SLOVENSKI STANDARD
SIST-TS CLC/TS 50136-10:2022

01-julij-2022

Alarmni sistemi - Sistemi in oprema za prenos alarma - 10. del: Zahteve za oddaljeni dostop

Alarm systems - Alarm transmission systems and equipment - Part 10: Requirements for remote access

Ta slovenski standard je istoveten z: CLC/TS 50136-10:2022

ICS:

13.320	Alarmni in opozorilni sistemi	Alarm and warning systems

SIST-TS CLC/TS 50136-10:2022 en

TECHNICAL SPECIFICATION

SPÉCIFICATION TECHNIQUE

TECHNISCHE SPEZIFIKATION

CLC/TS 50136-10

April 2022

ICS 13.320

English Version

Alarm systems - Alarm transmission systems and equipment - Part 10: Requirements for remote access

To be completed

Alarmanlagen - Alarmübertragungsanlagen und -einrichtungen - Teil 10: Anforderungen für den Fernzugriff

This Technical Specification was approved by CENELEC on 2022-02-04.

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, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, 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: Rue de la Science 23, B-1040 Brussels

Contents

Page

European foreword

This document (CLC/TS 50136-10:2022) 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 shall not be held responsible for identifying any or all such patent rights.

The CLC/TS 50136 series consists of the following parts, under the general title *Alarm systems – Alarm transmission systems*:

— Part 1 General requirements for alarm transmission systems;

— Part 2 Requirements for Supervised Premises Transceiver (SPT);

— Part 3 Requirements for Receiving Centre Transceiver (RCT);

— Part 4 Annunciation equipment used in alarm receiving centres;

— Part 7 Application guidelines;

— Part 9 Requirements for common protocol for alarm transmission using the internet protocol (IP).

— Part 10 Requirements for remote access

Any feedback and questions on this document should be directed to the users’ national committee. A complete listing of these bodies can be found on the CENELEC website.

Introduction

It has been common practice for many years to monitor the alarm and fault status of alarm systems installed in premises from remote locations.

Technological developments within alarm systems as well as the telecommunication paths now permit remote access to those alarm systems with a wide variety of available functions up to and including full operation and programming / parameters setting as if an authorized person was at site.

Remote access complements the at site visits of competent person(s) and also enables remote access for customers (end-users). In short, the overall service quality offered by the various types of professional services providers at time of installation, maintenance or operation increases significantly. End-users experience faster response times leading to higher system reliability and availability. Service providers can provide new services such as remote system interrogation, which improves also staff utilization.

This document uses the term alarm system to describe any safety and security system.

1 Scope

This document specifies minimum requirements for secure connection and session for remote access to one or more alarm systems, for example fire safety systems, intruder and hold-up alarm systems, electronic access control systems, external perimeter security systems, video surveillance systems, and social alarm systems.

This document specifies the requirements for the performance, reliability, integrity, and security characteristics of a Remote Access Infrastructure.

This document specifies the requirements for a Remote Access Infrastructure between a Remote Access Client and an alarm system at the supervised premises and may be either integrated as part of the ATS or a separate infrastructure. In either case, the requirements of this European technical specification should apply.

This document does not cover the provision of functions and features on the alarm system.

2 Normative references

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

EN 50136-1:2012,[1] *Alarm systems – Alarm transmission systems and equipment – Part 1: General requirements for alarm transmission systems*

[1] As impacted by EN 50136-1:2012/A1:2018.

3 Terms, definitions and abbreviations

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in EN 50136-1:2012**Error! Bookmark not defined.** and the following apply.

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

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

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

3.1.1
connection
communication link between parts of the RAI

3.1.2
remote access
provision of access for a remote user or third-party systems to an alarm system installed at the supervised premises to perform authorized activities remotely, for example remote servicing, remote support, remote operations or other functions

3.1.3
Remote Access Client
logical function used to gain remote access to functions of one or more alarm systems

Note 1 to entry: In this document the Remote Access Client is considered a function rather than a physical device.

3.1.4
Remote Access Endpoint
logical function that manages remote access to functions of one or more AS

Note 1 to entry: In this document RAE has to be interpreted as functions and not as equipment.

3.1.5
Remote Access Infrastructure
system incorporating the logical functions of the RAE, RAS and RAC

3.1.6
Remote Access Infrastructure Service Provider
entity responsible for the design, operation and maintenance of the RAI

3.1.7
Remote Access Server
logical functions used to manage multiple remote connections of multiple alarm systems and users

3.1.8
remote user
person using the RAI via the RAC to remotely access one or more alarm systems

Note 1 to entry: The remote user is not necessarily the same user as the AS user

3.1.9
session
temporary and interactive information interchange between a user and an AS or between third-party systems and an AS

3.1.10
third-party system
system or application communicating with the alarm system via the RAI that is not produced by the RAISP

EXAMPLES Building Management System (BMS), Automated remote servicing or other security systems.

3.2 Abbreviations

For the purposes of this document, the following abbreviations apply:

RAE Remote Access End point

RAS Remote Access Server

RAI Remote Access Infrastructure

RAISP Remote Access Infrastructure Service Provider

RAC Remote Access Client

4 General requirements

4.1 Additional application

RAI shared with other applications shall be arranged such that operation and maintenance does not prevent the RAI from meeting the requirements of this document.

4.2 Logical structure

The RAI hosts 3 functionalities: the RAE, the RAS and the RAC.

Remote access infrastructure logical diagram:

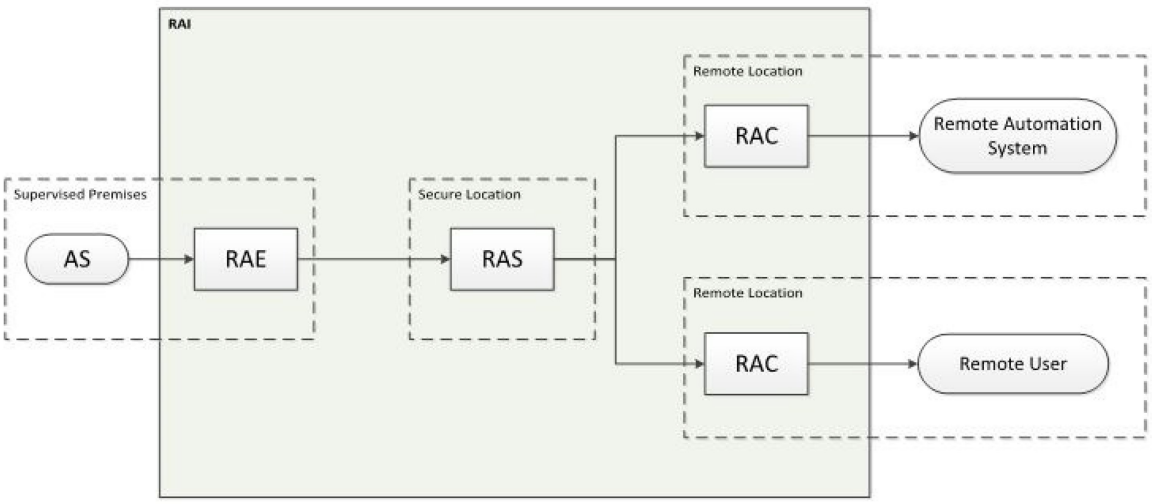

Figure 1 — Remote access infrastructure logical diagram

The RAI shall be designed in such a way that it only allows connections between RAE and RAS on one end, and connections between RAS and RAC on the other end.

The connection between the RAC and the RAE shall only be via the RAS.

It shall not be permitted to establish a direct connection between RAC and RAE.

5 Information security

5.1 General

All information stored and transferred within the RAI shall be secure. This section describes minimum requirements to achieve information security of the RAI.

The RAISP shall apply security measures to protect the RAI and its components against malicious attacks and inadvertent influences. The RAISP shall describe these security measures in their technical documentation.

NOTE Technical documentation does not need to include any information that the RAISP deems to be confidential.

All information security requirements listed in this section apply to communications between RAE and RAS, and between RAS and RAC.

The RAISP may delegate some responsibility through contracts with ATSPs, MARCs, transmission network operators etc. but retains overall responsibility.

5.2 Integrity and confidentiality

Data integrity shall be achieved for all sessions using hashing or digital signatures that meet the requirements of EN 50136-1:2012, 6.8.1.

All sessions shall be encrypted to achieve confidentiality. The same requirements for encryption as in EN 50136-1:2012, 6.8.1 apply.

NOTE Compliancy with this requirement can be achieved with the latest published TLS version.

5.3 Authentication

5.3.1 Connection authentication

Means shall be provided to authenticate RAE, RAS and RAC.

The RAS shall only allow connections from authenticated RAE and RAC. The RAISP shall specify how authentication is achieved and how the management of those authenticated functions are achieved.

5.3.2 Session authentication for Remote users

Means shall be provided to restrict remote access to the RAS to uniquely identified and validated remote user accounts by requiring the remote user to provide at least two of the following identification categories:

— Something the remote user has: software- or hardware-based factors (e.g. digital soft certificates, software-based token);

— Something the remote user knows (e.g. password, PIN, passphrase);

— Something the remote user is (e.g. fingerprint, eye iris).