SLOVENSKI STANDARD

SIST EN 50159-2:2002

prva izdaja

julij 2002

Železniške naprave – Komunikacijski, signalni in procesni sistemi – 2. del: Varnostna komunikacija v odprtih prenosnih sistemih

Railway applications - Communication, signalling and processing systems - Part 2: Safety-related communication in open transmission systems

ICS 35.240.60; 45.020

Referenčna številka
SIST EN 50159-2:2002(en)

EUROPEAN STANDARD **EN 50159-2**

NORME EUROPÉENNE

EUROPÄISCHE NORM March 2001

ICS 35.240.60; 45.020

English version

Railway applications - Communication, signalling and processing systems Part 2: Safety related communication in open transmission systems

Applications ferroviaires -
Systèmes de signalisation, de
télécommunication et de traitement
Partie 2: Communication de sécurité sur
des systèmes de transmission ouverts

Bahnanwendungen -
Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme
Teil 2: Sicherheitsrelevante
Kommunikation in offenen Übertragungssystemen

This European Standard was approved by CENELEC on 2000-01-01. 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 Central Secretariat 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 Central Secretariat has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Czech Republic, Denmark, Finland, France, Germany, Greece, Iceland, Ireland, Italy, Luxembourg, Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and 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

Foreword

This European Standard was prepared by SC 9XA, Communication, signalling and processing systems, of Technical Committee CENELEC TC 9X, Electrical and electronic applications for railways.

The text of the draft was submitted to the formal vote and was approved by CENELEC as EN 50159-2 on 2000-01-01.

The following dates were fixed:

– latest date by which the EN has to be implemented at national level by publication of an identical national standard or by endorsement	(dop)	2001-10-01
– latest date by which the national standards conflicting with the EN have to be withdrawn	(dow)	2003-01-01

Annexes designated “informative” are given for information only.
In this standard, annexes A, B, C and D are informative.

Contents

Introduction

If a safety-related electronic system involves the transfer of information between different locations, the communication system then forms an integral part of the safety-related system and it must be shown that the end to end transmission is safe in accordance with ENV 50129.

The safety requirements for a data communication system depend on its characteristics which can be known or not. In order to reduce the complexity of the approach to demonstrate the safety of the system two classes of transmission systems have been considered. The first class consists of the ones over which the safety system designer has some degree of control. It is the case of the closed transmission systems whose safety requirements are defined in EN 50159-1. The second class, named open transmission system, consists of all the systems whose characteristics are unknown or partly unknown. This standard defines the safety requirements addressed to the transmission through open transmission systems.

The transmission system, which is considered in this standard, has in general no particular preconditions to satisfy. It is from the safety point of view not or not fully trusted and is considered as a ”black box”.

This standard is closely related to EN 50159-1 ”Safety-related communication in closed transmission systems” and ENV 50129 ”Safety related electronic systems for signalling”.

The standard is dedicated to the requirements to be taken into account for the transmission of safety-related information over open transmission systems.

Cross-acceptance, aimed at generic approval and not at specific applications, is required in the same way as for ENV 50129 ”Safety related electronic systems for signalling”.

1 Scope

This European Standard is applicable to safety-related electronic systems using an open transmission system for communication purposes. It gives the basic requirements needed, in order to achieve safety-related transmission between safety-related equipment connected to the open transmission system.

This standard is applicable to the safety requirement specification of the safety-related equipment, connected to the open transmission system, in order to obtain the allocated safety integrity level.

The properties and behaviour of the open transmission system are only used for the definition of the performance, but not for safety. Therefore from the safety point of view the open transmission system can potentially have any property, as various transmission ways, storage of messages, unauthorised access, etc.. The safety process shall only rely on properties, which are demonstrated in the safety case.

The safety requirement specification is a precondition of the safety case of a safety-related electronic system for which the required evidences are defined in ENV 50129. Evidence of safety management and quality management has to be taken from ENV 50129. The communication related requirements for evidence of functional and technical safety are the subject of this standard.

This standard is not applicable to existing systems, which had already been accepted prior to the release of this standard.

This standard does not specify:

- the open transmission system,
- equipment connected to the open transmission system,
- solutions (e.g. for interoperability),
- which kinds of data are safety-related and which are not.

2 Normative references

This European Standard incorporates by dated or undated reference, provisions from other publications. These normative references are cited at appropriate places in the text and the publications are listed hereafter. For dated references, subsequent amendments to or revisions of these publications apply to this European Standard only when incorporated in it by amendment or revision. For undated references the latest edition of the publication referred to applies.

EN 50126	Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)
EN 50128	Railway applications - Communications, signalling and processing systems - Software for railway control and protection systems
ENV 50129	Railway applications - Safety related electronic systems for signalling

3 Definitions

For the purpose of this standard, the following definitions apply:

3.1
access protection
processes designed to prevent *unauthorised* access to read or to alter *information*, either within user *safety-related* systems or within the *transmission system*

3.1.1
hacker
a person trying deliberately to bypass *access protection*

3.2
authenticity
the state in which *information* is *valid* and known to have originated from the stated source

3.3
authorisation
the formal permission to use a product/service within specified application constraints

3.3.1
unauthorised access
a situation in which *user information* or *information* within the *transmission system* is accessed by unauthorised persons or *hackers*

3.3.2
confidentiality
the property that *information* is not made available to unauthorised entities

3.4
check
a process to increase assurance about the state of a system

3.4.1
redundancy check
a type of check that a predefined relationship exists between redundant data and user data within a *message*, to prove message *integrity*

3.5
cryptographic techniques
output data are calculated by an algorithm using input data and a key as a parameter. By knowing the output data, it is impossible within a reasonable time to calculate the input data without knowledge of the key. It is also impossible within a reasonable time to derive the key from the output data, even if the input data are known

3.6
data
a part of a *message* which represents some *information*

3.6.1
data corruption
the alteration of data

3.6.2
user data
data which represents the states or events of a *user process*, without any *additional data*. In case of communication between safety-related equipment, the user data contains safety-related data

3.6.3
additional data
data which is not of any use to the ultimate *user processes*, but is used for control, availability, and safety purposes

3.6.4
redundant data
additional data, derived, by a safety-related transmission process, from the *user data*

3.6.4.1
safety code
redundant data included in a *safety-related message* to permit data corruptions to be detected by the *safety-related* transmission *process*. Suitable encoding techniques may include

3.6.4.1.1
non cryptographic safety code
redundant data based on non cryptographic functions included in a safety-related message to permit data corruptions to be detected by the safety-related transmission process

3.6.4.1.1.1
cyclic redundancy check (CRC)
the CRC is based on cyclic codes, and is used to protect messages from the influence of data corruptions

3.6.4.1.2
cryptographic safety code
redundant data based on cryptographic functions included in a safety-related message to permit data corruptions and unauthorised access to be detected by the safety-related transmission process

3.6.4.1.2.1
message authentication code (MAC)
a *cryptographic* function of the whole message and a secret or public key. By the whole message is meant also any implicit data of the message which is not sent to the transmission system

3.6.4.1.2.2
manipulation detection code (MDC)
a function of the whole message, but in contrast to a *MAC* there is no secret key involved. By the whole message is meant also any implicit data of the message which is not sent to the transmission system. The MDC is often based on a hash function

3.6.4.2
sequence number
an additional data field containing a number that changes in a predefined way from *message* to message

3.6.4.3
time stamp
information attached to a *message* by the sender

3.6.4.3.1
relative time stamp
a time stamp referenced to the local clock of an entity is defined as a relative time stamp. In general there is no relationship to clocks of other entities

3.6.4.3.2
absolute time stamp
a time stamp referenced to a global time which is common for a group of entities using a transmission network is defined as an absolute time stamp

3.6.4.3.3
double time stamp
when two entities exchange and compare their time stamps, this is called double time stamp. In this case the time stamps in the entities are independent of each other

3.6.4.4
source and destination identifier
an identifier is assigned to each entity. This identifier can be a name, number or arbitrary bit pattern. This identifier will be used for the safety-related transmission. Usually the identifier is added to the user data

3.7
defence
a measure incorporated in the design of a safety communication system to counter particular *threats*

3.8
error
a deviation from the intended design which could result in unintended system behaviour or *failure*

3.9
failure
a deviation from the specified performance of a system. A failure is the consequence of an *fault* or *error* in the system

3.9.1
random failure
a *failure* that occurs randomly in time

3.9.2
systematic failure
a *failure* that occurs repeatedly under some particular combination of inputs, or under some particular environmental condition

3.10
fault
an abnormal condition that could lead to an *error* in a system. A fault can be random or systematic

3.10.1

random fault
the occurrence of a fault based on probability theory and previous performance

3.10.2
systematic fault
an inherent fault in the specification, design, construction, installation, operation or maintenance of a system, subsystem or equipment

3.11
hazard
a condition that can lead to an accident

3.11.1
hazard analysis
the process of identifying the hazards which a product or its use can cause

3.12
information
a representation of the state or events of a *process*, in a form understood by the process

3.13
integrity
the state in which *information* is complete and not altered

3.14
message
information, which is transmitted from a sender (data source) to one or more receivers (data sink)

3.14.1
valid message
a message whose form meets in all respects the specified user requirements

3.14.2
message integrity
a message in which *information* is complete and not altered

3.14.3
authentic message
a message in which *information* is known to have originated from the stated source

3.14.4
message stream
an ordered set of messages

3.14.5
message enciphering
transformation of bits by using a *cryptographic technique*_within a message, in accordance with an algorithm controlled by keys, to render casual reading of *data* more difficult. Does not provide protection against data corruption

3.14.6
feedback message
a feedback message is defined as a response from a receiver to the sender, via a return transmission channel

3.14.7
message handling
the *processes*, outside the direct control of the user, which are involved in the transmission of the message stream between participants

3.14.8
message errors
a set of all possible message *failure* modes which can lead to potentially dangerous situations, or to reduction in system availability. There may be a number of causes of each type of *error*

3.14.8.1
repeated message
a type of message error in which a single message is received more than once

3.14.8.2
deleted message
a type of message error in which a message is removed from the message stream

3.14.8.3
inserted message
a type of message error in which an additional message is implanted in the message stream

3.14.8.4
resequenced message
a type of message error in which the order of messages in the message stream is changed

3.14.8.5
corrupted message
a type of message error in which a data corruption occurs

3.14.8.6
delayed message
a type of message error in which a message is received at a time later than intended

3.14.8.7
masqueraded message
a type of inserted message in which a non-authentic message is designed to appear to be authentic

3.15
process

3.15.1
user process
a process within an application that contributes directly to the behaviour specified by the user of the system

3.15.2
transmission process
a process, within an application, that contributes only to the transmission of information between user processes, and not to the user processes themselves

3.15.3
access protection process
a process_within a system that contributes only to the *access protection* of information in the system, and not to the user processes or transmission processes themselves

3.16
safety
freedom from unacceptable levels of risk

3.16.1
safety-related
carries responsibility for safety

3.16.2
safety integrity level
a number which indicates the required degree of confidence that a system will meet its specified safety features

3.16.3
safety case
the documented demonstration that the product complies with the specified safety requirements

3.17
transmission system
a service used by the application to communicate *message streams* between a number of participants, who may be sources or sinks of information

3.17.1
closed transmission system
a fixed number or fixed maximum number of participants linked by a transmission system with well known and fixed properties, and where the risk of *unauthorised* access is considered negligible

3.17.2
open transmission system
a transmission system with an unknown number of participants, having unknown, variable and non-trusted properties, used for unknown telecommunication services, and for which the risk of *unauthorised access* shall be assessed

3.18
threat
a potential violation of *safety* including *access protection* of a communication system

3.19
timeliness
the state in which *information* is available at the right time according to requirements

3.20
validity
the state of meeting in all respects the specified user requirements.

4 Reference architecture

This reference architecture for a safety-related transmission system is based on:

- The non trusted transmission system, whatever internal transmission protection mechanisms are incorporated.
- The safety-related transmission functions.
- The safety-related access protection functions.

For the purposes of this standard, the open transmission system is assumed to consist of everything (hardware, software, transmission media, etc.) occurring between two or more safety-related equipment which are connected to the transmission system.

The open transmission system can contain some or all of the following:

- Elements which read, store, process or re-transmit data produced and presented by users of the transmission system in accordance with a program not known to the user. The number of the users is generally unknown, safety-related and non safety-related equipment and equipment which are not related to railway applications can be connected to the open transmission system.

- Transmission media of any type with transmission characteristics and susceptibility to external influences which are unknown to the user.

- Network control and management systems capable of routing (and dynamically re-routing) messages via any path made up from one or more than one type of transmission media between the ends of open transmission system, in accordance with a program not known to the user.

The open transmission system may be subject to the following:

- Other users of the transmission system, not known to the control and protection system designer, sending unknown amounts of information, in unknown formats.

- User of the transmission system who may attempt to gain access to data originating from other users, in order to read it and/or mimic it without authorisation from the system manager to do so.

- Any kind of additional threats to the integrity of the safety-related data.

A principle structure of the safety-related system using an open transmission system is illustrated in Figure 1. The principle model of a safety-related message is shown in Figure 2.