IEC 62280

Edition 1.0 2014-02

INTERNATIONAL STANDARD

NORME INTERNATIONALE

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 dans les systèmes de transmission

iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC 62280:2014
https://standards.iteh.ai/catalog/standards/sist/7d7769c3-7ab4-419e-ab23-3eea410e7b14/iec-62280-2014

IEC 62280:2014-02(EN-FR)

THIS PUBLICATION IS COPYRIGHT PROTECTED
Copyright © 2014 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'IEC ou du Comité national de l'IEC du pays du demandeur. Si vous avez des questions sur le copyright de l'IEC ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de l'IEC de votre pays de résidence.

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
info@iec.ch
www.iec.ch

About the IEC
The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications
The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

IEC Catalogue - webstore.iec.ch/catalogue
The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

IEC publications search - www.iec.ch/searchpub
The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and also once a month by email.

Electropedia - www.electropedia.org
The world's leading online dictionary of electronic and electrical terms containing more than 30 000 terms and definitions in English and French, with equivalent terms in 14 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary
More than 55 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

IEC Customer Service Centre - webstore.iec.ch/csc
If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: csc@iec.ch.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC 62280:2014
https://standards.iteh.ai/catalog/standards/sist/d7709c3-7ab4-419e-ab23-3eea410e7b14/iec-62280-2014

A propos de l'IEC
La Commission Electrotechnique Internationale (IEC) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications IEC
Le contenu technique des publications IEC est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Catalogue IEC - webstore.iec.ch/catalogue
Application autonome pour consulter tous les renseignements bibliographiques sur les Normes internationales, Spécifications techniques, Rapports techniques et autres documents de l'IEC. Disponible pour PC, Mac OS, tablettes Android et iPad.

Recherche de publications IEC - www.iec.ch/searchpub
La recherche avancée permet de trouver des publications IEC en utilisant différents critères (numéro de référence, texte, comité d'études,…). Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

IEC Just Published - webstore.iec.ch/justpublished
Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et aussi une fois par mois par email.

Electropedia - www.electropedia.org
Le premier dictionnaire en ligne de termes électroniques et électriques. Il contient plus de 30 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans 14 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

Glossaire IEC - std.iec.ch/glossary
Plus de 55 000 entrées terminologiques électrotechniques, en anglais et en français, extraites des articles Termes et Définitions des publications IEC parues depuis 2002. Plus certaines entrées antérieures extraites des publications des CE 37, 77, 86 et CISPR de l'IEC.

Service Clients - webstore.iec.ch/csc
Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: csc@iec.ch.

IEC 62280

Edition 1.0 2014-02

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Railway applications – Communication, signalling and processing systems – Safety related communication in transmission systems

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Applications ferroviaires – Systèmes de signalisation, de télécommunication et de traitement – Communication de sécurité dans les systèmes de transmission

IEC 62280:2014
https://standards.iteh.ai/catalog/standards/sist/...
3eea410e7b14/iec-62280-2014

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

PRICE CODE
CODE PRIX XB

ICS 45.060

ISBN 978-2-8322-1383-4

Warning! Make sure that you obtained this publication from an authorized distributor.
Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.

® Registered trademark of the International Electrotechnical Commission
Marque déposée de la Commission Electrotechnique Internationale

CONTENTS

iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC 62280:2014
https://standards.iteh.ai/catalog/standards/sist/7d7709c3-7ab4-419e-ab23-3eea410e7b14/iec-62280-2014

iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC 62280:2014
https://standards.iteh.ai/catalog/standards/sist/7d7709c3-7ab4-419e-ab23-3ee1f0e7014c/iec-62280-2014

iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC 62280:2014
https://standards.iteh.ai/catalog/standards/sist/7d7709c3-7ab4-419e-ab23-3eea410e7b14/iec-62280-2014

INTERNATIONAL ELECTROTECHNICAL COMMISSION

RAILWAY APPLICATIONS – COMMUNICATION, SIGNALLING AND PROCESSING SYSTEMS – SAFETY RELATED COMMUNICATION IN TRANSMISSION SYSTEMS

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.

2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.

3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.

4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.

5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC 62280:2014
https://standards.iteh.ai/catalog/standards/sist/7d7709e3-7a64-419e-ab23-3eea410e7b14/iec-62280-2014

6) All users should ensure that they have the latest edition of this publication.

7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.

8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.

9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 62280 has been prepared by IEC technical committee 9: Electrical equipment and systems for railways.

This standard is based on EN 50159.

This standard cancels and replaces IEC 62280-1 (2002) and IEC 62280-2 (2002). See Annex E.

The text of this standard is based on the following documents:

FDIS	Report on voting
9/1866A/FDIS	9/1885/RVD

Full information on the voting for the approval of this standard can be found in the report on voting indicated in the above table.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the IEC web site under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC 62280:2014
https://standards.iteh.ai/catalog/standards/sist/7d7709c3-7ab4-419e-ab23-3eea410e7b14/iec-62280-2014

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, this includes that the end to end communication is safe in accordance with IEC 62425.

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

The first category was previously covered by IEC 62280-1:2002, the others by IEC 62280-2:2002.

IEC 62280:2014
https://standards.iteh.ai/catalog/standards/sist/7d7709c3-7ab4-419e-ab23-3eea410e7b14/iec-62280-2014

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

RAILWAY APPLICATIONS – COMMUNICATION, SIGNALLING AND PROCESSING SYSTEMS – SAFETY RELATED COMMUNICATION IN TRANSMISSION SYSTEMS

1 Scope

This International 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 Internaitonal Standard gives the basic requirements needed to achieve safety related communication between safety related equipment connected to the transmission system.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

This International 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.

IEC 62280:2014
https://standards.iteh.ai/catalog/standards/sist/7d770f63-7ab4-4195-ab23-3eca410e7b14/iec-62280-2014

Safety requirements are generally implemented in the safety related equipment, designed according to IEC 62425. 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 IEC 62425. Evidence of safety management and quality management has to be taken from IEC 62425. The communication related requirements for evidence of functional and technical safety are the subject of this standard.

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

This International 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 International Standard however, as far as IT security is concerned, only intentional attacks by means of messages to safety related applications are considered.

This International 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.

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.

IEC 62278 (all parts), *Railway applications – Specification and demonstration of reliability, availability, maintainability and safety (RAMS)*

IEC 62425:2007, *Railway applications – Communication, signalling and processing systems – Safety related electronic systems for signalling*

3 Terms, definitions and abbreviations

3.1 Terms and definitions

iTeh STANDARD PREVIEW

For the purposes of this document, the following terms and definitions apply.

(standards.iteh.ai)

3.1.1
absolute time stamp
time stamp referenced to a global time which is common for a group of entities using a transmission system

IEC 62280:2014
https://standards.iteh.ai/catalog/standards/sist/7d7709c3-7ab4-419e-ab23-3eea410e7b14/iec-62280-2014

3.1.2
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

3.1.3
additional data
data which is not of any use to the ultimate user processes, but is used for control, availability, and safety purposes

3.1.4
authentic message
message in which information is known to have originated from the stated source

3.1.5
authenticity
state in which information is valid and known to have originated from the stated source

3.1.6
closed transmission system
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

3.1.7
communication
transfer of information between applications

3.1.8
confidentiality
property that information is not made available to unauthorised entities

3.1.9
corrupted message
type of message error in which a data corruption occurs

3.1.10
cryptographic techniques
producing output data, calculated by an algorithm using input data and a key as a parameter

Note 1 to entry: 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.

3.1.11
cyclic redundancy check
cyclic code, used to protect messages from the influence of data corruption

3.1.12
data
part of a message which represents some information

Note 1 to entry: See also definitions 3.1.64: user data, 3.1.3: additional data and 3.1.42: redundant data.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

3.1.13
data corruption
alteration of data

IEC 62280:2014
https://standards.iteh.ai/catalog/standards/sist/7d7709c3-7ab4-419e-ab23-3eea410e7b14/iec-62280-2014

3.1.14
defence
measure incorporated in the design of a safety related communication system to counter particular threats

3.1.15
delayed message
type of message error in which a message is received at a time later than intended

3.1.16
deleted message
type of message error in which a message is removed from the message stream

3.1.17
double time stamp
case when two entities exchange and compare their time stamps. In this case the time stamps in the entities are independent of each other

3.1.18
error
deviation from the intended design which could result in unintended system behaviour or failure

3.1.19
failure
deviation from the specified performance of a system

Note 1 to entry: A failure is the consequence of a fault or an error in the system.

3.1.20
fault
abnormal condition that could lead to an error in a system

Note 1 to entry: A fault can be random or systematic.

3.1.21
feedback message
response from a receiver to the sender, via a return channel

3.1.22
hacker
person trying deliberately to bypass access protection

3.1.23
hazard
condition that can lead to an accident

3.1.24
hazard analysis
process of identifying hazards and analysing their causes, and the derivation of requirements to limit the likelihood and consequences of hazards to an acceptable level

3.1.25
implicit data
additional data that is not transmitted but is known to the sender and receiver

iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC 62280:2014
https://standards.iteh.ai/catalog/standards/sist/7d7700c3-7ab4-419e-ab23-3eea410e7b14/iec-62280-2014

3.1.26
information
representation of the state or events of a process, in a form understood by the process

3.1.27
inserted message
type of message error in which an additional message is implanted in the message stream

3.1.28
integrity
state in which information is complete and not altered

3.1.29
manipulation detection code
function of the whole message without secret key

Note 1 to entry: 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. MDC is often based on a hash function.

3.1.30
masqueraded message
type of inserted message in which a non-authentic message is designed to appear to be authentic

3.1.31
message
information which is transmitted from a sender (data source) to one or more receivers (data sink)

3.1.32
message authentication code
cryptographic function of the whole message and a secret or public key

Note 1 to entry: By the whole message is meant also any implicit data of the message which is not sent to the transmission system.

3.1.33
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

3.1.34
message errors
set of all possible message failure modes which can lead to potentially dangerous situations, or to reduction in system availability. There can be a number of causes of each type of error

3.1.35
message integrity
message in which information is complete and not altered

3.1.36
message stream
ordered set of messages

iTeh STANDARD PREVIEW
(standards.iteh.ai)

3.1.37
non-cryptographic safety code
redundant data based on non-cryptographic functions included in a safety related message to permit data corruption to be detected by the safety related transmission function

IEC 62280:2014
https://standards.iteh.ai/catalog/standards/sist/7d7709c3-7ab4-419e-ab23-3eea410e7b14/iec-62280-2014

3.1.38
open transmission system
transmission system with an unknown number of participants, having unknown, variable and non-trusted properties, used for unknown telecommunication services and having the potential for unauthorised access

3.1.39
public network
network with unknown users, especially not under control of the railways

3.1.40
random failure
failure that occurs randomly in time

3.1.41
redundancy check
type of check that a predefined relationship exists between redundant data and user data within a message, to prove message integrity

3.1.42
redundant data
additional data, derived, by a safety related transmission function, from the user data

3.1.43
relative time stamp
time stamp referenced to the local clock of an entity. In general there is no relationship to clocks of other entities

3.1.44
repeated message
type of message error in which a single message is received more than once

3.1.45
re-sequenced message
type of message error in which the order of messages in the message stream is changed

3.1.46
safe fall back state
safe state of a safety related equipment or system as a deviation from the fault-free state and as a result of a safety reaction leading to a reduced functionality of safety related functions, possibly also of non-safety related functions

3.1.47
safety
freedom from unacceptable levels of risk

3.1.48
safety case
documented demonstration that the product (e.g. system/sub-system/equipment) complies with the specified safety requirements

3.1.49
safety code
redundant data included in a safety related message to permit data corruptions to be detected by the safety related transmission function

iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC 62280:2014
https://standards.iteh.ai/catalog/standards/sist/7d7709c3-7ab4-419e-ab23-3eea410e7b14/iec-62280-2014

3.1.50
safety integrity level
number which indicates the required degree of confidence that a system will meet its specified safety functions with respect to systematic failures

3.1.51
safety reaction
safety related protection taken by the safety process in response to an event (such as a failure of the transmission system), which may lead to a safe fall back state of the equipment

3.1.52
safety related
carries responsibility for safety

3.1.53
safety related transmission function
function incorporated in the safety related equipment to ensure authenticity, integrity, timeliness and sequence of data

3.1.54
sequence number
additional data field containing a number that changes in a predefined way from message to message

3.1.55
source and destination identifier
identifier which 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 communication. Usually the identifier is added to the user data