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

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

PRICE CODE
CODE PRIX XB

ICS 45.060

ISBN 978-2-8322-1383-4

CONTENTS

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.
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.

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.

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

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.

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.

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*

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

APPLICATIONS FERROVIAIRES – SYSTÈMES DE SIGNALISATION, DE TÉLÉCOMMUNICATION ET DE TRAITEMENT – COMMUNICATION DE SÉCURITÉ DANS LES SYSTÈMES DE TRANSMISSION

AVANT-PROPOS

1) La Commission Electrotechnique Internationale (CEI) 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, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de la CEI"). 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 de la CEI intéressés sont représentés dans chaque comité d'études.
3) Les Publications de la CEI se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de la CEI. Tous les efforts raisonnables sont entrepris afin que la CEI s'assure de l'exactitude du contenu technique de ses publications; la CEI ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de la CEI s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de la CEI dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de la CEI et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) La CEI elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de la CEI. La CEI n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à la CEI, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de la CEI, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de la CEI ou de toute autre Publication de la CEI, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de la CEI peuvent faire l'objet de droits de brevet. La CEI ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets et de ne pas avoir signalé leur existence.

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

Cette norme est basée sur l'EN 50159.

La présente norme annule et remplace la CEI 62280-1 (2002) et la CEI 62280-2 (2002). Voir Annexe E.

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
9/1866A/FDIS	9/1885/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 publication a été rédigée selon les Directives ISO/CEI, Partie 2.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant la date de stabilité indiquée sur le site web de la CEI sous "http://webstore.iec.ch" dans les données relatives à la publication recherchée. A cette date, la publication sera

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

INTRODUCTION

Si un système électronique relatif à la sécurité implique le transfert d'informations entre plusieurs emplacements, le système de transmission fait alors partie intégrante du système relatif à la sécurité. Il en découle que la communication de bout en bout est sécurisée, conformément à la CEI 62425.

Le système de transmission envisagé dans la présente norme qui sert au transfert d'informations entre différents emplacements n'a, de manière générale, aucune condition préalable particulière à remplir. Du point de vue de la sécurité, il est non approuvé ou non approuvé totalement.

La présente norme est consacrée aux exigences devant être prises en compte pour la communication d'informations relatives à la sécurité sur de tels systèmes de transmission.

Bien que cette norme ne traite pas de la mémoire RAM, il convient de garder à l'esprit qu'elle est un aspect essentiel de la sécurité globale.

Les exigences de sécurité dépendent des caractéristiques du système de transmission. Afin de réduire la complexité de l'approche visant à démontrer la sécurité du système, les systèmes de transmission ont été classifiés en trois catégories:

- La catégorie 1 regroupe les systèmes qui sont sous le contrôle du concepteur et réparés au cours de leur durée de vie.
- La catégorie 2 regroupe les systèmes qui sont partiellement inconnus ou non réparés, cependant l'accès non autorisé peut être exclu.
- La catégorie 3 regroupe les systèmes qui ne sont pas sous le contrôle du concepteur et pour lesquels l'accès non autorisé doit être envisagé.

La première catégorie était couverte par la CEI 62280-1:2002, les autres par la CEI 62280-2:2002.

Lorsque des systèmes de communication relatifs à la sécurité qui ont été approuvés conformément aux normes précédentes font l'objet de maintenance et/ou d'extensions, l'Annexe informative E peut être utilisée à des fins de traçabilité des articles ou paragraphes de la présente norme par rapport aux articles ou paragraphes de la série précédente.

APPLICATIONS FERROVIAIRES – SYSTÈMES DE SIGNALISATION, DE TÉLÉCOMMUNICATION ET DE TRAITEMENT – COMMUNICATION DE SÉCURITÉ DANS LES SYSTÈMES DE TRANSMISSION

1 Domaine d'application

La présente Norme internationale est applicable aux systèmes électroniques relatifs à la sécurité utilisant, à des fins de communication numérique, un système de transmission qui n'était pas nécessairement conçu pour des applications relatives à la sécurité et qui est:

- sous le contrôle du concepteur et réparé au cours de sa durée de vie, ou
- partiellement inconnu ou non réparé, mais pour lequel l'accès non autorisé peut être exclu, ou
- n'étant pas sous le contrôle du concepteur et pour lequel l'accès non autorisé doit être envisagé.

Des équipements relatifs à la sécurité et des équipements non relatifs à la sécurité peuvent être connectés au système de transmission.

La présente norme internationale donne les exigences de base nécessaires pour réaliser une communication relative à la sécurité entre des équipements relatifs à la sécurité connectés au système de transmission.

La présente norme internationale est applicable à la spécification des exigences de sécurité des équipements relatifs à la sécurité connectés au système de transmission, en vue d'obtenir les exigences d'intégrité de sécurité affectées.

Les exigences de sécurité sont généralement mises en œuvre dans les équipements relatifs à la sécurité conçus conformément à la CEI 62425. Dans certains cas, ces exigences peuvent être mises en œuvre dans d'autres équipements du système de transmission à conndition qu'il existe un contrôle par des mesures de sécurité pour satisfaire aux exigences d'intégrité de sécurité affectées.

La spécification des exigences de sécurité est une condition préalable du dossier de sécurité d'un système électronique relatif à la sécurité pour laquelle les preuves exigées sont définies dans la CEI 62425. Les preuves de la gestion de la sécurité et de la qualité doivent être issues de la CEI 62425. La présente norme concerne les exigences relatives à la communication pour les preuves de sécurité fonctionnelle et technique.

La présente norme internationale n'est pas applicable aux systèmes existants qui ont déjà été acceptés avant la publication de la présente norme.

La présente norme internationale ne spécifie pas:

- le système de transmission,
- les équipements connectés au système de transmission,
- les solutions (par exemple pour l'interopérabilité),
- les données qui sont relatives à la sécurité et celles qui ne le sont pas.

Un équipement relatif à la sécurité connecté via un système de transmission ouvert peut être soumis à de nombreuses menaces de sécurité informatique différentes contre lesquelles un programme global comprenant les aspects de gestion, techniques et opérationnels doit être défini.

Dans la présente norme internationale cependant, du point de vue de la sécurité informatique, seules les attaques intentionnelles par le biais de messages aux applications relatives à la sécurité sont envisagées.

La présente norme internationale ne couvre pas les problèmes généraux de sécurité informatique et ne couvre pas, en particulier, les problèmes de sécurité informatique relatifs à:

- la confidentialité des informations relatives à la sécurité,
- la surcharge du système de transmission.

2 Références normatives

Les documents suivants sont cités en référence de manière normative, en intégralité ou en partie, dans le présent document et sont indispensables pour son application. 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 62278-2 (toutes les parties), *Applications ferroviaires – Spécification et démonstration de la fiabilité, de la disponibilité, de la maintenabilité et de la sécurité (FDMS)*

CEI 62425:2007, *Applications ferroviaires – Systèmes de signalisation, de télécommunication et de traitement – Systèmes électroniques de sécurité pour la signalisation*