

**NORME
INTERNATIONALE
INTERNATIONAL
STANDARD**

**CEI
IEC**

62280-2

Première édition
First edition
2002-10

**Applications ferroviaires –
Systèmes de signalisation, de télécommunication
et de traitement –**

**Partie 2:
Communication de sécurité sur des systèmes
de transmission ouverts**

**Railway applications –
Communication, signalling and processing
systems –**

**Part 2:
Safety-related communication
in open transmission systems**



Numéro de référence
Reference number
CEI/IEC 62280-2:2002

Numérotation des publications

Depuis le 1er janvier 1997, les publications de la CEI sont numérotées à partir de 60000. Ainsi, la CEI 34-1 devient la CEI 60034-1.

Editions consolidées

Les versions consolidées de certaines publications de la CEI incorporant les amendements sont disponibles. Par exemple, les numéros d'édition 1.0, 1.1 et 1.2 indiquent respectivement la publication de base, la publication de base incorporant l'amendement 1, et la publication de base incorporant les amendements 1 et 2.

Informations supplémentaires sur les publications de la CEI

Le contenu technique des publications de la CEI est constamment revu par la CEI afin qu'il reflète l'état actuel de la technique. Des renseignements relatifs à cette publication, y compris sa validité, sont disponibles dans le Catalogue des publications de la CEI (voir ci-dessous) en plus des nouvelles éditions, amendements et corrigenda. Des informations sur les sujets à l'étude et l'avancement des travaux entrepris par le comité d'études qui a élaboré cette publication, ainsi que la liste des publications parues, sont également disponibles par l'intermédiaire de:

- Site web de la CEI (www.iec.ch)
- Catalogue des publications de la CEI

Le catalogue en ligne sur le site web de la CEI (http://www.iec.ch/searchpub/cur_fut.htm) vous permet de faire des recherches en utilisant de nombreux critères, comprenant des recherches textuelles, par comité d'études ou date de publication. Des informations en ligne sont également disponibles sur les nouvelles publications, les publications remplacées ou retirées, ainsi que sur les corrigenda.

- IEC Just Published

Ce résumé des dernières publications parues (http://www.iec.ch/online_news/justpub/jp_entry.htm) est aussi disponible par courrier électronique. Veuillez prendre contact avec le Service client (voir ci-dessous) pour plus d'informations.

- Service clients

Si vous avez des questions au sujet de cette publication ou avez besoin de renseignements supplémentaires, prenez contact avec le Service clients:

Email: custserv@iec.ch
Tél: +41 22 919 02 11
Fax: +41 22 919 03 00

Publication numbering

As from 1 January 1997 all IEC publications are issued with a designation in the 60000 series. For example, IEC 34-1 is now referred to as IEC 60034-1.

Consolidated editions

The IEC is now publishing consolidated versions of its publications. For example, edition numbers 1.0, 1.1 and 1.2 refer, respectively, to the base publication, the base publication incorporating amendment 1 and the base publication incorporating amendments 1 and 2.

Further information on IEC publications

The technical content of IEC publications is kept under constant review by the IEC, thus ensuring that the content reflects current technology. Information relating to this publication, including its validity, is available in the IEC Catalogue of publications (see below) in addition to new editions, amendments and corrigenda. Information on the subjects under consideration and work in progress undertaken by the technical committee which has prepared this publication, as well as the list of publications issued, is also available from the following:

- IEC Web Site (www.iec.ch)
- Catalogue of IEC publications

The on-line catalogue on the IEC web site (http://www.iec.ch/searchpub/cur_fut.htm) enables you to search by a variety of criteria including text searches, technical committees and date of publication. On-line information is also available on recently issued publications, withdrawn and replaced publications, as well as corrigenda.

- IEC Just Published

This summary of recently issued publications (http://www.iec.ch/online_news/justpub/jp_entry.htm) is also available by email. Please contact the Customer Service Centre (see below) for further information.

- Customer Service Centre

If you have any questions regarding this publication or need further assistance, please contact the Customer Service Centre:

Email: custserv@iec.ch
Tel: +41 22 919 02 11
Fax: +41 22 919 03 00

**NORME
INTERNATIONALE
INTERNATIONAL
STANDARD**

**CEI
IEC**

62280-2

Première édition
First edition
2002-10

**Applications ferroviaires –
Systèmes de signalisation, de télécommunication
et de traitement –**

**Partie 2:
Communication de sécurité sur des systèmes
de transmission ouverts**

**Railway applications –
Communication, signalling and processing
systems –**

**Part 2:
Safety-related communication
in open transmission systems**

© IEC 2002 Droits de reproduction réservés — Copyright - all rights reserved

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'éditeur.

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 the publisher.

International Electrotechnical Commission, 3, rue de Varembé, PO Box 131, CH-1211 Geneva 20, Switzerland
Telephone: +41 22 919 02 11 Telefax: +41 22 919 03 00 E-mail: inmail@iec.ch Web: www.iec.ch



Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

CODE PRIX
PRICE CODE

X

Pour prix, voir catalogue en vigueur
For price, see current catalogue

SOMMAIRE

AVANT-PROPOS	4
INTRODUCTION	8
1 Domaine d'application	10
2 Références normatives	10
3 Définitions.....	12
4 Architecture de référence	24
5 Menaces sur le système de transmission.....	28
6 Exigences en matière de défense.....	28
6.1 Introduction.....	28
6.2 Exigences générales	30
6.3 Défenses spécifiques	32
7 Applicabilité des défenses contre les menaces	42
7.1 Introduction.....	42
7.2 Matrice menaces/défenses.....	42
7.3 Choix et utilisation du code de sécurité et des techniques cryptographiques	42
Annexe A (informative) Guide pour les défenses.....	44
A.1 Applications de la datation.....	44
A.2 Choix et utilisation des codes de sécurité et des techniques cryptographiques	46
Annexe B (informative) Bibliographie	62
Annexe C (informative) Guide pour l'utilisation de la norme.....	64
C.1 Domaine d'application/objet.....	64
C.2 Classification des systèmes de transmission.....	64
C.3 Procédure	68
C.4 Exemple.....	70
Annexe D (informative) Menaces sur les systèmes de transmission ouverts	80
D.1 Vue système	80
D.2 Dédution des messages d'erreur de base	82
D.3 Menaces	84
D.4 Une approche possible pour élaborer le dossier de sécurité.....	88
D.5 Conclusions	94

CONTENTS

FOREWORD	5
INTRODUCTION	9
1 Scope	11
2 Normative references	11
3 Definitions	13
4 Reference architecture	25
5 Threats to the transmission system	29
6 Requirements for defences	29
6.1 Introduction	29
6.2 General requirements	31
6.3 Specific defences	33
7 Applicability of defences against threats	43
7.1 Introduction	43
7.2 Threats/defences matrix	43
7.3 Choice and use of safety code and cryptographic techniques	43
Annex A (informative) Guideline for defences	45
A.1 Applications of time stamps	45
A.2 Choice and use of safety codes and cryptographic techniques	47
Annex B (informative) Bibliography	63
Annex C (informative) Guidelines for use of the standard	65
C.1 Scope/purpose	65
C.2 Classification of transmission systems	65
C.3 Procedure	69
C.4 Example	71
Annex D (informative) Threats on open transmission systems	81
D.1 View system	39
D.2 Derivation of the basic message errors	83
D.3 Threats	85
D.4 A possible approach for building a safety case	89
D.5 Conclusions	95

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

APPLICATIONS FERROVIAIRES – SYSTÈMES DE SIGNALISATION, DE TÉLÉCOMMUNICATION ET DE TRAITEMENT –

Partie 2: Communication de sécurité sur des systèmes de transmission ouverts

AVANT-PROPOS

- 1) La CEI (Commission Électrotechnique Internationale) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de la CEI). La CEI a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, la CEI, entre autres activités, publie des Normes internationales. Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec la CEI, participent également aux travaux. La CEI collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
- 2) Les décisions ou accords officiels de la CEI concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux intéressés sont représentés dans chaque comité d'études.
- 3) Les documents produits se présentent sous la forme de recommandations internationales. Ils sont publiés comme normes, spécifications techniques, rapports techniques ou guides et agréés comme tels par les Comités nationaux.
- 4) Dans le but d'encourager l'unification internationale, les Comités nationaux de la CEI s'engagent à appliquer de façon transparente, dans toute la mesure possible, les Normes internationales de la CEI dans leurs normes nationales et régionales. Toute divergence entre la norme de la CEI et la norme nationale ou régionale correspondante doit être indiquée en termes clairs dans cette dernière.
- 5) La CEI n'a fixé aucune procédure concernant le marquage comme indication d'approbation et sa responsabilité n'est pas engagée quand un matériel est déclaré conforme à l'une de ses normes.
- 6) L'attention est attirée sur le fait que certains des éléments de la présente Norme internationale peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. La CEI ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et de ne pas avoir signalé leur existence.

La Norme internationale CEI 62280-2 a été établie par le comité d'études 9 de la CEI: Matériel et systèmes électriques ferroviaires.

La présente norme, basée sur la norme européenne EN 50159-2 (2001), a été préparée par le sous-comité 9XA: Systèmes de signalisation de télécommunications et de traitement, du Comité Technique 9X du CENELEC: Applications électriques et électroniques dans le domaine ferroviaire. Elle a été soumise aux Comités Nationaux pour vote suivant la procédure par voie express, par les documents suivants:

FDIS	Rapport de vote
9/697/FDIS	9/708/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à l'approbation de cette norme.

Cette norme est étroitement liée à la CEI 62280-1¹ et à la norme ENV 50129:1998.

¹ A publier.

INTERNATIONAL ELECTROTECHNICAL COMMISSION

**RAILWAY APPLICATIONS –
COMMUNICATION, SIGNALLING AND PROCESSING SYSTEMS –****Part 2: Safety-related communication in open transmission systems**

FOREWORD

- 1) The IEC (International Electrotechnical Commission) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of the 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, the IEC publishes International Standards. 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. The 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 the 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 National Committees.
- 3) The documents produced have the form of recommendations for international use and are published in the form of standards, technical specifications, technical reports or guides and they are accepted by the National Committees in that sense.
- 4) In order to promote international unification, IEC National Committees undertake to apply IEC International Standards transparently to the maximum extent possible in their national and regional standards. Any divergence between the IEC Standard and the corresponding national or regional standard shall be clearly indicated in the latter.
- 5) The IEC provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with one of its standards.
- 6) Attention is drawn to the possibility that some of the elements of this International Standard may be the subject of patent rights. The IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 62280-2 has been prepared by IEC technical committee 9: Electrical equipment and systems for railways.

This standard based on the European Norm EN 50159-2 (2001) has been prepared by subcommittee 9XA: Communication, signalling and processing systems of CENELEC Technical Committee 9X: Electrical and electronic applications for railways. It was submitted to the National Committees for voting under the Fast Track Procedure as the following documents:

FDIS	Report on voting
9/697/FDIS	9/708/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 standard is in closely related to IEC 62280-1¹ and ENV 50129:1998.

¹ To be published.

La présente norme ne suit pas les règles de structure des normes internationales comme le spécifie la Partie 2 des Directives ISO/CEI.

NOTE Cette norme a été reproduite sans modifications importantes de son contenu original ou de ses règles structurelles.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant 2008. A cette date, la publication sera

- reconduite;
- supprimée;
- remplacée par une édition révisée, ou
- amendée.

La CEI 62280 comprend les parties suivantes, présentées sous le titre général *Applications ferroviaires – Systèmes de signalisation, de télécommunication et de traitement*

- Partie 1: Communication de sécurité sur des systèmes de transmission fermés
- Partie 2: Communication de sécurité sur des systèmes de transmission ouverts.

iTeh Standards
(<https://standards.itih.ai>)
Document Preview

IEC 62280-2:2002

<https://standards.itih.ai/standards/iec/2bfe9f1-a4ff-42bf-9354-8416dc1dce73/iec-62280-2-2002>

This standard does not follow the rules for structuring International Standards as given in Part 2 of the ISO/IEC Directives.

NOTE This standard has been reproduced without significant modification to its original content or drafting.

The committee has decided that the contents of this publication will remain unchanged until 2008. At this date, the publication will be

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

IEC 62280 consists of the following parts, under the general title *Railway applications – Communication, signalling and processing systems*

- Part 1: Safety-related communication in closed transmission systems
- Part 2: Safety-related communication in open transmission systems.

iTeh Standards
(<https://standards.itih.ai>)
Document Preview

IEC 62280-2:2002

<https://standards.itih.ai/standards/iec/2bfe9f1-a4ff-42bf-9354-8416dc1dce73/iec-62280-2-2002>

INTRODUCTION

Si le système électronique de sécurité implique un transfert d'information entre des emplacements différents, alors le système de communication constitue une partie intégrante du système de sécurité et il est montré que la transmission de bout en bout est de sécurité conformément à l'ENV 50129.

Les exigences de sécurité pour un système de transmission de données dépendent des caractéristiques de ce dernier, lesquelles peuvent être connues ou non. Afin de réduire la complexité de l'approche de la démonstration de la sécurité du système, deux classes de systèmes de transmission ont été considérés. La première classe est celle sur laquelle le concepteur du système de sécurité a un certain contrôle. C'est le cas des systèmes de transmission fermés dont les exigences de sécurité sont définies dans la CEI 62280-1. La seconde classe, appelée système de transmission ouvert, est constituée par tous les systèmes dont les caractéristiques sont inconnues ou partiellement inconnues. Cette présente partie de la CEI 62280 définit les exigences de sécurité destinées à la transmission via des réseaux de transmission ouverts.

Dans cette norme, le système de transmission considéré n'a pas, en général, à satisfaire de conditions préliminaires particulières. Du point de vue de la sécurité, il n'est pas ou pas complètement sûr et est considéré comme une «boîte noire».

Cette norme est dédiée aux exigences à considérer pour la transmission des informations de sécurité via des réseaux de transmission ouverts.

La *cross-acceptance*, visant une approbation générique et non des applications spécifiques, est requise de la même manière que pour l'ENV 50129.

IEC 62280-2:2002

<https://standards.iteh.ai/en/standards/iec/2bfe9f1-a4ff-42bf-9354-8416dc1dce73/iec-62280-2-2002>

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 IEC 62280-1. The second class, named open transmission system, consists of all the systems whose characteristics are unknown or partly unknown. This part of IEC 62280 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".

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 .

iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

IEC 62280-2:2002

<https://standards.iteh.ai/catalog/standards/iec/2bfe9f1-a4ff-42bf-9354-8416dc1dce73/iec-62280-2-2002>

APPLICATIONS FERROVIAIRES – SYSTÈMES DE SIGNALISATION, DE TÉLÉCOMMUNICATION ET DE TRAITEMENT –

Partie 2: Communication de sécurité sur des systèmes de transmission ouverts

1 Domaine d'application

La présente partie de la CEI 62280 est applicable aux systèmes électroniques de sécurité s'appuyant sur un système de transmission ouvert à des fins de communication. Elle indique les exigences de base requises pour obtenir une transmission de sécurité entre équipements de sécurité raccordés au système de transmission ouvert.

Cette norme s'applique à la spécification des exigences de sécurité de l'équipement de sécurité raccordé au système de transmission ouvert, afin d'atteindre le niveau d'intégrité de sécurité alloué.

Les propriétés et le comportement du système de transmission ouvert n'interviennent que pour la définition des performances, mais pas pour la sécurité. Aussi, du point de vue de la sécurité, le système de transmission ouvert peut potentiellement présenter n'importe quelle propriété, telle que différents chemins de transmission, stockage de messages, accès non autorisés, etc. Le processus de sécurité ne doit s'appuyer que sur des propriétés dont la démonstration est faite dans la preuve de sécurité.

La spécification des exigences de sécurité est une condition préalable de la preuve de sécurité d'un système électronique de sécurité dont les caractéristiques sont définies dans l'ENV 50129. Les caractéristiques du management de la sécurité et du management de la qualité sont celles de l'ENV 50129. Les exigences liées à la communication pour faire la preuve de la sécurité fonctionnelle et technique est du ressort de cette norme.

Cette norme n'est pas applicable aux systèmes existants qui ont déjà été acceptés antérieurement à la mise en circulation de cette norme.

Cette norme ne spécifie pas

- le système de transmission ouvert,
- les équipements raccordés au système de transmission ouvert,
- des solutions (par exemple pour l'interopérabilité),
- quels types de données sont de sécurité et quels types de données ne le sont pas.

2 Références normatives

Les documents de référence suivants sont indispensables pour l'application du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

CEI 62278, *Applications ferroviaires – Spécification et démonstration de la fiabilité, de la disponibilité, de la maintenabilité et de la sécurité (FDMS)* ²

ENV 50129:1998, *Applications ferroviaires – Systèmes électroniques de sécurité pour la signalisation*

² A publier.

RAILWAY APPLICATIONS – COMMUNICATION, SIGNALLING AND PROCESSING SYSTEMS –

Part 2: Safety-related communication in open transmission systems

1 Scope

This part of IEC 62280 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, unauthorized 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

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 62278, *Railway applications – The specification and demonstration of reliability, availability, maintainability and safety (RAMS)* ²

ENV 50129:1998, *Railway applications – Safety-related electronic systems for signalling*

² To be published.

3 Définitions

Pour les besoins de la présente partie de la CEI 62280, les définitions suivantes s'appliquent.

3.1

protection d'accès

processus conçus pour empêcher un *accès non autorisé* de lire ou de modifier de l'*information*, soit dans les *systèmes de sécurité*, soit dans le *système de transmission*

3.1.1

hacker

personne essayant de shunter délibérément une *protection d'accès*

3.2

authenticité

état dans lequel une *information* est *reconnue comme valide* et originaire d'une source déclarée

3.3

autorisation

droit formel d'utiliser un produit/service à l'intérieur de contraintes d'application spécifiées

3.3.1

accès non autorisé

situation dans laquelle des personnes non autorisées ou des *hackers* ont accès à de l'*information utilisateur* ou à de l'*information dans le système de transmission*

3.3.2

confidentialité

propriété de non-mise à disposition de l'*information* à des entités non autorisées

3.4

contrôle

processus destiné à accroître l'assurance de l'état d'un système

3.4.1

contrôle de redondance

type de contrôle de l'existence d'une relation prédéfinie entre la redondance et les données utilisateur au sein d'un *message*, pour prouver l'*intégrité* du message

3.5

techniques cryptographiques

les données de sortie sont calculées au moyen d'un algorithme utilisant les données d'entrée et une clé comme paramètre. Connaissant les données de sortie, il est impossible de calculer les données d'entrée dans un délai raisonnable sans connaître la clé. Il est également impossible de déduire la clé des données de sorties dans un délai raisonnable, même si les données d'entrée sont connues

3.6

données

partie d'un *message* qui représente de l'*information*

3.6.1

corruption de données

altération de données