SLOVENSKI STANDARD
SIST-TS CLC/TS 50131-12:2016

01-december-2016

Alarmni sistemi - Sistemi za javljanje vloma in ropa - 12. del: Metode in zahteve za vklapljanje in izklapljanje sistemov za javljanje vloma (IAS)

Alarm systems - Intrusion and hold-up systems - Part 12: Methods and requirements for setting and unsetting of Intruder Alarm Systems (IAS)

Ta slovenski standard je istoveten z: CLC/TS 50131-12:2016

ICS:

13.310	Varstvo pred kriminalom	Protection against crime
13.320	Alarmni in opozorilni sistemi	Alarm and warning systems

SIST-TS CLC/TS 50131-12:2016 **en**

TECHNICAL SPECIFICATION

SPÉCIFICATION TECHNIQUE

TECHNISCHE SPEZIFIKATION

CLC/TS 50131-12

November 2016

ICS 13.320

English Version

Alarm systems - Intrusion and hold-up systems - Part 12: Methods and requirements for setting and unsetting of Intruder Alarm Systems (IAS)

To be completed

Alarmanlagen - Einbruch- und Überfallmeldeanlagen - Teil 12: Methoden und Anforderungen zur Scharf- und Unscharfschaltung von Einbruchmeldeanlagen (EMA)

This Technical Specification was approved by CENELEC on 2016-07-25.

CENELEC members are required to announce the existence of this TS in the same way as for an EN and to make the TS available promptly at national level in an appropriate form. It is permissible to keep conflicting national standards in force.

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

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

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

Ref. No. CLC/TS 50131-12:2016 E

Contents

Page

European foreword

This document (CLC/TS 50131-12:2016) has been prepared by CLC/TC 79 "Alarm systems".

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

Introduction

Unwanted alarms have been a significant problem for response authorities throughout Europe. A significant proportion of these are attributed to “operator error” during the entry and exit procedures. Recommendations are therefore made for the selection of methods of setting and unsetting an Intrusion Alarm System (IAS) that will minimize such errors.

1 Scope

This Technical Specification provides recommendations for those methods of setting and unsetting an Intrusion Alarm System (IAS) complying with EN 50131-1 that will reduce unwanted alarms arising from “operator error” in setting and unsetting the IAS and provide confidence that the conditions in which the system is installed are conducive to system reliability during the “set” period.

This document details optional methods by which these goals may be achieved, either in isolation, or in conjunction with verification methods.

These recommendations should be incorporated into the respective standards in the EN 50131 series.

This Technical Specification also provides (in Annex A) recommendations for equipment and (in Annex C) associated test requirements, in order to permit the manufacture of standardized equipment to provide the functionality needed by an IAS to meet these recommendations.

NOTE This standard includes requirements that are additional to those in EN 50131-1 which are relevant when the respective method of setting and unsetting is implemented.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

EN 50131-1:2006, *Alarm systems — Intrusion and hold-up systems — Part 1: System requirements*

CLC/TS 50131-2-10:2014, *Alarm systems — Intrusion and hold-up systems — Part 2-10: Intrusion detectors — Lock state contacts (magnetic)*

EN 50131-3:2009, *Alarm systems — Intrusion and hold-up systems — Part 3: Control and indicating equipment*

FprEN 50131-5-3:2016, *Alarm systems — Intrusion systems — Part 5-3: Requirements for interconnections equipment using radio frequency techniques*

CLC/TS 50131-9:2014, *Alarm systems — Intrusion and hold-up systems — Part 9: Alarm verification — Methods and principles*

3 Terms and definitions

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

3.1
unverified alarm
intruder or hold-up alarm that has not yet been sequentially, visually or audibly verified

[SOURCE: CLC/TS 50131-9: 2014, 3.1.14]

3.2
verified alarm
alarm considered genuine as a result of the use of alarm verification

[SOURCE: CLC/TS 50131-9: 2014, 3.1.16]

3.3
lock state monitoring device
apparatus which monitors the bolt position of a locking device, e.g. a bolt contact or a lock state contact as described in CLC/TS 50131-2-10

3.4
blocking function
logical function which prevents entry to the protected premises during the set state of the IAS.

Note 1 to entry: This function can be integrated in any device, e.g. lock, CIE (see Annex B).

3.5
blocking element
physical device which secures the entry door and is used in conjunction with blocking function

Note 1 to entry: See Annex B.

4 Methods of setting and unsetting

4.1 General

The methods of setting and unsetting described may be used as complementary to alarm verification technology (CLC/TS 50131-9) or as stand-alone methods of minimizing unwanted alarms arising from errors during setting and unsetting of an IAS.

In general, methods of setting and unsetting may be selected in any combination to suit the requirements of the specific alarm system installation. However, the “coerciveness” principle (4.2.3 and 4.3.4) should be considered as a single coherent set of recommendations covering both setting and unsetting.

If setting or unsetting is carried out by a combination of methods of authorization, the requirements of EN 50131-3:2009, 8.3.2.3 apply.

NOTE IAS should provide means to implement at least one of the methods of setting described in 4.2 and at least one of the methods of unsetting described in 4.3.

4.2 Methods of setting

4.2.1 General

Consideration should be given to the provision of an indication to the user and/or notification to the ARC if an attempt to set the IAS is not completed within the pre-determined time.

Completion of setting procedures should not rely solely on actions within the supervised premises (for example, simple timed exit procedure), but should require a specific action external to the supervised premises). Suitable methods include those given in 4.2.2 to 4.2.5.

4.2.2 The setting procedure is carried out from outside the supervised premises

The setting procedure shall comply with EN 50131-1:2006, 8.3.5. This may be achieved by mechanical or electronic means, or by provision of an indication such that the user is aware that the system is prevented from setting. An indication of completion of setting required by EN 50131-1:2006, 8.3.7 which can be perceived outside the supervised premises shall be provided

4.2.3 The setting procedure is carried out from outside the supervised premises incorporating additional measures to ensure the integrity of the IAS.

NOTE This describes the “coerciveness” principle, known in Germany as “Zwangsläufigkeit.”.

The setting procedure shall follow the recommendations of 4.2.2 with the following additional requirements:

a) all applicable requirements of EN 50131-1:2006, Table 4 shall apply in all grades of system;

b) for IAS with non-specific (e.g. wire-free) interconnections, no interference may be present in any shared interconnection for longer than 30 s;

c) for IAS with non-specific or wire-free interconnections, setting shall be permitted only if signals or messages have been received from all system components within 100 s;

d) the lock state monitoring devices are in a locked condition;

e) blocking shall be achieved by using blocking function and element as specified in A.2;

f) no configuration is in progress which could influence the operation of the IAS;

g) no remote diagnostic process is in progress which could influence the operation of the IAS.

On completion of setting and before the set indication is enabled, a mechanism shall be activated by the IAS, preventing unlocking of the designated entry door before the IAS is unset.

The last unset operation shall be completed and the IAS clear before a new setting operation can be commenced.

Where the opening of a window is detected the lock state shall also be monitored. Setting is permitted only when the window is closed and locked.

4.2.4 Setting is carried out by a 2-stage process

The setting procedure shall be started by a user action and be completed by a positive action outside of the supervised premises. Suitable methods of completion include:

a) the action of closing the final exit door;

EXAMPLE Response to closing of switch mounted on the door.

The CIE shall include a function to prevent spurious activation from any exit route detector from affecting the setting procedure (e.g. whilst a detector is stabilizing).

b) the action of locking the door (e.g. response to contacted lock);

c) a separate user action at the supervised premises to confirm successful closure of final exit door (e.g. operation of push button or other device).

There shall be an indication that the setting procedure has commenced. (see EN 50131-3:2009, 8.3.3.2).

An indication of completion of setting as required by EN 50131-1:2006, 8.3.7, which can be perceived outside the supervised premises, shall be provided.

4.2.5 Setting is carried out in conjunction with the ARC

Setting shall be carried out in accordance with an agreed secure procedure. As a minimum, this should include:

a) appropriate measures to prevent setting the system with persons inside the supervised premises;

b) exchange of authorization information at least equivalent to EN 50131-1:2006, 8.3.2.

The indication of completion of setting required by EN 50131-1:2006, 8.3.7 shall be communicated to the system user.

4.3 Methods of unsetting

4.3.1 General

The entry procedure should be designed to avoid the possibility of a user error resulting in an unwanted alarm condition. Suitable methods include those given in 4.3.2 to 4.3.9.