NORME INTERNATIONALE

INTERNATIONAL STANDARD

CEI
IEC
62280-1

Première édition
First edition
2002-10

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

Partie 1:
Communication de sécurité sur des systèmes de transmission fermés

Railway applications –
Communication, signalling and processing systems –

Part 1:
Safety-related communication in closed transmission systems

Numéro de référence
Reference number
CEI/IEC 62280-1:2002

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
62280-1

Première édition
First edition
2002-10

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

Partie 1: Communication de sécurité sur des systèmes de transmission fermés

Railway applications – Communication, signalling and processing systems –

Part 1: Safety-related communication in closed transmission systems

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 Q

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

SOMMAIRE

CONTENTS

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

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

Partie 1: Communication de sécurité sur des systèmes de transmission fermés

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 62280-1 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 60159-1 (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
9/696/FDIS	9/707/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 62279[1], à la CEI 62280-2[1] et à la norme ENV 50129: 1998.

[1] A publier.

INTERNATIONAL ELECTROTECHNICAL COMMISSION

RAILWAY APPLICATIONS – COMMUNICATION, SIGNALLING AND PROCESSING SYSTEMS –

Part 1: Safety-related communication in closed 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 62280-1 has been prepared by IEC technical committee 9: Electrical equipment and systems for railways.

This standard, based on the European Norm EN 60159-1 (2001), was 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
9/696/FDIS	9/707/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 closely related to IEC 62279[1], IEC 62280-2[1] 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

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

INTRODUCTION

La présente partie de la CEI 62280 s'applique à la communication en sécurité entre des équipements liés à la sécurité utilisant un système de transmission fermée. Pour les systèmes de transmission qui ne peuvent pas être considérés comme fermés, la CEI 62280-2 s'applique.

Les équipements liés à la sécurité et ceux qui ne le sont pas peuvent être connectés au système de transmission.

Dans le cas d'erreurs affectant la communication liée à la sécurité, il est nécessaire de

– détecter les erreurs,
– déclencher une réaction de protection.

Cette norme n'impose pas de prescriptions de sécurité au système de transmission non sécurisé lui-même, mais ses propriétés et ses caractéristiques physiques sont définies.

Pour les questions de sécurité, telles qu'elles sont examinées ici, un chemin de transmission physique est suffisant. Les aspects de sécurité sont couverts par l'application de procédures de sécurité et d'une partie de contrôle qui sont mis en oeuvre dans les équipements liés à la sécurité à la suite d'un protocole de communication non sécurisé dans un système de transmission.

Bien que cette norme ne traite pas de la fiabilité, il est recommandé de garder à l'esprit que la fiabilité est un aspect essentiel de la sécurité globale.

Cette norme s'applique non seulement aux bus des véhicules mais également aux systèmes de transmission similaires avec un nombre maximal connu d'éléments connectables et une structure topographique connue.

INTRODUCTION

This part of IEC 62280 deals with safety-related communication between safety-related equipment using a closed transmission system. For those transmission systems which cannot be considered as closed, IEC 62280-2 shall be applied.

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

In the case of errors affecting safety-related communication, it is necessary

– to detect errors,

– to initiate a safety reaction.

This standard does not impose safety requirements on the non-trusted transmission system itself, but its properties and its physical characteristics shall be defined.

For safety purposes as considered here, one physical transmission path is sufficient. Safety aspects are covered by applying safety procedures and a safety code which are implemented inside safety-related equipment – on top of a non-trusted communication protocol in a transmission system.

Although reliability is not considered in this standard, it is recommended to keep in mind that reliability is a major aspect of the global safety.

The applicability of the standard was also extended from a vehicle bus to all closed transmission systems with a known maximum number of connectable participants and known topographical structure.

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

Partie 1: Communication de sécurité sur des systèmes de transmission fermés

1 Domaine d'application

La présente partie de la CEI 62280 est applicable aux systèmes électroniques liés à la sécurité utilisant un système de transmission fermée pour les communications. Elle indique les prescriptions de base nécessaires pour obtenir une communication en sécurité entre les équipements liés à la sécurité connectés au système de transmission.

Cette norme s'applique à la spécification de prescription de sécurité et à la conception du système de communication pour obtenir le niveau assigné d'intégrité de la sécurité.

La spécification de prescription de sécurité est une condition préalable à la sécurité d'un système électronique lié à la sécurité pour lequel la preuve nécessaire est définie par l'ENV 50129. La preuve de la gestion de la sécurité et de la gestion de la qualité est à prendre dans l'ENV 50129. La preuve de la sécurité fonctionnelle et technique constitue le sujet de cette norme.

Cette norme n'est pas applicable aux systèmes existants qui ont déjà été acceptés avant sa publication. Cependant, si la pratique le permet, cette norme s'applique aux modifications et aux extensions des systèmes, sous-systèmes et équipements existants.

Cette norme s'applique à un système de transmission fermée avec les conditions préalables suivantes, pour lesquelles il faut fournir la preuve

– que seul l'accès agréé est permis;
– qu'il existe un nombre maximal connu d'éléments connectables;
– que le support de transmission est connu et fixé.

Les systèmes de transmission fermée ne sont pas nécessairement des bus de données. Ils peuvent également inclure par exemple des liaisons de balise ou de simples liaisons série entre deux ordinateurs liés à la sécurité.

Plus particulièrement, cette norme ne définit pas

– le système de transmission;
– l'équipement connecté au système de transmission;
– des solutions spécifiques (par exemple pour l'interopérabilité);
– quels sont les types de données liés ou non à la sécurité.

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).

RAILWAY APPLICATIONS – COMMUNICATION, SIGNALLING AND PROCESSING SYSTEMS –

Part 1: Safety-related communication in closed transmission systems

1 Scope

This part of IEC 62280 is applicable to safety-related electronic systems using a closed transmission system for communication purposes. It gives the basic requirements needed in order to achieve safety-related communication between safety-related equipment connected to the transmission system.

This standard is applicable to the safety requirement specification and design of the communication system in order to obtain the assigned safety integrity level (SIL).

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 ENV 50129. Evidence of safety management and quality management has to be taken form ENV 50129. Evidence of functional and technical safety is 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. However, as far as is reasonably practicable, this standard shall be applied to modifications and extensions to existing systems, subsystems and equipment.

This standard applies to a closed transmission system with the following preconditions, for which evidence shall be provided:

– only approved access is permitted;
– there is a known maximum number of connectable participants;
– the transmission media is known and fixed.

Closed transmission systems are not necessarily data buses. They can also include for instance balise links or simple serial links between two safety-related computers.

In particular this standard does not define

– the transmission system;
– the equipment connected to the transmission system;
– specific 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.

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

CEI 62279, *Applications ferroviaires – Logiciels pour systèmes de commande et de protection ferroviaire* [2]

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

3 Définitions

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

3.1
authenticité
état dans lequel une information est valide et réputée avoir été générée par la source déclarée

3.2
système de transmission fermée
nombre fixe ou nombre maximal fixe d'éléments reliés par un système de transmission dont les propriétés sont connues et fixées et où le risque d'accès non autorisé est considéré comme négligeable

3.3
CRC
contrôle de redondance cyclique: procédure pour calculer les données redondantes à ajouter au *message* pour détecter les erreurs qui peuvent apparaître pendant la transmission du fait de l'influence de perturbations par des données physiques

3.4
EMI
interférences électromagnétiques

3.5
intégrité
état dans lequel l'information est complète et correcte, ni altérée ni polluée

3.6
message
information qui est transmise par un émetteur (source de données) à un ou plusieurs récepteurs (collecteur de données)

3.7
non sécurisé
pas de précautions spécifiques en matière de sécurité

3.8
état de secours sûr
état sûr d'un équipement ou d'un système lié à la sécurité comme déviation par rapport à un état normal et comme résultat d'une réaction de protection conduisant à une fonctionnalité réduite des fonctions liées à la sécurité, voire également des fonctions non liées à la sécurité

---

2 A publier.

IEC 62278, *Railway applications – Specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)* [2]

IEC 62279, *Railway applications – Communications, signalling and processing systems – Software for railway control and protection systems* [2]

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

3 Definitions

For the purpose of this part of IEC 62280, the following definitions apply.

3.1
authenticity
the state in which information is valid and known to have originated from the stated source

3.2
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 unauthorized access is considered negligible

3.3
CRC
cyclic redundancy check: procedure to calculate redundant data to be added to the *message* in order to detect errors which may arise during the transmission from the influence of physical data corruptions

3.4
EMI
electromagnetic interference

3.5
integrity
the state in which information is complete and correct and not altered or corrupted

3.6
message
information, which is transmitted from a sender (data source) to one or more receivers (data sink)

3.7
non-trusted
no specific precautions towards safety

3.8
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

---

[2] To be published.

3.9
partie de contrôle
données redondantes incluses dans un message pour permettre la détection de données polluées à l'aide de vérification de redondance

3.10
réaction de protection
action qui peut être prise par le processus de sécurité en réponse à un événement (comme une défaillance du système de communication) qui conduit à un état de secours sûr de l'équipement

3.11
code de transmission
information redondante, ajoutée au message de sécurité ou d'une autre nature du système de transmission non sécurisé pour assurer l'intégrité du message pendant la transmission

3.12
système de transmission
service faisant appel à la communication de blocs de message entre un nombre de participants, qui peuvent être des sources ou des collecteurs d'information

3.13
données utilisateur
données qui représentent les états ou événements d'un processus de sécurité sans données complémentaires ou redondantes pour la commande, la disponibilité et la sécurité. Dans le cas de communication entre équipements liés à la sécurité, les données utilisateur incluent les données liées à la sécurité

4 Architecture de référence

Cette norme définit les prescriptions de sécurité pour une catégorie spéciale de systèmes de communication. Les caractéristiques de cette catégorie sont définies comme des conditions préalables (Pr1, Pr2, Pr3).

En général, les équipements liés à la sécurité et les équipements qui ne le sont pas peuvent être connectés à un système de transmission qui, d'un point de vue sécurité, n'est pas sécurisé (voir la figure 1).

Le système de transmission lié à la sécurité est défini comme suit:

– le système de transmission non sécurisé (y compris les fonctions de transmission mises en oeuvre dans les circuits hautement intégrés);
– les fonctions de transmission liées à la sécurité.

Le cas de sécurité pour le processus de sécurité doit être préparé en conformité avec l'ENV 50129. La preuve de la sécurité fonctionnelle et technique des fonctions de transmission liées à la sécurité doit être conforme à cette norme.

Aucune prescription de sécurité ne concerne le système de transmission non sécurisé. Les aspects de sécurité sont couverts en appliquant les procédures de sécurité et la partie de contrôle qui fonctionnent au sein de l'équipement lié à la sécurité (voir la figure 2).

Ainsi, cette norme est applicable à l'architecture définie si les conditions préalables suivantes sont remplies.

3.9
safety code
redundant data included in a message to permit data corruptions to be detected by redundancy checks

3.10
safety reaction
an action which may be taken by safety process in response to an event (such as a failure of the communication system) which leads to a safe fall back state of the equipment

3.11
transmission code
redundant information, added to the safety and non-safety message of the non-trusted transmission system in order to ensure the integrity of the message during the transmission

3.12
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

3.13
user data
data which represents the states or events of a user process, without any additional data. In the case of communication between safety-related equipment, the user data contains safety-related data

4 Reference architecture

This standard defines the safety requirements for a special class of communication systems. The characteristics of this class are defined as preconditions (Pr1, Pr2, Pr3).

In general, safety-related and non-safety-related equipment may be connected to a transmission system, which is from a safety point of view non-trusted (see figure 1).

The safety-related transmission system is defined as:

– the non-trusted transmission system (including the transmission functions implemented in highly integrated circuits);
– the safety-related transmission functions.

The safety case for the safety process shall be prepared in accordance with ENV 50129. The evidence of functional and technical safety of the safety-related transmission functions shall comply with this standard.

No safety requirements are placed upon the non-trusted transmission system. Safety aspects are covered by applying safety procedures and safety code which are running inside safety-related equipment (see figure 2).

Therefore this standard is applicable to the defined architecture if the following preconditions are fulfilled.

Pr1 Le système de transmission est fermé.

Pr2 Le nombre de parties d'équipement – liées à la sécurité ou non – connectable au système de transmission doit être connu et fixé. Comme la sécurité du système de transmission lié à la sécurité dépend de ce paramètre, le nombre maximal d'éléments autorisés à communiquer ensemble doit être indiqué dans la spécification de prescription de sécurité comme condition préalable [3].

Pr3 Les caractéristiques physiques du système de transmission (par exemple, support de transmission, environnement dans les pires conditions, ...) sont fixées. Elles doivent être conservées pendant le cycle de vie du système. Si des paramètres essentiels doivent être modifiés, tous les aspects liés à la sécurité doivent être réexaminés.

Les prescriptions concernant ces conditions préalables sont définies dans les articles suivants.

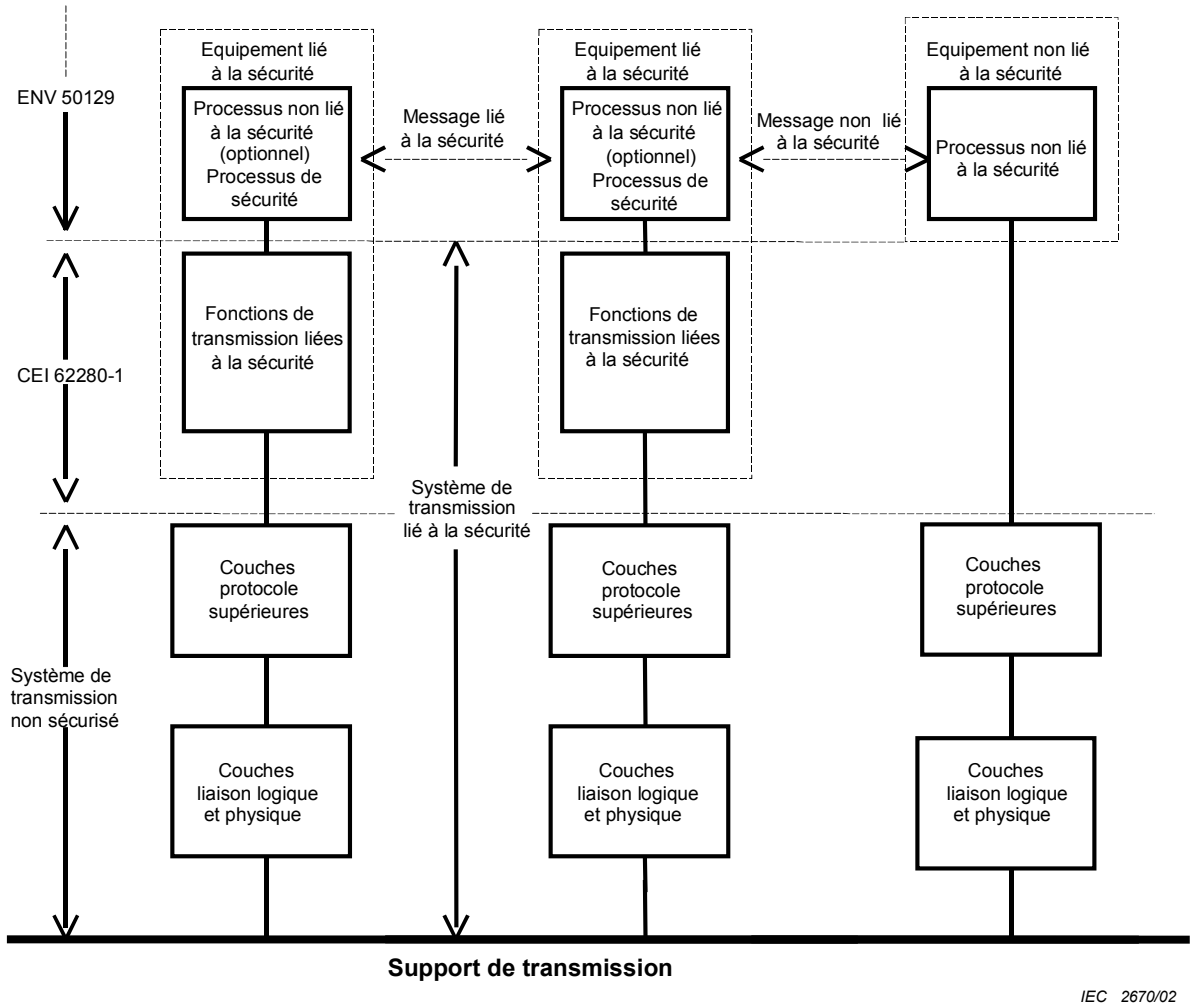

Figure 1 – Structure d'un système lié à la sécurité utilisant un système de transmission non sécurisé

[3] La configuration du système devra être définie/englobée dans le cas de sécurité. Il faut que tout ajout à cette configuration soit précédé par une revue de ses effets sur le cas de sécurité.

Pr1 The transmission system is closed.

Pr2 The number of pieces of connectable equipment – either safety-related or not – to the transmission system has to be known and fixed. As the safety of the safety-related transmission system depends on this parameter, the maximum number of participants allowed to communicate together shall be put into the safety requirement specification as a precondition.[3]

Pr3 The physical characteristics of the transmission system (e.g. transmission media, environment under worst case conditions, ...) are fixed. They shall be kept during the life cycle of the system. If major parameters are to be changed, all safety-related aspects shall be reviewed.

The requirements regarding these preconditions are defined in the following clauses.

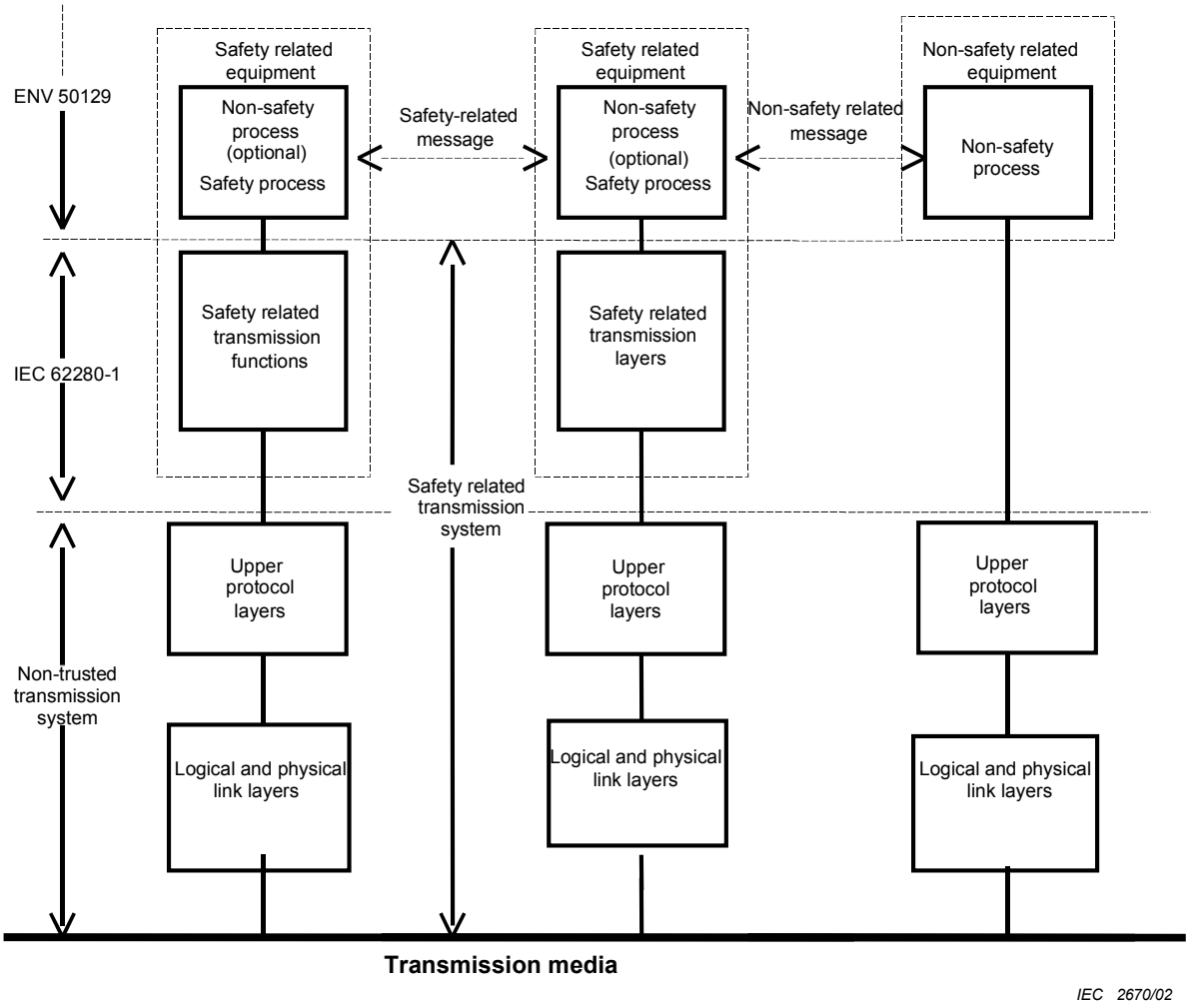

Figure 1 – Structure of safety-related system using a non trusted transmission system

[3] The configuration of the system shall be defined/embedded in the safety case. Any subsequent to that configuration must be preceded by a review of their effects on the safety case.

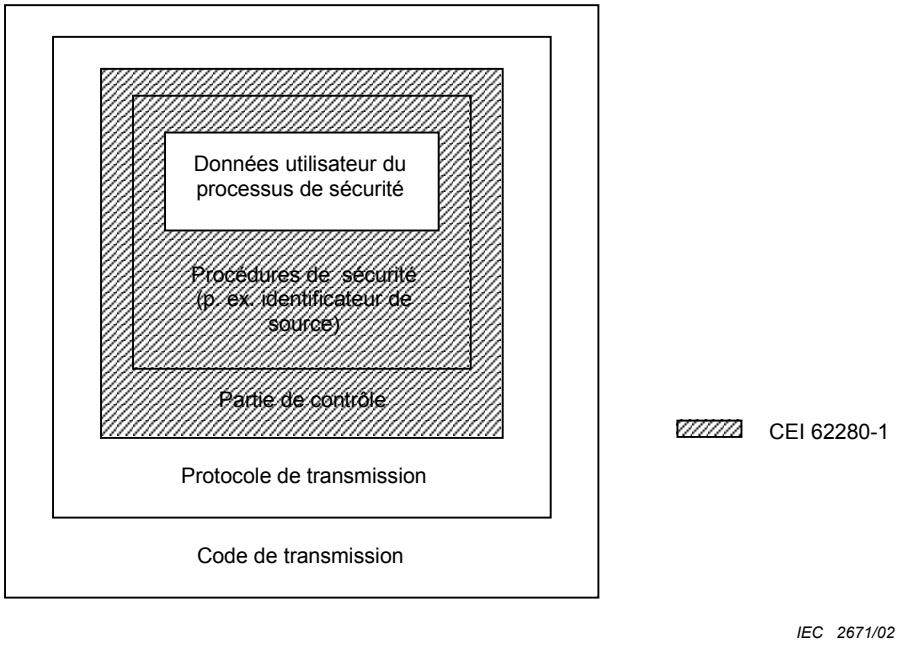

Figure 2 – Modèle de représentation de message sur le support de transmission

5 Relation entre les caractéristiques du système de transmission et les procédures de sécurité

La preuve de la sécurité fonctionnelle et technique suit le même processus que celui appliqué dans l'ENV 50129. Cependant, l'utilisation d'un système de transmission non sécurisé réduit le processus à une approche fonctionnelle. C'est pourquoi, le système de transmission lié à la sécurité doit être caractérisé par une spécification fonctionnelle avec un modèle d'erreur global. La spécification de prescription d'intégrité de sécurité doit être produite par l'analyse fonctionnelle du modèle d'erreur.

5.1 Prescription d'intégrité fonctionnelle

Cette analyse obligatoire correspond à l'analyse du risque fonctionnel.

Du point de vue du récepteur, les défauts suivants peuvent conduire à une situation présentant des risques:

- information erronée (erreur d'identité d'émetteur, erreur de type, erreur de valeur);
- erreurs temporelles (données retardées trop longtemps, erreur de séquence).

Pour éviter de telles situations, il est nécessaire de détecter les données erronées avant de les utiliser dans le processus de sécurité mis en oeuvre dans l'équipement de réception.

Les six mesures de protection suivantes doivent être fournies dans l'architecture de conception.

P1: Détection des erreurs d'identification d'émetteur.

P2: Détection des erreurs de type de données.

P3: Détection des erreurs de valeur de données.

P4: Détection des données dépassées ou des données qui n'ont pas été reçues en temps utile.

P5: Détection de la perte de communication après un délai prédéfini.

P6: Assurance de l'indépendance fonctionnelle des fonctions de transmission liées à la sécurité et des couches utilisées du système de transmission non sécurisé.

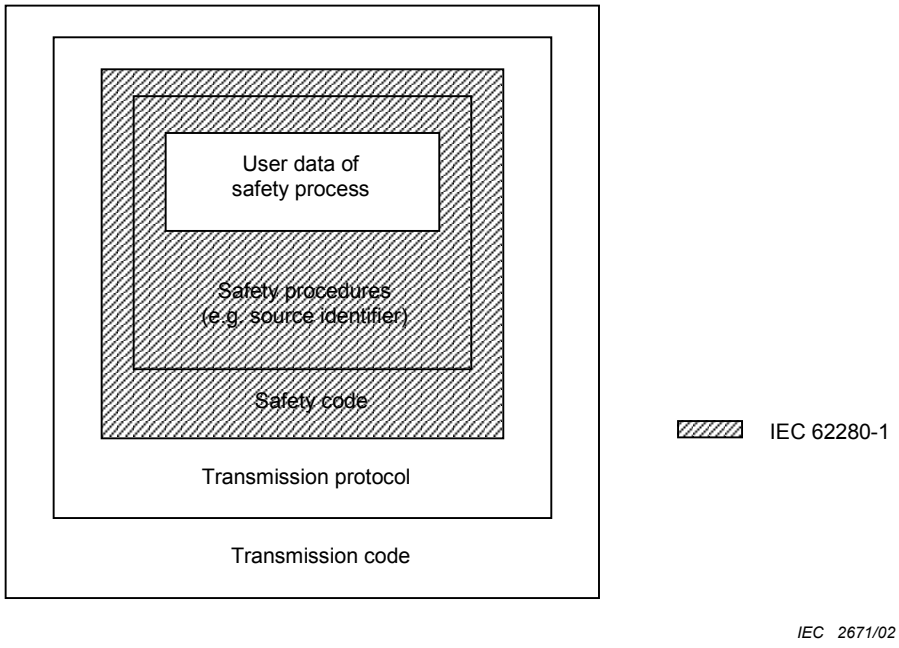

Figure 2 – Model of message representation on the transmission media

5 Relation between the characteristics of the transmission system and safety procedures

The evidence of functional and technical safety follows the same process as applied in ENV 50129. Nevertheless, the use of a non-trusted transmission system restricts the process to a functional approach. Therefore, the safety-related transmission system shall be characterized by a functional specification together with an overall error model. A safety integrity requirement specification shall be produced by functional analysis of the error model.

5.1 Functional integrity requirement

This mandatory analysis consists of the functional hazard analysis.

From the view point of the receiver, the following faults may lead to a hazardous situation:

- erroneous information (transmitter identity error, type error, value error);
- time errors (data delayed too long, sequencing error).

To avoid such situations, it is necessary to detect erroneous data before using it in the safety process implemented in the receiver equipment.

The following six protective measures shall be provided in the design architecture.

P1: Detect transmitter identifier error.

P2: Detect data type error.

P3: Detect data value error.

P4: Detect outdated data or data not received in due time.

P5: Detect the loss of communication after a predefined delay.

P6: Ensure the functional independence of the safety-related transmission functions and the used layers of the non-trusted transmission system.

5.2 Prescriptions d'intégrité de sécurité

Les six prescriptions suivantes doivent être remplies.

R1 La protection de sécurité doit être appliquée à la production des données à émettre.

R2 La réaction de protection doit être appliquée en cas de mauvais fonctionnement. Elle doit être en cohérence avec les prescriptions de sécurité du récepteur.

R3 Le mécanisme de détection d'erreur doit être appliqué au niveau du récepteur et doit être en cohérence avec les prescriptions de sécurité du récepteur.

R4 La mise en oeuvre de la réaction de protection R2 doit être fonctionnellement indépendante du système de transmission non sécurisé.

R5 Le taux résiduel d'erreur de données du système de transmission lié à la sécurité pour chaque échange d'information entre l'émetteur et le récepteur doit être inférieur à la valeur prédéfinie. Ce taux doit être compatible avec le niveau d'intégrité de sécurité de chaque récepteur.

R6 Le niveau d'intégrité de sécurité du système de transmission lié à la sécurité doit être en cohérence avec le niveau d'intégrité de sécurité le plus élevé des processus de sécurité.

Ces prescriptions de sécurité sont détaillées dans

- les prescriptions de procédures de sécurité (pour les précautions qualitatives, voir l'article 6);
- les prescriptions de la partie de contrôle (pour les précautions quantitatives, voir l'article 7).

6 Prescriptions de procédures de sécurité

6.1 Généralités

Afin d'obtenir la partie qualitative des niveaux d'intégrité de sécurité assignés, la réalisation des fonctions liées à la sécurité doit être obtenue en utilisant les procédures correspondantes – dépendant des niveaux d'intégrité de sécurité – définies dans l'ENV 50129.

Les trois cas de communications bidirectionnelles possibles sont examinés:

a) équipement lié à la sécurité et équipement lié à la sécurité (voir 6.2);

b) équipement lié à la sécurité et équipement non lié à la sécurité (voir 6.3);

c) équipement non lié à la sécurité et équipement non lié à la sécurité (voir 6.4).

6.2 Communication entre équipements liés à la sécurité

On doit s'assurer de l'authenticité, de l'intégrité et de l'opportunité des données.

Etant donné que les processus de sécurité n'ont pas accès aux fonctionnalités internes des circuits non sécurisés qui font partie du système de transmission non sécurisé, les processus de sécurité doivent assurer la vérification en plus de celle fournie par l'équipement pour s'assurer que des défauts n'échappent pas à la détection.

Des défauts peuvent intervenir lorsque la mémoire est contenue dans des circuits de protocole ou dans un équipement non lié à la sécurité. Un message lié à la sécurité, stocké dans un équipement non lié à la sécurité, pourrait à nouveau être transmis à un moment inopportun. La protection contre ce défaut doit être fournie.

5.2 Safety integrity requirements

The six following requirements shall be fulfilled.

R1 Safety protection shall be applied to the generation of the data to be transmitted.

R2 Safety reaction shall be applied in case of misoperation. This shall be consistent with the safety requirements of the receiver.

R3 Error detection mechanism shall be applied at the receiver and shall be consistent with the safety requirements of the receiver.

R4 The implementation of the safety reaction R2 shall be functionally independent of the non-trusted transmission system.

R5 The residual data error rate of the safety-related transmission system for each information interchange between transmitter and receiver shall be less than a pre-defined value. This rate shall be compatible with the safety integrity level of each receiver.

R6 The safety integrity level of the safety-related transmission system shall be consistent with the highest safety integrity level of the safety processes.

These safety requirements are detailed in the

- safety procedure requirements (for qualitative precautions, see clause 6);
- safety code-requirements (for quantitative precautions, see clause 7).

6 Safety procedure requirements

6.1 General

To obtain the qualitative part of the assigned SIL, the implementation of the safety-related functions shall be performed by using the corresponding – SIL dependent procedures – defined in ENV 50129.

The three possible cases of bi-directional communications are considered:

a) safety-related equipment with safety-related equipment (see 6.2);

b) safety-related equipment with non-safety-related equipment (see 6.3);

c) non-safety-related equipment with non-safety-related equipment (see 6.4).

6.2 Communication between safety-related-equipment

Authenticity, integrity and correct time of data shall be ensured.

As the safety processes have no access to the internal functionalities of non-trusted circuits being part of the non-trusted transmission system the safety processes shall perform checking in addition to that provided by this equipment to ensure that faults do not go undetected.

Faults may occur when memory is contained in protocol circuits or in non-safety-related equipment. A safety-related message, stored in non-safety-related equipment, could be transmitted again at the wrong time. Protection against this fault shall be provided.

Pour maintenir la sécurité nécessaire à la communication entre équipements liés à la sécurité, les prescriptions suivantes doivent être remplies.

R7 Si la source n'est pas uniquement identifiée dans le système de transmission, l'authenticité doit être fournie en ajoutant un identificateur de source aux données utilisateur.

R8 L'intégrité doit être fournie en ajoutant une partie de contrôle aux données utilisateur. Le processus de sécurité ne doit pas reposer sur le code de transmission produit et vérifié par les circuits intégrés faisant partie du système de transmission non sécurisé.

R9 Le degré d'actualité des données utilisateur doit être fourni en ajoutant des informations temporelles (par exemple, horodatage, numéros d'ordre, ...) aux données utilisateur. Le délai permis dépend de l'application.

R10 Si nécessaire, la séquence des messages doit être vérifiée par le processus de sécurité.

R11 Les procédures de sécurité pour les équipements liés à la sécurité doivent être fonctionnellement indépendantes des procédures utilisées par le système de transmission non sécurisé. En particulier, si les deux procédures utilisent le même mécanisme de codage, les paramètres (par exemple les polynômes) doivent être différents.

R12 Tous les équipements liés à la sécurité doivent surveiller les performances des prescriptions indiquées en R7, R8, R9 et R10. Si la qualité de transmission tombe en dessous d'un niveau prédéfini dans la spécification de prescription du système, alors la réaction de protection appropriée doit être déclenchée.

6.3 Communication entre équipements liés à la sécurité et équipements non liés à la sécurité

Comme défini précédemment, les équipements liés à la sécurité et ceux qui ne le sont pas peuvent être connectés au même système de transmission. Dans les équipements non liés à la sécurité, ou dans une interface non liée à la sécurité vers le système de transmission d'un équipement lié à la sécurité, les modes en cas de pannes peuvent ne pas être prévisibles. Si de tels défauts interviennent, des données liées à la sécurité peuvent être altérées de deux manières différentes:

a) un message lié à la sécurité produit par un équipement lié à la sécurité peut être perturbé et modifié (par exemple, en raison d'un collision dans le système de transmission);

b) l'équipement non lié à la sécurité produit un message qui pourrait engendrer un message lié à la sécurité.

Pour maintenir la sécurité nécessaire pour la liaison de communication entre équipement lié à la sécurité, les prescriptions suivantes doivent être remplies.

R13 Les messages qui sont liés à la sécurité et ceux qui ne sont pas liés à la sécurité doivent avoir des structures différentes obtenues en appliquant une partie de contrôle aux messages liés à la sécurité. Cette partie de contrôle doit être capable de protéger le système au niveau requis d'intégrité de sécurité (voir cible de sécurité, 7.2) pour qu'un message non lié à la sécurité ne se change pas en message lié à la sécurité.

R14 Les procédures de sécurité de l'équipement lié à la sécurité doivent être fonctionnellement indépendantes des procédures utilisées par le système de transmission non sécurisé et par l'équipement non lié à la sécurité.

6.4 Communication entre équipements non liés à la sécurité

La communication entre les équipements non liés à la sécurité ne fait pas partie du domaine d'application de cette norme. Si un équipement non lié à la sécurité utilise le même système de transmission non sécurisé qu'un équipement lié à la sécurité, alors les équipements doivent être conformes aux prescriptions R13 et R14.

To maintain the required safety for communication between safety-related equipment the following requirements shall be fulfilled.

R7 If the source is not uniquely identified in the transmission system, authenticity shall be provided by adding a source identifier to the user data.

R8 Integrity shall be provided by adding a safety code to the user data. The safety process shall not rely on the transmission code generated and checked by integrated circuits being part of the non-trusted transmission system.

R9 The timeliness of user data shall be provided by adding time information (e.g. time stamps, sequence numbers, ...) to the user data. The time delay which is allowed depends on the application.

R10 If necessary the sequence of messages shall be checked by the safety process.

R11 The safety procedures for the safety-related equipment shall be functionally independent of the procedures used by the non-trusted transmission system. In particular, if both procedures use the same coding mechanism, the parameters (e.g. polynomial) shall be different.

R12 All safety-related equipment shall monitor the performance of the requirements listed in R7, R8, R9 and R10. If the quality of the transmission falls below a level, which is pre-defined in the system requirement specification then an appropriate safety reaction shall be triggered.

6.3 Communication between safety-related and non-safety-related equipment

As defined previously, safety-related and non-safety-related equipment may be connected to the same transmission system. In non-safety-related equipment, or in a non-safety-related interface to the transmission system of a safety-related equipment, failure modes may be unpredictable. In the case of such faults, safety-related data may be corrupted in two different ways:

a) a safety-related message generated by a safety-related equipment may be disturbed and modified (e.g. due to a collision on the transmission system);

b) the non safety-related equipment generates a message which could emulate a safety-related message.

To maintain the required safety for the communication link between safety-related equipment, the following requirements shall be fulfilled.

R13 Safety-related and non-safety-related messages shall have different structures achieved by applying a safety code to safety-related messages. This safety code shall be capable of protecting the system to the required safety integrity level (see 7.2) that a non-safety-related message changes to a safety-related one.

R14 The safety procedures of the safety-related equipment shall be functionally independent from the procedures used by the non-trusted transmission system and by the non-safety-related equipment.

6.4 Communication between non-safety-related-equipment

The communication between non-safety-related equipment is not part of this standard. If non-safety-related equipment uses the same non-trusted transmission system as safety-related equipment, then the equipments shall comply with the requirements from R13 and R14.

7 Prescriptions de la partie de contrôle

7.1 Prescriptions générales

Pour obtenir la partie quantitative du niveau d'intégrité de sécurité assignée pour l'évaluation de la partie de contrôle et du code de transmission non sécurisé, il est nécessaire de distinguer entre

- les défauts dus au matériel de transmission non sécurisé défaillant;
- les erreurs aléatoires dues aux influences externes (par exemple EMI) sur le support de transmission.

On doit partir de l'hypothèse qu'il pourrait y avoir des trames erronées qui ne puissent pas être détectées par le code de transmission non sécurisé. Ces erreurs doivent être détectées par la partie de contrôle.

Si un système de transmission non sécurisé utilise un Correcteur d'Erreur Avancé (FEC), il faut prendre des précautions, du fait de l'influence statistique du FEC sur l'erreur de bit vue par la partie de contrôle.

De plus, il devrait être peu probable que le matériel de transmission non sécurisé soit capable de produire une expression de partie de contrôle correcte même si cet équipement connaît une défaillance.

La défaillance du vérificateur de code de transmission non sécurisé doit être prise en compte. Dans ce cas, tous les messages altérés pourraient être transférés à partir du système de transmission.

Prescriptions

R15 Pour remplir le niveau d'intégrité de sécurité requis (voir 7.2), il est nécessaire de détecter et d'agir sur les défauts typiques du système de transmission non sécurisé. Les défauts à examiner doivent au moins inclure:

- la ligne de transmission interrompue,
- tous les bits à la valeur logique 0,
- tous les bits à la valeur logique 1,
- l'inversion de message,
- le glissement de synchronisation (dans le cas d'une transmission série).

R16 Pour satisfaire le niveau requis de sécurité d'intégrité (voir 7.2, il est nécessaire de détecter et d'agir sur des erreurs typiques. Ces erreurs à prendre en considération doivent inclure au moins:

- des erreurs aléatoires,
- des paquets d'erreurs,
- des erreurs systématiques, par exemple des séquences répétées d'erreurs,
- des combinatoires de ce qui précède.

R17 La partie de contrôle doit être fonctionnellement indépendante du code de transmission.

R18 La partie de contrôle doit garantir que la probabilité que le système de transmission non sécurisé produise une expression de partie de contrôle correcte soit très faible.

NOTE Cette prescription pourrait être démontrée par une approche de sécurité utilisant des statistiques. Il est acceptable de prendre comme hypothèse qu'une partie de contrôle suffisamment complexe (par exemple CRC) remplit cette prescription.

7 Safety code requirements

7.1 General requirements

To obtain the quantitative part of the assigned safety integrity level, for the assessment of the safety code and non-trusted transmission code, it is necessary to distinguish between:

- faults due to failed non-trusted transmission hardware;
- random errors due to external influence (e.g. EMI) on the transmission media.

It shall be assumed that there could be error patterns which cannot be detected by the non-trusted transmission code. These errors shall be detected by the safety code.

If the non-trusted transmission system uses Forward Error Correction (FEC), precautions have to be taken which regard the influence of the FEC to the bit error statistics seen by the safety code.

Furthermore, it should be very unlikely that the non-trusted transmission hardware is able to generate a correct safety code word even if this hardware fails.

Failure of the non-trusted transmission code checker shall be taken into account. In this case, all corrupted messages could be passed from the transmission system.

Requirements

R15 To fulfil the required safety integrity level (see 7.2) it is necessary to detect and act on typical faults of the non-trusted transmission system. The faults to be considered shall at least include:

- interrupted transmission line,
- all bits logical 0,
- all bits logical 1,
- message inversion,
- synchronization slip (in case of serial transmission).

R16 To fulfil the required safety integrity level (see 7.2) it is necessary to detect and act on typical errors. These errors to be considered shall at least include:

- random errors,
- burst errors,
- systematic errors, for example repeated error patterns,
- combinations of the above.

R17 The safety code shall be functionally independent from the transmission code.

R18 The safety code shall guarantee that the non-trusted transmission system shall be very unlikely to be able to generate a correct safety code word.

NOTE This requirement could be demonstrated by a probabilistic safety approach. It is acceptable to assume that a sufficiently complex safety code (e.g. a CRC) meets this requirement.

7.2 Cible de sécurité

Le niveau d'intégrité de sécurité de l'ensemble du système, dont le système de communication lié à la sécurité fait partie, étant donné, le taux de défaillance de risque pour l'ensemble du système R_H doit être déduit selon les procédures données par la CEI 62278 et l'ENV 50129.

7.3 Longueur de la partie de contrôle

On doit fournir une longueur pour la partie de contrôle qui soit compatible avec le cible de sécurité du système de transmission. Le calcul dépend du taux de défaillance de risque R_H trouvé auparavant et des principes de technologie choisis. Un modèle des modes en cas de panne doit être fourni et toutes les affirmations faites pour les calculs doivent être vérifiées et validées. Un exemple de tels calculs est donné à l'annexe A.

7.2 Safety target

Given the safety integrity level for the entire system, of which the safety-related communication system is a part, the hazardous failure rate for the entire system R_H shall be derived according to the procedures given in IEC 62278 and ENV 50129.

7.3 Length of safety code

A length of safety code compatible with the transmission system safety target has to be provided. The calculation depends on the hazardous failure rate R_H previously found and the chosen technology principles. A model of the failure modes shall be provided and all assumptions made for the calculations shall be verified and validated. An example of such calculation is given in annex A.

Annexe A
(informative)

Longueur de la partie de contrôle

Cette annexe donne des formules simples pour calculer la longueur de la partie de contrôle.

NOTE La justification de ces formules est donnée dans un rapport du CENELEC «*Safety Analysis for a Closed Transmission System*». Si les prescriptions données sont remplies, on a la garantie que la cible de sécurité est atteinte.

Le modèle de base pour le calcul de la longueur de la partie de contrôle est représenté à la figure A.1.

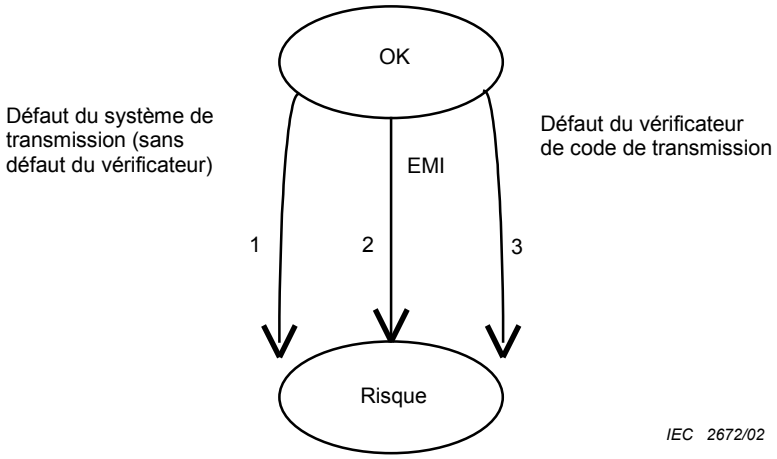

Figure A.1 – Modèle d'erreur de base

Le risque peut être créé de trois manières différentes:

1) le matériel de transmission connaît une défaillance, les messages sont altérés;
2) des erreurs binaires apparaissent à cause d'EMI et ne sont pas détectées par le codage de transmission;
3) des défauts apparaissent dans le vérificateur de code de transmission si bien que tous les messages altérés peuvent passer du circuit commercial non sécurisé à l'équipement lié à la sécurité.

Les définitions suivantes sont données:

R_H Taux de défaillance de risque du système de transmission dans son ensemble

R_{HW} Taux de défaillance de matériel du système de transmission non sécurisé

p_{US} Probabilité de défaillances non détectées en raison des performances de la partie de contrôle

p_{UT} Probabilité de défaillances non détectées en raison des performances du code de transmission

NOTE Quand les systèmes de transmission non sécurisés ne contiennent pas de mécanismes de codage de la transmission, il faut alors supposer que $P_{UT} = 1$.

Annex A
(informative)

Length of safety code

This annex gives simple formulae for calculating the length of the safety code.

NOTE The justification for these formulae is given in a CENELEC report *"Safety Analysis for a Closed Transmission System"*. Fulfilling the given requirements guarantees that the safety target will be reached.

The basic model for calculating the length of the safety code is shown in figure A.1.

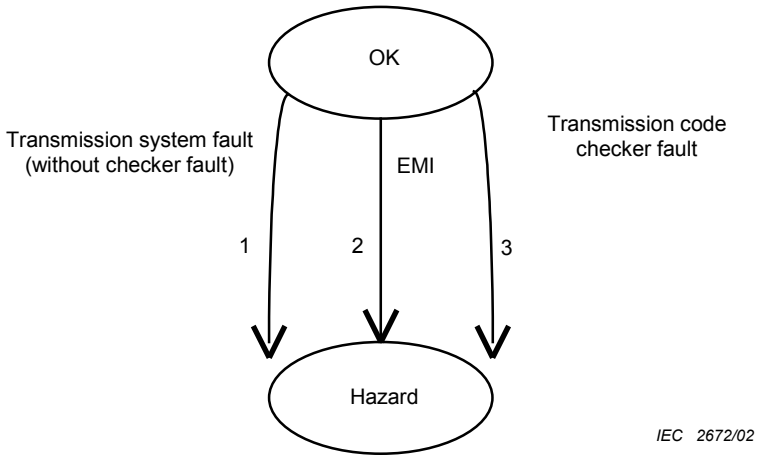

Figure A.1 – Basic error model

There are three ways in which a hazard may be created:

1) the transmission hardware fails, so the messages are corrupted;
2) bit errors arise due to EMI and are not detected by the transmission coding;
3) faults occur in the transmission code checker, in such a way that every corrupted message could be passed from the non-trusted commercial circuit to the safety-related equipment.

The following definitions are given:

R_H Hazardous failure rate of the complete transmission system

R_{HW} Hardware failure rate of the non-trusted transmission system

p_{US} Probability of undetected failure due to the performance of the safety code

p_{UT} Probability of undetected failure due to the performance of the transmission code

NOTE When the non-trusted transmission systems contain no transmission coding mechanisms then P_{UT} = 1 has to be assumed.

f_M Fréquence maximale des messages pour un récepteur

f_W Fréquence des messages erronés (altérés)

T Intervalle de temps, si plus d'un nombre défini de messages altérés est reçu pendant ce temps, au cours duquel l'état de secours sûr interviendra

k_1 Facteur pour les défauts matériels y compris la marge de sécurité

k_2 Facteur qui décrit le pourcentage de défauts matériels qui donnent lieu à l'annulation non détectée du décodage de la transmission

m Facteur de sécurité inclus dans k_1

n Nombre de messages altérés consécutifs jusqu'à l'état de secours sûr

Les inéquations suivantes doivent être remplies avec ces définitions:

$$R_{HW} \times p_{US} \times k_1 \leq R_{H1} \quad \text{(défauts matériels)} \tag{1}$$

$$p_{UT} \times p_{US} \times f_W \leq R_{H2} \quad \text{(EMI)} \tag{2}$$[4]

$$k_2 \times p_{US} \times \frac{1}{T} \leq R_{H3} \quad \text{(défaut de code de transmission)} \tag{3}$$

La somme de ces trois taux ne doit pas être supérieure à R_H:

$$R_{H1} + R_{H2} + R_{H3} \leq R_H$$

Comme il n'est pas possible de prendre comme hypothèse que la défaillance est une défaillance aléatoire, il est nécessaire de prendre en compte une marge de sécurité m dans le facteur k_1. Le facteur k_1 doit être calculé conformément à la formule suivante:

$$k_1 \geq n \times m.$$

Le facteur m représente la marge de sécurité avec $m \geq 5$.

La fréquence maximale de messages erronés f_W doit être estimée

- soit par l'estimation du pire des cas $f_W = f_M$,
- soit en limitant le taux maximal ou le nombre de messages erronés où des compteurs sûrs et/ou des minuteries sûres sont mis en oeuvre. Si plus d'un message erroné est reçu dans un intervalle de temps défini, la communication sûre doit être interrompue et l'état de secours sûr doit intervenir. Une déduction mathématique prouve qu'une certaine limite ne peut pas être dépassée.

En transmission cyclique, la fréquence f_M est bien définie. Dans le cas d'une transmission non cyclique, on doit prendre la fréquence maximale possible.

En utilisant un CRC approprié, la valeur maximale de P_{UT} peut être estimée comme étant

$$P_{UT} = 2^{-b}$$

où b donne le nombre de bits de redondance.

Si d'autres codes sont utilisés, par exemple une combinaison de deux codes, l'erreur de bloc la plus grave utilisant le modèle de «canal symétrique binaire»[5] doit être prise.

---

[4] Cela suppose que la partie de contrôle et le code de transmission sont indépendants. Cela peut s'avérer très difficile à prouver. Une approche plus conservatrice consiste à ne s'appuyer que sur la partie de contrôle.

f_M Maximum frequency of messages for one receiver

f_W Frequency of wrong (corrupted) messages

T Time span, if more than a defined number of corrupted messages were received within this time, the safe fall back state will be entered

k_1 Factor for hardware faults including safety margin

k_2 Factor which describes the percentage of hardware faults that result in undetected disabling of transmission decoding

m Safety factor included within k_1

n Number of consecutive corrupted messages until the safe fall-back state is entered

With these definitions the following inequations have to be fulfilled:

$$R_{HW} \times p_{US} \times k_1 \leq R_{H1} \quad \text{(hardware faults)} \tag{1}$$

$$p_{UT} \times p_{US} \times f_W \leq R_{H2} \quad \text{(EMI)} \tag{2}$$[4]

$$k_2 \times p_{US} \times \frac{1}{T} \leq R_{H3} \quad \text{(transmission code fault)} \tag{3}$$

The sum of all three rates shall not exceed R_H:

$$R_{H1} + R_{H2} + R_{H3} \leq R_H$$

Because it cannot be assumed that the failure is a random failure, it is necessary to take into account a safety margin m in the factor k_1. The factor k_1 shall be calculated according to the following formula:

$$k_1 \geq n \times m.$$

The factor m represents the safety margin with $m \geq 5$.

The maximum frequency of wrong messages f_W shall be estimated

- either by the worst case estimation $f_W = f_M$,
- or by limiting the maximum rate or number of wrong messages where safe counters and/or safe timers are implemented. If more than one wrong message within a definite time interval is received, the safe communication shall be aborted and the safe fall back state shall be entered. A mathematical derivation proves that a certain limit cannot be exceeded.

In cyclic transmission the frequency f_M is well-defined. In the case of non-cyclic transmission, the maximum possible frequency must be taken.

By using proper CRC, the maximum value of P_{UT} may be estimated as

$$P_{UT} = 2^{-b}$$

where b denotes the number of redundancy bits.

If other codes are used, for example a combination of two codes, the worst case block error probability using the model of “binary symmetric channel"[5] shall be taken.

---

4 This assumes that the safety code and the transmission code are independent. This can be very hard to prove. A more conservative approach is to rely only on the safety code.

Le facteur k_2 est difficile à estimer. Si la vérification périodique du travail correct du mécanisme de codage de transmission est possible, alors le facteur k_2 pourrait être négligé.

Sans justification, on doit prendre $k_2 = 1$.

NOTE La déduction suivante n'est donnée que pour information:

– si un défaut matériel apparaît, dans 1 cas sur 10 000 seulement le vérificateur de code de transmission connaît une défaillance sans que celle-ci soit détectée;

– dans ce cas, la durée moyenne (sans EMI) de cet état est

$$T = MTBF_{HW} = \frac{1}{R_{HW}}$$

Noter qu'une faible dégradation de la qualité de transmission conduirait en général à l'état de secours sûr, cette estimation est donc très pessimiste.

Avec ces hypothèses, la valeur $k_2 = 10^{-4}$ peut être prise.

L'inéquation (3) conduit à un intervalle minimal au cours duquel seulement une erreur détectée par la partie de contrôle est permise. Si un tel mécanisme n'est pas utilisé, il faut que le retour à l'état de secours sûr intervienne immédiatement après la première erreur détectée si aucune autre mesure contre de possibles conditions d'erreur n'a été introduite.

La probabilité maximale d'erreurs non détectées de la partie de contrôle avec c chiffres doit être estimée comme

$$p_{US} = 2^{-c}$$

Cette formule peut être utilisée comme une estimation approximative de la probabilité de défauts ayant échappé à la détection. Cela est valable pour une large catégorie de codes (par exemple codes BCH, codes cryptographiques, ...) dans le cadre d'estimations réalistes. Cependant, il doit être démontré que le caractère approprié[6] du code choisi est rempli.

En répétant chaque message et en vérifiant l'homogénéité de deux messages mutuellement indépendants, la valeur de c peut être divisée par deux au minimum. En fait, on peut obtenir une amélioration supplémentaire mais pour éviter des calculs mathématiques complexes, l'estimation pessimiste donnée devrait être la limite.

6 Etre approprié signifie que la relation entre la probabilité d'erreur sur les bits et la probabilité d'erreur non détectée est monotone.

The factor k_2 is difficult to estimate. If periodic checking of the correct working of transmission encoding mechanism is possible, then the factor k_2 could be neglected.

Without any justifications $k_2 = 1$ shall be taken.

NOTE The following derivation is given for information only:

– if a hardware fault occurs, in only 1 of 10 000 cases the transmission code checker fails undetected;

– in this case the average duration (without EMI) of this state is

$$T = MTBF_{HW} = \frac{1}{R_{HW}}$$

Note that a small degradation of transmission quality would usually lead to the safe fall back state, so this estimation is very pessimistic.

Under these assumptions, the value $k_2 = 10^{-4}$ can be taken.

Inequation (3) leads to a minimum time interval, in which only one error detected by the safety code is allowed. If such a mechanism is not used, the safe fall back state must be entered immediately after the first detected error if no other measures against possible error conditions are introduced.

The maximum probability for undetected errors of the safety code with c digits shall be estimated as

$$p_{US} = 2^{-c}$$

This formula can be used as a rough estimation of the probability of undetected faults. This is valid for a large class of codes (e.g. BCH-codes, cryptographic codes, ...) under realistic assumptions. Nevertheless, it has to be demonstrated that the properness[6] of the chosen code is fulfilled.

By repeating each message and checking the consistency of two mutually independent messages, the value of c can be halved at least. In fact, one can gain some further improvement, but in order to avoid intricate mathematical calculations, the given pessimistic estimation should be the limit.

———————

6 Properness means that the relation between bit error probability and probability of undetected error is monotone.

Standards Survey

The IEC would like to offer you the best quality standards possible. To make sure that we continue to meet your needs, your feedback is essential. Would you please take a minute to answer the questions overleaf and fax them to us at +41 22 919 03 00 or mail them to the address below. Thank you!

Customer Service Centre (CSC)

International Electrotechnical Commission
3, rue de Varembé
1211 Genève 20
Switzerland

or

Fax to: **IEC**/CSC at +41 22 919 03 00

Thank you for your contribution to the standards-making process.

Nicht frankieren
Ne pas affranchir

Non affrancare
No stamp required

A Prioritaire

RÉPONSE PAYÉE

SUISSE

Customer Service Centre (CSC)
International Electrotechnical Commission
3, rue de Varembé
1211 GENEVA 20
Switzerland

Q1 Please report on **ONE STANDARD** and **ONE STANDARD ONLY**. Enter the exact number of the standard: *(e.g. 60601-1-1)*

.....

Q2 Please tell us in what capacity(ies) you bought the standard *(tick all that apply).* I am the/a:

purchasing agent ❑
librarian ❑
researcher ❑
design engineer ❑
safety engineer ❑
testing engineer ❑
marketing specialist ❑
other.....

Q3 I work for/in/as a: *(tick all that apply)*

manufacturing ❑
consultant ❑
government ❑
test/certification facility ❑
public utility ❑
education ❑
military ❑
other.....

Q4 This standard will be used for: *(tick all that apply)*

general reference ❑
product research ❑
product design/development ❑
specifications ❑
tenders ❑
quality assessment ❑
certification ❑
technical documentation ❑
thesis ❑
manufacturing ❑
other.....

Q5 This standard meets my needs: *(tick one)*

not at all ❑
nearly ❑
fairly well ❑
exactly ❑

Q6 If you ticked NOT AT ALL in Question 5 the reason is: *(tick all that apply)*

standard is out of date ❑
standard is incomplete ❑
standard is too academic ❑
standard is too superficial ❑
title is misleading ❑
I made the wrong choice ❑
other .....

Q7 Please assess the standard in the following categories, using the numbers:
(1) unacceptable,
(2) below average,
(3) average,
(4) above average,
(5) exceptional,
(6) not applicable

timeliness.....
quality of writing.....
technical contents.....
logic of arrangement of contents .....
tables, charts, graphs, figures.....
other .....

Q8 I read/use the: *(tick one)*

French text only ❑
English text only ❑
both English and French texts ❑

Q9 Please share any comment on any aspect of the IEC that you would like us to know:

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

Enquête sur les normes

La CEI ambitionne de vous offrir les meilleures normes possibles. Pour nous assurer que nous continuons à répondre à votre attente, nous avons besoin de quelques renseignements de votre part. Nous vous demandons simplement de consacrer un instant pour répondre au questionnaire ci-après et de nous le retourner par fax au +41 22 919 03 00 ou par courrier à l'adresse ci-dessous. Merci !

Centre du Service Clientèle (CSC)

Commission Electrotechnique Internationale
3, rue de Varembé
1211 Genève 20
Suisse

ou

Télécopie: **CEI**/CSC +41 22 919 03 00

Nous vous remercions de la contribution que vous voudrez bien apporter ainsi à la Normalisation Internationale.

Nicht frankieren
Ne pas affranchir

Non affrancare
No stamp required

A Prioritaire

RÉPONSE PAYÉE

SUISSE

Centre du Service Clientèle (CSC)
Commission Electrotechnique Internationale
3, rue de Varembé
1211 GENÈVE 20
Suisse

Q1 Veuillez ne mentionner qu'**UNE SEULE NORME** et indiquer son numéro exact: (*ex. 60601-1-1)*

.....

Q2 En tant qu'acheteur de cette norme, quelle est votre fonction?
(cochez tout ce qui convient)
Je suis le/un:

agent d'un service d'achat ❑
bibliothécaire ❑
chercheur ❑
ingénieur concepteur ❑
ingénieur sécurité ❑
ingénieur d'essais ❑
spécialiste en marketing ❑
autre(s).....

Q3 Je travaille:
(cochez tout ce qui convient)

dans l'industrie ❑
comme consultant ❑
pour un gouvernement ❑
pour un organisme d'essais/ certification ❑
dans un service public ❑
dans l'enseignement ❑
comme militaire ❑
autre(s).....

Q4 Cette norme sera utilisée pour/comme
(cochez tout ce qui convient)

ouvrage de référence ❑
une recherche de produit ❑
une étude/développement de produit ❑
des spécifications ❑
des soumissions ❑
une évaluation de la qualité ❑
une certification ❑
une documentation technique ❑
une thèse ❑
la fabrication ❑
autre(s).....

Q5 Cette norme répond-elle à vos besoins:
(une seule réponse)

pas du tout ❑
à peu près ❑
assez bien ❑
parfaitement ❑

Q6 Si vous avez répondu PAS DU TOUT à Q5, c'est pour la/les raison(s) suivantes:
(cochez tout ce qui convient)

la norme a besoin d'être révisée ❑
la norme est incomplète ❑
la norme est trop théorique ❑
la norme est trop superficielle ❑
le titre est équivoque ❑
je n'ai pas fait le bon choix ❑
autre(s) .....

Q7 Veuillez évaluer chacun des critères ci-dessous en utilisant les chiffres
(1) inacceptable,
(2) au-dessous de la moyenne,
(3) moyen,
(4) au-dessus de la moyenne,
(5) exceptionnel,
(6) sans objet

publication en temps opportun .....
qualité de la rédaction.....
contenu technique .....
disposition logique du contenu .....
tableaux, diagrammes, graphiques, figures.....
autre(s) .....

Q8 Je lis/utilise: *(une seule réponse)*

uniquement le texte français ❑
uniquement le texte anglais ❑
les textes anglais et français ❑

Q9 Veuillez nous faire part de vos observations éventuelles sur la CEI:

.....
.....
.....
.....
.....
.....

ISBN 2-8318-6678-2

ICS 45.060

Typeset and printed by the IEC Central Office
GENEVA, SWITZERLAND