 in EN 50131-6 to be the same as Table 14 in CLC/TS 50131-3:

Table 4 – Tamper protection

	Grade 1		Grade 2		Grade 3		Grade 4	
	Int	Ext	Int	Ext	Int	Ext	Int	Ext
Severity level (IK code)	04	06	04	06	04	06	04	06
Impact energy (Joule)	0,5	1	0,5	1	0,5	1	0,5	1
NOTE Int = inside the supervised premises Ext = outside the supervised premises (indoor or outdoor).								

2.2.5 Subclause 8.2.14

2.2.5.1 Question

Items b) and c) are mutually contraindicating disconnecting of EPS. Will it be changed ?

2.2.5.2 CLC/TC 79 response

Accept the comment: Subclause 8.2.14 is to be modified as follows:

8.2.14 Low output voltage

a) Object

To demonstrate the ability of the PS to generate a power output fault signal, when the voltage at any or all of the PS outputs falls below the minimum power output voltage level with the EPS disconnected and SD connected.

b) Principle

The test consists of applying a load of 100 % of the maximum rating of the PS with the EPS disconnected and monitoring the voltage until a low voltage output signal is generated.

c) Test conditions

For types A and B PS the EPS shall be disconnected and a charged storage device shall be connected. For type C PS a charged SD shall be connected.