Railway applications — Communication, signalling and processing systems — Safety-related communication in transmission systems
National foreword

This British Standard is the UK implementation of EN 50159:2010. It supersedes BS EN 50159-1:2001 and BS EN 50159-2:2001 which are withdrawn.

The UK participation in its preparation was entrusted to Technical Committee GEL/9, Railway Electrotechnical Applications.

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.

© BSI 2010

ISBN 978 0 580 67552 2

ICS 35.240.60; 45.020

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 31 October 2010.

Amendments issued since publication

Date Text affected
Railway applications -
Communication, signalling and processing systems -
Safety-related communication in transmission systems

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

Bahnanwendungen -
Telekommunikationstechnik,
Signalttechnik und
Datenverarbeitungssysteme -
Sicherheitsrelevante Kommunikation
in Übertragungssystemen

This European Standard was approved by CENELEC on 2010-09-01. 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, 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 and the United Kingdom.
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. It was submitted to the formal vote and was approved by CENELEC as EN 50159 on 2010-09-01.


The contents of both standards have been merged; the informative Annex E gives a mapping between these previous editions and the present document.

This European Standard is closely related to EN 50129:2003.

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

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) 2011-09-01
- latest date by which the national standards conflicting with the EN have to be withdrawn (dow) 2013-09-01

This draft European Standard has been prepared under a mandate given to CENELEC by the European Commission and the European Free Trade Association and covers essential requirements of EC Directives 96/48/EC (HSR), recast by EC Directives 2008/57/EC (RAIL). See Annex ZZ.
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>5</td>
</tr>
<tr>
<td>1 Scope</td>
<td>6</td>
</tr>
<tr>
<td>2 Normative references</td>
<td>7</td>
</tr>
<tr>
<td>3 Terms, definitions and abbreviations</td>
<td>7</td>
</tr>
<tr>
<td>3.1 Terms and definitions</td>
<td>7</td>
</tr>
<tr>
<td>3.2 Abbreviations</td>
<td>12</td>
</tr>
<tr>
<td>4 Reference architecture</td>
<td>13</td>
</tr>
<tr>
<td>5 Threats to the transmission system</td>
<td>16</td>
</tr>
<tr>
<td>6 Classification of transmission systems</td>
<td>17</td>
</tr>
<tr>
<td>6.1 General</td>
<td>17</td>
</tr>
<tr>
<td>6.2 General aspects of classification</td>
<td>17</td>
</tr>
<tr>
<td>6.3 Criteria for the classification of transmission systems</td>
<td>17</td>
</tr>
<tr>
<td>6.4 Relationship between transmission systems and the threats</td>
<td>18</td>
</tr>
<tr>
<td>7 Requirements for defences</td>
<td>18</td>
</tr>
<tr>
<td>7.1 Preface</td>
<td>18</td>
</tr>
<tr>
<td>7.2 General requirements</td>
<td>19</td>
</tr>
<tr>
<td>7.3 Specific defences</td>
<td>20</td>
</tr>
<tr>
<td>7.4 Applicability of defences</td>
<td>26</td>
</tr>
<tr>
<td>Annex A (informative) Threats on open transmission systems</td>
<td>28</td>
</tr>
<tr>
<td>A.1 System view</td>
<td>28</td>
</tr>
<tr>
<td>A.2 Derivation of the basic message errors</td>
<td>29</td>
</tr>
<tr>
<td>A.3 Threats</td>
<td>30</td>
</tr>
<tr>
<td>A.4 A possible approach for building a safety case</td>
<td>31</td>
</tr>
<tr>
<td>A.5 Conclusions</td>
<td>35</td>
</tr>
<tr>
<td>Annex B (informative) Categories of transmission systems</td>
<td>37</td>
</tr>
<tr>
<td>B.1 Categories of transmission systems</td>
<td>37</td>
</tr>
<tr>
<td>B.2 Relationship between the category of transmission systems and threats</td>
<td>39</td>
</tr>
<tr>
<td>Annex C (informative) Guideline for defences</td>
<td>40</td>
</tr>
<tr>
<td>C.1 Applications of time stamps</td>
<td>40</td>
</tr>
<tr>
<td>C.2 Choice and use of safety codes and cryptographic techniques</td>
<td>41</td>
</tr>
<tr>
<td>C.3 Safety code</td>
<td>46</td>
</tr>
<tr>
<td>C.4 Length of safety code</td>
<td>49</td>
</tr>
<tr>
<td>C.5 Communication between safety-related and non safety-related applications</td>
<td>51</td>
</tr>
<tr>
<td>Annex D (informative) Guidelines for use of the standard</td>
<td>53</td>
</tr>
<tr>
<td>D.1 Procedure</td>
<td>53</td>
</tr>
<tr>
<td>D.2 Example</td>
<td>54</td>
</tr>
<tr>
<td>Annex E (informative) Mapping from previous standards</td>
<td>59</td>
</tr>
<tr>
<td>Annex ZZ (informative) Coverage of Essential Requirements of EC Directives</td>
<td>62</td>
</tr>
<tr>
<td>Bibliography</td>
<td>63</td>
</tr>
</tbody>
</table>
Figures
Figure 1 – Reference architecture for safety-related communication ................................................. 15
Figure 2 – Cyclic transmission of messages ....................................................................................... 21
Figure 3 – Bi-directional transmission of messages ........................................................................... 22
Figure A.1 – Hazard tree ....................................................................................................................... 29
Figure A.2 – Causes of threats ............................................................................................................. 32
Figure C.1 – Classification of the safety-related communication system ............................................. 42
Figure C.2 – Model of message representation within the transmission system (Type A0, A1) ............... 43
Figure C.3 – Use of a separate access protection layer ........................................................................ 44
Figure C.4 – Model of message representation within the transmission system (Type B0) ...................... 45
Figure C.5 – Model of message representation within the transmission system (Type B1) ...................... 46
Figure C.6 – Basic error model ............................................................................................................ 49
Figure C.7 – Communication between non safety-related and safety-related applications ................. 52
Figure D.1 – Fault tree for the hazard “accident” .................................................................................. 55
Figure D.2 – Fault tree for case 1 ......................................................................................................... 56
Figure D.3 – Fault tree for case 2 ......................................................................................................... 58

Tables
Table 1 – Threats/Defences matrix ....................................................................................................... 26
Table A.1 – Relationship between hazardous events and threats ......................................................... 36
Table B.1 – Categories of transmission systems .................................................................................. 38
Table B.2 – Threat/Category relationship ............................................................................................ 39
Table C.1 – Assessment of the safety encoding mechanisms ............................................................... 48
Table E.1 – Mapping from EN 50159-1:2001 into EN 50159:201X ....................................................... 60
Table E.2 – Mapping from EN 50159-2:2001 into EN 50159:201X ....................................................... 61
**Introduction**

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

The transmission system considered in this standard, which serves the transfer of information between different locations, has in general no particular preconditions to satisfy. It is from the safety point of view not trusted, or not fully trusted.

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

Although the RAM aspects are not considered in this standard it is recommended to keep in mind that they are a major aspect of the global safety.

The safety requirements depend on the characteristics of the transmission system. In order to reduce the complexity of the approach to demonstrate the safety of the system, transmission systems have been classified into three categories:

− Category 1 consists of systems which are under the control of the designer and fixed during their lifetime;
− Category 2 consists of systems which are partly unknown or not fixed, however unauthorised access can be excluded;
− Category 3 consists of systems which are not under the control of the designer, and where unauthorised access has to be considered.

The first category was covered by EN 50159-1:2001, the others by EN 50159-2:2001.

When safety-related communication systems, which have been approved according to the previous standards, are subject of maintenance and/or extensions, the informative Annex E can be used for traceability purposes of (sub)clauses of this standard with the (sub)clauses of the former series.
1 Scope

This European Standard is applicable to safety-related electronic systems using for digital communication purposes a transmission system which was not necessarily designed for safety-related applications and which is

- under the control of the designer and fixed during the lifetime, or
- partly unknown or not fixed, however unauthorised access can be excluded, or
- not under the control of the designer, and also unauthorised access has to be considered.

Both safety-related equipment and non safety-related equipment can be connected to the transmission system.

This standard gives the basic requirements needed to achieve safety-related communication between safety-related equipment connected to the transmission system.

This European Standard is applicable to the safety requirement specification of the safety-related equipment connected to the transmission system, in order to obtain the allocated safety integrity requirements.

Safety requirements are generally implemented in the safety-related equipment, designed according to EN 50129. In certain cases these requirements may be implemented in other equipment of the transmission system, as long as there is control by safety measures to meet the allocated safety integrity requirements.

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

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

This European Standard does not specify
- the transmission system,
- equipment connected to the transmission system,
- solutions (e.g. for interoperability),
- which kind of data are safety-related and which are not.

A safety-related equipment connected through an open transmission system can be subjected to many different IT security threats, against which an overall program has to be defined, encompassing management, technical and operational aspects.

In this European Standard however, as far as IT security is concerned, only intentional attacks by means of messages to safety-related applications are considered.

This European Standard does not cover general IT security issues and in particular it does not cover IT security issues concerning

- ensuring confidentiality of safety-related information,
- preventing overloading of the transmission system.