

---

**Alarmni sistemi - Sistemi in oprema za prenos alarma - 1. del: Splošne zahteve za sisteme za prenos alarmov - Dopolnilo A1**

Alarm systems - Alarm transmission systems and equipment - Part 1: General requirements for alarm transmission systems

Alarmanlagen - Alarmübertragungsanlagen und -einrichtungen - Teil 1: Allgemeine Anforderungen an Alarmübertragungsanlagen

Systèmes d'alarme - Systèmes et équipements de transmission d'alarme - Partie 1: Exigences générales pour les systèmes de transmission d'alarme

<https://standards.iteh.ai/catalog/standards/sist/33c083e8-2daf-49e6-b8e1-06718fe883f3/sist-en-50136-1-2012-a1-2018>

**Ta slovenski standard je istoveten z: EN 50136-1:2012/A1:2018**

---

**ICS:**

13.320 Alarmni in opozorilni sistemi Alarm and warning systems

**SIST EN 50136-1:2012/A1:2018****en,fr**

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

[SIST EN 50136-1:2012/A1:2018](https://standards.iteh.ai/catalog/standards/sist/33c083e8-2daf-49e6-b8e1-06718fe883f3/sist-en-50136-1-2012-a1-2018)

<https://standards.iteh.ai/catalog/standards/sist/33c083e8-2daf-49e6-b8e1-06718fe883f3/sist-en-50136-1-2012-a1-2018>

EUROPEAN STANDARD  
NORME EUROPÉENNE  
EUROPÄISCHE NORM

**EN 50136-1:2012/A1**

November 2018

ICS 13.320

English Version

**Alarm systems - Alarm transmission systems and equipment -  
Part 1: General requirements for alarm transmission systems**

Systèmes d'alarme - Systèmes et équipements de  
transmission d'alarme - Partie 1: Exigences générales pour  
les systèmes de transmission d'alarme

Alarmanlagen - Alarmübertragungsanlagen und -  
einrichtungen - Teil 1: Allgemeine Anforderungen an  
Alarmübertragungsanlagen

This amendment A1 modifies the European Standard EN 50136-1:2012; it was approved by CENELEC on 2018-04-23. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this amendment the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CENELEC member.

This amendment exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

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, 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**

<b>Contents</b>	<b>Page</b>
European foreword.....	3
1 Modification to Clause 2, Normative references.....	4
2 Modifications to Clause 4, Terms, definitions and abbreviations .....	4
3 Modification to Clause 5, General requirements .....	5
4 Modifications to Clause 6, System requirements.....	6
5 Modification to Clause 7, Verification of performance .....	8
6 Modification to Annex A (informative), ATS configurations examples.....	8
7 Deletion of Annex D, Classes for category C.....	9
8 Modification to the Bibliography .....	9

## iTeh STANDARD PREVIEW (standards.iteh.ai)

SIST EN 50136-1:2012/A1:2018

<https://standards.iteh.ai/catalog/standards/sist/33c083e8-2daf-49e6-b8e1-06718fe883f3/sist-en-50136-1-2012-a1-2018>

## European foreword

This document (EN 50136-1:2012/A1:2018) has been prepared by CLC/TC 79, "Alarm systems".

The following dates are fixed:

- latest date by which this document has (dop) 2019-05-02  
to be implemented at national level by  
publication of an identical national  
standard or by endorsement
- latest date by which the national (dow) 2021-11-02  
standards conflicting with this document  
have to be withdrawn

This document supersedes EN 50136-1:2012.

EN 50136-1:2012/A1:2018 includes the following significant technical changes with respect to EN 50136-1:2012:

Amendment 1 to this standard improves the additional requirements for so-called hosted RCT alarm transmission systems and makes miscellaneous changes to correct errors and to reflect better the current state of the art.

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.

**iTeh STANDARD PREVIEW**  
(standards.iteh.ai)  
SIST EN 50136-1:2012/A1:2018  
<https://standards.iteh.ai/catalog/standards/sist/33c083e8-2daf-49e6-b8e1-06718fe883f3/sist-en-50136-1-2012-a1-2018>

## 1 Modification to European foreword

**Add the following:**

"Part 9 – Requirements for common protocol for alarm transmission using the internet protocol (IP)"

## 2 Modification to Clause 2, Normative references

**Replace the existing text with the following:**

"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 50136-2, Alarm systems - Alarm transmission systems and equipment - Part 2: Requirements for Supervised Premises Transceiver (SPT)

EN 50136-3, Alarm systems - Alarm transmission systems and equipment - Part 3: Requirements for Receiving Centre Transceiver (RCT)

## 3 Modifications to Clause 4, Terms, definitions and abbreviations

**Replace term and definition 4.1.7 with:**

**"4.1.7**

**alarm transmission service provider**

person or an entity that is responsible for design, operation, management and the verification of performance of one or more ATSN

Note 1 to entry: The ATSP may delegate some responsibility through contracts with customers, MARCs, transmission network operators etc. but retains overall responsibility.

<https://standards.iteh.ai/catalog/standards/sist/33c083e8-2daf-49e6-b8e1-3fe883f3/sist-en-50136-1-2012-a1-2018>

**Replace term and definition 4.1.28 with:**

**"4.1.28**

**receiving centre transceiver**

equipment located at a secure location and has as a minimum the functionality to receive and deliver alarm messages to the AMS

Note 1 to entry: The RCT may include management functions for the ATS."

**Replace term and definition 4.1.37 with:**

**"4.1.37**

**transmission time**

time from when a change of state occurs or alarm message is presented for transmission at the SPT interface to the AS until the time that the new state or message is reported at the RCT interface to the AMS"

**Add the following new terms and definitions:**

**"4.1.38**

**secure location**

location that is a MARC or another location that complies with a published data centre standard

Note 1 to entry: Examples of published data centre standards or accepted best practices are: a data centre designed and maintained to EN 50600 series. Availability class 3, Protection class 4 or ARC category I in accordance to EN 50518; or as best practices Uptime Institute Tier 3.

**4.1.39**

**monitoring and alarm receiving centre**

continuously manned centre where information concerning the status of one or more AS is reported, and additionally where the status of one or more ATS is monitored

#### 4.1.40

##### alarm management system

system at a MARC which stores, organizes, controls, manages and allows retrieval of client data and is interfaced to the alarm receiving equipment (RCT) for automatic annunciation of messages for each alarm system

#### 4.1.41

##### hosted RCT

RCT that consists of two parts, where one part is located in a secure location (RCT-H) and another part is installed in the ARC (RCT-A)”

**Add** abbreviations in 4.2

“AMS	Alarm Management System
I <sub>RCT</sub>	Interface of the AMS to the RCT
MARC	Monitoring and Alarm Receiving Center
RCT-H	Hosted part of the RCT used in a hosted ATS solution
RCT-A	Part of the hosted RCT installed in the ARC, partner of the RCT-H.”

## 4 Modification to Clause 5, General requirements

**Add** the following paragraph to 5.2.1:

“An ATSP shall be identified for both direct and hosted ATS for the appropriate categories as defined per Table 1.”.

**Replace** Table 1 with the following table:  
<https://standards.iteh.ai/catalog/standards/sist/33c083e8-2daf-49e6-b8e1-06718fe883f3/sist-en-50136-1-2012-a1-2018>

**Table 1 — ATS configuration**

	SP1	SP2	SP3	SP4	SP5	SP6	DP1	DP2	DP3	DP4
SPT primary network interface	M	M	M	M	M	M	M	M	M	M
SPT alternative network interface	Op	Op	Op	Op	Op	Op	M	M	M	M
Alternative RCT	Op	Op	Op	Op	Op	Op	M	M	M	M
RCT primary network interface	M	M	M	M	M	M	M	M	M	M
RCT alternative network interface	Op	Op	Op	Op	Op	Op	M	M	M	M
ATSP for non-hosted ATS	Op	Op	Op	M	M	M	Op	M	M	M
ATSP for hosted ATS	M	M	M	M	M	M	M	M	M	M
<b>Key</b> M = Mandatory Op = Optional										
NOTE ATSP is not required for non-hosted ATS solutions for categories SP1, SP2, SP3 and DP1 because there are no requirements for availability (see Table 6).										

## EN 50136-1:2012/A1:2018 (E)

Replace 5.2.2 with:

### 5.2.2 Custom category

Where an application cannot be satisfied by any of the categories of this standard a new custom category, category C, shall be defined and it shall include the rationale for the choice of the custom category and there shall be sufficient documentation for the verification of performance.

A statement shall be made referring to the requirements listed in Tables 1, 2, 3, 4, 5, 6, 7, 8 and 9. All other clauses of this standard shall apply.”.

## 5 Modifications to Clause 6, System requirements

In 6.3.3.3.1, **replace** Table 3 with:

“

Table 3 — Maximum reporting time

	SP1	SP2	SP3	SP4	SP5	SP6	DP1	DP2	DP3	DP4
<b>Primary ATP failure Reporting time</b>	<b>32 days</b>	<b>25 h</b>	<b>30 min</b>	<b>3 min</b>	<b>90 s</b>	<b>20 s</b>	<b>25 h</b>	<b>30 min</b>	<b>3 min</b>	<b>90 s</b>
<b>Alternative ATP failure Maximum period when primary operational</b>	<b>Op</b>	<b>Op</b>	<b>Op</b>	<b>Op</b>	<b>Op</b>	<b>Op</b>	<b>50 h</b>	<b>25 h</b>	<b>25 h</b>	<b>5 h</b>
<b>Alternative ATP failure Maximum period when primary failed</b>	<b>Op</b>	<b>Op</b>	<b>Op</b>	<b>Op</b>	<b>Op</b>	<b>Op</b>	<b>25 h</b>	<b>30 min</b>	<b>3 min</b>	<b>90 s</b>
<b>Failure of all ATPs at the same time*</b>	<b>32 days</b>	<b>25 h</b>	<b>30 min</b>	<b>3 min</b>	<b>90 s</b>	<b>20 s</b>	<b>25 h</b>	<b>31 min</b>	<b>4 min</b>	<b>3 min</b>

\*Where an ATS includes two or more ATPs the reporting time shall meet the requirements of this table.

“

In 6.3.3.3.2, **delete** NOTE 3 and insert the following new paragraph: “

“Where an ATS remains operational a single path line fault shall be presented to the ATSP, but can be delayed presenting it to the AMS where it is agreed between the interested parties. The maximum delay shall not exceed 96 h.”.

**Replace** Note 4 with Note 3.



In 6.6, replace Table 4 with:

“

**Table 4 — RCT to AMS alarm reporting**

Alarm	SP1	SP2	SP3	SP4	SP5	SP6	DP1	DP2	DP3	DP4
ATS failure	M	M	M	M	M	M	M	M	M	M
ATP failure	Na	Na	Na	Na	Na	Na	M	M	M	M
M = Mandatory Na = Not applicable										
NOTE 1 The SP categories have only one ATP, in this instance only an ATS failure needs to be reported.										
NOTE 2 The alarm transmission service provider should document the messages used to report the required alarms to the AMS.										
NOTE 3 For category DP1, DP2, DP3 and DP4 the method of alarm reporting of all paths failed to the AMS should be either an 'ATS primary path failure' and an 'ATS alternative path failure' message, and/or as an 'all paths failed' message. The method of reporting shall be documented by the ATSP.										
NOTE 4 For category DP1, DP2, DP3 and DP4 where the reporting of ATP failures to the AMS are delayed, confusion may arise if the user of the alarm system is made aware of ATP failures (see Table 5). It is therefore recommended in these cases that ATP failures are not reported to the AS.										

“

In 6.6, **replace** the paragraph (under Table 5) with:

“Single path systems

Failure of the ATS shall be reported to the AS in accordance with the requirements of Table 5.

Dual path systems

Failure of the ATS shall be reported to the AS in accordance with the requirements of Table 5.

ATP failures need not be reported to the AS unless specified and agreed between the interested parties.

In 6.7.5, **replace** the existing text above Table 6 with the following:

#### **“6.7.5 ATS availability recording**

For the purpose of performance monitoring and verification ATP and ATS availability shall be recorded.

Where the ATS availability fails to meet the requirements of Table 6 it shall be clearly indicated in the availability records.

For categories DP2, DP3 and DP4 where the ATP availability is less than 95 % in any 7-day period it shall be clearly indicated in the availability records.

The ATSP shall have in place processes and procedures to make the availability reports available to the interested parties for the purpose of maintaining the required performance level. Further details of these processes and procedures are provided in TS 50136-7.”.

In 6.8.1 **replace** the text with the following:

#### **“6.8.1 General security requirements**

The ATSP shall describe means to protect the ATS and its components (e.g. SPTs, RCTs and hosted RCTs) against malicious attacks and inadvertent influences.

To achieve substitution and information security cryptographic techniques shall be used.

When symmetric encryption algorithms are used, key length shall be no less than 128 bits. When other algorithms are deployed, they shall provide similar level of cryptographic strength. Any hash functions used shall give a minimum of 128 bits output. Regular automatic key changes shall be used with machine generated randomized keys.

Use of cryptographic algorithms as defined in ISO/IEC 18033 is recommended. Use of hash functions as defined in ISO/IEC 10118 is recommended.