BS EN 50136-1:2012

BSI Standards Publication

Alarm systems — Alarm transmission systems and equipment -

Part 1: General requirements for alarm transmission systems

bsi.

...making excellence a habit.™

National foreword

This British Standard is the UK implementation of EN 50136-1:2012. It supersedes BS EN 50136-1-1:1998+A2:2008, BS EN 50136-1-2:1998, BS EN 50136-1-3:1998, BS EN 50136-1-4:1998 and BS EN 50136-1-5:2008 which are withdrawn.

The UK participation in its preparation was entrusted to Technical Committee GW/1/5, Transmission equipment and networks.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

ISBN 978 0 580 62588 6

ICS 13.320

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 September 2012.

Amendments issued since publication

Date	Text affected

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 50136-1

January 2012

ICS 13.320

Supersedes EN 50136-1-1:1998 + A1:2001 + A2:2008, EN 50136-1-2:1998, EN 50136-1-3:1998, EN 50136-1-4:1998, EN 50136-1-5:2008

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 European Standard was approved by CENELEC on 2011-12-26. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard 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 European Standard 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, 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.

CENELEC

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

Management Centre: Avenue Marnix 17, B - 1000 Brussels

Ref. No. EN 50136-1:2012 E

Contents

Figures

Tables

Foreword

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

The following dates are fixed:

• latest date by which this document has to be implemented at national level by publication of an identical national standard or by endorsement	(dop)	2012-12-26
• latest date by which the national standards conflicting with this document have to be withdrawn	(dow)	2014-12-26

This document supersedes EN 50136-1-1:1998 + A1:2001 + A2:2008, EN 50136-1-2:1998, EN 50136-1-3:1998, EN 50136-1-4:1998 and EN 50136-1-5:2008.

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

- Part 1 General requirements for alarm transmission systems;
- Part 2[1)] Requirements for Supervised Premises Transceiver (SPT);
- Part 3[1)] Requirements for Receiving Centre Transceiver (RCT);
- Part 4 Annunciation equipment used in alarm receiving centres;
- Part 5[2)] (free);
- Part 6[2)] (free);
- Part 7 Application guidelines.

1) At draft stage.

2) Under consideration.

1 Scope

This European Standard specifies the requirements for the performance, reliability and security characteristics of alarm transmission systems.

It specifies the requirements for alarm transmission systems providing alarm transmission between an alarm system at a supervised premises and annunciation equipment at an alarm receiving centre.

This European Standard applies to transmission systems for all types of alarm messages such as fire, intrusion, access control, social alarm, etc. Different types of alarm systems may in addition to alarm messages also send other types of messages, e.g. fault messages and status messages. These messages are also considered to be alarm messages in the context of this standard. The term alarm is used in this broad sense throughout the document.

Additional alarm transmission requirements of specific types of alarm systems are given in the relevant European Standards.

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 50136-2[1)]		*Alarm systems — Alarm transmission systems and equipment — Part 2: Requirements for Supervised Premises Transceiver (SPT)*
EN 50136-3[1)]		*Alarm systems — Alarm transmission systems and equipment — Part 3: Requirements for Receiving Centre Transceiver (RCT)*
ISO/IEC 10118	series	*Information technology — Security techniques — Hash-functions*
ISO/IEC 18033	series	*Information technology — Security techniques — Encryption algorithms*

3 Object

The object of this European Standard is to specify the general requirements for the performance, reliability, resilience and security of alarm transmission systems and to ensure their suitability for use with different types of alarm systems and annunciation equipment.

An alarm transmission system may use any type of transmission network.

When the ATS functions are integrated into an alarm system or annunciation equipment the requirements of this standard shall apply.

The intended users of this European Standard include alarm transmission service providers, alarm receiving centre operators, fire departments, insurance companies, telecommunication network operators, internet service providers, equipment manufacturers, alarm companies, end users and others.

4 Terms, definitions and abbreviations

4.1 Terms and definitions

For the purposes of this standard the following terms and definitions apply.

NOTE The definitions below should be read in conjunction with Figure 1.

4.1.1
alarm condition
condition of an AS, or part thereof, which results from the response of the system, or part thereof, to the presence of a hazard

4.1.2
alarm receiving centre
continuously manned centre to which information concerning the status of one or more AS is reported

4.1.3
alarm system
electrical installation, which responds to the manual or automatic detection of the presence of a hazard

Note 1 to entry: The AS is not part of the ATS.

4.1.4
alarm transmission equipment
collective term to describe SPT, MCT and RCT

4.1.5
alarm transmission path
route an alarm message travels between an individual AS and its associated AE

Note 1 to entry: The ATP starts at the interface between AS and SPT and ends at the interface between RCT and AE. For notification and surveillance purposes the reverse direction may also be used.

4.1.6
alarm transmission service network
group of ATSs of the same category

Note 1 to entry: An ATSN consists of one or more ATSs of the same category, functioning under supervision of the same management and monitoring centre.

4.1.7
alarm transmission service provider
person or an entity that is responsible for design, operation and the verification of performance of one or more ATSN

Note 1 to entry: The ATSP may take responsibility for the ATS provision and performance monitoring of one or more ATSN as the design authority, through contracts with customers, ARCs, transmission network operators, etc.

4.1.8
alarm transmission system
ATE and networks used to transfer information concerned with the state of one or more ASs at a supervised premises to one or more AEs of one or more ARCs

Note 1 to entry: An ATS may consist of more than one ATP.

4.1.9
ATS category
set of parameters that define the performance requirements of an alarm transmission system

Note 1 to entry: A category defines minimum ATS requirements.

Note 2 to entry: The alarm system application should specify the appropriate ATS category.

Note 3 to entry: Where resilience and reliability are considered important for the Alarm System application, the use of a dual path ATS is recommended.

4.1.10
ATS management system
part of the ATS that is used to manage alarm transmission equipment, supervise alarm transmission equipment and networks and may help to keep the ATS in operation

Note 1 to entry: The management system may also be used to collect data about the ATS availability.

4.1.11
ATS monitoring centre
centre in which the status and performance of one or more ATS is monitored

Note 1 to entry: A monitoring centre may be a separate centre or part of an ARC.

Note 2 to entry: A monitoring centre may be the place where MCTs are located.

Note 3 to entry: A monitoring centre may be the place where a management system is located.

4.1.12
annunciation equipment
equipment located at an ARC which secures and displays the alarm status, or the changed alarm status of ASs in response to the receipt of incoming alarms before sending a confirmation

Note 1 to entry: The AE is not part of the ATS.

4.1.13
authentication
exchange of a code to identify that a SPT has not been substituted by a similar equipment without this code, or that the information message transmitted has not been modified

4.1.14
availability, general
percentage of time a system or parts of a system are functioning in accordance with the requirements of this standard

4.1.15
diverse technology
technologies used in transmission paths in such a way that a single point of failure, or tampering of a single point, cannot cause both ATPs of a dual path system to fail simultaneously

4.1.16
dual path ATS
ATS consisting of one primary ATP and one secondary ATP using diverse technology, having two transmission network interfaces at the SPT, to connect one or more AS of one supervised premises to one or more AEs of one or more ARCs

4.1.17
encryption
systematic encoding of a bit stream before transmission, so that the information contained in the bit stream cannot be deciphered by an unauthorised party

4.1.18
fault condition
condition of a system which prevents a system or part thereof from functioning normally

4.1.19
fault message/signal
message or signal generated as a result of a fault condition

4.1.20
hashing technique
use of a mathematical transformation that takes an input and returns a fixed-size string, which is called the hash value

Note 1 to entry: Hash value is used to detect any alteration of the input and therefore verify the contents in an easy way.

4.1.21
message
series of transmitted signals which include identification, function data and the various means for providing its own integrity, immunity and proper reception

4.1.22
monitoring centre
centre in which the status of one or more ATSNs is monitored

4.1.23
monitoring centre transceiver
ATE within the ATS that enables monitoring and management information regarding the status of alarm transmission equipment and networks

Note 1 to entry: The monitoring centre transceiver may be located at the alarm receiving centre or at a separate centre.

4.1.24
multiple path ATS
ATS where more than one independent ATPs are combined to connect one or more ASs of one supervised premises to one or more AEs of one or more ARCs

4.1.25
network equipment on site
equipment that is part of the ATP, but is not considered to be ATE

4.1.26
packet switched network
transmission network that uses packet switching

Note 1 to entry: Messages are broken into packets, which are addressed individually and routed through the network, possibly using different routes. At the end node the packets are re-assembled to be converted back to the original message.

Note 2 to entry: The most prominent example of a packet switched data network is the Internet, making use of the Internet protocol suite, which is specified by the internet engineering task force (IETF) in so called requests for comments (RFCs).

4.1.27
peer review
when used in reference to cryptographic algorithms, means there is published evidence that the cryptographic community has confirmed the robustness of the algorithm against attack

4.1.28
receiving centre transceiver
ATE at the ARC including the interface to one or more AE(s) and the interface to one or more transmission networks and being part of one or more ATPs

Note 1 to entry: In some systems this transceiver may be able to indicate changes of the status of an AS and to store log-files. This may be needed to increase the ATS availability in case of AE failure.

4.1.29
reporting time
period from the time a fault occurs in the ATS until the fault information is reported to the RCT, the AS at the supervised premises and the MCT (if provided)

4.1.30
secured message
message which cannot be lost (e.g.: in the case of power failure) and which can be retrieved

4.1.31
signalling security
method(s) used to prevent or detect deliberate attempts to interfere with the transmission of an alarm by blocking or substitution

4.1.32
single path ATS
ATS that consists of one ATP to connect one or more AS of one supervised premises to one or more AEs of one or more ARCs

4.1.33
supervised premises transceiver
ATE at the supervised premises including the interface to the AS and the interface to one or more transmission networks and being part of one or more ATPs

4.1.34
system capacity
maximum number of ASs that can be connected to an ATSN

4.1.35
transmission link
part of a transmission network used to carry one or more ATPs

Note 1 to entry: An ATP can be established by switching together transmission links in several ways (in parallel, in series and in combinations thereof).

Note 2 to entry: A transmission link can carry several ATPs or sections of ATPs.

4.1.36
transmission network
network between two or more items of ATE

Note 1 to entry: Where the network is provided by a common carrier (e.g. a public telephone network operator) the network may include items of general transmission equipment, which may not be covered by the requirements of EN 50136-2, e.g. public telephone network operator equipment, mobile telephone operator equipment, ADSL modems, SDSL modems, Routers, Ethernet switches, Ethernet hubs, Firewalls and network wiring.

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 AE

4.2 Abbreviations

For the purposes of alarm transmission standard documents from EN 50136 / CLC/TS 50136 series, the following abbreviations apply.

ADSL Asymmetric Digital Subscriber Line

AE Annunciation Equipment

ARC Alarm Receiving Centre

AS Alarm System

ATE Alarm Transmission Equipment

ATP Alarm Transmission Path

ATS Alarm Transmission System

ATSN Alarm Transmission Service Network

ATSP Alarm Transmission Service Provider

DSL	Digital Subscriber Line
DTMF	Dual Tone Multi Frequency
GSM	Global System Mobile
ISO	International Standardisation Organisation
ISDN	Integrated Service Digital Network
MCT	Monitoring Centre Transceiver
OSI	Open Systems Interconnection
PSN	Packet Switched Network
PSTN	Public Switched Telephone Network
RCT	Receiving Centre Transceiver
SPT	Supervised Premises Transceiver
SDSL	Symmetric Digital Subscriber Line

5 General requirements

5.1 ATS configuration

The logical configuration of an ATS shall be as shown in Figure 1. The main function of an ATS is to provide a reliable and secure transmission network from the interface of the AS to the SPT to the interface of the RCT to the AE for the transmission of alarms.

Depending upon the required reliability and resilience of the ATS and the operational features of the ARC, various ATS configurations may be used, including the use of more than one ATP between an AS and one or more RCTs connected to one or more AEs. Each ATP shall have its own transmission network interface at the SPT.

NOTE For example an SPT may use a fixed line network and a radio network.

Selection of the category of ATS used for an AS shall be determined by the required reliability and security for the associated application. Reference should be made to the category of ATS required and the options that may be selected.

5.2 ATS categories

5.2.1 General

An alarm transmission system shall be selected from one of ten categories described by this European Standard. An ATS shall be allocated a category which will determine its performance and resilience.

Categories SP1 to SP6 are based on single ATP ATSs.

Categories DP1 to DP4 add resilience by requiring alternate ATPs.

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
Key M = Mandatory Op = Optional										

5.2.2 Custom category

5.2.2.1 General

Where an application cannot be satisfied by any of the categories of this standard a new custom category, category C, shall be defined within an application specific standard using parameters from the classes defined in Annex D.

Where a custom category is used reference shall be made to the tables in Annex D instead of the category tables, Table 1 to Table 9. All other requirements of this standard shall apply.

5.2.2.2 Documentation

Where there is a requirement for a custom category C, it shall include the rationale for the choice of a 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, 4, 5 and 6.

5.3 Applicable network standards

Equipment and systems shall meet local, national and European requirements and regulations for attachment to, establishment and termination of connection and transmission via public telephone and data networks and/or the regulations for transmission via the use of radio, power distribution systems or cable TV distribution systems.

6 System requirements

6.1 General

The ATS shall provide communication between one or more ASs at one supervised premises and one or more AEs of one or more ARCs.

6.2 Transmission link requirements

6.2.1 General

An ATP may include permanent dedicated links, permanent virtual links or switched links which may use equipment that is not covered by the requirements of EN 50136-2 and EN 50136-3 or may be affected by other applications sharing the transmission links.

An ATP may include:

- a transmission link that is shared with non-alarm data applications,
- a transmission link that carries other ATPs,
- equipment from a third party transmission network provider, which is not located at either the supervised premises or the alarm receiving centre and is not classified as ATE,
- equipment from a third party which is located at the supervised premises but is not classified as ATE.

The performance (reliability) of an ATS may be affected by:

- unwanted, malformed or otherwise malicious incoming data at the interfaces of the SPT or RCT,
- transmission network congestion as a result of transmission link sharing,
- transmission network unavailability due to equipment failure and/or maintenance.

6.2.2 Transmission links shared with other applications

Transmission links shared with other applications shall be arranged such that operation and maintenance does not prevent the ATS from meeting the requirements of this European Standard.

6.2.3 Transmission network equipment

Transmission equipment that is connected between the transmission network interface of the SPT and the transmission network interface of the RCT and/or MCT is not subject to the requirements of EN 50136-2 and EN 50136-3.

NOTE 1 Examples of SPT integrated network interfaces include analogue modems, DTMF transceivers, ISDN terminal adapters, Ethernet modules, and GSM radio modules. No technologies are excluded.

NOTE 2 Equipment at the supervised premises will be subject to the application guidelines provided within CLC/TS 50136-7.

NOTE 3 Local network interface failures may be detected and reported by the SPT to the RCT using the remaining operational transmission path; however interface monitoring cannot be used to provide confirmation that a transmission path is operational.

6.2.4 ATSN capacity

The ATSP shall provide a statement regarding the number of ASs that can be connected to the ATSN that will ensure compliance with the requirements of Table 2.

Any single ATP shall continue to meet the requirements of the appropriate transmission time and the maximum transmission time of Table 2:

a) at a rate equivalent to one such message per minute from each of a number of ASs representing at least 0,1 % of the system capacity, and

b) at a rate of at least 2 alarms per minute at the RCT interface to the AE.

The evaluation shall be done when the ATSN is in a normal condition with the stipulated rate of messages.

6.2.5 Denial of service

The ATS shall protect itself against Denial of Service (DoS) attacks from the transmission network.

Any form of incoming data or signal received from a transmission network shall not prevent the ATP from performing as specified, unless the amount of incoming data leads to congestion of the transmission link. ATP performance deterioration is not allowed when there is enough remaining network capacity to carry ATP signalling.

Any malicious data received by a transmission network interface, shall not affect the operation of the ATE (SPT, RCT or MCT) or the operation of any other transmission network interface. This applies even if the malicious data rate reaches the capacity of a single interface, rendering the interface itself inoperable.

If the performance of the ATS is affected by a DoS attack, a fault signal shall be generated according to the monitoring and fault reporting requirements of applicable category.

NOTE 1 This requirement is intended to emphasize the need to protect against attacks where malicious data or signalling is used to interfere with the operation of the ATE. These attacks can be performed either by malicious signalling designed to impair the ATE or by overloading the communications with large amounts of data.

NOTE 2 DoS attacks may be present in any network, e.g. IP networks, PSTN networks. Examples of such attacks are: devices deliberately overloading the IP network, automatic dialling facilities to overload parts of PSTN networks, jamming devices to interfere with radio communications, etc.

6.3 Performance

6.3.1 General

For the categorisation of the ATS the following parameters are used:

- transmission time; average, 95th percentile and maximum;
- reporting time;
- monitoring of interconnections;
- ATSN availability.

6.3.2 Transmission time

The arithmetic mean of the alarm transmission time and 95th percentile of the measurements of the transmission time shall not exceed the values specified in Table 2 for the appropriate category.

Any transmission time exceeding the maximum acceptable transmission time of Table 2 for a specific system shall, for each incident, be classified as a transmission system fault in accordance with NOTE 7.

The time is measured from the time 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 AE.

The transmission time applies to all changes of state or message that are transmitted from the AS through the SPT interface to the ATS.

NOTE 1 Where the SPT interface to the AS is not accessible the measurement may be made from a more accessible point before the SPT interface to the AS and an appropriate correction applied to the result.

NOTE 2 Where the RCT interface to the AE is not accessible, or where it is more convenient, the measurement may be made to a point after the RCT interface to the AE and an appropriate correction applied to the result.

NOTE 3 Times within the AS and within the AE will be specified in other standards.

NOTE 4 For most ATS(s) there exists a direct relation between the classification of Tables 2 and 3.

NOTE 5 The transmission time includes the time to establish a connection.

Table 2 — Transmission time

transmission time	SP1	SP2	SP3	SP4	SP5	SP6	DP1	DP2	DP3	DP4
Arithmetic mean of all transmissions	120 s	60 s	20 s	20 s	10 s	10 s	60 s	20 s	20 s	10 s
95th percentile of all transmissions	240 s	90 s	30 s	30 s	15 s	15 s	90 s	30 s	30 s	15 s
Maximum acceptable transmission time	480 s	120 s	60 s	60 s	30 s	30 s	120 s	60 s	60 s	30 s

Where the transmission time cannot be measured directly then it is acceptable that the round-trip time may be measured. In this case the round-trip time shall meet the same requirements as the transmission time for the appropriate category in Tables 2 and 3.

NOTE 6 The transmission time may not be equal to half the round-trip time.

NOTE 7 The round-trip time is the time measured 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 positive acknowledge signal or message is presented to the AS (at the SPT interface to the AS).

6.3.3 Monitoring of interconnections

6.3.3.1 General

All of the following links and interconnections of the ATS shall be monitored and faults shall be detected, reported and logged:

- AS to SPT interconnection monitoring this also applies for integrated AS and SPT solutions;
- ATP end-to-end monitoring;
- RCT to AE interconnection monitoring.

6.3.3.2 Monitoring of the interconnection with the AS

In the event of a fault on the interconnection between the AS and the SPT a fault or alarm signal shall be generated and transmitted to relevant AE and if applicable the MCT(s) within the times specified in Table 2 for the appropriate category.

NOTE Where the interconnection used for alarm transmission between the AS and SPT is not available, an independent connection between the AS and SPT can be used to signal that interconnection fault to the AS.

6.3.3.3 Monitoring of the ATS

6.3.3.3.1 General

The reporting time shall not exceed the values specified in Table 3 for the appropriate ATS category.

Transmission faults shall be presented to the AE and AS as described in Table 4 and Table 5.

All transmission faults shall be presented to the ATSP for appropriate action.

All ATPs shall be monitored in line with the requirements listed in Table 3.

NOTE 1 The frequency of the exchange of status messages should be greater than the reporting times in Table 3 to minimise the generation of false alarms. Where required by the ATS Category, status messages should be encrypted and substitution protected.

NOTE 2 Local network interface failures may be detected and reported by the SPT to the RCT using the remaining operational transmission path; however interface monitoring cannot be used to provide confirmation that a transmission path is operational.

Table 3 — Maximum reporting time

	SP1	SP2	SP3	SP4	SP5	SP6	DP1	DP2	DP3	DP4
Primary ATP Reporting time	32 days	25 h	30 min	3 min	90 s	20 s	25 h	30 min	3 min	90 s
Alternative ATP Maximum period when primary operational	Op	Op	Op	Op	Op	Op	50 h	25 h	25 h	5 h
Alternative ATP Maximum period when primary failed	Op	Op	Op	Op	Op	Op	25 h	30 min	3 min	90 s
ATS reporting time [a]	32 days	25 h	30 min	3 min	90 s	20 s	50 h	60 min	6 min	3 min

Key
OP = Optional

[a] Where an ATS includes more than two ATPs the ATS reporting time shall meet the requirements of this table.

6.3.3.3.2 Dual path ATS (DP1-DP4)

Where an ATS category requires more than one ATP, the ATPs shall use diverse interfaces to connect the SPT to the transmission networks in such a way that a single tamper action on the transmission network cannot cause all ATPs to fail simultaneously.

NOTE 1 For example fixed line alarm transmission path and a radio transmission path using a mobile service provider network.

NOTE 2 Dual path ATS requirements apply to all ‘D’ categories as defined throughout this standard.

One of the ATPs, of a dual path system, shall be identified as the primary ATP and include a primary ATP reporting time as specified in Table 3.

Whilst the primary ATP is known to be operational the alternative ATP shall not exceed a maximum reporting time as specified in Table 3.

The alternative ATP shall have a maximum reporting time as specified in Table 3 when the primary ATP is failed to make sure the ATS maximum reporting time is not exceeded.

The reporting time for the loss of both ATPs shall not exceed the ATS reporting time defined in Table 3 for the appropriate category.

NOTE 3 As long as service is not lost a single path line fault should be presented to the ATSP, but can be delayed presenting it to the AE where it is agreed between the interested parties (see 6.7.2).

NOTE 4 It is permitted to have more than two paths.

6.3.3.4 Monitoring of the interconnection with the AE

The interconnection between the RCT and the AE shall be monitored. In the event of failure of the interconnection a fault signal shall be recorded and presented to relevant AE and RCT or monitoring centre. The reporting time of the fault signal shall meet the shortest reporting time requirement of any associated ATP.

6.4 Securing of messages in the alarm transmission system

Messages shall not be lost in the event of power failure or any other event generated internally by the SPT or RCT as for example software reset.

6.5 Alarm transmission acknowledgement

A means shall be provided to confirm that each alarm received at the SPT from the AS, and each alarm generated by the ATS, is delivered correctly to the AE. This may be delivered as either a positive acknowledgement of alarm delivered or a fault message on failure of delivery shall be send to the AS by the SPT.

6.6 ATS generated alarms

The ATS is required to report all alarms and path failures as specified in Table 4 for each category to the AE.

In the event of an ATS failure a fault or alarm signal shall be generated and transmitted to relevant AE and if applicable the MCT(s) within the times specified in Table 2 for the appropriate category.

All ATS faults shall be presented to the ATSP for appropriate action.

Table 4 — RCT to AE 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	Op	Op	Op	Op

Key
M = Mandatory
Op = Optional
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 AE.

NOTE 3 For category DP1, DP2, DP3 and DP4 the method of alarm reporting of all paths failed to the AE 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.

Table 5 — SPT to AS alarm reporting

Alarm	SP1	SP2	SP3	SP4	SP5	SP6	DP1	DP2	DP3	DP4
ATS failure	Op	M	M	M	M	M	M	M	M	M
ATP failure	Na	Na	Na	Na	Na	Na	Op	Op	Op	Op
Key M = Mandatory Op = Optional Na = not applicable										

The ATS is required to report all alarms and path failures as for each category specified in Table 5 to the AS.

NOTE The requirement to report alarms and path failures to the AS does not specify how this shall be processed by the AS. The AS requirements are defined in the appropriate application standard.

6.7 Availability

6.7.1 General

The availability of the ATP, ATS and ATSN is the percentage of time during which the ATP, ATS and ATSN are known to operate within the requirements of the appropriate performance category.

NOTE 1 The availability of the ATP, ATS and ATSN should not be confused with transmission network availability. For the purpose of calculating the ATP and system availability the availability of the SPT, the transmission network and the RCT should be considered as serial availabilities.

NOTE 2 Where an ATS uses more than one ATP the availability of the ATPs should be considered parallel.

NOTE 3 The ATSN availability is used to provide a performance indication of the ATSN to an ATSP.

The ATS shall be such that, except under alarm or fault conditions, the status of the ATS shall be monitored to verify its integrity. The monitoring shall be of a sufficient frequency to meet the fault reporting requirements for the appropriate reporting time in Table 3.

It is required to provide evidence that availability can be recorded and is available for inspection at any time.

6.7.2 Redundancy/duplication

Where several interfaces to the ATS exist at the SPT or at the RCT the ATS shall be considered to be available in the event of a fault affecting one or more such interfaces provided:

a) at least one ATP exists between one interface at the AS and one interface at the AE; and

b) either:

   1) messages are normally transmitted and received on all such interfaces, or

   2) messages are normally transmitted and received on one primary interface at each end, but that in the event of a failure the system automatically changes to an alternative interface.

6.7.3 ATS unavailability

For the purposes of calculating the system availability the following situations shall be considered:

a) all faults in the ATS, which will prevent an alarm from being transmitted to its intended ARC(s) within the requirements of the appropriate category;

b) unavailability due to maintenance of the ATS, unless alternative facilities are provided.

The ATS shall be considered to be unavailable while any of the above conditions exist.

6.7.4 Duration of faults

The time for which the ATS shall be considered to be unavailable shall be the period from the last time the system was known to be available (i.e. with no faults) until the time when a fault is detected, repaired and the system confirmed to be available again.

NOTE Faults caused by deliberate attempts to compromise the system should not be included provided that they are detected and reported within the time specified in Table 3 for the appropriate category.

6.7.5 ATS availability recording

For the purpose of performance monitoring and verification, a fault shall be recorded when the ATS fails to meet the requirement of Table 6.

This fault recording shall, if required by Table 6, be made available to the customer upon request. The records shall be kept as required by 7.5.1.

NOTE The purpose of measuring ATS availability is to identify faults, analyse and fix them to restore the ATS operation.

Table 6 — ATS availability recording

	SP1	SP2	SP3	SP4	SP5	SP6	DP1	DP2	DP3	DP4
ATS availability in any 7-day period (%)	Op	Op	Op	97,0	99,0	99,8	Op	99,0	99,8	99,8
Key Op = Optional, i.e. no requirement NOTE The use of an alternative ATP is mandatory according to 5.2 and Table 1.										

6.7.6 ATSN availability

The yearly availability of an ATSN shall not be less than the values specified in Table 7 for all ATS of the same category. If an ATSN fails to meet the requirement of Table 7 a fault shall be recorded.

Table 7 — ATSN availability

	SP1	SP2	SP3	SP4	SP5	SP6	DP1	DP2	DP3	DP4
ATSN availability yearly (%)	Op	Op	97,0	99,0	99,5	99,9	Op	99,5	99,9	99,9
Key Op = Optional, i.e. no requirement										

6.8 Security

6.8.1 General security requirements

The ATSP shall describe means to protect the ATS and its components 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 randomised 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.

These security measures apply to all data and management functions of the ATS including remote configuration, software/firmware changes of all ATE.

Cryptography used for alarm applications and transmissions shall be fully documented, be in the public domain and have passed peer review as suitable for this application.

It is accepted that some unit identification data, data encapsulation and any error checking data added subsequent to the core message creation may not be encrypted for transmission, but should be protected from alteration. The requirement of alteration protection applies to the application data only, and doesn't apply to any network or link-related information.

6.8.2 Substitution security

Protection against unauthorised substitution of the SPT with identical or simulation equipment along the ATS shall be provided.

Authentication always requires a sufficient number of keys to provide each connected SPT and RCT with a unique code.

Table 8 — SPT substitution security requirements

	SP1	SP2	SP3	SP4	SP5	SP6	DP1	DP2	DP3	DP4
Substitution protection	Op	Op	Op	M	M	M	Op	Op	M	M
Key M = Mandatory Op = Optional										

6.8.3 Information security

The ATS will be classified according to its ability to meet the information security requirement.

Protection of the information transmitted by the ATS shall be provided by measures to prevent unauthorised reading and to detect unauthorised modification of the information transmitted.

Table 9 — Information security requirements

	SP1	SP2	SP3	SP4	SP5	SP6	DP1	DP2	DP3	DP4
Information security	Op	Op	Op	M	M	M	Op	Op	M	M
Key M = Mandatory Op = Optional										

7 Verification of performance

The verification of performance of an ATS shall be carried out by the ATSP to ensure that the monitoring of all parts of the ATS is effective and that fault signals are generated and successfully transmitted in the event of detected ATS faults.

7.1 General

The performance verification of an ATS shall comprise of a number of aspects as listed below:

a) verification that the basic operation of the system conforms to the requirements of this European Standard and to any related standards; this shall include testing to establish that alarms are transmitted, and that the ATS is monitored;

b) such additional regular or routine verification as required to establish or confirm the availability of the ATS.

NOTE Testing of the supervised premises interface to the AS is described in detail in EN 50136-2.

7.2 ATSN performance

For the purposes of performance verification of an ATSN, all the ATSs of one category shall be considered.

Where ASs form a number of geographically distinct groups and where these groups communicate with separate receivers within the receiving centre or can otherwise be separately identified then each group may be verified as a separate ATSN. Where this division is used the verification shall be carried out separately on each of the identified groups.

The ATSP shall document what criteria is used to group ATSs to build a single ATSN.

Performance verification of the ATSN shall ensure that, for the system configuration and the anticipated number of connected ASs that the ATSN is capable of meeting the requirements of 6.2. This shall be done by practical performance verification of all associated fully commissioned ATSs.

7.3 Transmission time

The correct transmission of alarms shall be verified, including the transmission of alarms associated with ATS monitoring. The time taken to transmit an alarm, e.g. a test alarm, shall be in accordance with Table 2.

The time taken to recognise and transmit a fault signal resulting from a fault of the ATP from the AS at the supervised premises to the AE at the ARC shall be in accordance with Table 3.

7.4 Verification interval

The verification of performance detailed in Table 2 and Table 3 of an ATS shall be carried out either continuously or in the case of the following events:

a) the initial commissioning of the ATS;

b) following any ATS changes (ATE and/or transmission network).

Where the rate of transmission of alarms through the system varies predictably with time or where the use of the ATS by other services using the same equipment varies with time (e.g. systems using a public switched telephone network or a shared PSN) then the distribution of times when performance verification is carried out shall reflect the distribution of times during the day or week that actual messages are expected to occur.

The results of the verification on each ATS and ATSN shall be analysed over successive periods of three months. This does not imply that each ATS and ATSN shall have been activated and tested in every three-month period.

7.5 Availability

7.5.1 Records

Records of all faults and of all performance verification carried out on all ATSs and ATSNs shall be maintained and recorded by the ATSP.

Records shall be maintained of all ATS faults, including those affecting alternative paths or equipment, where these are required in order to comply with the specified availability for the appropriate category.

Records for each ATS fault shall include:

a) the time and date when the fault was identified,

b) the time and date when the solution was implemented and the system restored to normal operation.

Records shall be kept for not less than three years.

Availability records of the ATS and ATSN shall be given to the customer when requested.

7.5.2 Inspection of records

These records shall be open to inspection by a representative from an accredited certification body, or a representative from some other independent organisation (e.g. insurance approvals body). It shall be possible to trace the inclusion of individual system faults in the summarised data required to meet this European Standard, and to trace published performance figures back to individual performance verifications or faults.

7.5.3 Calculations

7.5.3.1 General

The records of all performance verification carried out on an ATS and/or ATSN shall be used to determine the availability of the ATS and the ATSN.

7.5.3.2 ATS availability calculations

For each occasion when a single ATS is unavailable (see 6.7.3) the duration of each single fault shall be determined.

For each seven-day period the availability of the ATS shall be calculated as:

$$WA = \left(1 - \frac{WF}{10\,080}\right) \times 100\,\%$$

where

WA = weekly availability, expressed in percent;

WF = sum of fault times in any seven-day period, expressed in minutes calculated as defined in 6.7.4).

NOTE 10 080 is the number of minutes in a week, 7d × 24h × 60min.

7.5.3.3 ATSN availability calculations

The weighted fault time of the ATSN is calculated as follows:

$$FT = DF \times NA$$

where

FT = weighted fault time, expressed in minutes;

DF = duration of a single fault, expressed in minutes, calculated as described in 6.7.4

NA = the number of affected ASs;

$$YA = \left(1 - \frac{YF}{525\,600 \times NC}\right) \times 100\,\%$$

where

YA = any one-year period availability, expressed in percent;

YF = sum of weighted fault times in any one-year period, expressed in minutes:

$$YF = \sum_{i=1}^{n} FTi$$

NC = the total number of connected ASs;

NOTE 525 600 is the number of minutes in a year, 365d × 24h × 60min.

The sum of fault times shall be for all faults cleared during a one-year period. The number of deployed ATSs shall be that at midnight on the last day of the one-year period. The yearly system availability will be the arithmetic mean of the weekly availabilities for 52 successive weeks.

Where a system is expanded or reduced then the availability of the new system size need not change the rolling seven-day period .

The results and the calculations shall be kept for a period not less than three years.

8 Documentation

The ATSP(s) shall maintain documentation sufficient for planning, installation, commissioning, service and operation of the ATS. ATE Instructions shall be structured to reflect the access levels of the different type of users. Documentation shall include ATS categorization according to Table 1, Table 2, Table 3, Table 4, Table 5, Table 6, Table 7, Table 8 and Table 9, and 6.8.

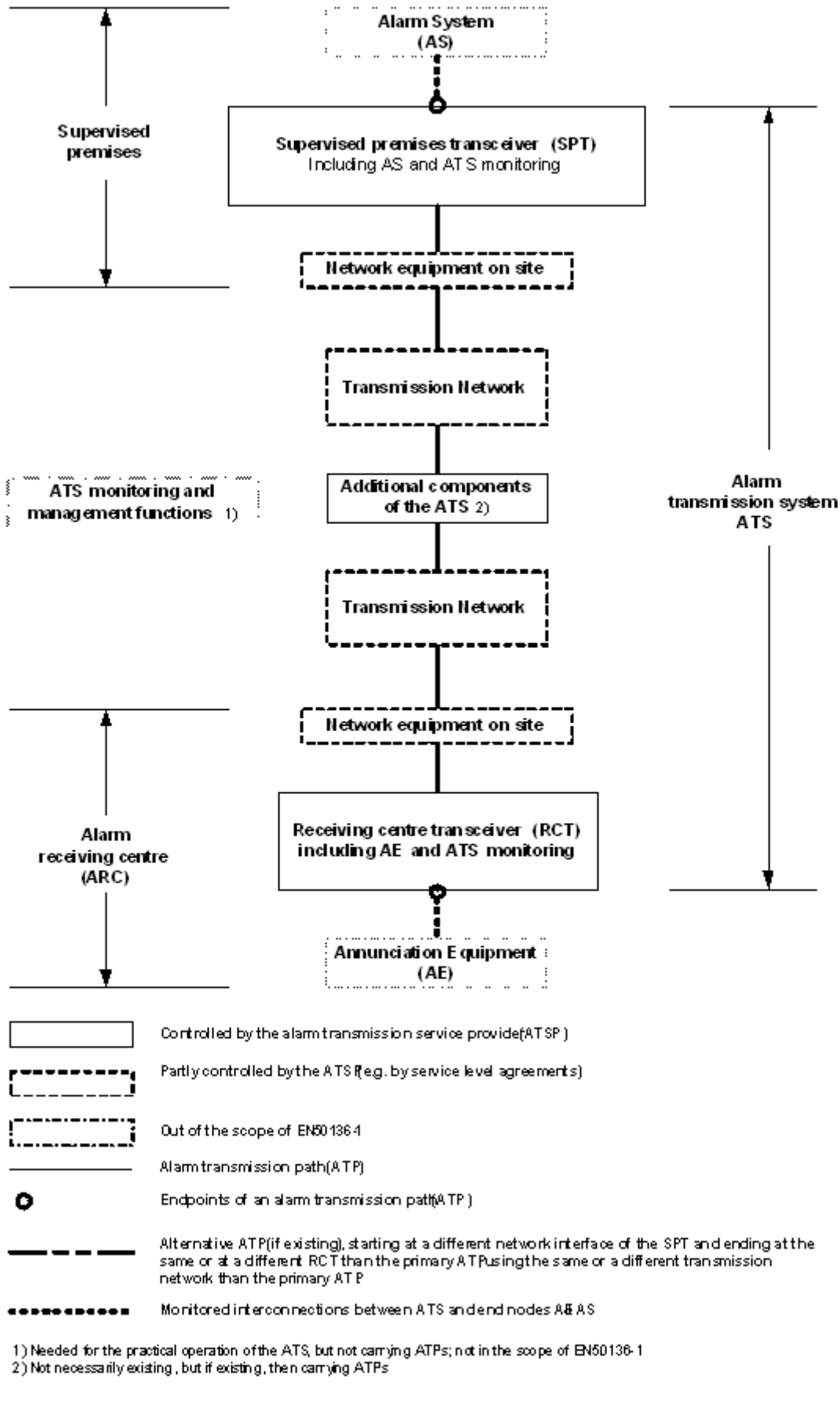


Figure 1 — Logical representation of an ATS

Annex A
(informative)

ATS configurations examples

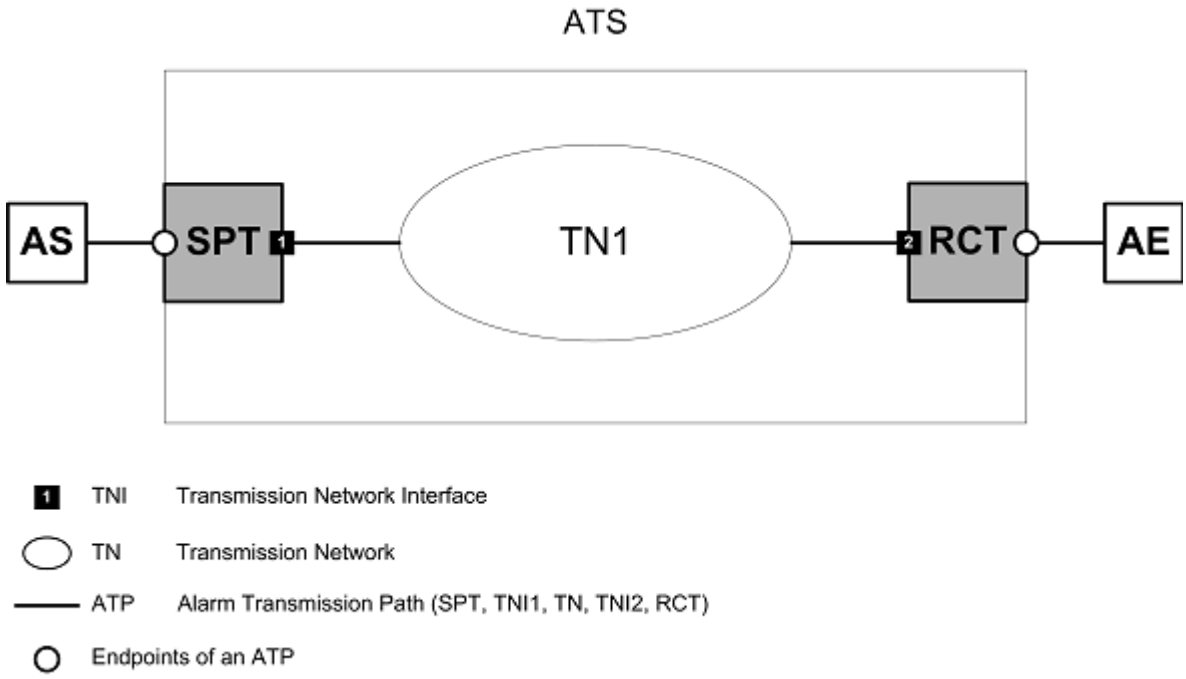


Figure A.1 — Example of a simple single path alarm transmission system

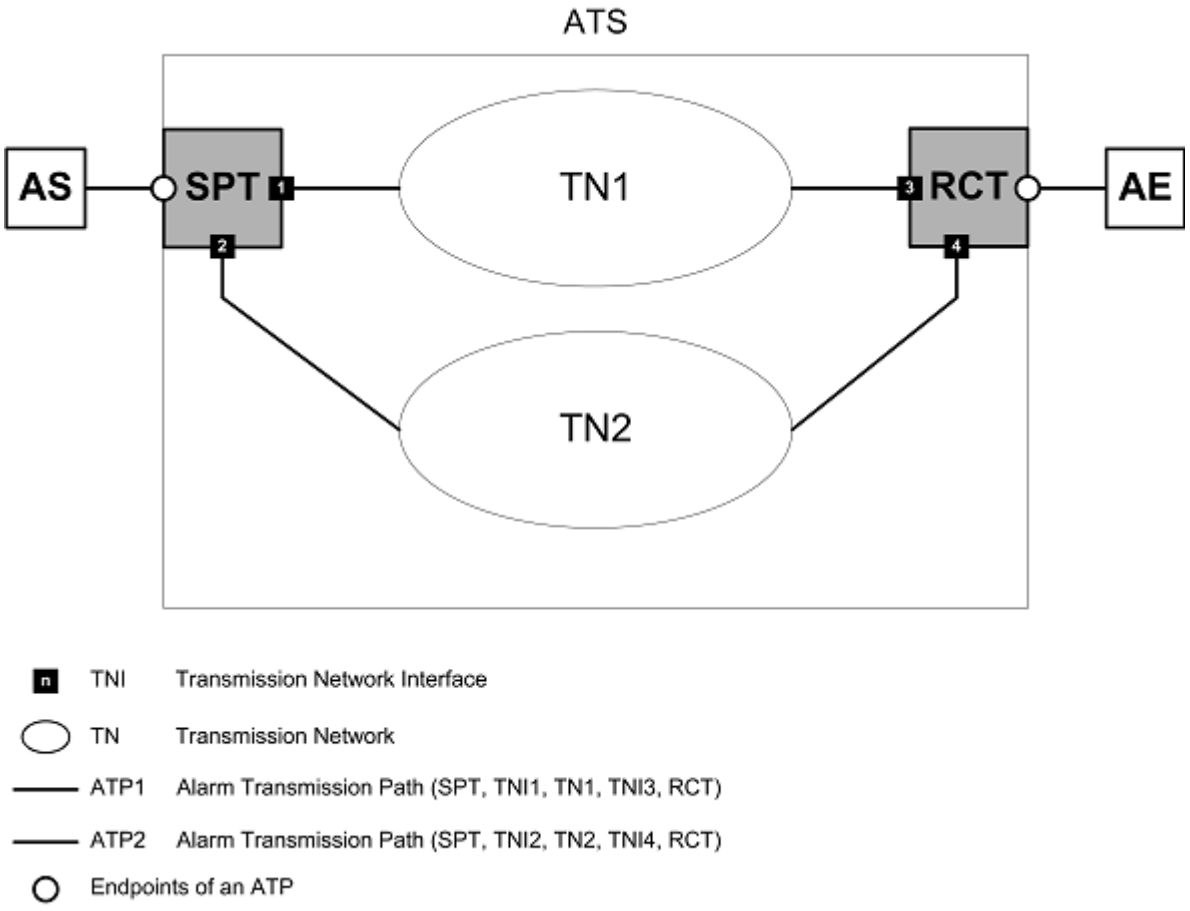
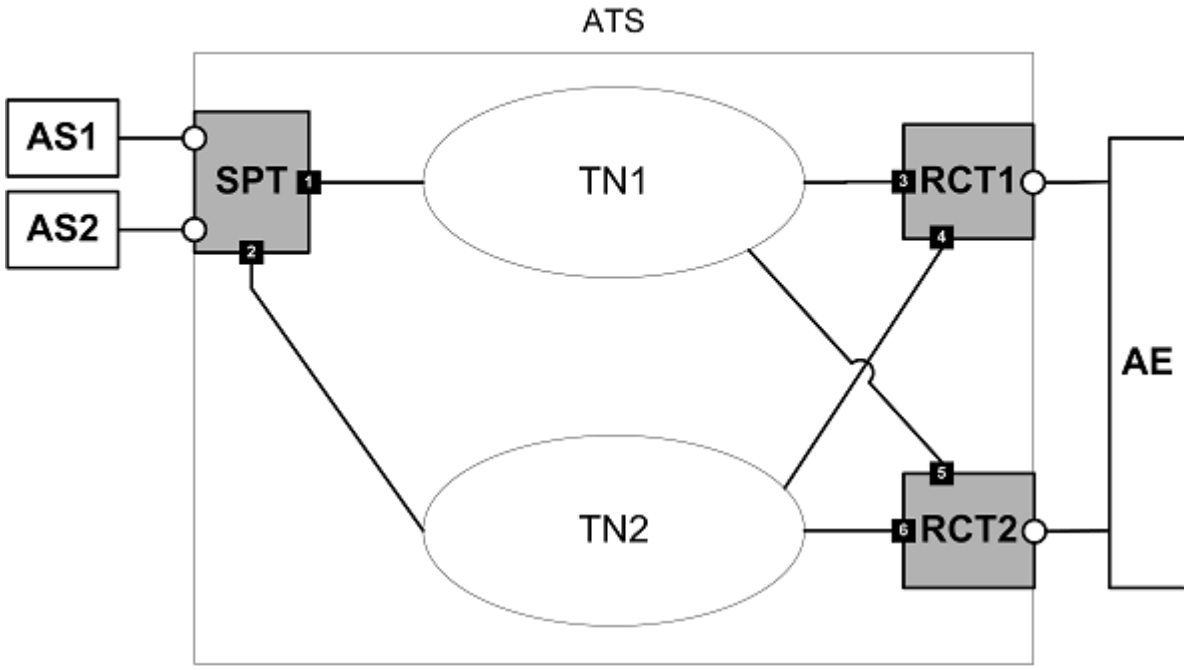


Figure A.2 — Example of a simple dual path alarm transmission system



n TNI Transmission Network Interface

TN Transmission Network

ATP1 Alarm Transmission Path 1 (SPT, TNI1, TN1, TNI3, RCT1 or TNI5, RCT2)

ATP2 Alarm Transmission Path 2 (SPT, TNI2, TN2, TNI4, RCT1 or TNI6, RCT2)

Endpoints of an ATP

Figure A.3 — Example of a dual path alarm transmission system

Annex B
(informative)

Availability examples

An availability figure of 99,8 % comes down to 0,2 % unavailability, this is 20,16 min in seven days (10 080 min).

There is a direct relation between the ATS and the ATSN availability. For example in an ATSN an outage of 20 min in a week affecting 10 % of all ATSs of the same category which results in an ATSN availability of 99,989 %. The ATSN availability requirement is therefore much higher than the single ATS availability requirement.

Any major transmission network outage of 17 h (in a year) affecting all ASs will result in an ATSN availability of 99,8 %.

Annex C
(informative)

Verification of performance

C.1 Introduction

The purpose of this verification is to list requirements that can enable assessment by test house personnel of the performance of ATE when used in conjunction with the corresponding ATS. The requirements are intended to demonstrate that messages from the ATE sent over the ATS can successfully reach the ARC within defined time limits and with an acceptable level of reliability. Requirements are also given for the maximum reporting times in the event of a failure of a transmission link.

Satisfactory performance assessment by test house to the requirements and verification is required prior to approval and listing of the product(s) by a certifying body.

The ATS shall be verified according to its specified category.

C.2 Set up configuration

Equipment number	Description	Manufacturer	Type	Ser. no.	SW ver. / Other info

Block diagram:

Figure C.1

The block diagram describes the set-up for normal operation and monitoring of the ATS.

C.3 System evaluation and functional verification

The numbers in the below tables allocated to each verification are the same as the numbers given in the EN-standards. The requirements, evaluations and results of the evaluations are given in tables below. Passed in the "Result"- column means the interpretation of the EN-standards and the verification result leaves no doubt that the requirement is met. If the requirement is not met or if doubt exists, "Not passed" is stated. "Not relevant" is stated if the requirement is not relevant for the specific ATS tested.

C.4 Functional verification

Clause Numbers (CN) in this European Standard.

Table C.1 — Verification Results Table

CN	Requirement	Comments	Results
5.1	ATS configuration	The set up according configuration in Figure 1. Including ARC under the verification.	
5.3	Applicable network standards	Equipment EN 50136-2.	
6.2	Transmission link requirements		
6.2.2	Transmission links shared with other applications		
6.2.3	Transmission network equipment		
6.2.4	ATSN capacity		
6.2.5	Denial of service		
6.3	Performance		
6.3.2	Transmission time		
6.3.3	Monitoring of interconnections		
7	Verification of performance		
7.1	General		
7.2	ATSN performance		
7.3	Transmission time		
7.4	Verification interval		
7.5.1	Records		
7.5.2	Inspection of records		
7.5.3	Calculations		
8	Documentation		

Annex D
(normative)

Classes for category C

For the purpose of creating custom categorization for applications the following tables shall be used for reference.

Table D.1 — Transmission time classification

Class	Transmission time s				
	D0	D1	D2	D3	D4
Arithmetic mean of all transmissions	-	120	60	20	10
95 % of all transmissions	240	240	80	30	15

Table D.2 — Transmission time, maximum values

Class	Maximum time s				
	M0	M1	M2	M3	M4
Maximum acceptable transmission time	-	480	120	60	20

Table D.3 — Reporting time classification

Class	Reporting time							
	T1	T1a	T2	T3	T3a	T4	T5	T6
Maximum period	32 days	49 h	25 h	5 h	30 min	180 s	90 s	20 s

Table D.4 — Availability classification

Class	Availability					
	A0	A1	A2	A3	A4	A4a
ATSN availability yearly (%)	No req.	97 %	99 %	99,5 %	99,8 %	99,9%
Monthly availability	No req.	75 %	91 %	95 %	98,5 %	99,3%

Table D.5 — Substitution security

Class	Substitution security		
	S0	**S1**	**S2**
Substitution security measures	No measures	Measures to detect substitution of the supervised premises transceiver by methods as described by the manufacturer or ATSP.	Measures to detect substitution of the supervised premises transceiver as described in 6.8.1

Table D.6 — Information security

Class	Information			
	I0	**I1**	**I2**	**I3**
Information security measures	No measures	Measures to prevent unauthorized reading of the information transmitted by methods as described by the manufacturer or ATSP.	Measures to prevent unauthorized modification of the information transmitted by methods as described by the manufacturer or ATSP.	Measures to prevent unauthorized reading and unauthorized modification of the information transmitted as described in 6.8.1

Bibliography

EN 54-21	2006	*Fire detection and fire alarm systems — Part 21: Alarm transmission and fault warning routing equipment*
EN 50131-1	2006	*Alarm systems — Intrusion and hold-up systems — Part 1: System requirements*
EN 50134-1		*Alarm systems — Social alarm systems — Part 1: System requirements*
CLC/TS 50136-7	2004	*Alarm systems — Alarm transmission systems and equipment — Part 7: Application guidelines*
IEC 56/1197		*Guidance on Communication Network Dependability Engineering*

This page deliberately left blank

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email bsmusales@bsigroup.com.

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Copyright

Useful Contacts:

Customer Services
Tel: +44 845 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 845 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

bsi.

...making excellence a habit.™