# NORME INTERNATIONALE

# INTERNATIONAL STANDARD

**CEI**
**IEC**
**62280-2**

Première édition
First edition
2002-10

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

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

# Railway applications – Communication, signalling and processing systems –

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

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

## Numérotation des publications

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

## Editions consolidées

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

## Informations supplémentaires sur les publications de la CEI

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

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

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

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

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

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

## Publication numbering

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

## Consolidated editions

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

## Further information on IEC publications

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

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

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

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

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

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

.

# NORME INTERNATIONALE

# INTERNATIONAL STANDARD

**CEI**
**IEC**
**62280-2**

Première édition
First edition
2002-10

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

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

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

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



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

Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

CODE PRIX
PRICE CODE X

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

# SOMMAIRE

# CONTENTS

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

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

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

## AVANT-PROPOS

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

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

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

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

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

Cette norme est étroitement liée à la CEI 62280-1[1] et à la norme ENV 50129:1998.

[1] A publier.

INTERNATIONAL ELECTROTECHNICAL COMMISSION

# RAILWAY APPLICATIONS – COMMUNICATION, SIGNALLING AND PROCESSING SYSTEMS –

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

## FOREWORD

1) The IEC (International Electrotechnical Commission) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of the IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, the IEC publishes International Standards. Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. The IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of the IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested National Committees.
3) The documents produced have the form of recommendations for international use and are published in the form of standards, technical specifications, technical reports or guides and they are accepted by the National Committees in that sense.
4) In order to promote international unification, IEC National Committees undertake to apply IEC International Standards transparently to the maximum extent possible in their national and regional standards. Any divergence between the IEC Standard and the corresponding national or regional standard shall be clearly indicated in the latter.
5) The IEC provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with one of its standards.
6) Attention is drawn to the possibility that some of the elements of this International Standard may be the subject of patent rights. The IEC shall not be held responsible for identifying any or all such patent rights.

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

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

| FDIS | Report on voting |
|---|---|
| 9/697/FDIS | 9/708/RVD |

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

This standard is in closely related to IEC 62280-1[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

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

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

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

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

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

# INTRODUCTION

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

The safety requirements for a data communication system depend on its characteristics which can be known or not. In order to reduce the complexity of the approach to demonstrate the safety of the system two classes of transmission systems have been considered. The first class consists of the ones over which the safety system designer has some degree of control. It is the case of the closed transmission systems whose safety requirements are defined in IEC 62280-1. The second class, named open transmission system, consists of all the systems whose characteristics are unknown or partly unknown. This part of IEC 62280 defines the safety requirements addressed to the transmission through open transmission systems.

The transmission system, which is considered in this standard, has in general no particular preconditions to satisfy. It is from the safety point of view not or not fully trusted and is considered as a ”black box”.

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

*Cross-acceptance*, aimed at generic approval and not at specific applications, is required in the same way as for ENV 50129 .

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

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

## 1 Domaine d'application

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

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

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

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

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

Cette norme ne spécifie pas

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

## 2 Références normatives

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

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

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

---

2 A publier.

# RAILWAY APPLICATIONS – COMMUNICATION, SIGNALLING AND PROCESSING SYSTEMS –

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

## 1 Scope

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

This standard is applicable to the safety requirement specification of the safety-related equipment, connected to the open transmission system, in order to obtain the allocated safety integrity level.

The properties and behaviour of the open transmission system are only used for the definition of the performance, but not for safety. Therefore, from the safety point of view, the open transmission system can potentially have any property, as various transmission ways, storage of messages, unauthorized access, etc. The safety process shall only rely on properties, which are demonstrated in the safety case.

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

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

This standard does not specify

– the open transmission system,
– equipment connected to the open transmission system,
– solutions (e.g. for interoperability),
– which kinds of data are safety-related and which are not.

## 2 Normative references

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

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

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

---

2 To be published.

## 3 Définitions

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

**3.1**
**protection d'accès**
processus conçus pour empêcher un *accès non autorisé* de lire ou de modifier de l'*information*, soit dans les *systèmes de sécurité*, soit dans le *système de transmission*

**3.1.1**
**hacker**
personne essayant de shunter délibérément une *protection d'accès*

**3.2**
**authenticité**
état dans lequel une *information* est *reconnue comme valide* et originaire d'une source déclarée

**3.3**
**autorisation**
droit formel d'utiliser un produit/service à l'intérieur de contraintes d'application spécifiées

**3.3.1**
**accès non autorisé**
situation dans laquelle des personnes non autorisées ou des *hackers* ont accès à de *l'information utilisateur* ou à de l'*information* dans le *système de transmission*

**3.3.2**
**confidentialité**
propriété de non-mise à disposition de l'*information* à des entités non autorisées

**3.4**
**contrôle**
processus destiné à accroître l'assurance de l'état d'un système

**3.4.1**
**contrôle de redondance**
type de contrôle de l'existence d'une relation prédéfinie entre la redondance et les données utilisateur au sein d'un *message*, pour prouver l'*intégrité* du message

**3.5**
**techniques cryptographiques**
les données de sortie sont calculées au moyen d'un algorithme utilisant les données d'entrée et une clé comme paramètre. Connaissant les données de sortie, il est impossible de calculer les données d'entrée dans un délai raisonnable sans connaître la clé. Il est également impossible de déduire la clé des données de sorties dans un délai raisonnable, même si les données d'entrée sont connues

**3.6**
**données**
partie d'un *message* qui représente de l'*information*

**3.6.1**
**corruption de données**
altération de données

## 3 Definitions

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

**3.1**
**access protection**
processes designed to prevent *unauthorized* access to read or to alter *information*, either within user *safety-related* systems or within the *transmission system*

**3.1.1**
**hacker**
a person trying deliberately to bypass *access protection*

**3.2**
**authenticity**
the state in which *information* is *valid* and known to have originated from the stated source

**3.3**
**authorization**
the formal permission to use a product/service within specified application constraints

**3.3.1**
**unauthorized access**
a situation in which *user information* or *information* within the *transmission system* is accessed by unauthorized persons or *hackers*

**3.3.2**
**confidentiality**
the property that *information* is not made available to unauthorized entities

**3.4**
**check**
a process to increase assurance about the state of a system

**3.4.1**
**redundancy check**
a type of check that a predefined relationship exists between redundant data and user data within a *message*, to prove message *integrity*

**3.5**
**cryptographic techniques**
output data are calculated by an algorithm using input data and a key as a parameter. By knowing the output data, it is impossible within a reasonable time to calculate the input data without knowledge of the key. It is also impossible within a reasonable time to derive the key from the output data, even if the input data are known

**3.6**
**data**
a part of a *message* which represents some *information*

**3.6.1**
**data corruption**
the alteration of data

**3.6.2**
**données utilisateur**
données représentant les états ou événements d'un *processus utilisateur*, sans *données additionnelles*. Dans le cas d'une communication entre des équipements de sécurité, les données utilisateur contiennent des données de sécurité

**3.6.3**
**données additionnelles**
données inutiles pour les *processus utilisateur* finals, mais utilisées à des fins de contrôle, de disponibilité et de sécurité

**3.6.4**
**données redondantes**
*données additionnelles* dérivées des *données utilisateur*, par un processus de transmission de sécurité

**3.6.4.1**
**code de sécurité**
données redondantes incluses dans un *message de sécurité* afin de détecter la corruption des données par un *processus de transmission de sécurité*. Des techniques de codage adéquates peuvent comprendre:

**3.6.4.1.1**
**code de sécurité non cryptographique**
données redondantes, basées sur des fonctions non cryptographiques, incluses dans un *message de sécurité*, afin de rendre possible la détection de la corruption des données, par un *processus de transmission de sécurité*

**3.6.4.1.1.1**
**contrôle de redondance cyclique (CRC)**
le CRC est basé sur des codes cycliques et est utilisé pour protéger les messages de l'influence de la corruption des données

**3.6.4.1.2**
**code de sécurité cryptographique**
données redondantes, basées sur des fonctions cryptographiques, incluses dans un *message de sécurité*, afin de rendre possible la détection de la corruption des données et de l'accès non autorisé, par un *processus de transmission de sécurité*

**3.6.4.1.2.1**
**code d'authentification de message (MAC)**
une fonction *cryptographique* de tout le message et d'une clé secrète ou publique. Par tout le message, on comprend également toute donnée implicite du message qui n'est pas envoyé au système de transmission

**3.6.4.1.2.2**
**code de détection de manipulation (MDC)**
une fonction de tout le message, mais, par opposition au MAC, aucune clé secrète n'est impliquée. Par tout le message, on comprend également toute donnée implicite du message qui n'est pas envoyé au système de transmission. Le MDC est souvent basé sur une fonction de brouillage

**3.6.4.2**
**numéro de séquence**
un champ de donnée additionnel contenant un nombre qui varie d'une manière prédéfinie de *message* à message

**3.6.2**
**user data**
data which represents the states or events of a *user process*, without any *additional data*. In case of communication between safety-related equipment, the user data contains safety-related data

**3.6.3**
**additional data**
data which is not of any use to the ultimate *user processes*, but is used for control, availability, and safety purposes

**3.6.4**
**redundant data**
*additional data*, derived, by a safety-related transmission process, from the *user data*

**3.6.4.1**
**safety code**
redundant data included in a *safety-related message* to permit data corruptions to be detected by the *safety-related* transmission *process*. Suitable encoding techniques may include:

**3.6.4.1.1**
**non-cryptographic safety code**
redundant data based on non-cryptographic functions included in a *safety-related message* to permit data corruptions to be detected by the *safety-related transmission process*

**3.6.4.1.1.1**
**cyclic redundancy check (CRC)**
the CRC is based on cyclic codes, and is used to protect messages from the influence of data corruptions

**3.6.4.1.2**
**cryptographic safety code**
redundant data based on cryptographic functions included in a *safety-related message* to permit data corruptions and unauthorized access to be detected by the *safety-related transmission process*

**3.6.4.1.2.1**
**message authentication code (MAC)**
a *cryptographic* function of the whole message and a secret or public key. By the whole message is meant also any implicit data of the message which is not sent to the transmission system

**3.6.4.1.2.2**
**manipulation detection code (MDC)**
a function of the whole message, but in contrast to a *MAC* there is no secret key involved. By the whole message is meant also any implicit data of the message which is not sent to the transmission system. The MDC is often based on a hash function

**3.6.4.2**
**sequence number**
an additional data field containing a number that changes in a predefined way from *message* to message

**3.6.4.3**
**datation**
la date est une information attachée à un *message* par l'émetteur

**3.6.4.3.1**
**date relative**
date référencée par rapport à l'horloge locale d'une entité. En général, il n'y a pas de relation avec les horloges des autres entités

**3.6.4.3.2**
**date absolue**
date référencée par rapport à un temps global, commun à un groupe d'entités utilisant un réseau de transmission

**3.6.4.3.3**
**date double**
cas où deux entités échangent et comparent leurs dates. Dans ce cas, les dates des entités sont indépendantes entre elles

**3.6.4.3.4**
**identificateurs de source et de destination**
un identificateur est assigné à chaque entité. L'identificateur peut être un nom, un nombre ou un motif de bits arbitraire. L'identificateur sera utilisé pour une transmission de sécurité. L'identificateur est rajouté d'habitude aux données utilisateur

**3.7**
**défense**
mesure introduite dans la conception du système de communications de sécurité pour contrer des *menaces* particulières

**3.8**
**erreur**
écart par rapport à la conception prévue qui pourrait se traduire par un comportement non prévu du système ou par une *défaillance*

**3.9**
**défaillance**
écart par rapport à la performance spécifiée d'un système. Une défaillance est la conséquence d'une *faute* ou d'une *erreur* dans un système

**3.9.1**
**défaillance aléatoire**
une *défaillance* qui se produit aléatoirement dans le temps

**3.9.2**
**défaillance systématique**
une *défaillance* d'occurrence répétitive moyennant des combinaisons particulières d'entrée ou des conditions particulières d'environnement

**3.10**
**faute**
condition anormale qui pourrait conduire à une *erreur* dans un système. Une faute peut être aléatoire ou systématique

**3.10.1**
**faute aléatoire**
occurrence d'une faute basée sur la théorie des probabilités et les performances antérieures

**3.6.4.3**
**time stamp**
information attached to a *message* by the sender

**3.6.4.3.1**
**relative time stamp**
a time stamp referenced to the local clock of an entity is defined as a relative time stamp. In general, there is no relationship to clocks of other entities

**3.6.4.3.2**
**absolute time stamp**
a time stamp referenced to a global time which is common for a group of entities using a transmission network is defined as an absolute time stamp

**3.6.4.3.3**
**double time stamp**
when two entities exchange and compare their time stamps, this is called double time stamp. In this case, the time stamps in the entities are independent of each other

**3.6.4.3.4**
**source and destination identifier**
an identifier is assigned to each entity. This identifier can be a name, number or arbitrary bit pattern. This identifier will be used for the safety-related transmission. Usually the identifier is added to the user data

**3.7**
**defence**
a measure incorporated in the design of a safety communication system to counter particular *threats*

**3.8**
**error**
a deviation from the intended design which could result in unintended system behaviour or *failure*

**3.9**
**failure**
a deviation from the specified performance of a system. A failure is the consequence of an *fault* or *error* in the system

**3.9.1**
**random failure**
a *failure* that occurs randomly in time

**3.9.2**
**systematic failure**
a *failure* that occurs repeatedly under some particular combination of inputs, or under some particular environmental condition

**3.10**
**fault**
an abnormal condition that could lead to an *error* in a system. A fault can be random or systematic

**3.10.1**
**random fault**
the occurrence of a fault based on probability theory and previous performance

**3.10.2**
**faute systématique**
faute inhérente à la spécification, la conception, la construction, l'installation, le fonctionnement ou la maintenance d'un système, sous-système ou équipement

**3.11**
**danger**
condition pouvant conduire à un accident

**3.11.1**
**analyse des dangers**
processus d'identification des dangers que peut causer un produit ou son utilisation

**3.12**
**information**
une représentation de l'état ou des événements d'un *processus*, dans une forme compréhensible par le processus

**3.13**
**intégrité**
état dans lequel une *information* est complète et non altérée

**3.14**
**message**
*information* transmise d'un émetteur (source de données) vers un ou plusieurs récepteurs (puits de données)

**3.14.1**
**message valide**
message satisfaisant dans sa forme à toutes les spécifications de l'utilisateur

**3.14.2**
**intégrité du message**
message dans lequel l'*information* est complète et non altérée

**3.14.3**
**message authentique**
message dont l'*information* est reconnue provenir de la source indiquée

**3.14.4**
**flux de messages**
suite ordonnée de messages

**3.14.5**
**cryptage de message**
transformation de bits en appliquant une *technique de cryptage* à un message, suivant un algorithme piloté par clés, afin de rendre plus difficile une lecture fortuite des *données*. Ne protège pas contre la corruption des données

**3.14.6**
**message en retour**
réponse d'un récepteur à l'émetteur, via un canal de transmission en retour

**3.14.7**
**traitement de message**
*processus* non directement contrôlés par l'utilisateur, impliqués dans le flux de messages entre participants

**3.10.2**
**systematic fault**
an inherent fault in the specification, design, construction, installation, operation or maintenance of a system, subsystem or equipment

**3.11**
**hazard**
a condition that can lead to an accident

**3.11.1**
**hazard analysis**
the process of identifying the hazards which a product or its use can cause

**3.12**
**information**
a representation of the state or events of a *process*, in a form understood by the process

**3.13**
**integrity**
the state in which *information* is complete and not altered

**3.14**
**message**
*information*, which is transmitted from a sender (data source) to one or more receivers (data sink)

**3.14.1**
**valid message**
a message whose form meets in all respects the specified user requirements

**3.14.2**
**message integrity**
a message in which *information* is complete and not altered

**3.14.3**
**authentic message**
a message in which *information* is known to have originated from the stated source

**3.14.4**
**message stream**
an ordered set of messages

**3.14.5**
**message enciphering**
transformation of bits by using a *cryptographic technique* within a message, in accordance with an algorithm controlled by keys, to render casual reading of *data* more difficult. Does not provide protection against data corruption

**3.14.6**
**feedback message**
a feedback message is defined as a response from a receiver to the sender, via a return transmission channel

**3.14.7**
**message handling**
the *processes*, outside the direct control of the user, which are involved in the transmission of the message stream between participants

**3.14.8**
**erreurs de message**
ensemble de tous les modes de *défaillance* de message possibles, pouvant conduire à des situations potentiellement dangereuses ou à une réduction de la disponibilité du système. Plusieurs causes peuvent être associées à un type d'*erreur* donné

**3.14.8.1**
**répétition de message**
type d'erreur de message dans lequel un message unique est reçu plus d'une fois

**3.14.8.2**
**suppression de message**
type d'erreur de message dans lequel un message est retiré d'un flux de messages

**3.14.8.3**
**insertion de message**
type d'erreur de message dans lequel un message est ajouté dans le flux de messages

**3.14.8.4**
**reséquencement de messages**
type d'erreur de message dans lequel l'ordre des messages est modifié dans le flux de messages

**3.14.8.5**
**corruption de message**
type d'erreur de message dans lequel se produit une altération des données

**3.14.8.6**
**retard de message**
type d'erreur de message dans lequel un message est reçu plus tard que prévu

**3.14.8.7**
**mascarade de message**
insertion d'un message non authentique, déguisé pour passer pour authentique

**3.15**
**processus**

**3.15.1**
**processus utilisateur**
processus d'une application contribuant directement au comportement spécifié par l'utilisateur du système

**3.15.2**
**processus de transmission**
processus d'une application contribuant uniquement à la transmission d'information entre les processus utilisateur et non aux processus utilisateur eux-mêmes

**3.15.3**
**processus de protection d'accès**
processus d'un système contribuant uniquement à la *protection d'accès* de l'information dans le système et non aux processus utilisateur ou aux processus de transmission eux-mêmes

**3.16**
**sécurité**
absence de niveau de risque inacceptable

**3.14.8**
**message errors**
a set of all possible message *failure* modes which can lead to potentially dangerous situations, or to reduction in system availability. There may be a number of causes of each type of *error*

**3.14.8.1**
**repeated message**
a type of message error in which a single message is received more than once

**3.14.8.2**
**deleted message**
a type of message error in which a message is removed from the message stream

**3.14.8.3**
**inserted message**
a type of message error in which an additional message is implanted in the message stream

**3.14.8.4**
**resequenced message**
a type of message error in which the order of messages in the message stream is changed

**3.14.8.5**
**corrupted message**
a type of message error in which a data corruption occurs

**3.14.8.6**
**delayed message**
a type of message error in which a message is received at a time later than intended

**3.14.8.7**
**masqueraded message**
a type of inserted message in which a non-authentic message is designed to appear to be authentic

**3.15**
**process**

**3.15.1**
**user process**
a process within an application that contributes directly to the behaviour specified by the user of the system

**3.15.2**
**transmission process**
a process, within an application, that contributes only to the transmission of information between user processes, and not to the user processes themselves

**3.15.3**
**access protection process**
a process within a system that contributes only to the *access protection* of information in the system, and not to the user processes or transmission processes themselves

**3.16**
**safety**
freedom from unacceptable levels of risk

**3.16.1**
**de sécurité**
porte la responsabilité de la sécurité

**3.16.2**
**niveau d'intégrité de sécurité**
une valeur indiquant le degré de confiance requis pour qu'un système atteigne les propriétés de sécurité spécifiées

**3.16.3**
**dossier de sécurité**
démonstration documentée qu'un produit satisfait aux exigences de sécurité spécifiées

**3.17**
**système de transmission**
service utilisé par une application pour transmettre des *flux de messages* entre des participants pouvant être des sources ou des puits d'information

**3.17.1**
**système de transmission fermé**
nombre fixe d'utilisateurs, ou à maximum fixé, reliés par un système de transmission à propriétés fixées et bien connues, où le risque *d'accès non autorisé* est considéré comme négligeable

**3.17.2**
**système de transmission ouvert**
système de transmission à nombre d'utilisateurs inconnu, ayant des propriétés non connues, variables et dans lesquelles on ne peut avoir confiance, utilisé pour des services de télécommunication inconnus et pour lequel le risque *d'accès non autorisé* doit être évalué

**3.18**
**menace**
violation potentielle de la *sécurité* incluant la *protection d'accès* d'un système de communications

**3.19**
**ponctualité**
état correspondant à une mise à disposition de l'*information* au bon moment conformément aux exigences

**3.20**
**validité**
état de satisfaction aux exigences spécifiées par l'utilisateur

**3.16.1**
**safety-related**
carries responsibility for safety

**3.16.2**
**safety integrity level**
a number which indicates the required degree of confidence that a system will meet its specified safety features

**3.16.3**
**safety case**
the documented demonstration that the product complies with the specified safety requirements

**3.17**
**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

**3.17.1**
**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

**3.17.2**
**open transmission system**
a transmission system with an unknown number of participants, having unknown, variable and non-trusted properties, used for unknown telecommunication services, and for which the risk of *unauthorized access* shall be assessed

**3.18**
**threat**
a potential violation of *safety* including *access protection* of a communication system

**3.19**
**timeliness**
the state in which *information* is available at the right time according to requirements

**3.20**
**validity**
the state of meeting, in all respects, the specified user requirements

## 4 Architecture de référence

L'architecture de référence d'un système de transmission de sécurité est basée sur

- le système de transmission non de sécurité, quels que soient les mécanismes internes de protection de la transmission incorporés;
- les fonctions de transmission de sécurité;
- les fonctions de protection d'accès de sécurité.

Dans le cadre de cette norme, le système de transmission ouvert est supposé constitué de tout (matériel, logiciel, media de transmission, etc.) ce qui peut se trouver entre deux ou plusieurs équipements de sécurité connectés au système de transmission.

Le système de transmission ouvert peut comporter tout ou partie des entités ci-après.

- Eléments lisant, stockant, traitant ou retransmettant des données produites et présentées par des utilisateurs du système de transmission, selon un programme inconnu de l'utilisateur. Le nombre d'utilisateurs est généralement inconnu. Des équipements de sécurité ou non de sécurité et des équipements non apparentés aux applications ferroviaires peuvent être raccordés au système de transmission ouvert.
- Média de transmission de n'importe quel type, de caractéristiques de transmission et de susceptibilité aux influences externes inconnues de l'utilisateur.
- Systèmes d'administration de réseaux capables de router (et de re-router dynamiquement) des messages via n'importe quel chemin constitué d'un ou de plusieurs média de transmission entre les extrémités du réseau de transmission ouvert, selon un programme inconnu de l'utilisateur.

Le système de transmission ouvert peut être influencé

- par d'autres utilisateurs du système de transmission, non connus du concepteur du système de commande et de protection, envoyant des quantités d'information inconnues dans des formats inconnus;
- par un utilisateur du réseau de transmission qui peut tenter d'accéder aux données provenant des autres utilisateurs, afin de les lire et/ou de les contrefaire sans autorisation du système d'exploitation;
- par n'importe quelle menace additionnelle à l'intégrité des données de sécurité.

Une structure de principe d'un système de sécurité s'appuyant sur un système de transmission ouvert est donnée à la figure 1. Le modèle de principe d'un message de sécurité est donnée à la figure 2.

Aucune exigence de sécurité ne doit s'appuyer sur les caractéristiques non sûres du système de transmission ouvert. Les aspects sécurité sont pris en charge en appliquant des procédures de sécurité et des codages de sécurité aux fonctions de transmission de sécurité.

## 4 Reference architecture

This reference architecture for a safety-related transmission system is based on

- the non-trusted transmission system, whatever internal transmission protection mechanisms are incorporated;
- the safety-related transmission functions;
- the safety-related access protection functions.

For the purposes of this standard, the open transmission system is assumed to consist of everything (hardware, software, transmission media, etc.) occurring between two or more safety-related equipment which are connected to the transmission system.

The open transmission system can contain some or all of the following.

- Elements which read, store, process or re-transmit data produced and presented by users of the transmission system in accordance with a program not known to the user. The number of users is generally unknown. Safety-related and non-safety-related equipment and equipment which is not related to railway applications can be connected to the open transmission system.
- Transmission media of any type with transmission characteristics and susceptibility to external influences which are unknown to the user.
- Network control and management systems capable of routing (and dynamically re-routing) messages via any path made up from one or more than one type of transmission media between the ends of the open transmission system, in accordance with a program not known to the user.

The open transmission system may be subject to the following:

- other users of the transmission system, not known to the control and protection system designer, sending unknown amounts of information, in unknown formats;
- user of the transmission system who may attempt to gain access to data originating from other users, in order to read it and/or mimic it without authorization from the system manager to do so;
- any kind of additional threats to the integrity of the safety-related data.

A principle structure of the safety-related system using an open transmission system is illustrated in Figure 1. The principle model of a safety-related message is shown in Figure 2.

No safety requirements shall be placed upon the non-trusted characteristics of the open transmission system. Safety aspects are covered by applying safety procedures and safety encoding to the safety-related transmission functions.

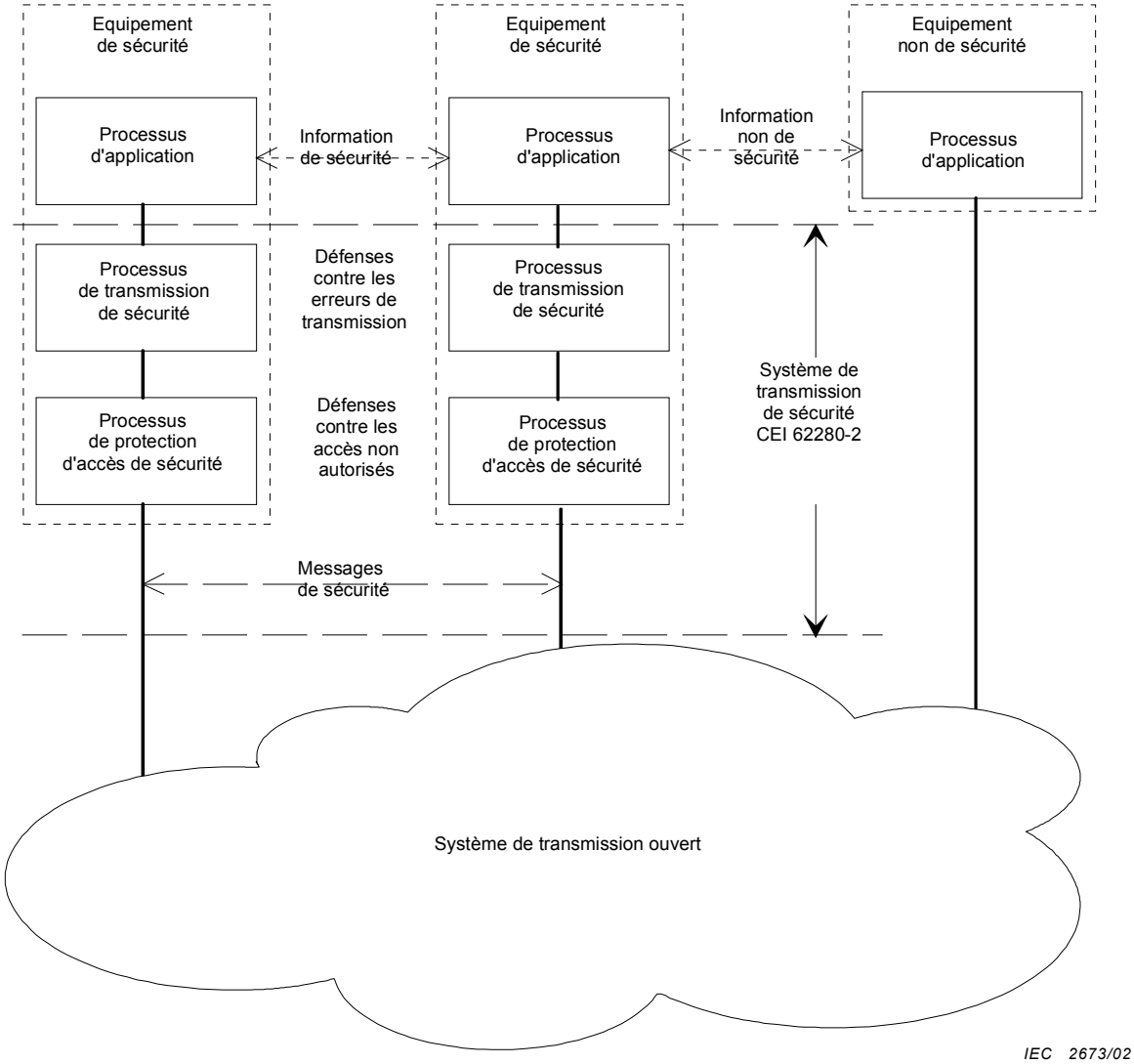



**Figure 1 – Structure d'un système de sécurité utilisant un système de transmission non de sécurité**

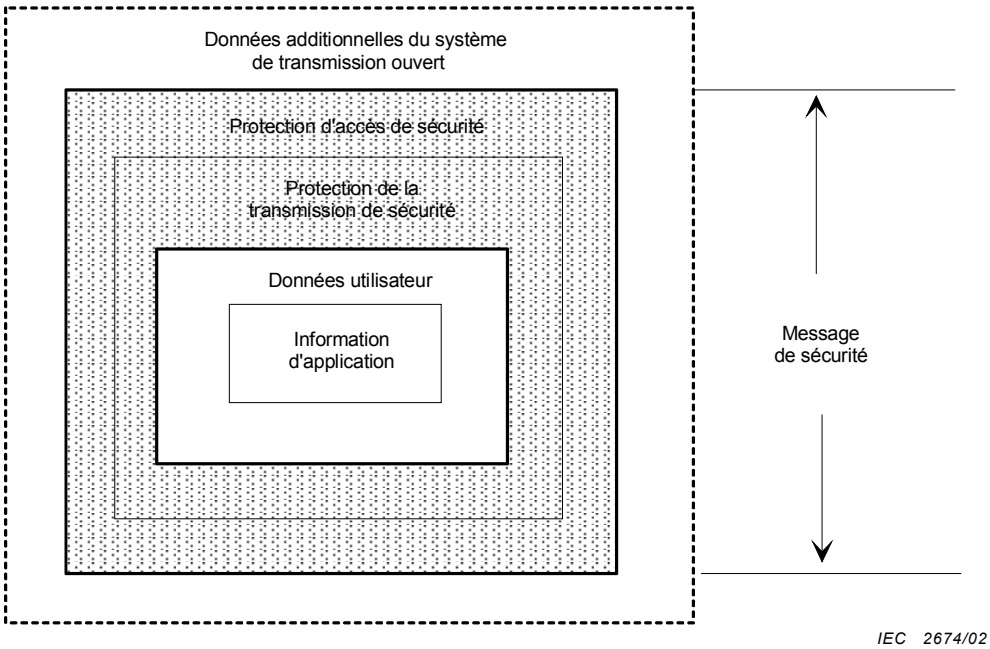



**Figure 2 – Modèle d'un message de sécurité**

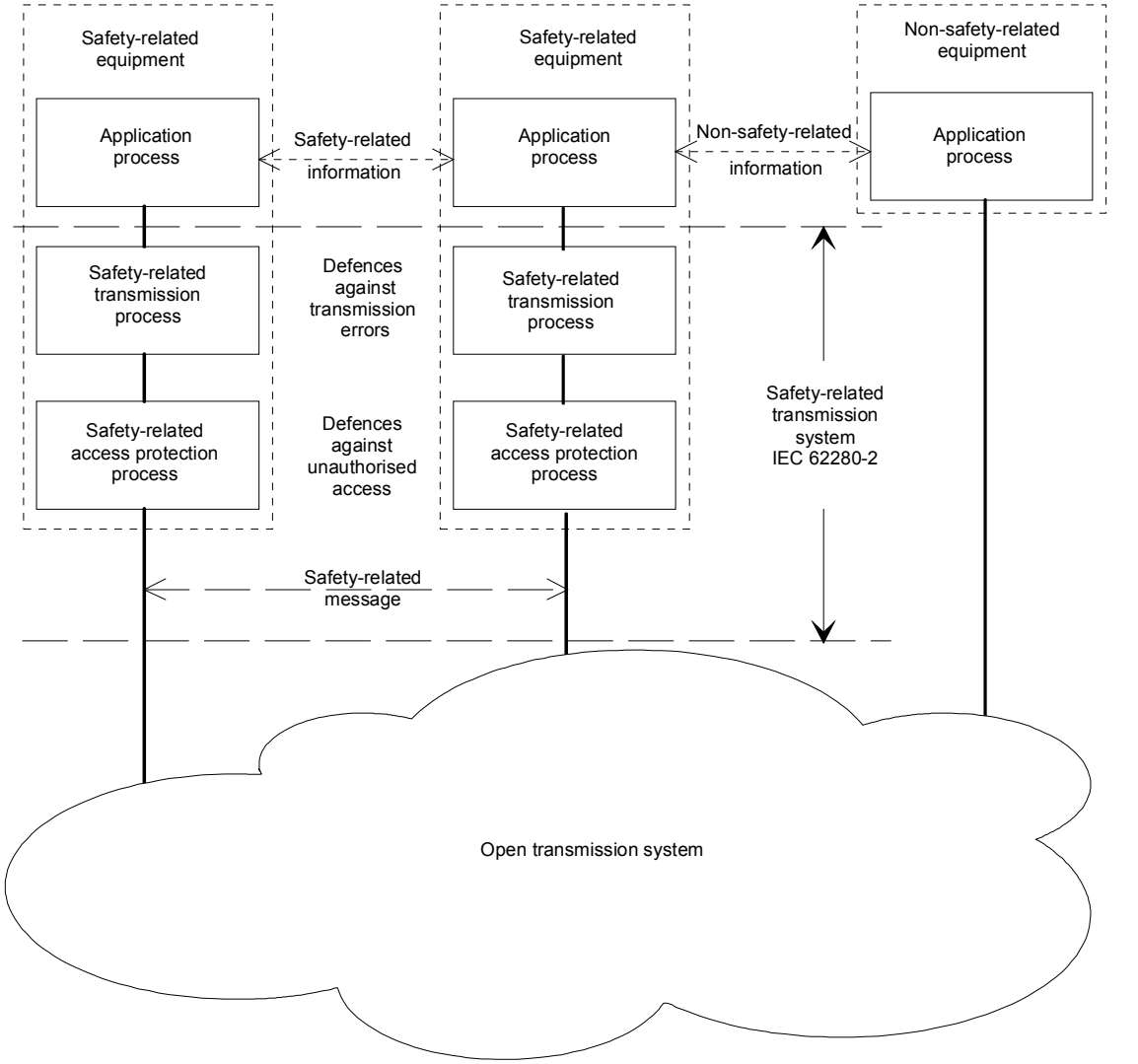



**Figure 1 – Structure of safety-related system using a non-trusted transmission system**

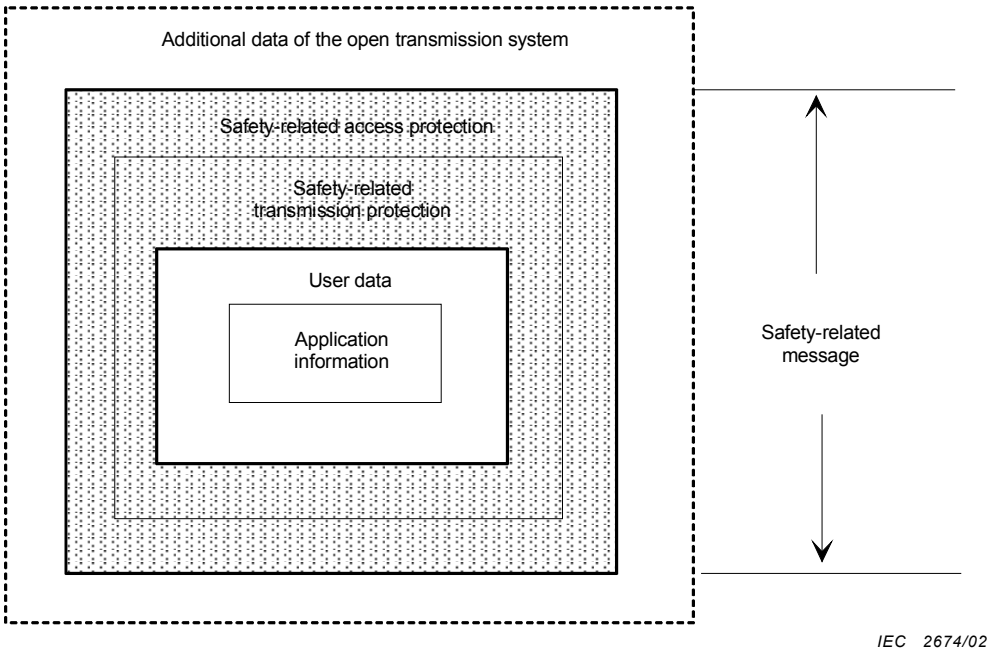



**Figure 2 – Model of a safety-related message**

## 5 Menaces sur le système de transmission

Ne sont considérées ici que les menaces relatives aux systèmes de transmission. Les menaces relatives aux systèmes de sécurité sont à traiter en conformité avec l'ENV 50129.

Cette norme se rapporte aux communications entre applications génériques utilisant un système de transmission dont les caractéristiques sont (au moins en partie) inconnues.

Aussi est-il nécessaire de définir un danger majeur pour la sécurité indépendamment de la fonctionnalité d'une application particulière et des caractéristiques du réseau; une définition pertinente est: *«Défaillance d'obtention d'un message authentique et valide à l'extrémité réceptrice».*

Un ensemble d'erreurs de message de base possibles a été défini dans l'annexe D.

Les menaces correspondantes sont les suivantes:

- répétition;
- suppression;
- insertion;
- reséquencement;
- corruption;
- retard;
- mascarade.

La satisfaction aux exigences de cette norme ne protège pas contre les usages abusifs volontaires ou involontaires en provenance de sources autorisées. Le dossier de sécurité doit traiter ces aspects.

## 6 Exigences en matière de défense

### 6.1 Introduction

Certaines techniques ont été adoptées par le passé dans les systèmes de transmission de données (de sécurité ou non). Elles constituent une «librairie» de méthodes possibles accessibles au concepteur du système de protection et de contrôle-commande, assurant la protection contre chaque menace identifiée ci-avant.

Ces techniques, qui peuvent être considérées comme des défenses logiques, ne constituent pas un ensemble exhaustif. De nouvelles techniques peuvent être développées dans le futur, elles offriraient ainsi de nouvelles possibilités au concepteur. De telles techniques peuvent être utilisées pour se protéger de ces menaces, sous réserve que leur domaine d'action ait été analysé et bien compris.

Pour réduire les risques associés aux menaces identifiées dans l'article précédent, les services de sécurité suivants doivent être pris en considération et fournis dans le mesure requise par l'application:

- authenticité du message;
- intégrité du message;
- ponctualité du message;
- séquence de messages.

## 5 Threats to the transmission system

Only threats to the transmission systems shall be considered. Threats to the safety-related equipment shall be considered in accordance with ENV 50129.

This standard refers to communications between generic applications using a transmission system whose characteristics are (at least partially) unknown.

It is, therefore, necessary to define a main hazard for safety independently from the functionality of the particular application and of the characteristics of the network; the pertinent definition is: ”*Failure to obtain an authentic (and consequently valid) message at the receiver end*”.

With reference to annex D, a set of possible basic message errors has been derived.

The corresponding threats are

- repetition;
- deletion;
- insertion;
- resequence;
- corruption;
- delay;
- masquerade.

Meeting the requirements of this standard does not give protection against intentional or unintentional misuse coming from authorized sources. The safety case shall address these aspects.

## 6 Requirements for defences

### 6.1 Introduction

Certain techniques have been adopted in data transmission systems (non-safety-related, safety-related) in the past. These techniques form a ”library” of possible methods accessible to the control and protection system designer, to provide protection against each threat identified above.

These techniques that can be seen as logical defences are not a complete set. New techniques may be developed in the future which offer new possibilities to the designer. Such new techniques may be used to provide protection against these threats, provided that the coverage of the techniques is well understood and has been analyzed.

To reduce the risk associated with the threats identified in the preceding clause, the following safety services shall be considered and provided to the extent needed for the application:

- message authenticity;
- message integrity;
- message timeliness;
- message sequence.

L'ensemble suivant de défenses connues a été mis en exergue:

a) numéro de séquence;
b) datation;
c) temps écoulé;
d) identificateurs de la source et de la destination;
e) message en retour;
f) procédure d'identification;
g) code de sécurité;
h) techniques cryptographiques.

### 6.2 Exigences générales

1) Des défenses adéquates sont à opposer à toutes les menaces identifiées contre la sécurité de systèmes utilisant des réseaux de communications ouverts. L'aval des autorités de tutelle en matière de sécurité et/ou des autorités ferroviaires est nécessaire pour les menaces non prises en considération. Ces dernières doivent être incluses dans les conditions d'application de sécurité. L'annexe D donne une liste de menaces possibles, à utiliser comme guide.
2) Les exigences particulières relatives aux défenses nécessaires à l'application doivent prendre en compte les points ci-après:
   – le niveau de risque (fréquence/conséquence) identifié pour chaque menace, et
   – le niveau d'intégrité de sécurité des données et processus concernés.

   L'annexe A guide la sélection des techniques courantes connues pour se protéger des menaces. Lors du choix de la défense, il faut considérer avec soin les résultats visés en terme d'efficacité indiqués dans cette annexe.
3) Les exigences relatives aux défenses doivent être incluses dans la spécification des exigences du système et dans la spécification des exigences de sécurité du système pour l'application. Elles doivent être une entrée de la partie «assurance d'un fonctionnement correct» du dossier de sécurité.
4) Toutes les défenses doivent être réalisées conformément aux exigences définis dans l'ENV 50129. Cela implique que les défenses
   – doivent être implantées entièrement dans l'équipement de transmission de sécurité du système, ou
   – peuvent inclure des mesures de protection d'accès non implantées dans l'équipement de sécurité. Dans ce cas, le fonctionnement correct permanent des processus de protection d'accès doit être vérifié au moyen de techniques de sécurité adéquates pour l'application.
5) Les exigences obligatoires pour des défenses particulières sont indiquées dans les paragraphes suivants. Elles s'appliquent lorsque la défense en question est utilisée.
6) Il est possible d'utiliser d'autres défenses que celles indiquées dans cette norme, sous réserve que l'analyse de leur efficacité contre les menaces soit incluse dans le dossier de sécurité.
7) Le dossier de sécurité, conformément à la description incluse dans l'ENV 50129, doit comporter
   – l'analyse de chaque défense utilisée dans le système de transmission de sécurité;
   – la réaction de sécurité en cas de détection d'une erreur de transmission.

The following set of known defences has been outlined:

a) sequence number;
b) time stamp;
c) time-out;
d) source and destination identifiers;
e) feedback message;
f) identification procedure;
g) safety code;
h) cryptographic techniques.

### 6.2 General requirements

1) Adequate defences shall be provided against all identified threats to the safety of systems using open communication networks. Any threats which are not to be assumed shall be agreed with the safety authority and/or railway authority and shall be put into the safety-related application conditions. Annex D derives a possible list of threats, to be used as guidance.
2) Detailed requirements for the defences needed for the application shall take into account
   – the level of risk (frequency/consequence) identified for each particular threat, and
   – the safety integrity level of the data and process concerned.

   Annex A (guidelines for defences) gives guidance on the selection of currently known techniques to give defence against threats. Issues of effectiveness addressed in this annex should be carefully considered when the defence is chosen.
3) The requirements for the defences needed shall be included in the system requirements specification and in the system safety requirements specification for the application, and shall form input to the ”assurance of correct operation” portion of the safety case for the application.
4) All defences shall be implemented according to the requirements defined in ENV 50129. This implies that the defences
   – shall be implemented completely within the safety-related transmission equipment of the system, or
   – may include access protection measures not implemented within the safety-related equipment. In this case, the continued correct functioning of the access protection processes shall be checked with adequate safety-related techniques for the application.
5) Mandatory requirements for particular defences are given in the following subclauses. They apply when the particular defence is used.
6) Other defences than those described in this standard may be used, provided that analysis of their effectiveness against threats is included in the safety case.
7) The safety case, as described in ENV 50129 shall include
   – analysis of each defence used in the safety transmission system,
   – the safety reaction in case of a detected transmission error.

### 6.3 Défenses spécifiques

Les paragraphes ci-après indiquent de courtes introductions et les exigences de défenses spécifiques, qui sont efficaces soit seules, soit en combinaison, contre une menace isolée ou une combinaison de menaces. Toutes les exigences générales listées ci-devant doivent être appliquées.

Une description plus détaillée des défenses et leurs relations avec toutes les menaces possibles fait l'objet de l'annexe A pour information (guide des défenses).

#### 6.3.1 Numéro de séquence

##### 6.3.1.1 Introduction

Numéroter une séquence consiste à ajouter un nombre courant (appelé numéro de séquence) à chaque message échangé entre un émetteur et un récepteur. Cela permet au récepteur de vérifier la séquence des messages provenant de l'émetteur.

##### 6.3.1.2 Exigences

Le dossier de sécurité doit faire la preuve de l'adéquation de la défense, en liaison avec le niveau d'intégrité de sécurité du processus et la nature du processus de sécurité:

- de la longueur du numéro de séquence;
- de la disposition prise pour initialiser le numéro de séquence;
- de la disposition prise pour réinitialiser après l'interruption de la séquence des messages.

#### 6.3.2 Datation

##### 6.3.2.1 Introduction

Lorsqu'une entité reçoit de l'information, la signification de l'information est souvent liée au temps. Le degré de dépendance entre l'information et le temps peut différer selon l'application. Selon le cas, une information ancienne peut être inutile et inoffensive ou constituer un danger potentiel pour l'utilisateur. La solution peut être différente selon le comportement temporel des processus qui échangent de l'information (cyclique, déclenché par un événement, etc.).

Une solution couvrant les relations temporelles est l'addition d'une date à l'information. Ce type d'information peut être utilisé en lieu et place ou en combinaison avec le numéro de séquence, selon les exigences de l'application. Différents exemples de datation et leurs propriétés sont indiqués à l'annexe A.

##### 6.3.2.2 Exigences

Le dossier de sécurité doit faire la preuve de l'adéquation de la défense, en liaison avec le niveau d'intégrité de sécurité du processus et la nature du processus de sécurité:

- de la valeur de l'incrément temporel;
- de la précision de l'incrément temporel;
- de la taille de la temporisation;
- de la valeur absolue de la temporisation (par exemple TUC – temps universel coordonné – ou de tout autre horloge globale);
- de la synchronisation des temporisations dans les différentes entités;
- du retard entre la création de l'information et l'addition de la date;
- du retard entre le contrôle de la date et l'utilisation de l'information.

### 6.3 Specific defences

The following subclauses show short introductions and the requirements for specific defences, which are effective either alone or in combination against single or combined threats. All general requirements listed above shall be applied.

More detailed descriptions of the defences and the relation with all possible threats are given in informative annex A (guidelines for defences).

#### 6.3.1 Sequence number

##### 6.3.1.1 Introduction

Sequence numbering consists of adding a running number (called sequence number) to each message exchanged between a transmitter and a receiver. This allows the receiver to check the sequence of messages provided by the transmitter.

##### 6.3.1.2 Requirements

The safety case shall demonstrate the appropriateness in relation to the safety integrity level of the process, and the nature of the safety-related process, of the following:

- the length of the sequence number;
- the provision for initialization of the sequence number;
- the provision for recovery following interruption of the sequence of the messages.

#### 6.3.2 Time stamp

##### 6.3.2.1 Introduction

When an entity receives information, the meaning of the information is often time related. The degree of dependence between information and time may differ between applications. In certain cases, old information can be useless and harmless and in other cases the information could be a potential danger for the user. Depending on the behaviour in time of the processes which interchange information (cyclic, event controlled etc.) the solution may differ.

One solution which covers time-information relationships is to add time stamps to the information. This kind of information can be used in place of or combined with sequence numbers depending on application requirements. Different uses of time stamps and their properties are shown in annex A.

##### 6.3.2.2 Requirements

The safety case shall demonstrate the appropriateness in relation to the safety integrity level of the process, and the nature of the safety-related process, of the following:

- the value of the time increment;
- the accuracy of the time increment;
- the size of the timer;
- the absolute value of the timer (e.g. UTC (universal co-ordinated time) or any other global clock);
- the synchronism of the timers in the various entities;
- the time delay between originating of information and adding a time stamp to it;
- the time delay between checking the time stamp and using the information.

### 6.3.3 Temps écoulé

#### 6.3.3.1 Introduction

Dans une transmission (typiquement cyclique), le récepteur peut vérifier si le délai entre deux messages dépasse une durée maximale prédéterminée. Si tel est le cas, on doit présumer une erreur.

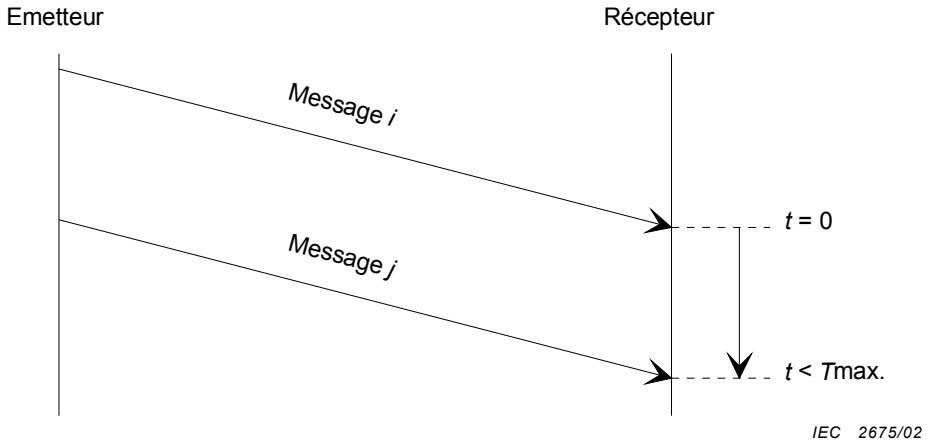



**Figure 3 – Transmission cyclique de messages**

Si un canal de retour est disponible, l'émetteur peut superviser la transmission. L'émetteur arme une temporisation lors de l'émission d'un message *i*. Le récepteur du message *i* répond avec un message d'acquittement *j* corrélé au message reçu *i*. Si l'émetteur ne reçoit pas le message d'acquittement correspondant *j* pendant une durée prédéfinie, on doit présumer une erreur.

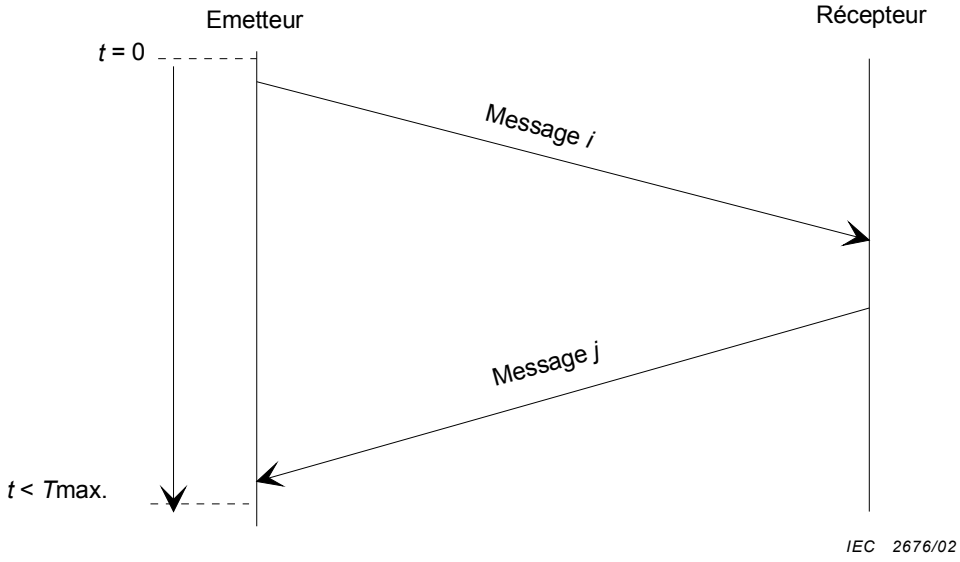



**Figure 4 – Transmission bidirectionnelle de messages**

#### 6.3.3.2 Exigences

Le dossier de sécurité doit faire la preuve de l'adéquation de la défense, en liaison avec le niveau d'intégrité de sécurité du processus et la nature du processus de sécurité:

- du délai acceptable;
- de la précision sur le temps écoulé.

### 6.3.3 Time-out

#### 6.3.3.1 Introduction

In transmission (typically cyclic) the receiver can check if the delay between two messages exceeds a predefined allowed maximum time. If this is the case, an error shall be assumed.

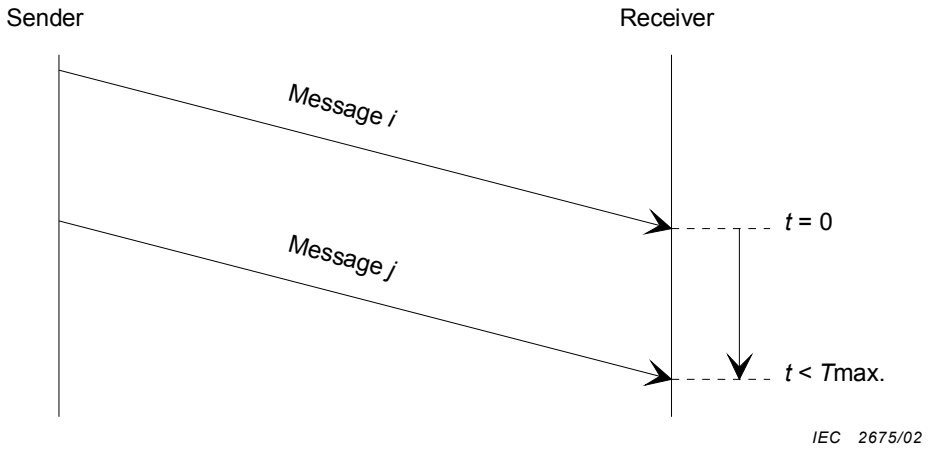



**Figure 3 – Cyclic transmission of messages**

If a back channel is available, supervision can be performed by the sender. The sender starts a timer when sending a message *i*. The receiver of message *i* responds with an acknowledge message *j* related to the received message *i*. If the sender does not receive the corresponding acknowledge message *j* within a predefined time, an error shall be assumed.

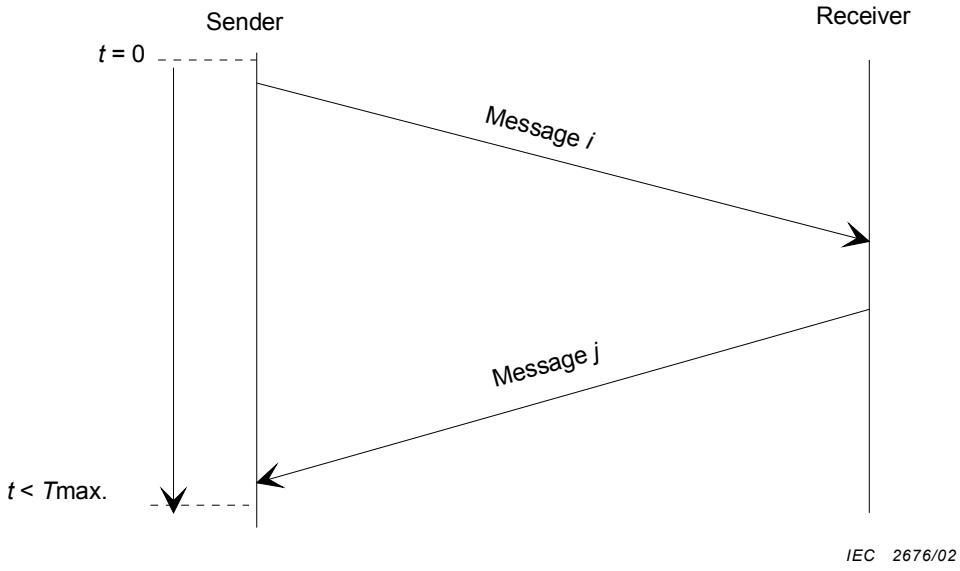



**Figure 4 – Bi-directional transmission of messages**

#### 6.3.3.2 Requirements

The safety case shall demonstrate the appropriateness in relation to the safety integrity level of the process and the nature of the safety-related process of the following:

- the acceptable delay;
- the accuracy of the time-out.

### 6.3.4 Identificateurs de la source et de la destination

#### 6.3.4.1 Introduction

Les processus mettant en jeu des communications entre plusieurs parties nécessitent des moyens adéquats pour contrôler la source de toute information reçue avant exploitation. Les messages doivent contenir des données additionnelles pour le permettre.

Les messages peuvent contenir un identificateur de source unique ou un identificateur de destination unique, ou les deux. Ces identificateurs sont ajoutés dans les fonctions de transmission de sécurité pour l'application.

- L'inclusion d'un identificateur de source dans les messages peut permettre aux utilisateurs de vérifier que les messages proviennent de la source voulue, sans nécessité de dialogue entre utilisateurs. Cela peut être utile, par exemple, dans les systèmes de communication unidirectionnels ou de diffusion.
- L'inclusion d'un identificateur de destination dans les messages peut permettre aux utilisateurs de vérifier que les messages leur sont adressés, sans nécessité de dialogue entre utilisateurs. Cela peut être utile, par exemple, dans les systèmes de communication unidirectionnels ou de diffusion. Les identificateurs de destination peuvent être choisis pour des destinataires individuels ou des groupes d'usagers.

#### 6.3.4.2 Exigences

Le dossier de sécurité doit faire la preuve de l'adéquation de la défense, en liaison avec le niveau d'intégrité de sécurité du processus et la nature du processus de sécurité:

- de l'unicité des identificateurs des entités pour tout le système de transmission;
- de la taille du champ de données de l'identificateur.

### 6.3.5 Message en retour

#### 6.3.5.1 Introduction

Lorsqu'un canal de transmission adéquat est disponible, un message en retour peut être envoyé par le destinataire de l'information de sécurité vers l'émetteur. Le contenu du message en retour doit inclure

- des données dérivées du contenu du message d'origine, identiques ou modifiées;
- des données ajoutées par le destinataire, dérivées de l'information de son propre processus utilisateur local;
- des données additionnelles à des fins de sécurité ou de sûreté.

L'utilisation d'un tel message en retour peut contribuer à la sécurité du processus de différente manière:

- en fournissant une confirmation positive de la réception de messages valides et opportuns;
- en fournissant une confirmation positive de la réception de messages altérés, afin de prendre une action adéquate;
- en confirmant l'identité de l'équipement récepteur;
- en facilitant la synchronisation des horloges des équipements émetteurs et récepteurs;
- en rendant les procédures de vérification dynamique entre parties plus faciles;
- etc.

### 6.3.4 Source and destination identifiers

#### 6.3.4.1 Introduction

Multi-party communication processes need adequate means for checking the source of all information received, before it is used. Messages shall include additional data to permit this.

Messages may contain a unique source identifier, or a unique destination identifier, or both. The choice is made according to the safety-related application. These identifiers are added in the safety-related transmission functions for the application.

- Inclusion of a source identifier in messages can enable users of the messages to verify that messages are from the intended source, without the need for any dialogue between users. This can be useful, for example, in uni-directional or broadcast communication systems.
- Inclusion of a destination identifier in messages can enable users of the messages to verify that messages are intended for them, without the need for any dialogue between users. This can be useful, for example, in uni-directional or broadcast communication systems. Destination identifiers can be chosen to identify individual destinations, or groups of users.

#### 6.3.4.2 Requirements

The safety case shall demonstrate the appropriateness, in relation to the safety integrity level of the process and the nature of the safety-related process, of the following:

- the uniqueness of the identifiers for entities in the entire transmission system;
- the size of the identifier data field.

### 6.3.5 Feedback message

#### 6.3.5.1 Introduction

Where an appropriate transmission channel is available, a feedback message may be sent from the receiver of safety-critical information to the sender. The contents of this feedback message may include

- data derived from the contents of the original message, in identical or altered form;
- data added by the receiver, derived from its own local user process information;
- additional data for safety or security purposes.

The use of such a feedback message can contribute to the safety of the process in a variety of ways:

- by providing positive confirmation of reception of valid and timely messages;
- by providing positive confirmation of reception of corrupted messages, to enable appropriate action to be taken;
- by confirming the identity of the receiving equipment;
- by facilitating synchronization of clocks in sending and receiving equipment;
- by facilitating dynamic checking procedures between parties;
- etc.

#### 6.3.5.2 Exigences

L'existence d'un canal en retour ne fournit pas une défense intrinsèque contre une menace identifiée; il s'agit d'un mécanisme permettant d'autres défenses au niveau utilisateur. Il n'y a donc pas d'exigences de sécurité spécifiques pour un tel canal en retour.

### 6.3.6 Procédure d'identification

#### 6.3.6.1 Introduction

Le paragraphe précédent couvrait les exigences relatives aux entités à identifier.

Les réseaux de transmission ouverts peuvent en outre introduire le risque de messages d'autres utilisateurs (inconnus) pouvant être confondus avec l'information issue d'une source voulue (une forme de mascarade).

Une procédure d'identification de conception adéquate dans un processus de sécurité peut fournir une défense contre cette menace.

On peut distinguer deux types de procédure d'identification:

- identification bidirectionnelle

  Là où un canal de communications retour est disponible, l'échange des identificateurs entre émetteurs et récepteurs d'information peut fournir une assurance supplémentaire que la communication se fait bien entre les parties voulues;

- procédures d'identification dynamiques

  Un échange dynamique d'informations entre émetteurs et récepteurs, incluant la transformation et le retour de l'information reçue vers l'émetteur, peut fournir une assurance que les parties en communications non seulement affirment posséder la bonne identité mais encore se comportent de la manière attendue. Ce type de procédure d'identification dynamique peut être utilisé en préliminaire de la transmission d'information entre processus de sécurité communicants et/ou il peut être utilisé pendant la transmission d'information proprement dite.

#### 6.3.6.2 Exigences

Une procédure d'identification est une partie du processus de sécurité utilisateur. Les exigences détaillées doivent être définies dans la spécification des exigences de sécurité.

### 6.3.7 Code de sécurité

#### 6.3.7.1 Introduction

En général, dans un système de transmission ouvert, des codes de transmission sont utilisés pour la détection des erreurs bit et/ou trame et pour accroître la qualité de la transmission par des techniques de correction d'erreurs.

Le processus de sécurité ne doit pas faire confiance à des codes de transmission du point de vue de la sécurité. C'est pourquoi un code de sécurité additionnel est requis, sous le contrôle du processus de sécurité, pour détecter l'altération des messages.

#### 6.3.7.2 Exigences

Le dossier de sécurité doit faire la preuve de l'adéquation de la défense, en liaison avec le niveau d'intégrité de sécurité du processus et la nature du processus de sécurité:

- de l'aptitude à détecter les erreurs de tout type attendues;
- de la probabilité de détection d'un message altéré.

Un guide pour le choix des codes de sécurité est donné en annexe A.

#### 6.3.5.2 Requirements

The existence of a return channel does not intrinsically provide a defence against any identified threat; it is an enabling mechanism for other defences at the application level. Therefore, there are no specific safety requirements for such a feedback channel.

### 6.3.6 Identification procedure

#### 6.3.6.1 Introduction

The previous subclause covered the requirements for entities to be identified.

Open transmission systems may additionally introduce the risk of messages from other (unknown) users being confused with information originating from an intended source (a form of masquerade).

A suitably designed identification procedure within the safety-related process can provide a defence against this threat.

Two types of identification procedure can be distinguished:

- bi-directional identification

  Where a return communication channel is available, exchange of entity identifiers between senders and receivers of information can provide additional assurance that the communication is actually between the intended parties.

- dynamic identification procedures

  Dynamic exchange of information between senders and receivers, including transformation and feedback of received information to the sender, can provide assurance that the communicating parties not only claim to possess the correct identity, but also behave in the manner expected. This type of dynamic identification procedure can be used to preface the transmission of information between communicating safety-related processes and/or it can be used during the information transmission itself.

#### 6.3.6.2 Requirements

Identification procedure forms a part of the safety-related application process. The detailed requirements shall be defined in the safety requirement specification.

### 6.3.7 Safety code

#### 6.3.7.1 Introduction

In an open transmission system, in general, transmission codes are used to detect bit and/or burst errors, and to improve the transmission quality by error correction techniques.

The safety-related process shall not trust those transmission codes from the point of view of safety. Therefore, an additional safety code under the control of the safety-related process is required to detect message corruption.

#### 6.3.7.2 Requirements

The safety case shall demonstrate the appropriateness, in relation to the safety integrity level of the process and the nature of the safety-related process, of the following:

- the capability for detection of all expected types of errors;
- the probability of detection of message corruption.

Guidance for selection of safety codes is given in annex A.

### 6.3.8 Techniques cryptographiques

#### 6.3.8.1 Introduction

Les techniques cryptographiques sont utilisables si on ne peut exclure une attaque malveillante dans un réseau de transmission ouvert.

Cela est généralement le cas si le système de transmission de sécurité s'appuie sur

- un réseau public;
- un système de transmission radio;
- un système de transmission relié aux réseaux publics.

Ces techniques peuvent être combinées avec le mécanisme de codage de sécurité ou fournies séparément. L'annexe A montre quelques solutions possibles.

Les techniques cryptographiques impliquent l'usage de clés et d'algorithmes. Le degré d'efficacité est fonction de la puissance des algorithmes et du secret des clés. Le secret d'une clé dépend de sa longueur et de sa gestion.

#### 6.3.8.2 Exigences

Le dossier de sécurité doit faire la preuve de l'adéquation de la défense, en liaison avec le niveau d'intégrité de sécurité du processus et la nature du processus de sécurité:

- du choix technique des techniques cryptographiques, incluant:
  - la performance de l'algorithme de cryptage,
  - la justification de la longueur de la clé sélectionnée,
  - la fréquence du changement de clé,
  - le stockage physique des clés;
- des activités de gestion, incluant:
  - la génération, le stockage, la distribution et l'invalidation des clés confidentielles,
  - la gestion des équipements,
  - le processus de révision de l'adéquation des techniques cryptographiques, en liaison avec le risque d'attaque malveillante.

L'algorithme cryptographique doit s'appliquer à toutes les données utilisateur et peut être appliqué à des données additionnelles non transmises mais connues de la source et du destinataire (données implicites).

Des hypothèses raisonnables doivent être décrites quant à la nature, aux motivations, aux moyens financiers et techniques d'un attaquant potentiel, prenant également en compte des modifications susceptibles de se produire pendant la durée de vie du système (à la fois techniques, comme l'augmentation de la puissance des ordinateurs, la décroissance des coûts des processeurs rapides, la diffusion de la connaissance des algorithmes, et «sociaux» comme les conflits économiques, l'aggravation du vandalisme, ...).

Des techniques normalisées de gestion des clés sont hautement recommandées (par exemple selon l'ISO/IEC 11770).

### 6.3.8 Cryptographic techniques

#### 6.3.8.1 Introduction

Cryptographic techniques can be used if malicious attacks within the open transmission network cannot be ruled out.

This is usually the case when the safety-related transmission system uses a

- public network;
- radio transmission system;
- transmission system with connections to public networks.

These techniques can be combined with the safety encoding mechanism or provided separately. Annex A shows some possible solutions.

Cryptographic techniques imply the use of keys and algorithms. The degree of effectiveness depends on the strength of the algorithms and the secrecy of the keys. The secrecy of a key depends on its length and its management.

#### 6.3.8.2 Requirements

The safety case shall demonstrate the appropriateness, in relation to the safety integrity level of the process and the nature of the safety-related process, of the following:

- technical choice of cryptographic techniques, including
  - performance of encryption algorithm,
  - justification of selected key length,
  - frequency of key change,
  - physical storage of keys;
- management activities, including
  - production, storage, distribution and revocation of confidential keys,
  - management of equipment,
  - review process of adequacy of cryptographic techniques, in relation to risks of malicious attacks.

The cryptographic algorithm shall be applied to all user data and it may be applied over some additional data that is not transmitted but is known to the sender and receiver (implicit data).

Reasonable assumptions shall be described about nature, motivations, financial and technical means of potential attacker, taking into account also modifications (both technical, as increase of power of computers, decrease of costs of fast processors, spread of knowledge about algorithms, and ”social”, as economic conflicts, worsening of vandalism, ...) that can be expected during the life-time of the system.

For key management, standardized techniques are highly recommended (e.g. according to ISO/IEC 11770).

# 7 Applicabilité des défenses contre les menaces

## 7.1 Introduction

Les défenses présentées à l'article 6 peuvent être reliées à l'ensemble des menaces possibles définies à l'article 5. Chaque défense peut assurer une protection vis-à-vis d'une ou de plusieurs menaces de la transmission. Dans le dossier de sécurité, la preuve doit être faite qu'il y a au moins une défense ou combinaison de défenses pour l'ensemble des menaces possibles définies dans le tableau 1.

## 7.2 Matrice menaces/défenses

Les «X» dans le tableau 1 indiquent qu'une défense assure une protection contre la menace correspondante.

**Tableau 1 – Matrice menaces/défenses**

| Menaces | Défenses | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | Numéro de séquences | Datation | Temps écoulé | Identificateurs de la source et de la destination | Message en retour | Procédure d'identification | Code de sécurité | Techniques cryptographiques |
| Répétition | X | X | | | | | | |
| Suppression | X | | | | | | | |
| Insertion | X | | | X 2) | X 1) | X 1) | | |
| Reséquencement | X | X | | | | | | |
| Corruption | | | | | | | X 3) | X |
| Retard | | X | X | | | | | |
| Mascarade | | | | | X 1) | X 1) | | X 3) |

1) Dépend de l'application.

2) Uniquement applicable à l'identificateur de source.

Ne détecte qu'une insertion d'une source non valide.

S'il n'est pas possible de définir des identificateurs uniques du fait d'utilisateurs inconnus, il y a lieu d'utiliser une technique cryptographique, voir 6.3.8.

3) Voir 7.3 et l'article A.2.

## 7.3 Choix et utilisation du code de sécurité et des techniques cryptographiques

Le choix du code de sécurité et des techniques cryptographiques doit être fait en tenant compte

- de la possibilité d'avoir un accès autorisé ou non,
- du type de code cryptographique proposé,
- de la séparation ou non du processus de sécurité et du processus protection d'accès de sécurité.

Des conseils à ce sujet se trouvent à l'article A.2.

# 7 Applicability of defences against threats

## 7.1 Introduction

The defences outlined in clause 6 can be related to the set of possible threats, defined in clause 5. Each defence can provide protection against one or more threats to the transmission. In the safety case, it shall be demonstrated that there is at least one corresponding defence or combination of defences for the defined possible threats in accordance with Table 1.

## 7.2 Threats/defences matrix

The X's in Table 1 indicate that a defence can provide a protection against the corresponding threat.

**Table 1 – Threats/defences matrix**

| Threats | Defences | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | **Sequence number** | **Time stamp** | **Time-out** | **Source and destination identifiers** | **Feed-back message** | **Identifi-cation procedure** | **Safety code** | **Crypto-graphic techniques** |
| Repetition | X | X | | | | | | |
| Deletion | X | | | | | | | |
| Insertion | X | | | X [2)] | X [1)] | X [1)] | | |
| Resequence | X | X | | | | | | |
| Corruption | | | | | | | X [3)] | X |
| Delay | | X | X | | | | | |
| Masquerade | | | | | X [1)] | X [1)] | | X [3)] |

1) Application dependent

2) Only applicable for source identifier

Will only detect insertion from invalid source

If unique identifiers cannot be determined because of unknown users, a cryptographic technique shall be used, see 6.3.8.

3) See 7.3 and Clause A.2.

## 7.3 Choice and use of safety code and cryptographic techniques

The choice of safety code and cryptographic techniques shall be determined according to the following:

- whether or not unauthorised access can be ruled out;
- the type of cryptographic code proposed;
- whether or not the safety-related access protection process is separated from the safety-related process.

Guidance on these issues is given in Clause A.2.

# Annexe A
(informative)

# Guide pour les défenses

## A.1 Applications de la datation

Une date peut être utilisée à différentes fins.

1) Affirmer que la date d'un événement dans une entité est importante pour le processus recevant l'information. Les événements peuvent être reliés temporellement entre eux. S'il est possible d'avoir connaissance du temps et des valeurs d'une suite d'événements, il est possible d'interpoler entre les valeurs et d'augmenter la précision des valeurs calculées (par exemple pour la vitesse, l'accélération). Les délais de transmission peuvent être traités.

   Contraintes:

   – si on utilise une date absolue, le temps doit être synchronisé dans les entités. Chaque entité doit avoir un contrôle du temps en sécurité et une mise à jour du temps global. Les délais du réseau ont un effet sur la distribution du temps global, la validité des informations et la performance du processus;

   – l'absence de messages n'est pas détectée s'il n'y a pas de procédure de dialogue.

2) Ordonner des séquences d'événements à des fins de contrôle par le récepteur.

   Contraintes:

   – si la granularité du temps est trop grossière, les propriétés de séquencement des événements peuvent être indéterminées. Dans ce cas, les informations sont à compléter par un numéro de séquence;

   – l'ordre des messages est affecté par le routage des messages dans le réseau et les délais de transmission dans le réseau;

   – l'absence de messages n'est pas détectée s'il n'y a pas de procédure de dialogue.

3) Mesurer le temps entre événements reçus d'une entité émettant une séquence de messages et par là-même vérifiant que les événements ne sont pas retardés.

   Si de l'information d'une entité (A) doit être reçu continûment d'une autre entité (B), alors cette dernière reçoit de l'information de l'horloge locale du correspondant via les dates. Cette information peut être corrélée avec sa propre horloge en prenant en compte les délais de transmission. Une horloge logique a été crée à partir de l'horloge locale de l'entité (B).

   Contraintes:

   – l'horloge logique est influencée par les délais variables dans le réseau et les processus de l'entité (A).

4) Vérifier la validité de l'information de l'entité (A) en exigeant un retour de la date de l'entité (B) dans un message précédent à l'entité (A). Cela garantit une réponse spécifique (identité) et vérifie également une boucle temporelle prédéfinie. Un numéro de séquence (ou marquage) créé et dont le temps est surveillé dans l'entité (B) aura la même fonction. Aucune date absolue n'est nécessaire (sauf si cela est demandé par d'autres applications).

   Le récepteur détecte la perte d'information par mesure du temps écoulé.

   Contraintes:

   – la procédure doit traiter les interruptions dues à l'initialisation et aux conditions erronées;

   – la procédure ne garantit pas l'authenticité des messages.

# Annex A
(informative)

# Guideline for defences

## A.1 Applications of time stamps

A time stamp can be used for different purposes.

1) To state the time of an event in an entity which is of importance for the process receiving the information. Events can be time related to each other. If we have knowledge of times and values for a sequence of events, it is possible to interpolate between values and increase the accuracy of calculated values (e.g. for speed, acceleration). Transmission delays can be handled.

   Constraints:

   – if an absolute time stamp is used, the time in the entities needs to be synchronized. Each entity needs to have a safe time checking and update of the global time. The network delays have an effect on global clock distribution, information validity and process performance;

   – absence of messages will not be detected if a dialogue communication procedure is not provided.

2) To order event sequences which can be checked by the receiver.

   Constraints:

   – if the time granularity is too coarse, the sequencing properties of events can be indeterminate. In such cases, the information shall be complemented with sequence numbers;

   – the order of messages is affected by network routing of messages and time delays in the network;

   – absence of messages will not be detected if a dialogue communication procedure is not provided.

3) To measure time between events received from an entity sending a sequence of messages thereby also checking for events not being delayed.

   If information from an entity (A) is requested repeatedly from another entity (B), then the latter gets information of the partner's local clock from the time stamps. This information can be related to its own clock by taking the transfer delays into account. A logical clock has been created from the local clock of entity (B).

   Constraints:

   – the logical clock is affected by varying time delays in the network and the processing in entity (A).

4) To check the validity of information of an entity (A) by requiring a return of a time stamp delivered from an entity (B) in a previous message to the entity (A). This ensures a specific response (identity) and also checks against a predefined loop time. A sequence number (or label) created and time supervised in entity (B) will do the same work. No global time is needed (unless required by other applications).

   The receiver detects loss of information using a time-out.

   Constraints:

   – the procedure shall handle interruption due to initialization or fault conditions;

   – the procedure will not guarantee authentication of the messages.

5) Créer une procédure appelée double datation [A155] [3]. Cette procédure bénéficie des propriétés d'une combinaison des cas 2, 3 et 4. La procédure de double datation permet l'emploi d'horloges asynchrones dans les entités, évitant par là-même les problèmes de mise à jour des entités par le temps global. La méthode peut être utilisée pour

   a) créer une horloge logique à partir de l'horloge locale des partenaires et des dates relatives à partir de sa propre horloge (et de synchroniser les horloges entre deux entités);

   b) rattacher des événements aux dates relatives incluant les délais de réseau;

   c) vérifier l'ordre correct des messages;

   d) vérifier l'horloge du partenaire pour vérifier que sa propre horloge est correcte (dépendante de l'application).

   La communication est valable pour un dialogue point à point ou pour une relation de type maître à esclave. Cette dernière est plus utilisable à des fins de transmission cyclique plutôt que la datation d'événements uniques où le temps est important pour une fonction spéciale.

   Contraintes:

   – si la granularité du temps est trop grossière, les propriétés de séquencement des événements peuvent être indéterminées. Dans ce cas, les informations sont à compléter par un numéro de séquence;

   – la double datation peut nécessiter la connaissance du délai de la boucle de transmission si l'application prend en considération le cas 1 ci-devant.

Des schémas plus élaborés que la double datation ont été conçus permettant des événements ordonnés se produisant dans plus de deux systèmes [TBaum].

## A.2 Choix et utilisation des codes de sécurité et des techniques cryptographiques

Bien que le système de communication puisse être inconnu ou variable durant sa durée de vie, dans la plupart des cas on peut déterminer si un accès non autorisé peut être exclus ou non. Cette distinction est très utile car dans le cas d'un accès non autorisé, il est requis des mécanismes cryptographiques à clé secrète. Il est recommandé de faire cette distinction le plus tôt possible afin de limiter le nombre de fonctions de sécurité. Dans le cas d'un accès non autorisé, une couche de protection d'accès séparée peut être utilisée ou la protection peut être fournie par le protocole de sécurité basé sur des mécanismes cryptographiques (voir figure A.1).

[3] Les éléments entre crochets renvoient à l'annexe B (Bibliographie).

5) To create a procedure called double time stamping [A155][3] This procedure inherits the properties of a combination of cases 2, 3 and 4. The double time stamping procedure allows for asynchronous clocks in the entities thereby avoiding problems associated with keeping entities updated with global time. The method can be used for

   a) creating a logical clock from the partners' local clock and relative time stamps from the own local clock (and organizing a clock synchronization between the two entities);

   b) relating events to the relative time stamps including network delay;

   c) checking the correct order of messages;

   d) checking the partners' clock to verify the correctness of your own clock (application dependent).

   The communication is valid for a two-partner dialogue or for a master-slave relation. The latter is more usable for cyclic transmission purposes rather than time stamping single events where time is important for a special function.

   Constraints:

   – if the time granularity is too coarse, the sequencing properties of events can be indeterminate. In such cases the information shall be complemented with sequence numbers;

   – double time stamping may require knowledge about the round-trip transmission delays if the application considers case 1 above.

More elaborated schemes than the double time stamps have been conceived which allow ordering events occurring on more than two systems [TBaum].

## A.2 Choice and use of safety codes and cryptographic techniques

Although the communication system could be unknown or variable during the life time, in most cases one can determine whether unauthorized access can be excluded or not. This distinction is very useful because in cases of the possibility of unauthorized access, cryptographic mechanisms with secret keys are demanded. It is recommended to make this distinction in an early stage in order to limit the amount of safety-related functions. In the case of the possibility of unauthorized access, a separate access protection layer can be applied or the protection is provided by the safety protocol using cryptographic mechanisms (see Figure A.1).

[3] The information given in square brackets refers to Annex B (Bibliography).

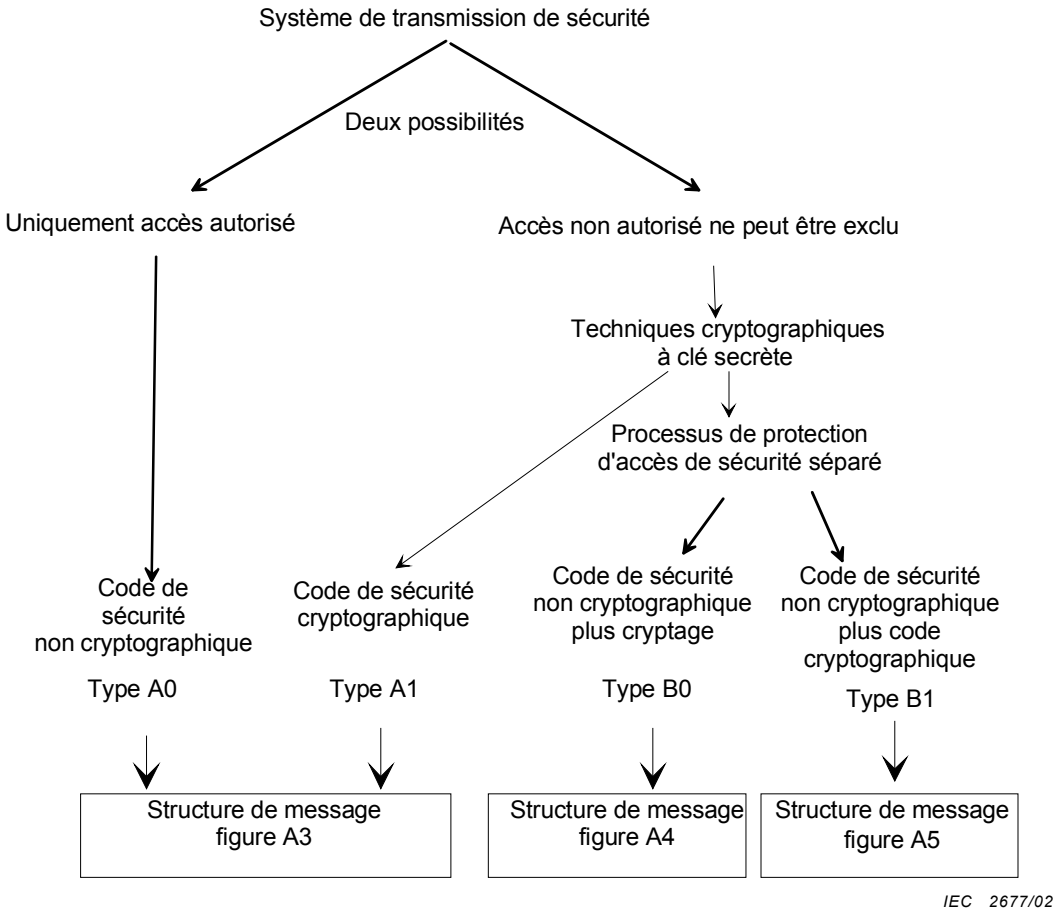



**Figure A.1 – Classification des systèmes de transmission de sécurité**

Des couches de protection d'accès séparées sont utiles lorsque des groupes d'ordinateurs de sécurité connectés sur un réseau local (LAN) ont à communiquer via un système de transmission ouvert (voir figure A.2). Le matériel et le logiciel cryptographiques peuvent être concentrés sur les points d'entrée du système de transmission ouvert. Les fonctions cryptographiques peuvent être combinées avec des fonctions de passerelle normalement requises lorsqu'un réseau local est connecté par exemple à un réseau étendu.

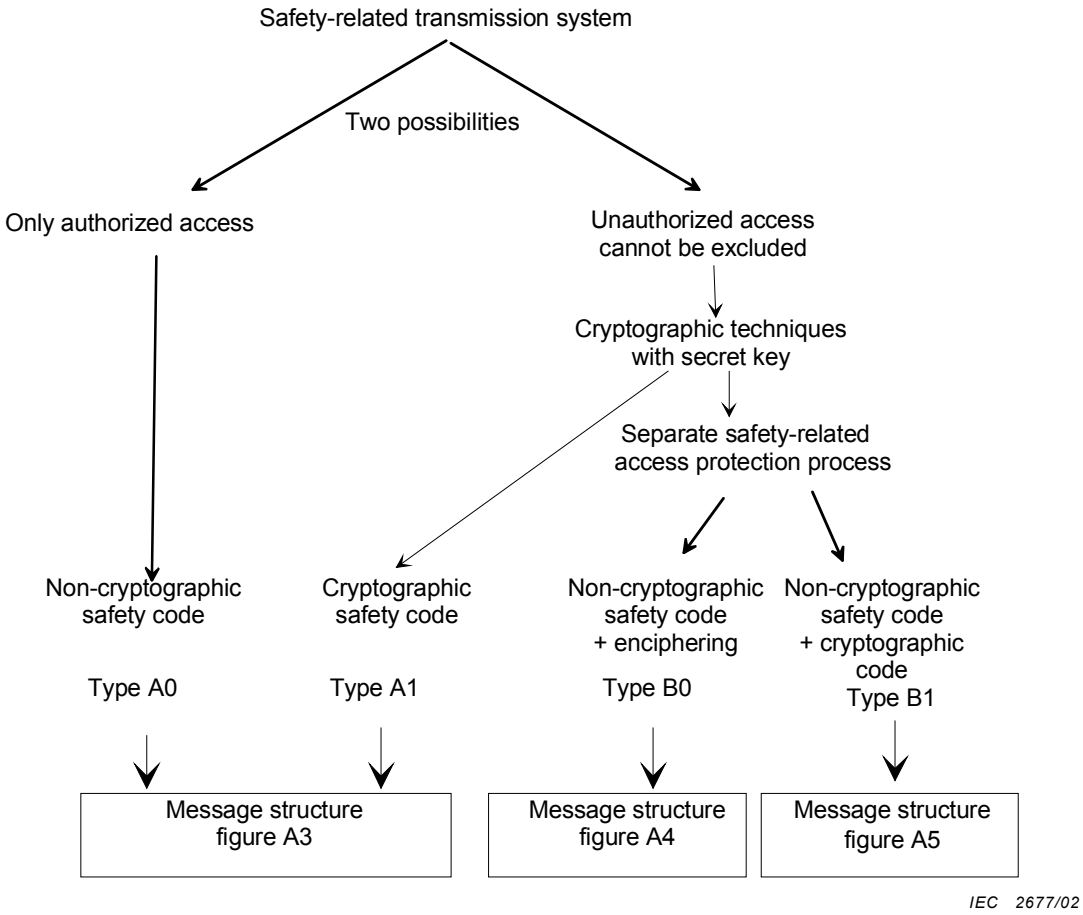



**Figure A.1 – Classification of the safety-related transmission system**

Separate access protection layers are useful where groups of safety-related computers which are connected by a local area network (LAN), have to communicate over open transmission systems (see Figure A.2). The cryptographic hardware and software can be concentrated on the entry points to the open transmission system. The cryptographic functions can be combined with gateway functions which are normally required when a LAN is connected for example to a wide area network.

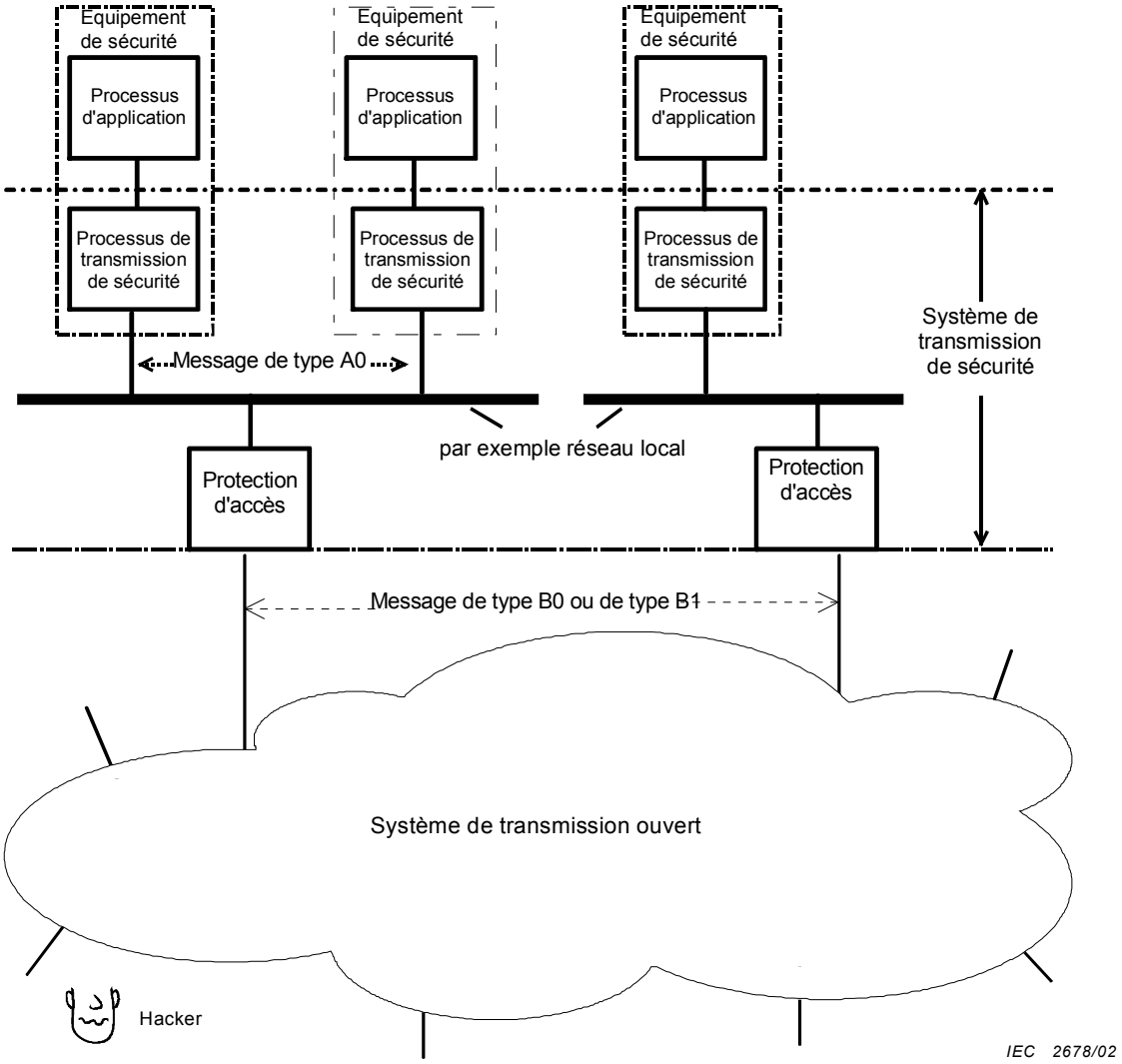



**Figure A.2 – Utilisation d'une couche de protection d'accès séparée**

Le processus de protection d'accès peut être réalisé de différentes manières:

1) cryptage des messages;
2) addition d'un code cryptographique.

Dans les deux cas, un code de sécurité est appliqué avant d'envoyer le message de sécurité vers la couche de protection d'accès. L'équipement comportant la couche de protection d'accès n'a pas à être de sécurité, voir les exigences générales en 6.2. Noter qu'il y a lieu de prendre en considération les défaillances du processus de protection d'accès.

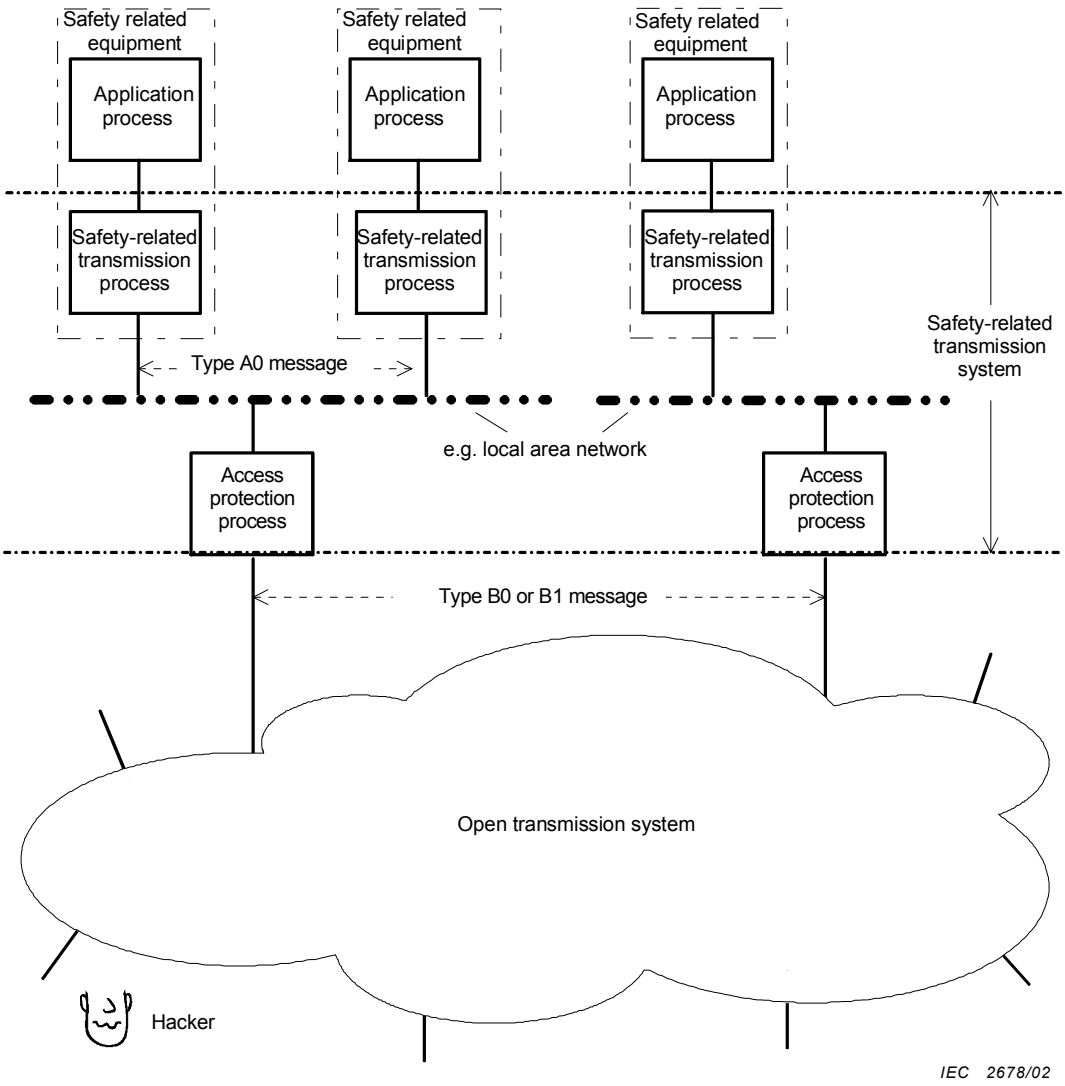



**Figure A.2 – Use of a separate access protection layer**

The access protection process can be performed by different modes:

1) enciphering of the messages;
2) adding a cryptographic code

In both cases, a safety code is applied before a safety-related message is sent to the access protection layer. The equipment containing the access protection layer, does not have to be safe by itself, see general requirements in 6.2. Note, those failures of the access protection process shall be considered.

Les principes de structure des messages dépendent des différents modes. Des exemples sont donnés dans les figures A.3, A.4 et A.5.

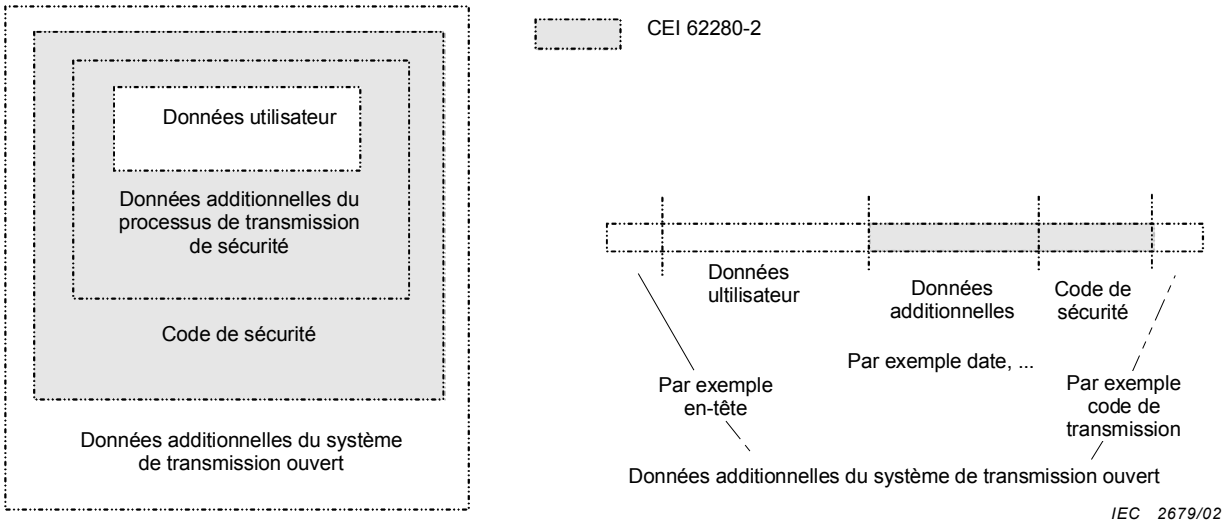



**Figure A.3 – Modèle de représentation de message dans un système de transmission (types A0, A1)**

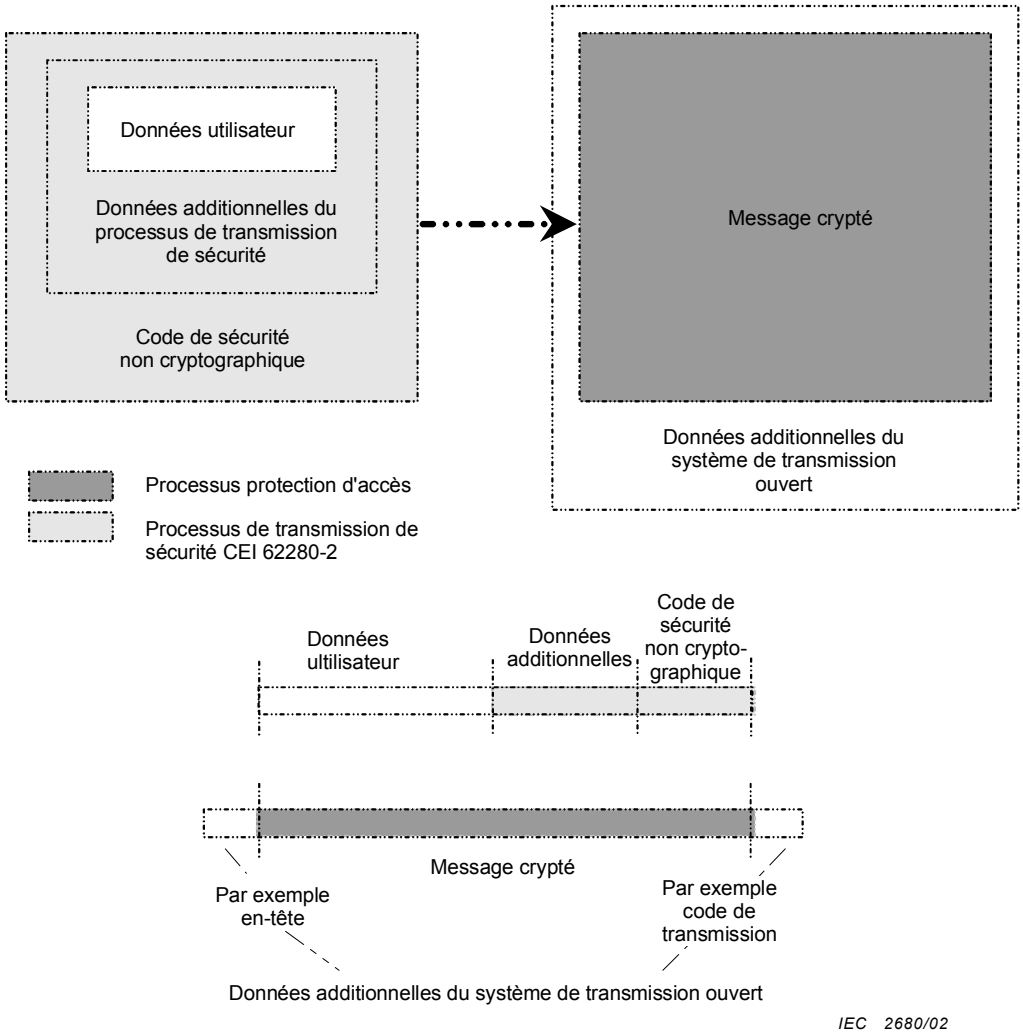



**Figure A.4 – Modèle de représentation de message dans un système de transmission (type B0)**

The principles of message structures depend on the different modes. Examples are depicted in Figures A.3, A.4 and A.5.

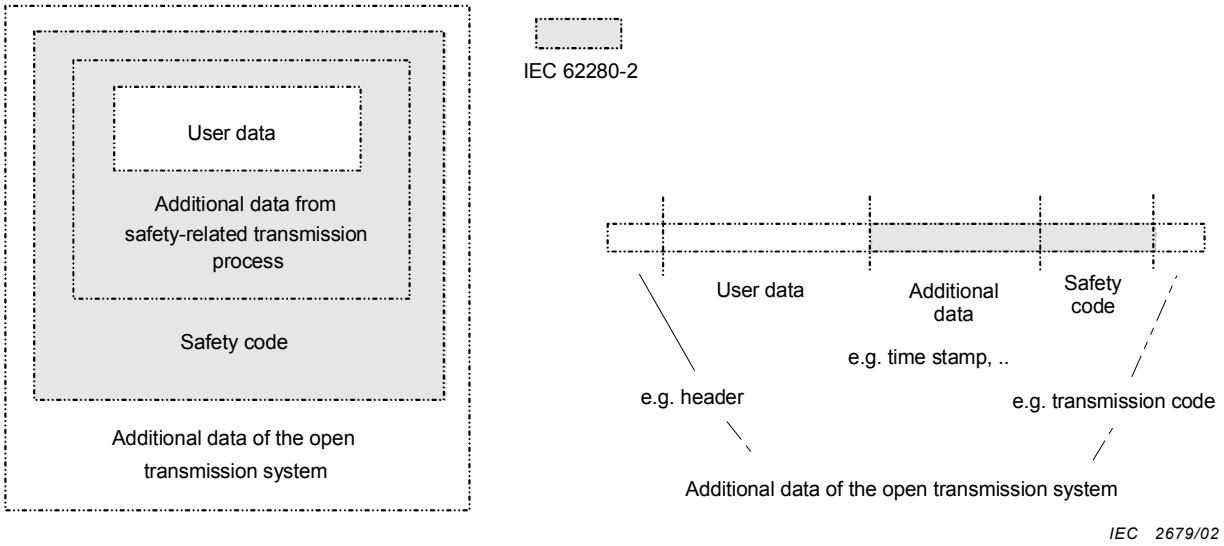



**Figure A.3 – Model of message representation within the transmission system (type A0, A1)**

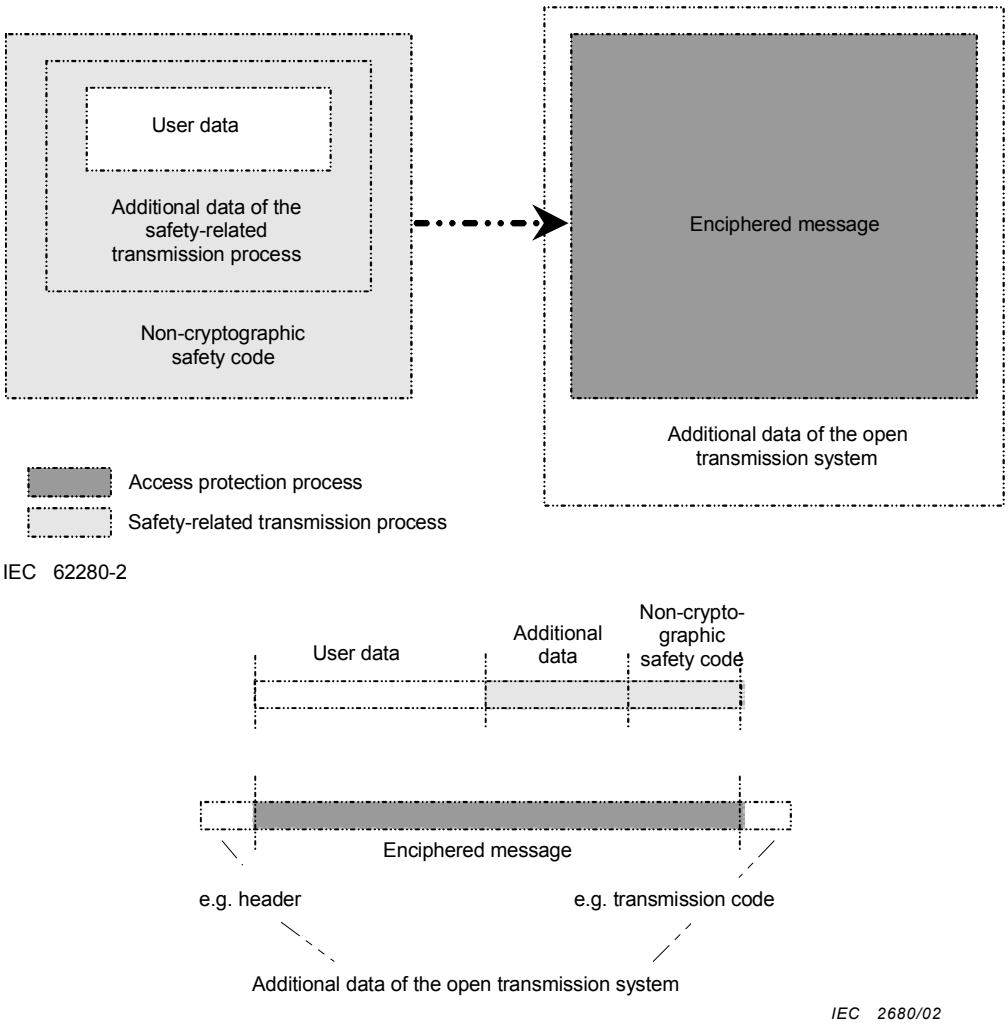



**Figure A.4 – Model of message representation within the transmission system (type B0)**

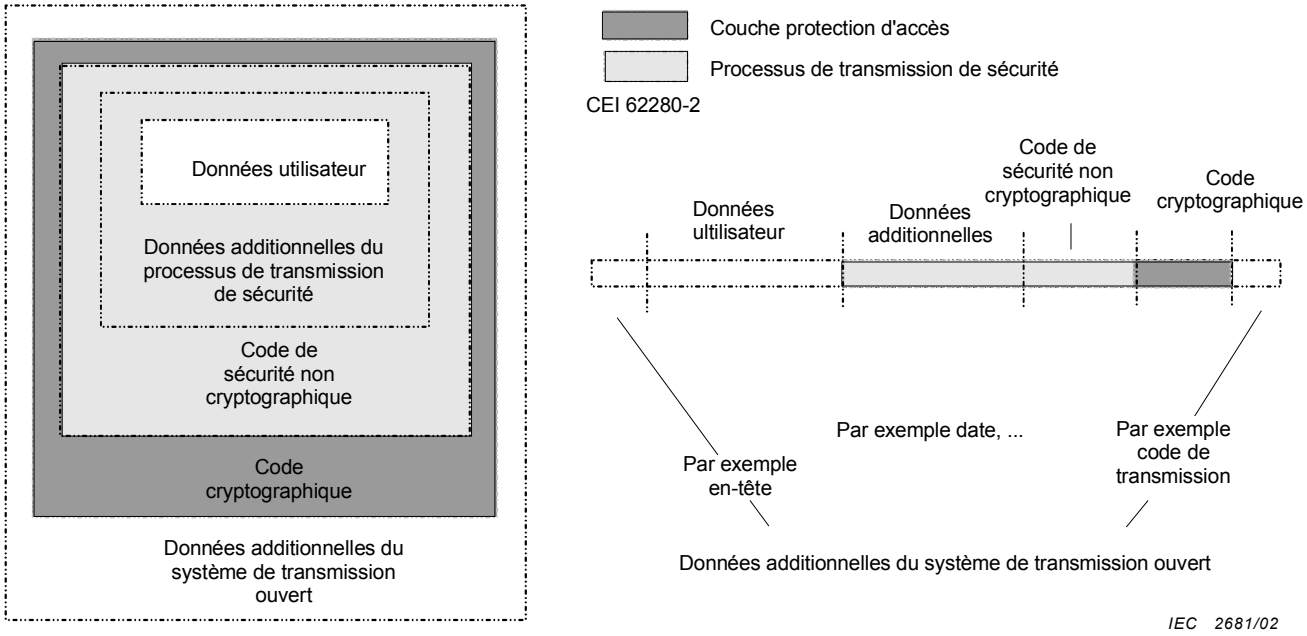



**Figure A.5 – Modèle de représentation de message dans un système de transmission (type B1)**

### A.2.1 Code de sécurité

Les propriétés exigées du code de sécurité dépendent des caractéristiques du réseau de transmission ouvert et de l'architecture du système de transmission de sécurité (voir figure A.1).

Si un accès non autorisé du réseau ouvert peut être exclus, le code de sécurité doit détecter toutes les erreurs aléatoires et systématiques. Il est à noter que d'habitude le réseau de transmission ouvert protège ses messages avec son propre code de transmission, qui est déjà conçu pour atteindre une qualité et un taux d'erreur bit donnés. Si donc un réseau de transmission ouvert délivre un message non valide, soit la perturbation du canal de transmission était telle que le code de transmission a été pris en défaut, soit qu'une défaillance s'est produite. Dans les deux cas, on doit considérer que les bits d'erreur résiduels ne sont pas aléatoires et qu'on ne peut pas avoir n'importe quel poids de Hamming [Peterson].

Si un accès non autorisé ne peut être exclus, une attaque malveillante ne peut être empêchée mais elle peut être détectée et rendue inoffensive. La manière habituelle d'empêcher une attaque malveillante est l'application d'algorithmes de cryptographie à au moins une clé secrète. Le code de sécurité lui-même peut être basé sur un tel algorithme, ou une couche de protection d'accès séparée avec des fonctions cryptographiques peut être mise en oeuvre. Dans ce dernier cas, le code de sécurité peut également détecter des défaillances de l'équipement de protection d'accès.

#### A.2.1.1 Principaux codes en blocs

Les alinéas suivants décrivent brièvement quelques codes et leurs principales caractéristiques.

**Codes linéaires**

Un code est linéaire si, et seulement si, la somme de n'importe quels mots du code est également un mot du code.

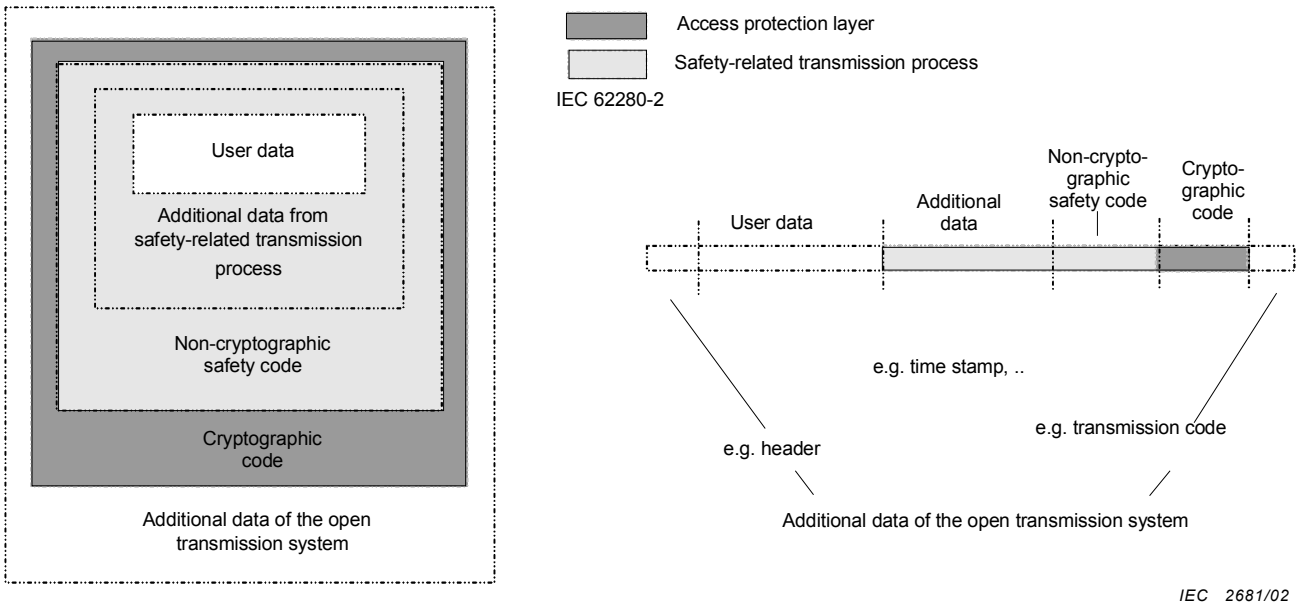



**Figure A.5 – Model of message representation within the transmission system (type B1)**

### A.2.1 Safety code

The required properties of the safety code depend on the characteristics of the open transmission system and the architecture of the safety-related transmission system (see Figure A.1).

If unauthorized access on the open transmission system can be excluded, the safety code has to detect all kinds of random and systematic bit errors. Note, that usually the open transmission system protects its messages with its own transmission code, which is already designed to meet a defined quality and bit error rate. Hence, if the open transmission system delivers an invalid message, either the disturbance on the transmission channel was so high that the transmission code has failed, or a failure has occurred. In either case, it shall be considered that residual bit errors are not random, and can have any Hamming Weight [Peterson].

If unauthorized access cannot be excluded, malicious attack cannot be prevented but can be detected and rendered harmless. The usual way to prevent a malicious attack is the application of cryptographic algorithms with at least one secret key. The safety code itself can be based on such an algorithm, or a separate access protection layer with cryptographic functions can be implemented. In the latter case, the safety code also can detect failures of the access protection equipment.

#### A.2.1.1 Main block codes

The following paragraphs briefly describe some codes and their main characteristics.

**Linear block codes**

A block code is linear if, and only if, the sum of any code words is also a code word.

La plupart des codes utilisés pour le contrôle des erreurs sont des codes binaires linéaires. On utilise également des codes non binaires tels les codes de Reed-Solomon. Les codes sont excellents pour lutter contre les erreurs aléatoires et les rafales d'erreurs. Les codes peuvent être conçus avec une distance de Hamming spécifique minimale *d*. Cela signifie qu'on détecte à 100 % jusqu'à *d*-1 erreurs bit. De part leur linéarité, les codes peuvent également être testés pour leur capacité à détecter des erreurs systématiques.

**Codes cycliques (CRC)**

Un code linéaire est dit cyclique si chaque décalage cyclique d'un mot du code est également un mot du code. Les CRC peuvent être décrits par des polynômes. La formulation mathématique des codes peut être trouvée par exemple dans [Peterson].

Les codes sont excellents pour lutter contre les erreurs aléatoires et les rafales d'erreurs. Les codes peuvent être conçus avec une distance de Hamming spécifique minimale *d*. Les codes peuvent également être testés pour leur capacité à détecter des erreurs systématiques.

Dans certaines applications, la nature cyclique du code peut être exploitée pour éviter le danger d'une synchronisation sur un faux mot de code. Pour cela, il faut étendre le code mais le résultat final est supérieur aux systèmes reposant sur des caractères de synchronisation séparés.

**Codes de brouillage**

Les codes de brouillage peuvent être linéaires ou non linéaires. Les plus importantes sont les fonctions non linéaires à sens unique qui réduisent les données d'entrée par compression à une «empreinte». Du fait de leur non-linéarité, on ne peut déterminer de distance de Hamming minimale exception faite de petits cas triviaux. L'aptitude à la détection d'erreur est cependant élevée pour de bons codes de brouillage. La modification d'un seul bit des données d'entrée change, en moyenne, la moitié des bits de la valeur brouillée. Etant donnée une valeur brouillée, un traitement ne permet pas de déterminer la donnée d'entrée dont le brouillage conduit à cette valeur (propriété d'unidirectionnalité) et étant la donnée d'entrée, un traitement ne permet pas de trouver une autre donnée d'entrée qui conduise à la même valeur par brouillage (propriété de collision des fonctions de faible brouillage) et un traitement ne permet pas de trouver un quelconque couple de données d'entrée qui, par brouillage, conduit à la même valeur (propriété de collision des fonctions de fort brouillage).

L'ISO/CEI 10118-1 définit de manière générale les fonctions de brouillage à des fins de sûreté. L'ISO/CEI 10118-2 décrit des fonctions de brouillage utilisant un algorithme de chiffrement à blocs de *n*-bits, sans utiliser de clé. On peut également utilisé un MAC comme fonction de brouillage, mais dans ce cas une clé est nécessaire.

On peut obtenir de bonnes performances en logiciel avec les algorithmes de condensation de message MD4 et MD5 [Rivest] qui sont dans le domaine public et qui appartiennent à la classe MDC. Il n'est pas requis d'exigences élevées en matière de critère de collision car on pare aux attaques malveillantes par d'autres moyens. Ce qui veut dire soit qu'on utilise un code de cryptage (MAC), soit que le processus de protection d'accès applique une protection cryptographique sur tout le message de sécurité, y compris la valeur brouillée.

**Signatures digitales**

Nombre de bits fonction de tous les bits des données d'entrée (données utilisateur et données additionnelles) et aussi d'une clé secrète. Son exactitude peut être vérifiée en utilisant une clé publique [Davies].

Most of the codes in use for error control are linear binary codes. Non-binary codes are also used, for example Reed-Solomon codes. The codes are excellent for combating random errors and burst errors. The codes can be designed with a specific minimum Hamming distance *d*. That means, that up to *d*-1 bit errors are detected to 100 %. Because of their linearity, the codes can also be tested for systematic error detection capability.

**Cyclic block codes (CRC)**

A linear block code is called cyclic if every cyclic shift of a code word is also a code word. CRC can be described by polynomials. The mathematics of codes can be found for example in [Peterson].

The codes are excellent for combating random errors and burst errors. The codes can be designed with a specific minimum Hamming distance *d*. The codes can also be tested for systematic error detection capability.

In certain applications, the cyclic nature of the code can be exploited to avoid the danger of false code word synchronization. To achieve this, it is necessary to extend the code but the end result will be superior to systems relying on separate synchronization characters.

**Hash block codes**

Hash codes can be linear or non-linear. The most important are non-linear one-way functions, which compress input data to a ”fingerprint”. Because of their non-linearity, a minimum Hamming distance cannot be derived except for trivial small cases. However, the error detection capability is high for good hash codes. A single bit change in the input data changes, on the average, half of the bits in the hash value. Given a hash value, it is computationally unfeasible to find the input data that hash to that value (one-wayness property) and, given the input data, it is computationally unfeasible to find another input data that hash to the same value (collision property for weak hash functions) and it is computationally unfeasible to find any couple of input data that hash to the same value (collision property for strong hash functions).

ISO/IEC 10118-1 defines in a general way hash codes for security purposes. ISO/IEC 10118-2 describes hash codes using an *n*-bit block cipher algorithm without applying a key. Also, a MAC can be used as a hash code, but in this case a key is required.

Good performance in software can be obtained with the public domain message digest algorithms MD4 and MD5 [Rivest] which are classes of MDC. No high requirements on collisions' criteria are demanded because malicious attacks are defended by other means. That means that either a cryptographic block code (MAC) is used, or the access protection process applies a cryptographic protection over the entire safety-related message including the hash value.

**Digital signatures**

A number of bits depending on all the bits of the input data (user data and additional data) and also on a secret key. Its correctness can be verified by using a public key [Davies].

**Codes cryptographiques**

Les codes cryptographiques sont une sorte de code de brouillage non linéaire basé sur des algorithmes cryptographiques. Leur avantage est de protéger des attaques malveillantes s'ils sont basés sur des clés. Le code le plus connu est le code d'authentification de message (MAC) qui est normalisé dans l'ISO/IEC 9797.

### A.2.1.2 Recommandations pour l'application des codes de sécurité

Des exemples d'évaluation des diverses techniques de base sont donnés dans le tableau A.1. Les symboles utilisés ont la signification suivante:

«HR» La technique est hautement recommandée pour cette architecture. Si cette technique n'est pas utilisée, les raisons de sa non-utilisation devraient être détaillée dans le Rapport Technique de Sécurité.

«R» La technique est recommandée pour cette architecture. Ceci est un niveau de recommandation plus faible que 'HR'.

«–» Il n'y a pas de recommandation pour ou contre l'emploi de cette technique.

«US» La technique est inadéquate comme défense dans cette catégorie de système.

**Tableau A.1 – Evaluation des mécanismes d'encodage de sécurité [5)]**

| Type[1)] | Référence, voir annexe B | Type de système de transmission de sécurité, voir figure A.1 | | | |
|---|---|---|---|---|---|
| | | A0 | A1 | B0[4)] | B1[4)] |
| CRC[3)] | [Peterson] | R | US[2)] | –[6)] | R |
| MAC[3)] | ISO/IEC 9797 | R | HR | R | R |
| Codes de brouillage[3)] | ISO/IEC 10118 series | R | US[2)] | HR | HR |
| Signature digitale[3)] | ISO/IEC 9796 | R | R | R | R |

1) D'autres mesures de sécurité sont possibles mais n'ont pas été considérées ici.

2) Clé secrète requise. Ne peut être fait par ce mécanisme.

3) Capacité de détection d'erreur similaire pour la même en-tête.

4) Code de sécurité non cryptographique uniquement. Protection d'accès de sécurité à considérer séparément.

5) Là où il est recommandé plus d'un mécanisme d'encodage de sécurité, il y a lieu de choisir une combinaison appropriée d'un ou de plusieurs mécanismes.

6) Si le processus de protection d'accès repose sur des techniques de cryptage de suites continues, il est interdit d'utiliser un CRC comme code de sécurité. Sinon, un agresseur peut créer des messages de sécurité ayant un CRC valide, en ajoutant un message arbitraire avec un CRC valide au message crypté de la suite continue, sans avoir à briser la clé.

Bien que la connaissance des caractéristiques d'erreur d'un canal particulier puisse permettre de négliger quelque type d'erreur et qu'on puisse revendiquer une meilleure performance, on ne peut supposer une telle connaissance dans un canal «ouvert» (canal opaque). Dans ce scénario, la solution idéale serait un code aléatoire. C'est pour cette raison qu'il ne peut être revendiqué, pour un code de sécurité, une probabilité d'erreur non détectée $p_{UE}$, qui soit inférieure à celle du code aléatoire qui est $p_{UE} = 2^{-r}$ , où $r$ indique le nombre de bits de redondance.

**Cryptographic block codes**

Cryptographic block codes are a kind of non-linear hash block codes based on cryptographic algorithms. The advantage is that they can protect against malicious attacks if they are based on keys. The most well-known code is the message authentication code MAC that is standardized in ISO/IEC 9797.

### A.2.1.2 Recommendations for the application of safety codes

Examples for the assessment of diverse basic techniques are given in Table A.1. The symbols have the following meaning:

'HR' This symbol means that the technique is Highly Recommended for this architecture. If this technique is not used then the rationale behind not using it should be detailed in the Technical Safety Report.

'R' This symbol means that the technique is Recommended for this architecture. This is a lower level of recommendation than a 'HR'.

'-' This symbol means that the technique or measure has no recommendation for or against being used.

'US' This symbol means that this technique is unsuitable as a defence in this category of system.

**Table A.1 – Assessment of the safety encoding mechanisms [5)]**

| Type[1)] | Reference, see annex B | Type of safety-related transmission system, see Figure A.1 | | | |
|---|---|---|---|---|---|
| | | A0 | A1 | B0[4)] | B1[4)] |
| CRC[3)] | [Peterson] | R | US[2)] | –[6)] | R |
| MAC[3)] | ISO/IEC 9797 | R | HR | R | R |
| Hash code[3)] | ISO/IEC 10118 series | R | US[2)] | HR | HR |
| Digital signature[3)] | ISO/IEC 9796 | R | R | R | R |

1) Other safety measures are possible but not considered here.

2) Secret key demanded, cannot be performed by this mechanism.

3) The error detection capability is similar for the same overhead.

4) Non cryptographic safety code only. Safety-related access protection to be considered separately.

5) Where more than one safety encoding mechanism is recommended, an appropriate combination of one or several mechanisms shall be selected.

6) If the access protection process uses stream ciphering techniques then applying a CRC as safety code is forbidden. Otherwise, an attacker can create safety-related messages with a valid CRC by adding an arbitrary message with a valid CRC. to the stream ciphered message, without breaking the key.

Although knowledge of the error characteristics of a particular channel may enable some type of error to be disregarded, and better performance to be claimed, in an ”open” channel (black channel) no such knowledge can be assumed. In this scenario, the ideal solution would be a random code. For this reason, no claim for the probability of undetected error $p_{UE}$ of a safety code should be made, which is lower than the performance of the random code, which is $p_{UE} = 2^{-r}$ where $r$ denotes the number of redundancy bits.

### A.2.2 Techniques cryptographiques

Lorsqu'on emploie des techniques de cryptage, il est recommandé de faire appel à des modes opératoires normalisés, par exemple l'ISO/CEI 10116. Cette norme ne recommande pas le mode dictionnaire chiffré électronique (ECB) pour des longueurs excédant la longueur du bloc de l'algorithme de cryptage. Les algorithmes de cryptage peuvent être enregistrés conformément à l'ISO/CEI 9979, mais l'enregistrement lui-même ne garantit pas la puissance des algorithmes.

Des algorithmes bien connus et bien testés, tel le [DES], sont recommandés.

**Cryptographic techniques**

When using ciphering techniques, standardized modes of operation are recommended, for example according to ISO/IEC 10116. This standard does not recommend the Electronic Codebook mode (ECB) for input lengths which exceed the block length of the enciphering algorithm. Cryptographic algorithms can be registered according to the rules of the international standard ISO/IEC 9979, but the registration itself does not guarantee the strength of the algorithms.

Well-known and well-tested algorithms like [DES] are recommended.

# Annexe B
(informative)

# Bibliographie

CEI 62280-1, Applications ferroviaires – Systèmes de signalisation, de télécommunication et de traitement – Partie 1: Communication de sécurité sur des systèmes de transmission fermés

ISO/IEC 9796:1991, Technologies de l'information – Techniques de sécurité – Schéma de signature numérique rétablissant le message

ISO/IEC 9797:1994, Technologies de l'information – Techniques de sécurité – Mécanisme d'intégrité des données utilisant une fonction de contrôle cryptographique employant un algorithme de chiffrement par bloc

ISO/IEC 9979:1999, Technologies de l'information – Techniques de sécurité – Procédures d'enregistrement des algorithmes cryptographiques

ISO/IEC 10116:1997, Technologies de l'information – Techniques de sécurité – Modes opératoires d'un chiffrement par blocs de *n*-bits

ISO/IEC 10118, Technologies de l'information – Techniques de sécurité – Fonctions de brouillage –
Partie 1: Généralités (2000)
Partie 2: Hash-functions using an *n*-bit block cipher (2001) [4]

ISO/IEC 11770, Technologies de l'information – Techniques de sécurité – Gestion de clés –
Partie 1: Cadre général (1997)
Partie 2: Mécanismes utilisant des techniques symétriques (1996)
Partie 3: Mécanismes utilisant des techniques asymétriques (1999)

[TBaum] A. Tanenbaum: Distributed Systems, Pretince Hall 1995

[A155] UIC/ORE A155.1 rapport RP 4, Septembre 1984: Etude des moyens disponibles pour protéger durant la transmission les informations intéressant la sécurité (*également disponible en anglais et en allemand*)

[DES] FIPS PUB 46, 15.1.1977: Specifications for the Data Encryption Standard

[Peterson] W. Wesly Peterson: Error correction Codes, M.I.T. Press, 1967

[Schneier] Bruce Schneier: Applied Cryptography, J. Wiley & Sons, Inc, 2nd edition 1995

[Rivest] R. Rivest: The MD4 Message-Digest Algorithm, 4/92, published within Internet

[Davies] D.W. Davies and W.L. Price: Security for Computer Networks, 2. edition, J. Wiley & Sons, Chichester

4 Titre en français non disponible.

# Annex B
(informative)

# Bibliography

IEC 62280-1, Railway applications – Communication, signalling and processing systems – Part1: Safety-related communication in closed transmission systems

ISO/IEC 9796:1991, Information technology – Security techniques – Digital signatures scheme giving message recovery

ISO/IEC 9797:1994, Information technology – Security techniques – Data integrity mechanism using a cryptographic check function employing a block cipher algorithm

ISO/IEC 9979:1999, Information technology – Security techniques – Procedures for the registration of cryptographic algorithms

ISO/IEC 10116:1997, Information technology – Security techniques – Modes of operation for an *n*-bit block cipher

ISO/IEC 10118, Information technology – Security techniques – Hash-functions –
Part 1: General (2000)
Part 2: Hash-functions using an *n*-bit block cipher (2001)

ISO/IEC 11770, Information technology – Security techniques – Key management –
Part 1: Framework (1997)
Part 2: Mechanisms using symmetric techniques (1996)
Part 3: Mechanisms using asymmetric techniques (1999)

[TBaum] A. Tanenbaum: Distributed Systems, Prentice Hall 1995

[A155] UIC/ORE A155.1 Report RP 4, September 1984: Survey of available measures for protection of safety information during transmission (also available in German and French)

[DES] FIPS PUB 46, 15.1.1977: Specifications for the Data Encryption Standard

[Peterson] W. Wesly Peterson: Error correction Codes, M.I.T. Press, 1967

[Schneier] Bruce Schneier: Applied Cryptography, J. Wiley & Sons, Inc, 2nd edition 1995

[Rivest] R. Rivest: The MD4 Message-Digest Algorithm, 4/92, published within Internet

[Davies] D.W. Davies and W.L. Price: Security for Computer Networks, 2. edition, J. Wiley & Sons, Chichester

# Annexe C
(informative)

# Guide pour l'utilisation de la norme

## C.1 Domaine d'application/objet

Cette annexe guide l'utilisation de cette norme. Elle contient une classification des systèmes de transmission, identifiant les caractéristiques de tels systèmes susceptibles d'influencer le choix des défenses à inclure dans l'application de sécurité. Elle suggère une procédure d'identification et de quantification des menaces, et de sélection et de définition des performances des défenses. Elle inclut un exemple d'application simple (imaginaire), choisi pour illustrer la possibilité de défenses requérant différents niveaux d'intégrité de sécurité (SIL).

## C.2 Classification des systèmes de transmission

Il est difficile de classer les systèmes de transmission de manière générique; il existe différents facteurs possibles pouvant influer sur les décisions relatives aux menaces à considérer. Il est possible que l'utilisateur du système de signalisation se procure des services de transmission auprès des opérateurs de télécommunications publiques ou privés, via des contrats de service, qui peuvent limiter la responsabilité du fournisseur de service pour garantir la performance du système de transmission.

L'importance des menaces (et par voie de conséquence les exigences en matière de défense) peut dépendre du degré de contrôle exercé sur le réseau de transmission, incluant les points suivants.

Les propriétés techniques du système, incluant des garanties en matière de fiabilité et de disponibilité du système, la taille de mémoire des données inhérentes au système (susceptible d'avoir un impact sur les délais ou le reséquencement des messages), la consistance de la performance du système pendant sa durée de vie (par exemple lorsque surviennent des modifications du réseau ou de la base de l'utilisateur), et les effets de la charge du trafic sur d'autres utilisateurs.

L'accès au système, dépendant du fait que le réseau est privé ou public, le degré de contrôle d'accès exercé par l'opérateur sur d'autres utilisateurs, la possibilité de mauvais emploi du système par d'autres utilisateurs, et l'accès aux services de maintenance pour reconfigurer le système, ou la possibilité d'accès au médium de transmission lui-même.

Les tableaux suivants contiennent une classification possible des systèmes de transmission et une évaluation simple des menaces pouvant être considérées pour chaque type.

# Annex C
(informative)

# Guidelines for use of the standard

## C.1 Scope/purpose

This annex gives guidance on the use of this standard. It includes some guidance on the classification of transmission systems, identifying features of such systems that can affect the choice of defences for inclusion in the safety application. It suggests a procedure for identifying and quantifying threats, and for selecting and defining the performance of defences. It includes a simple (imaginary) example application, chosen to illustrate the possibility of defences requiring different safety integrity levels (SIL).

## C.2 Classification of transmission systems

It is difficult to classify transmission systems in a generic manner; there are many possible factors which can influence the decisions taken about the threats which need to be considered. It is possible that transmission services may be obtained by the signalling system user from private or public telecommunications service providers, under service provision contracts, which may limit the responsibility of the service provider for guaranteeing performance of the transmission system.

The significance of threats (and therefore, the requirements for defences) may depend on the extent of control exercised over the transmission network, including the following issues.

The technical properties of the system, including guarantees of reliability or availability of the system, the extent of storage of data inherent in the system (which could affect delay or resequencing of messages), the consistency of the performance of the system over its life (e.g. as changes to the network, and changes to the user base are made), and traffic loading effects of other users.

Access to the system, depending on whether the network is private or public, the degree of access control exerted by the operator over other users, the opportunity for misuse of the system by other users, and the access available to maintainers to reconfigure the system, or gain access to the transmission medium itself.

The following tables give a possible classification of transmission systems, and a simple assessment of the threats which might be considered for each type.

**Tableau C.1 – Classes de systèmes de transmission ouverts**

| Type | Caractéristiques principales | Exemples | Commentaires |
|---|---|---|---|
| Classe 1 | Toutes les propriétés sont connues et invariables pendant la durée de vie<br>Groupe unique d'utilisateurs | Réseaux locaux propriétaires, PROFIBUS, MVB (bus embarqué multi-usage proposé par la CEI) invariables pendant la durée de vie | Utiliser la CEI 62280-1 |
| Classe 2 | Quelques propriétés sont connues et invariables pendant la durée de vie<br>Extension limitée<br>Stockage limité<br>Groupe unique d'utilisateurs | Identiques à la classe 1, mais il existe la possibilité de changer de système de transmissions pendant la durée de vie | – |
| Classe 3 | Quelques propriétés sont connues et invariables pendant la durée de vie<br>Extension limitée<br>Stockage pratiquement illimité<br>Groupes multiples d'utilisateurs connus | Réseaux locaux | – |
| Classe 4 | Propriétés inconnues et/ou variables pendant la durée de vie<br>Utilisation exclusive de réseaux sûrs<br>Groupes multiples d'utilisateurs (connus) | Réseaux longue distance d'entreprise appartenant aux chemins de fer | – |
| Classe 5 | Propriétés inconnues et/ou variables pendant la durée de vie<br>Parfois utilisation de réseaux non sûrs.<br>Groupes multiples d'utilisateurs | Utilisation du réseau téléphonique public à des instants aléatoires | Par exemple: télédiagnostic de systèmes d'enclenchement |
| Classe 6 | Propriétés inconnues et/ou variables pendant la durée de vie<br>Utilisation du réseau téléphonique public<br>Mauvais usage<br>Groupes multiples d'utilisateurs | Réseau téléphonique public | – |
| Classe 7 | Propriétés inconnues et/ou variables pendant la durée de vie<br>Utilisation du réseau téléphonique public<br>Mauvais usage fréquent | Internet | – |

**Table C.1 – Classes of open transmission systems**

| Type | Main characteristics | Examples | Comments |
|---|---|---|---|
| Class 1 | All properties are known and invariable during their life time<br>Single user group | Proprietary local networks, PROFIBUS, MVB (multi-purpose vehicle bus proposed by IEC) invariable during their life time | Use IEC 62280–1 |
| Class 2 | Some properties are known and invariable during their life time<br>Limited extension<br>Limited storage<br>Single user group | Same as class 1, but the possibility exists that the transmission system could be substituted by another transmission system during their life time | – |
| Class 3 | Some properties are known and invariable during their life time<br>Limited extension<br>Nearly unlimited storage<br>Known multiple users groups | LAN | – |
| Class 4 | Properties are unknown and/or variable during their life time<br>Only using trusted networks<br>(Known) multiple users groups | WAN belonging to the railways | – |
| Class 5 | Properties are unknown and/or variable during their life time<br>Sometimes using non-trusted networks<br>Multiple users groups | Use of public telephone network at unpredictable times | For example remote diagnostic of interlocking systems |
| Class 6 | Properties are unknown and/or variable during their life time<br>Use of public telecommunication network<br>Misuse remote<br>Multiple users groups | Public telephone network | – |
| Class 7 | Properties are unknown and/or variable during their life time<br>Use of public telecommunication network<br>Frequent misuse | Internet | – |

Relation entre la classe du système de transmission et les menaces.

Le tableau C.2 montre une ébauche d'assignation aux menaces de la classe.

**Tableau C.2 – Relation menace/classe**

| Type | Menace | | | | | | |
|---|---|---|---|---|---|---|---|
| | **Répétition** | **Suppression** | **Insertion** | **Reséquence-ment** | **Corruption** | **Retard** | **Mascarade** |
| Classe 1 | ++ | ++ | + | + | ++ | ++ | – |
| Classe 2 | ++ | ++ | ++ | + | ++ | ++ | – |
| Classe 3 | ++ | ++ | ++ | ++ | ++ | ++ | – |
| Classe 4 | ++ | ++ | ++ | ++ | ++ | ++ | – |
| Classe 5 | ++ | ++ | ++ | ++ | ++ | ++ | – |
| Classe 6 | ++ | ++ | ++ | ++ | ++ | ++ | + |
| Classe 7 | ++ | ++ | ++ | ++ | ++ | ++ | ++ |

Légende:

– : Menace pouvant être négligée.

+ : Menace existante mais rare; des contre-mesures allégées sont suffisantes.

++ : Menace existante; de fortes contre-mesures s'imposent.

A ce niveau générique, il n'est pas possible d'allouer des SIL, en fonction de la classe du système de transmission, aux défenses nécessaires à chaque menace; il est fondamental d'analyser l'application particulière concernée pour allouer un SIL.

## C.3 Procédure

Différentes étapes peuvent être identifiées pour réaliser les activités de conception de système couvertes par l'ENV 50129.

Ces phases sont identifiées ci-après:

Application

↓

Analyse des dangers

↓

Réduction des risques

↓

Allocation de SIL et objectifs quantitatifs

↓

Spécifications des exigences de sécurité

Chacune de ces étapes est décrite plus en détail dans les paragraphes ci-après.

Relationship between class of transmission system and the threats.

Table C.2 shows a rough assignment of the threats to the class.

**Table C.2 – Threat/class relationship**

| Type | Threat | | | | | | |
|---|---|---|---|---|---|---|---|
| | Repetition | Deletion | Insertion | Resequence | Corruption | Delay | Masquerade |
| Class 1 | ++ | ++ | + | + | ++ | ++ | - |
| Class 2 | ++ | ++ | ++ | + | ++ | ++ | - |
| Class 3 | ++ | ++ | ++ | ++ | ++ | ++ | - |
| Class 4 | ++ | ++ | ++ | ++ | ++ | ++ | - |
| Class 5 | ++ | ++ | ++ | ++ | ++ | ++ | - |
| Class 6 | ++ | ++ | ++ | ++ | ++ | ++ | + |
| Class 7 | ++ | ++ | ++ | ++ | ++ | ++ | ++ |

Key

– : Threat can be neglected.

+ : Threat existent, but rare; weak countermeasures sufficient.

++ : Threat existent; strong countermeasures required.

At this generic level, it is not possible to allocate SILs, according to the class of transmission system, to the defences needed for each threat; it is essential to analyze the particular application in order to allocate SIL.

## C.3 Procedure

A number of distinct steps can be identified to carry out the system design activities covered by ENV 50129.

These steps are identified below:

Application

↓

Hazard analysis

↓

Risk reduction

↓

Allocation of SIL and quantitative targets

↓

Safety requirements specifications

Each of these steps is described in more detail in the following subclauses:

### C.3.1 Application

Le concepteur du système doit comprendre l'application du système de transmission. Les flux de données, les types de données et la fréquence et la nature des mises à jour (par exemple cyclique ou à l'événement), tous ont un impact sur la conception des systèmes de transmission. L'objectif global de sécurité (taux ou paramètres qualitatifs et paramètres non fonctionnels) du système doit également être défini (par l'utilisateur ou l'autorité de sécurité).

### C.3.2 Analyse des dangers

L'analyse qualitative des dangers du système (comme requise par la CEI 62278) doit identifier les dangers de niveau le plus élevé pouvant survenir comme le résultat de défaillances des équipements d'émission et de réception, ou du lien de transmission lui-même. L'analyse doit prendre en compte les conditions opérationnelles ou autres externes susceptibles d'exposer le système au danger. Pour chaque menace du système, on peut indiquer la possibilité d'inclure une défense dans la conception du système.

### C.3.3 Réduction des risques

De l'objectif quantitatif global de sécurité du système et de l'analyse qualitative des dangers, le concepteur du système peut assigner des objectifs de sécurité par rapport à chaque menace identifiée. Les allocations de tels objectifs peuvent être itératives, en commençant par une allocation simple puis en raffinant en accord avec une analyse plus détaillée et une compensation entre les cas. Partant d'une information quantitative sur la fréquence d'apparition des conditions externes soumettant le système au danger, on peut déterminer la réduction de risque requise de chaque défense.

### C.3.4 Allocation de SIL et objectifs quantitatifs

Les SIL peuvent être alloués en fonction de la réduction de risque nécessaire à chaque défense, au moyen des procédures définies dans l'ENV 50129. Le SIL de la défense étant connu, une conception appropriée peut être choisie pour l'utilisation de cette défense.

Du taux d'erreur contraire à la sécurité quantifié associé à la défense, une conception du matériel peut être choisi sur la base des tableaux de l'ENV 50129, et le taux d'erreur contraire à la sécurité du aux défaillances aléatoires peut être calculé.

### C.3.5 Spécifications des exigences de sécurité (SRS)

Les défenses identifiées comme étant nécessaires à un fonctionnement en sécurité du système, les SIL pour la réalisation de ces défenses et les objectifs de sécurité quantifiés du système doivent être enregistrés dans les SRS du système.

## C.4 Exemple

L'exemple ci-après ne montre que quelques principes de base de la procédure. L'intention n'était pas de décrire un exemple complet correct dans tous ses détails.

### C.4.1 Application

Des commandes d'autorisation de circulation sont à envoyer à des trains sur une ligne secondaire, aux moyens de messages transitant sur un réseau de radiocommunications public.

L'objectif de sécurité global du système est fixé à $10^{-x}$ par heure.

### C.3.1 Application

The system designer must understand the application of the transmission system. The data flows, types of data, and the frequency and the nature of updates (e.g. periodic or event driven) all affect the decisions to be made in designing the transmission system. The global safety target (rate or by qualitative parameters and non-functional parameters) for the system must also be defined (by the user or the safety authority).

### C.3.2 Hazard analysis

Qualitative hazard analysis of the system (as required by IEC 62278) must identify the top-level hazard(s) which can arise as a result of failures of the sending and receiving equipment, or of the transmission link itself. This analysis must consider operational or other external conditions which could expose the system to the hazard. For each threat to the system, the possibility of including a defence in the system design can be included.

### C.3.3 Risk reduction

From the global quantitative safety target for the system, and the qualitative hazard analysis, the system designer can apportion safety targets to each threat identified. The allocation of such targets may be iterative, beginning from a simplistic allocation, and refined in accordance with more detailed analysis and trade-off between cases. Using quantitative information about the occurrence of external conditions exposing the system to hazard, the extent of risk reduction needed from each defence can be determined.

### C.3.4 Allocation of SIL and quantitative targets

Depending on the extent of risk reduction needed for each defence, SIL can be allocated, using the procedures defined in ENV 50129. Knowing the SIL for the defence, appropriate design techniques can be selected, for use in work associated with that defence.

From the quantified unsafe (wrong-side) failure rate identified for the defence, hardware design techniques can be chosen using the tables in ENV 50129, and the rate of occurrence of unsafe failures due to random faults can be calculated.

### C.3.5 Safety requirements specifications (SRS)

The defences identified as being necessary for safe operation of the system, the SIL for the implementation of those defences and quantified safety targets for the system must be recorded in the SRS for the system.

## C.4 Example

The following example shows only some basic principles of the procedure. It was not intended to describe a complete example which is correct in all details.

### C.4.1 Application

Movement authority commands are sent to trains on a secondary line by means of messages over a public radio network.

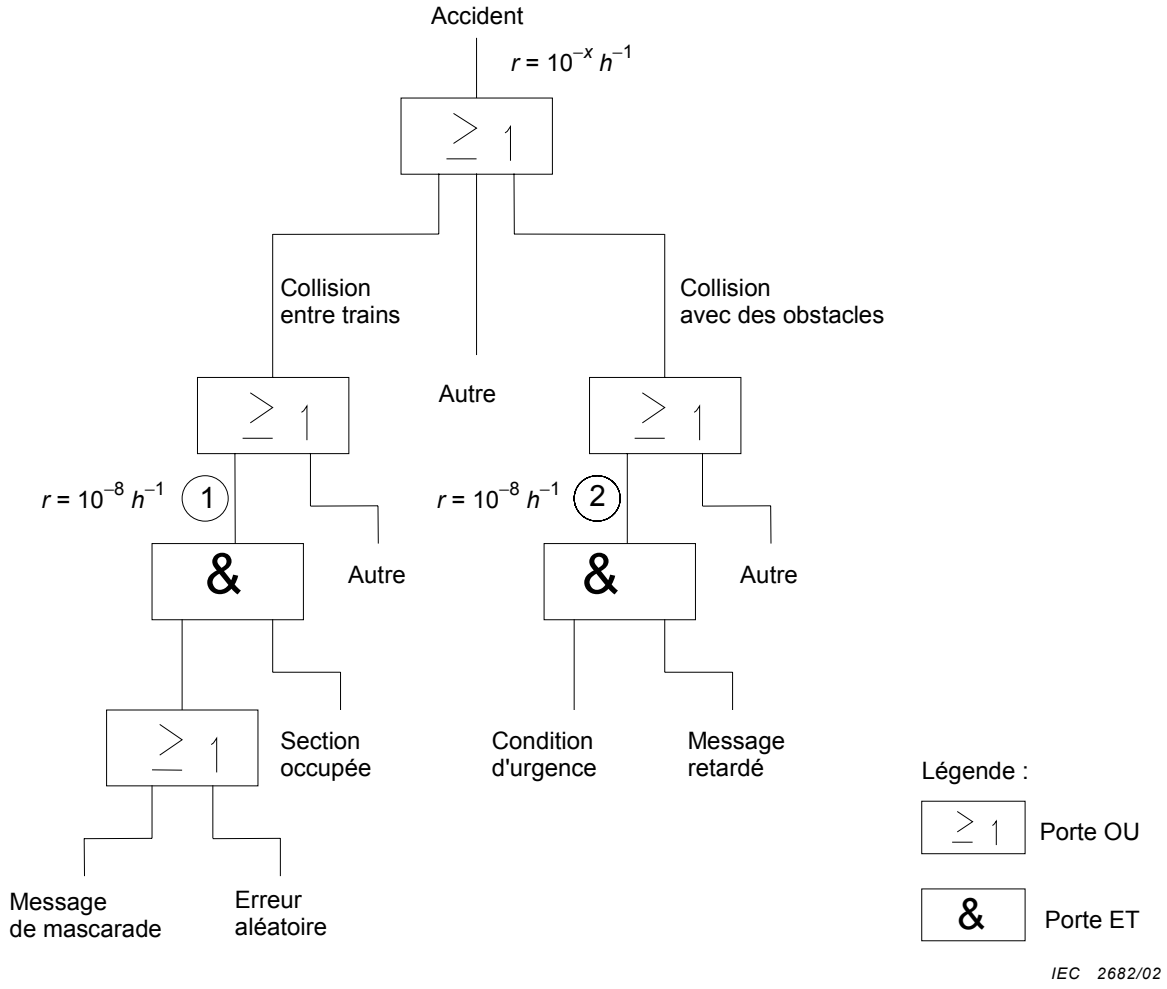
A global safety target of $10^{-x}$ per hour is defined for the system.

### C.4.2 Analyse des dangers

Deux dangers particuliers peuvent être identifiés (entre autres non considérés ici):

1) La réception d'un message incorrect (contraire à la sécurité) à bord d'un train pourrait conduire à une pénétration intempestive dans une section occupée et à une collision avec un autre train.
2) Un retard dans la réception d'un message d'arrêt d'urgence pourrait se traduire par une collision avec une obstruction de la voie.

Cela est montré sur un arbre des défaillances (figure C.1), comme un exemple d'une méthode de réalisation de l'analyse des dangers.




NOTE Symboles préférentiels selon la CEI 61025.

**Figure C.1 – Arbre des défaillances pour le danger «accident»**

L'objectif de sécurité global du système de $10^{-x}$ par heure est réparti et l'objectif alloué aux cas 1 et 2 est (par exemple) de $10^{-8}$ par heure dans chacun des cas.

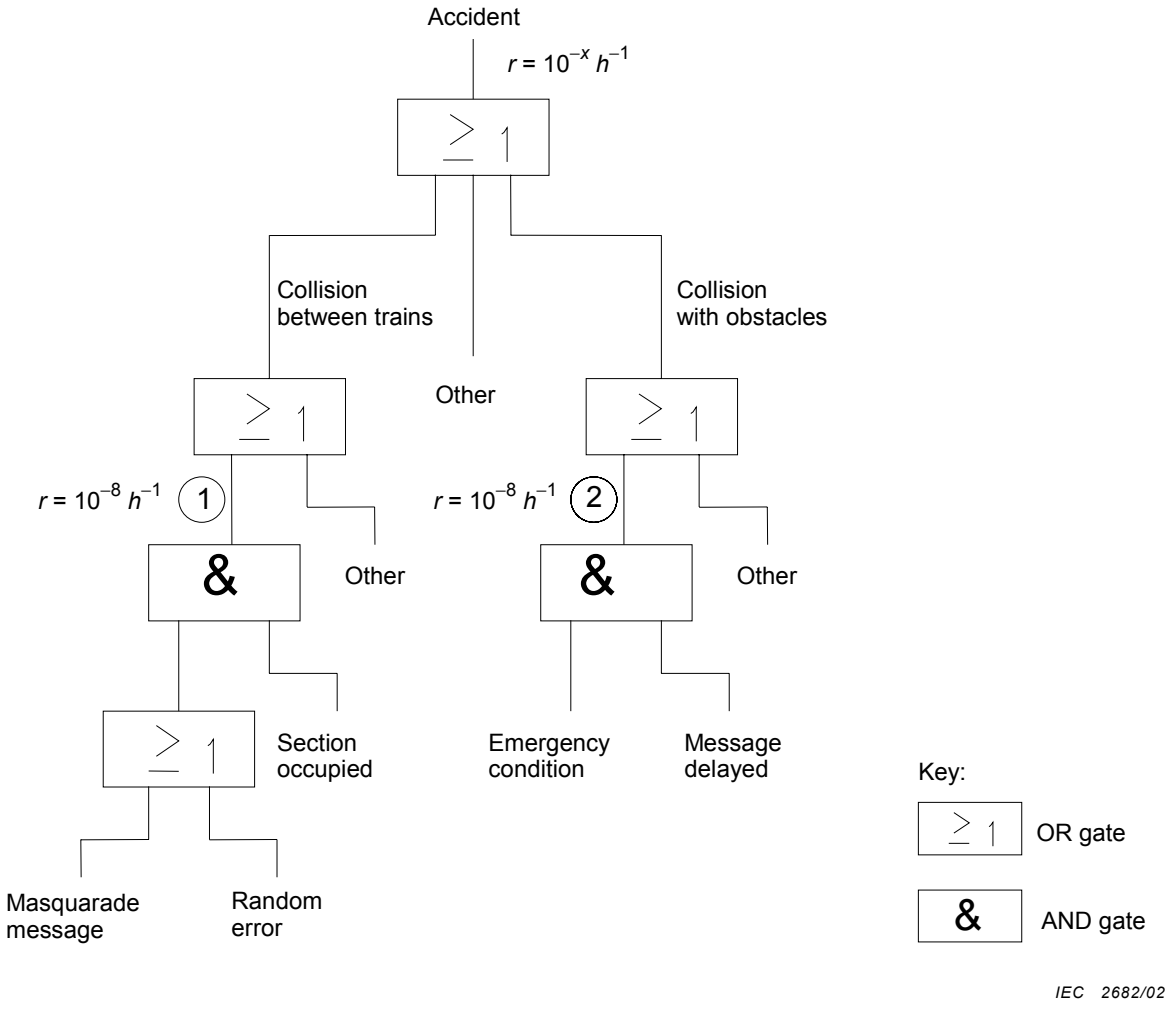
Les cas 1 et 2 sont examinés en détail.

### C.4.2 Hazard analysis

Two particular hazards can be identified (among others not considered here):

1) reception of an incorrect (wrong-side) message on-board a train could result in the train entering an occupied section, and colliding with another train;
2) delay in receiving an emergency stop message could result in a train colliding with an obstruction on the track.

These are shown on a fault tree (Figure C.1), as an example of one method of performing the hazard analysis.




NOTE Preferred symbols according to IEC 61025.

**Figure C.1 – Fault tree for the hazard "accident"**

The $10^{-x}$ per hour global safety target for the system is apportioned, and the target allocated for cases 1 and 2 is (for example) $10^{-8}$ per hour in each case.

Cases 1 and 2 will be considered in detail.

### C.4.3 Cas 1

*Réduction des risques*

Si un message vers un train est corrompu par des erreurs aléatoires, le train peut être autorisé à pénétrer sur une section occupée et entrer en collision avec un autre train.

De plus, des tentatives délibérées pourraient être faites d'insertion d'un message incorrect dans le système (par exemple par un hacker).

Supposons que la probabilité d'occupation de la section est de $10^{-1}$.

La présente norme suggère qu'une défense possible contre la corruption de message est l'utilisation d'un code de sécurité lié à l'information utilisateur du message.

L'introduction de cette défense dans la partie de l'arbre des défaillances correspondant à ce cas conduit à la figure C.2.

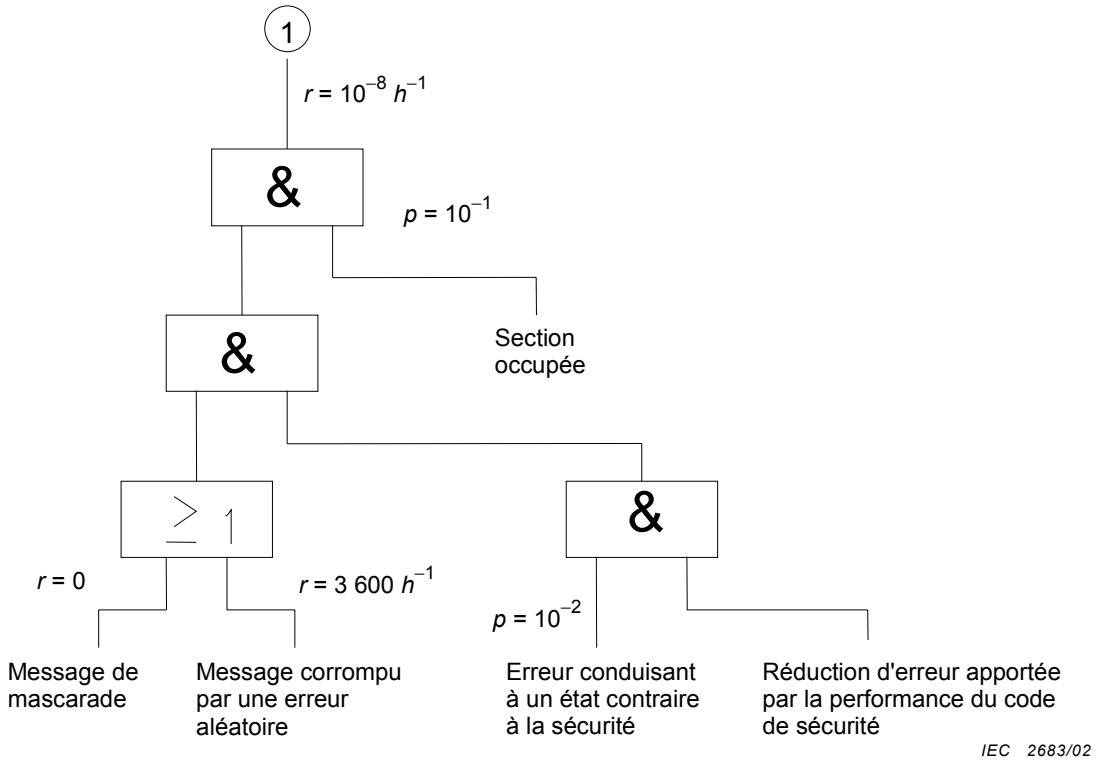



**Figure C.2 – Arbre des défaillances pour le cas 1**

Considérant les objectifs quantifiés de sécurité, il faut admettre que, dans un réseau ouvert, chaque message peut être corrompu (c'est-à-dire une probabilité de 1). Cependant, chaque message corrompu n'autorise pas un train à pénétrer dans une section particulière. Supposons que cette probabilité soit de $10^{-2}$, et supposons qu'un message de 100 bits est envoyé au train via un canal de débit 100 bits/s (soit 3 600 messages par heure). Il est clair que le code de sécurité doit garantir une probabilité de non-détection d'erreur inférieure à $3 \times 10^{-9}$ par message ou encore que la fréquence de ce type d'événement ne doit pas dépasser $10^{-5}\ h^{-1}$.

### C.4.3 Case 1

*Risk reduction*

If a message to a train is corrupted due to random errors, it may permit the train to enter an occupied section, and collide with another train.

In addition, deliberate attempts could be made to insert an incorrect message into the system (e.g. by a hacker).

Suppose the probability of the section being occupied is judged to be $10^{-1}$.

This standard suggests that a possible defence against message corruption is to use a safety code attached to the user information in the message.

Introducing this defence into the portion of the fault tree for this case, gives the following results shown in Figure C.2.

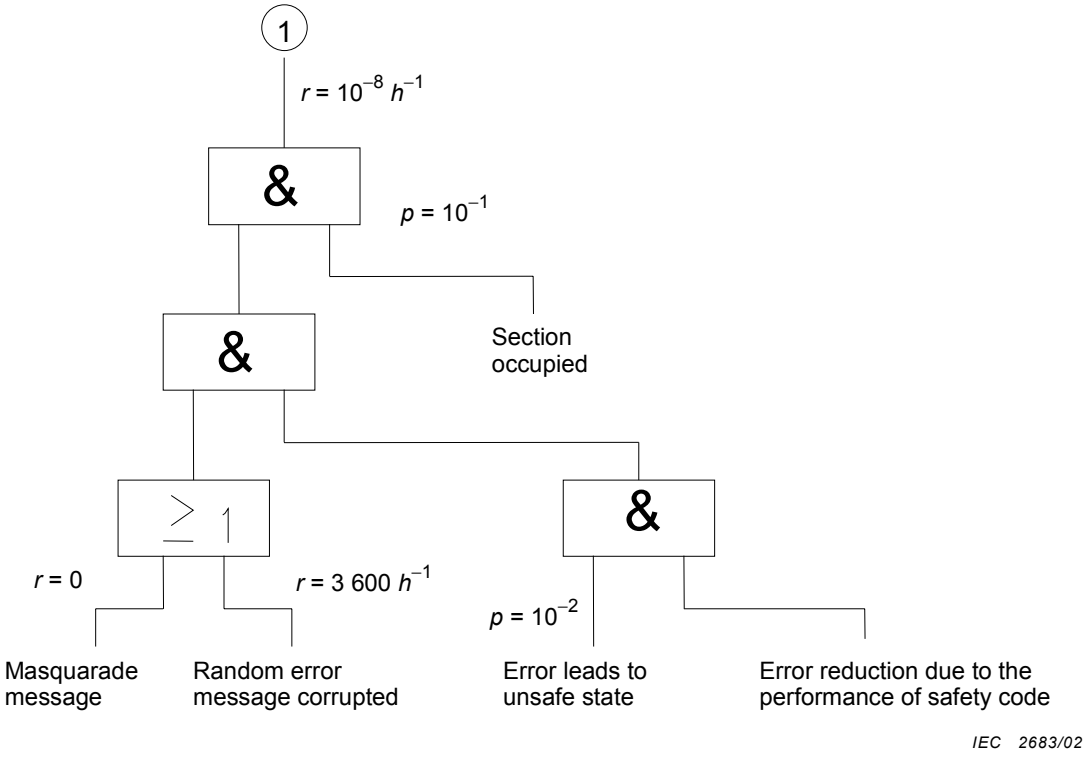



**Figure C.2 – Fault tree for case 1**

Considering quantitative safety targets, it shall be assumed that, in an open system, every message could be corrupted (i.e. probability = 1). However, not every corrupted message will authorize the train into the particular section. Assuming this probability is $10^{-2}$, and assuming that a message with the length of 100 bits is sent to a train over a channel with the bit rate of 100 bits/s (i.e. 3 600 messages per hour), it is clear that the safety code for the message must guarantee a probability of undetected error of less than $3 \times 10^{-9}$ per message, or the frequency of this kind of events shall not exceed $10^{-5}\,h^{-1}$.

*Allocation de SIL et objectifs quantitatifs*

Conformément à l'ENV 50129, un SIL peut être dérivé pour la réalisation de la fonction «traitement du code de sécurité». Ce SIL pourrait être plus faible que pour tout élément du système «système de transmission de sécurité».

Le concepteur du système doit sélectionner un code de sécurité de longueur suffisante pour atteindre la performance requise.

Cette norme suggère qu'il est nécessaire de prendre en compte la possibilité de tentative délibérée de créer des messages incorrects dans un système de transmission ouvert. La classification des systèmes de transmission présentée ci-devant suggère que dans le cas d'une transmission peu fréquente de messages courts, la vraisemblance de tentatives délibérées de créer des accidents est relativement faible. Ces facteurs peuvent influer sur la décision d'adopter ou nom un code de sécurité cryptographique et, si oui, sur le choix des paramètres (longueur de la clé, etc.) de ce code.

### C.4.4 Cas 2

*Réduction des risques*

Dans le cas d'une situation d'urgence (par exemple l'obstruction de la voie), un retard du message d'urgence au train peut provoquer une collision. Supposons que de telles conditions d'urgence surviennent avec une fréquence d'occurrence de $10^{-4}$ par heure.

Supposons qu'on utilise un réseau de radiocommunications public en partage avec un nombre non contrôlé d'autres utilisateurs; aucun délai maximal de transmission du message n'est garanti. Le retard doit donc être pris en compte (c'est-à-dire que la probabilité de retard est de 1).

La présente norme suggère qu'une défense possible contre le retard d'un message est la supervision du temps écoulé dans le récepteur, associée avec une transmission de message cyclique.

L'introduction de cette défense dans la partie de l'arbre des défaillances correspondant à ce cas conduit à la figure C.3.

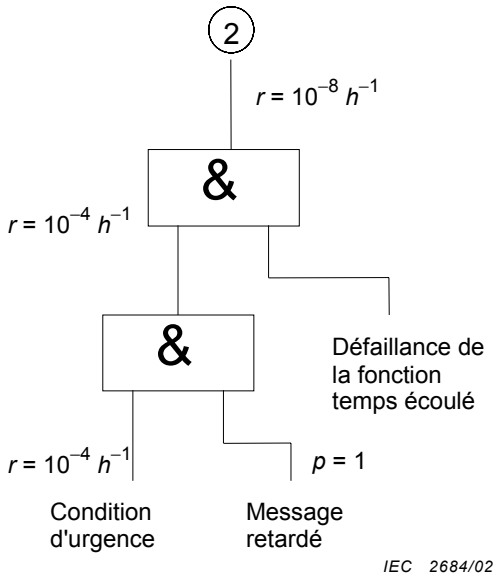



**Figure C.3 – Arbre des défaillances pour le cas 2**

*SIL allocation and quantified target*

According to ENV 50129 a SIL for the implementation of the function ”computing of safety code” can be derived. This SIL could be lower than for the entire system element ”safety-related transmission system”.

The designer of the system must select a safety code with a sufficient length to achieve the required performance.

This standard suggests that it is necessary to consider the possibility of deliberate attempts to create incorrect messages in an open transmission system. The classification of transmission systems suggested above suggests that, for infrequent transmission of short messages, the likelihood of deliberate attempts to create accidents is relatively low. These factors may influence the decision on whether to adopt a cryptographic safety code, and if so, on the choice of parameters (key length, etc.) for this code.

### C.4.4 Case 2

*Risk reduction*

If, when an emergency condition (e.g. obstruction on the track) occurs, the emergency stop message to the train is delayed a collision could result. Suppose that such emergency conditions are judged to occur with a frequency of $10^{-4}$ per hour.

Suppose that, using a public radio network shared with an uncontrolled number of other users, no maximum message delay is guaranteed, and delay shall therefore be assumed (i.e. the delay is assumed to have a probability of 1).

This standard suggests that a possible defence against message delay is to use a time-out in the receiving equipment, together with cyclic message transmission.

Introducing this defence into the portion of the fault tree for this case, gives the following results shown in Figure C.3.

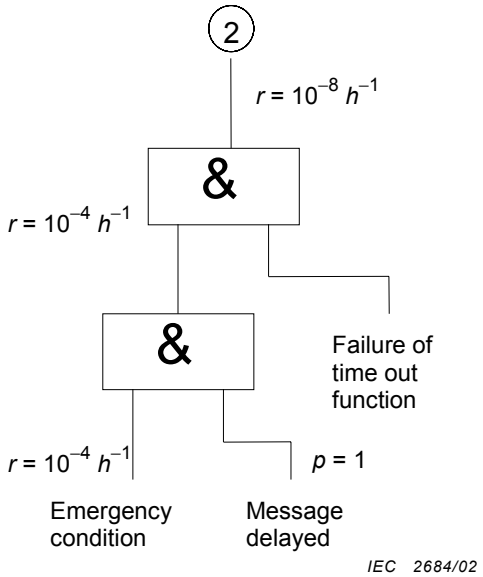



**Figure C.3 – Fault tree for case 2**

La prise en compte des objectifs quantifiés de sécurité montre clairement que la défense «temps écoulé» doit avoir une probabilité d'erreur contraire à la sécurité de moins de $10^{-4}$.

*Allocation de SIL et objectifs quantitatifs*

L'ENV 50129 indique comment obtenir le SIL exigé.

La réalisation de cette fonction doit être faite conformément aux techniques de conception suggérées dans l'ENV 50129 pour le niveau de SIL déterminé, à moins que la réalisation soit intégrée dans d'autres fonctions ayant un SIL plus élevé (par exemple dans un système à processeur).

Considering quantitative safety targets, it is clear that the time-out shall have a wrong side error probability of not more than $10^{-4}$ on demand.

*SIL allocation and quantified target*

Reference to ENV 50129 indicates, how to achieve the required SIL.

The implementation of this function shall therefore be designed using techniques suggested in ENV 50129 as being appropriate for derived SIL, unless the implementation is integrated with other functions with a higher SIL (e.g. in a processor system).

# Annexe D
(informative)

# Menaces sur les systèmes de transmission ouverts

## D.1 Vue système

Les menaces sur les messages émis sur le lien par le système de commande et de protection, résultent de changements possibles dans les performances du lien susceptibles de se produire soit dans des conditions normales (par exemple en l'absence de défaillances), soit dans des conditions anormales (par exemple suite à défaillance dans le système de communication).

L'approche adoptée pour déduire un ensemble de menaces consiste à éclater l'analyse du danger, réalisée sous forme d'arbre (voir figure D.1), en trois niveaux séparés:

1) niveau utilisateur;
2) niveau réseau;
3) niveau environnement extérieur.

Ces trois niveaux suivent une approche *top-down* (de haut en bas), partant du *danger principal* (MH), défini comme «*la défaillance à obtenir un message correct à l'extrémité récepteur*».

A partir de l'analyse des comportements possibles des messages vus côté récepteur, les situations potentiellement dangereuses (*dangers de base*) mises en exergue et un ensemble d'*erreurs de message de base* (BME) a été esquissé, dans une optique de taxinomie de tous les modes de défaillance de message possibles.

La déduction des *menaces* correspondantes qu'il faut considérer comme des modes de défaillance des réseaux (c'est-à-dire les erreurs de message de base vues du point de vue réseau) est immédiate. En fait, la menace est l'entité qui crée une situation dangereuse pour la sécurité (c'est-à-dire qui peut conduire à un accident) et est donc une cause (au niveau réseau) d'une erreur de message de base possible: en conséquence, la relation menace-erreur de message de base est de 1:1.

A son tour, une menace peut être crée par un ensemble de causes appelées *événements dangereux* (HE) pouvant être présents à la fois dans le réseau et dans l'environnement extérieur. Le même événement dangereux peut de toute évidence être lié à différentes menaces.

L'éclatement de l'analyse en différents niveaux fournit également (au moins) trois niveaux de défense possibles:

1) au niveau *système/application* utilisateur, traitant de la réalisation du système, indépendamment du champ de transmission; par exemple la suppression qui peut s'avérer inoffensive si le système a été conçu dans un sens tel que les messages supprimés ne constituent pas un danger;
2) au niveau de la *structure logique du message*, par exemple l'ensemble des codes possibles s'appliquant au message ou des contre-mesures spécifiques telles que la numérotation des messages, la datation, etc.;
3) au niveau *physique*, par exemple le blindage pour éviter l'altération par les interférences électromagnétiques.

La suite de cette annexe ne traite pas plus de ce sujet qui n'a été mentionné que pour donner une vision générale de la méthodologie adoptée.

# Annex D
(informative)

# Threats on open transmission systems

## D.1 System view

The threats to messages sent over the link by the control and protection system occur as a result of the possible changes in performance of the link, which may arise either in normal conditions (i.e. without failures) or abnormal conditions (i.e. following failures of the communication equipment).

The adopted approach for deriving a set of threats has been that of splitting the hazard analysis, performed in form of a tree (see Figure D.1), in three separate levels:

1) the user level;
2) the network level;
3) the external environment level.

These levels follow a top-down approach, starting from the *main hazard* (M.H.), defined as "*the failure to obtain correct message at the receiver end*".

Through the analysis of the possible message behaviours observed at the receiver part, the potentially dangerous situations (*basic hazards*) have been highlighted and a set of *basic message errors* (BME), intended as the taxonomy of all possible message failure modes, is outlined.

The derivation of the corresponding *threats*, to be understood as the network failure modes (i.e. the basic message errors seen from a network point of view), is straightforward. The threat, as a matter of fact, is the entity that creates a dangerous situation for the safety (i.e. can lead to an accident) and is therefore a cause (at the network level) of a possible basic message error: the relationship threat-basic message error is consequently 1:1.

In its turn, a threat can be generated by a set of causes, called *hazardous events* (HE), that can be present at both the network and the external environment level. The same hazardous event can obviously be related to different threats.

The splitting of the analysis in different levels provides also the possibility of (at least) three levels of defences:

1) one at a *system/user application* level, treating with the implementation of the system, independently from the transmission field; an example is the deletion, that can turn out to be absolutely not dangerous if the system has been designed in such a way that deleted messages do not represent a hazard;
2) one regarding the *message logical structure*, an example are all the possible codes that can be applied to the message or specific countermeasures such as sequence numbers, time stamps, etc.;
3) one at a *physical* level, an example is the shielding in order to avoid the corruption due to an electromagnetic interference.

This annex will not deal further with this topic, that has been mentioned only with the aim of supplying an overall picture of the adopted methodology.

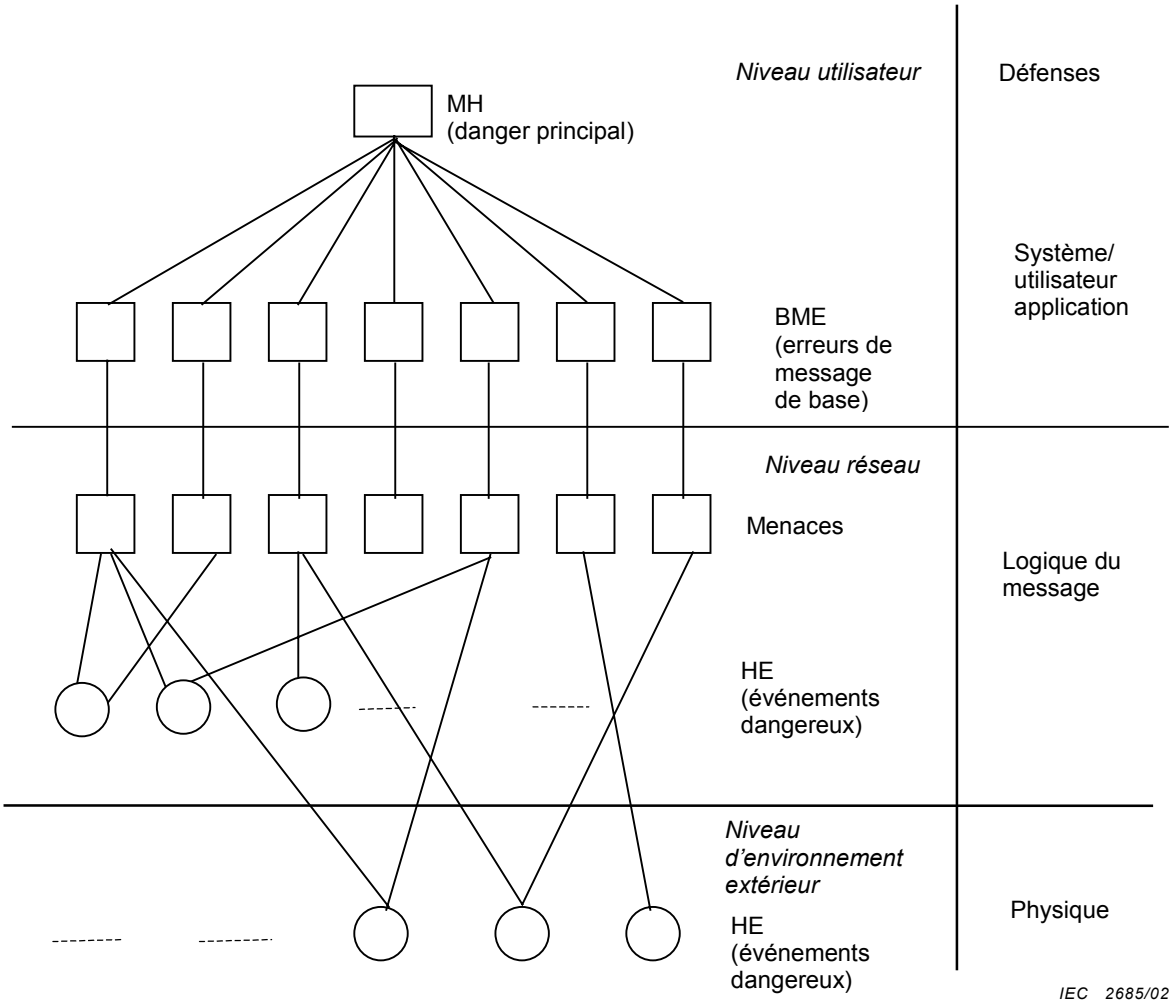



**Figure D.1 – Arbre des dangers**

## D.2 Déduction des messages d'erreur de base

Le message est le sujet principal de toute l'analyse. Le processus de communication a été étudié du point de vue du récepteur. Un message peut être défini comme «*l'information utile crée par une source, à délivrer dans un intervalle de temps* $\Delta t$ *à partir du début de la transmission*».

L'intégrité du flux de messages est le point principal à considérer dans l'identification des dangers qui peuvent se produire en transmettant une communication de sécurité sur un réseau de transmission ouvert.

Un «flux de messages» est défini comme un ensemble ordonné de messages unique pour chaque fenêtre temporelle et récepteur dans un réseau, s'il ne se produit aucune défaillance, attaque ou traitement incorrect.

Le flux de messages effectivement reçu peut être différent de celui attendu pour différentes raisons. Les sous-classes particulières (dangers de base) sont spécifiées comme suit:

- plus de messages reçus qu'attendus;
- moins de messages reçus qu'attendus;
- nombre de messages reçus égal au nombre de messages attendus.

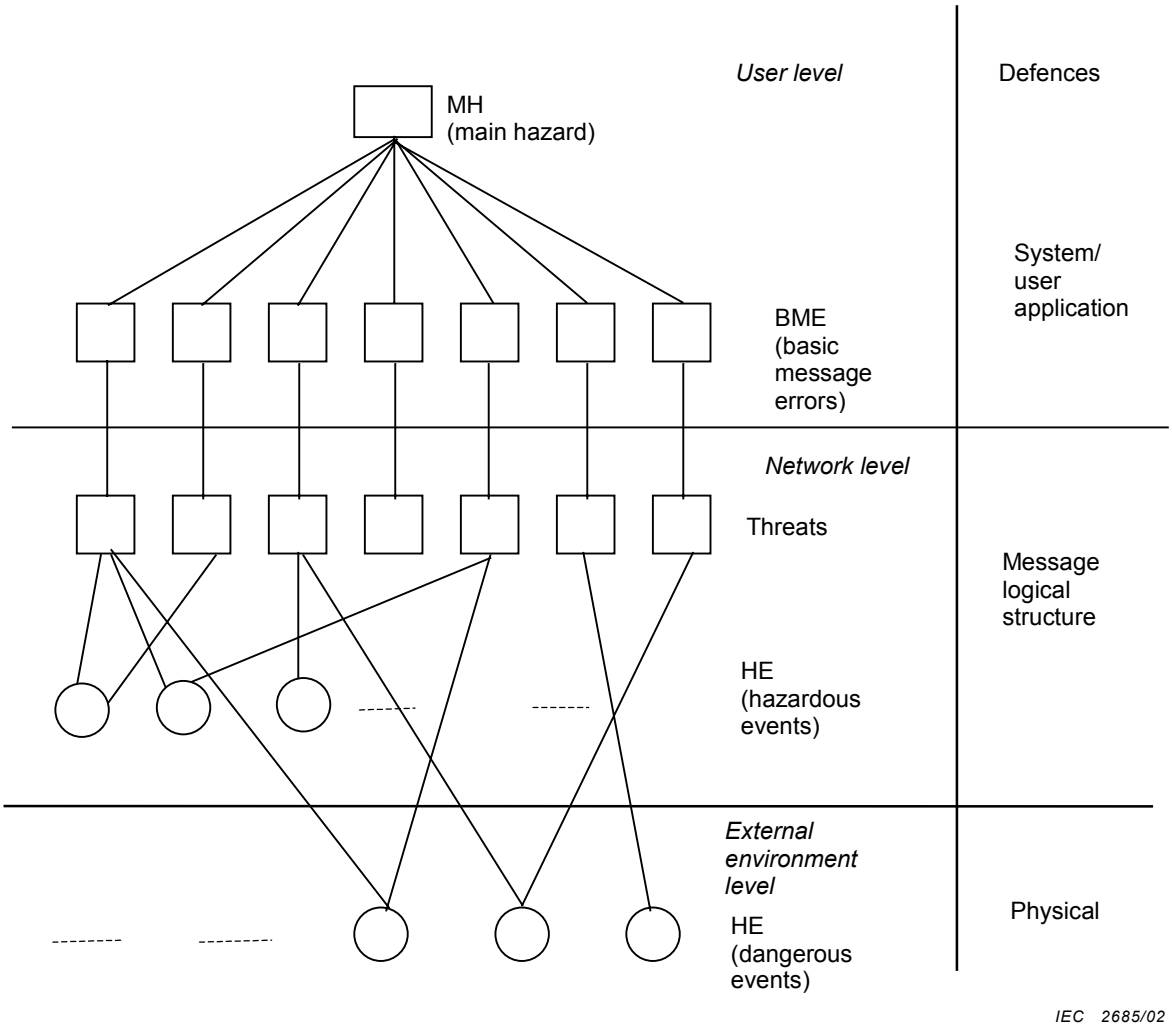



**Figure D.1 – Hazard tree**

## D.2 Derivation of the basic message errors

The message is the main subject of the whole analysis, so the communication process has been studied from the point of view of the receiver. A message can be defined as "*useful information originated by a source to be delivered within a time* $\Delta t$ *from the beginning of the transmission*".

The integrity of the message stream is the main consideration in identifying the hazards that can occur in transmitting a safety-related communication over an open transmission system

A "message stream" is defined as an ordered set of messages, and is unique for each time window and receiver in a network if no failures, attacks or incorrect operations occur.

The message stream actually received can be different from the expected one for a number of reasons. Three particular subclasses are specified (basic hazards):

- more messages received than expected;
- fewer messages received than expected;
- same number of received and expected messages.

**Plus de messages reçus qu'attendus**

Dans ce cas, un ou plusieurs messages ont été répétés ou un message externe a été inséré sur la ligne. L'erreur de message de base est donc le *message répété, inséré*.

**Moins de messages reçus qu'attendus**

Dans ce cas, un ou plusieurs messages ont été supprimés. L'erreur de message de base est donc le *message supprimé*.

**Nombre de messages reçus égal au nombre de messages attendus**

Plusieurs cas ont pu se produire:

- tous les messages sont corrects du point de vue contenu et temps de transit mais la séquence est incorrecte: il y a eu reséquencement;
- la réception d'un message du flux a dépassé le $\Delta t$ nominal: il s'est produit un retard;
- le message a été modifié: il y a eu corruption.
- le récepteur prend l'émetteur du message pour un autre: il y a eu mascarade.

Dans ces deux derniers sous-cas, on a considéré l'intégrité d'un simple message. Les erreurs de message de base sont donc le *message reséquencé, retardé, corrompu, déguisé*.

On a donc identifié l'ensemble ci-après d'erreurs de message de base:

- message répété;
- message supprimé;
- message inséré;
- message reséquencé;
- message corrompu;
- message retardé;
- message déguisé.

Les erreurs de message de base définies ci-devant ne sont pas mutuellement exclusives. Il se peut que plusieurs messages d'un flux soient affectés ou même qu'un simple message soit touché par plusieurs modes d'erreur.

## D.3 Menaces

Des erreurs de message de base de l'article D.1, on déduit directement les menaces correspondantes.

Soit A-B et C-D deux couples de parties autorisées se communiquant des messages de sécurité et soit X un agresseur.

Il y a lieu de relever que des défaillances aléatoires et systématiques logicielles et matérielles sont prises en compte dans la liste des menaces; les explications ci-après ne sont que des exemples et ne sont donc pas exhaustifs.

**Répétition**

- X copie un message ('Vitesse maximale: 250 km/h') et le repasse dans une situation qui peut nuire au récepteur (lorsque le train se trouve sur une section à faible vitesse de circulation)

**More messages received than expected**

In this case, one or more messages have been repeated, or an external message has been inserted on the line. The basic message errors are therefore *repeated, inserted message*.

**Fewer messages received than expected**

In this case, one or more messages have been deleted. The basic message error is therefore *deleted message*.

**Same number of received and expected messages**

In this case, several possibilities can occur:

- all the messages in the stream are correct in content and in transit time but the sequence is wrong: resequencing has taken place;
- for a message in the stream it took longer than nominal $\Delta t$ to reach the receiver: delay has taken place;
- the message has been modified: corruption has taken place;
- the receiver believes that the sender of a message is another than the real one: masquerade has taken place.

In the last two sub-cases, the integrity of the single message has been considered. The basic message errors are *resequenced, delayed, corrupted, masqueraded message*.

The following set of basic message errors has therefore been identified:

- repeated message;
- deleted message;
- inserted message;
- resequenced message;
- corrupted message;
- delayed message;
- masqueraded message.

The above defined basic message errors are not mutually exclusive. It is possible that more messages in a stream and even a single message are affected by more than one error mode.

## D.3 Threats

Being the basic message errors the ones specified in D.1, the derivation of the corresponding threats is straightforward.

Let A-B and C-D be the two couples of authorized parties that communicate safety-related messages, while X is the attacker.

It has to be noted that also random and systematic HW/SW failures are taken into account in the list of threats; the following explanations are only examples and are therefore not exhaustive.

**Repetition**

- X copies a message [‘Maximum speed: 250 km/h’] and replays it in a situation where it may harm the receiver [while the train is in a slow speed track section]

ou

- suite à une défaillance matérielle, le système de transmission non de sécurité répète un ancien message.

**Suppression**

- X détruit un message (X détruit le message 'Arrêt d'urgence' ou 'Vitesse maximale: 250 km/h')

ou

- un message est détruit suite à défaillance matérielle.

**Insertion**

- X insère un message ('Vitesse maximale: 250 km/h')

ou

- un tiers autorisé C insère involontairement un message dans le flux d'information de A vers B (ou vice versa).

**Reséquencement**

- X modifie intentionnellement la séquence des messages pour B (par exemple en retardant un message ou en obligeant un message à prendre un chemin différent dans le réseau)

ou

- la séquence des messages est modifiée suite à une défaillance matérielle.

**Corruption**

- Le message est modifié fortuitement (par exemple par influence électromagnétique [EMI] en un autre message formellement correct

ou

- X modifie un message ('Vitesse maximale: 30 km/h' en 'Vitesse maximale: 250 km/h') de manière plausible de telle sorte que A et/ou B ne peuvent détecter la modification.

**Retard**

- Le système de transmission est surchargé par le trafic normal (par exemple suite à une conception erronée ou par une pointe accidentelle de grand trafic.)

ou

- X crée une surcharge dans le système de transmission en générant des messages d'erreur de telle sorte que le service soit retardé ou arrêté.

**Mascarade**

- A et B veulent se communiquer des données sensibles
- C et D veulent se communiquer des données sensibles
- X prétend être B vis-à-vis de A ou A vis-à-vis de B (ou les deux) pour avoir accès à ces données sensibles ou pour être considéré comme un utilisateur légal du système

ou

- par suite d'une erreur de réseau, B croît de manière erronée que le message vient de A alors que la source réelle est C.

or

- due to a hardware failure the non-safe transmission system repeats an old message.

**Deletion**

- X deletes a message [X deletes the message ‘Emergency Stop’ or ‘Maximum speed: 250 km/h’]

or

- a message is deleted due to a hardware failure.

**Insertion**

- X inserts a message [‘Maximum speed: 250 km/h’]

or

- an authorized third party C involuntary inserts a message in between the information flow from A to B (or vice versa).

**Resequencing**

- X intentionally changes the sequence of messages for B (e.g. by delaying a message or by forcing the message to take a different path through the network)

or

- due to a hardware failure the message sequence is changed.

**Corruption**

- The message is accidentally changed (e.g. EMI) to another formally correct message

or

- X alters a message [‘Maximum speed: 30 km/h’ to ‘Maximum speed: 250 km/h’] in a plausible way so that A and/or B cannot detect the modification.

**Delay**

- The transmission system is overloaded by the normal traffic (e.g. because of wrong design or an accidental high amount of traffic.)

or

- X creates an overload on the transmission system by generating bogus messages so that the service is delayed or stopped.

**Masquerade**

- A and B want to communicate sensitive data
- C and D want to communicate sensitive data
- X pretends towards A to be B or towards B to be A (or both) to get access to the sensitive data or to be regarded as a legal user of the system

or

- due to a network error, B believes erroneously that the message is coming from A, while the real source is C.

## D.4 Une approche possible pour élaborer le dossier de sécurité

L'approche esquissée ci-après est un exemple et n'est pas le seul à pouvoir être suivi. Une analyse de danger complète nécessite une connaissance approfondie de l'application concernée afin de réaliser également une évaluation correcte du risque.

### D.4.1 Méthodes structurées pour l'identification des événements dangereux

Par la suite, l'analyse repose sur le fait que le cas examiné traite d'un réseau interagissant avec l'environnement extérieur. Ces deux entités sont structurées en sous-entités (soulignées dans la figure D.2) pouvant être considérées comme les causes des événements dangereux possibles par rapport au système analysé. L'entité réseau est subdivisée conformément aux différentes étapes de son cycle de vie, alors que la subdivision de l'environnement extérieur prend en considération les deux caractéristiques possibles: physiques et humaines.

Les feuilles de l'arbre de la figure D.2 représentent les causes des dangers: pour chaque cause, on identifie les événements dangereux générés correspondants. Cette procédure facilite l'allocation de probabilité à chaque événement dangereux produit, une fois définie la probabilité d'une cause particulière.

Dans ce qui suit, chaque cause est éclatée en un nombre d'événements dangereux possibles; cet éclatement n'est pas exhaustif: durant l'analyse des dangers, d'autres événements dangereux possibles peuvent être pris en considération dépendant de l'application spécifique.

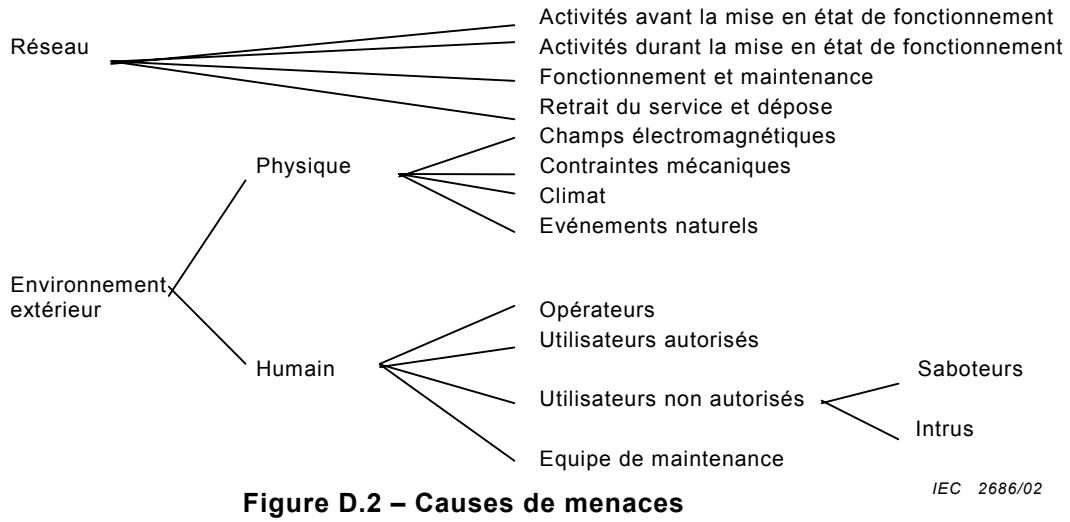



**Figure D.2 – Causes de menaces**

#### D.4.1.1 Réseau

Les phases du cycle de vie du réseau peuvent être définies conformément à la CEI 62278. Pour le domaine concerné par cette annexe (par exemple l'identification des événements dangereux consécutifs aux «erreurs» dans chaque phase), elles peuvent être groupées ensemble comme suit:

- concept, définition système et conditions d'application, analyse de risques, exigences du système, répartition des exigences, conception et mise en oeuvre, fabrication: toutes ces phases sont liées à des activités précédant la mise en état de fonctionnement du système;
- installation, validation du système et acceptation du système: toutes ces phases sont liées à la mise en état de fonctionnement du système;
- fonctionnement et maintenance;
- retrait du service et dépose.

## D.4 A possible approach for building a safety case

The approach that will be outlined hereinafter is an example and is not the only one that can be followed. A complete hazard analysis needs the deep knowledge of the application to which it is related, in order to perform also a proper risk assessment.

### D.4.1 Structured methods for hazardous events identification

In the following, the analysis starts from the consideration that the examined case is dealing with a network interacting with the external environment. These two entities are structured in sub-entities (underlined in Figure D.2) that can be considered as the causes of the possible hazardous events to the analyzed system. The network entity is subdivided according to the several steps of its life-cycle, while the splitting of the external environment entity takes care of its two possible characteristics: the physical and the human ones.

The leaves of the tree in Figure D.2 represent the causes of hazards: for each cause the corresponding generated hazardous events are identified. This way of proceeding makes it also easier, once defined the probability of a single cause, the allocation of probability for each hazardous event produced.

In the following, each cause is split into one number of possible hazardous events; this splitting is not exhaustive: during the hazard analysis some other hazardous events might be taken into account depending on the specific application.

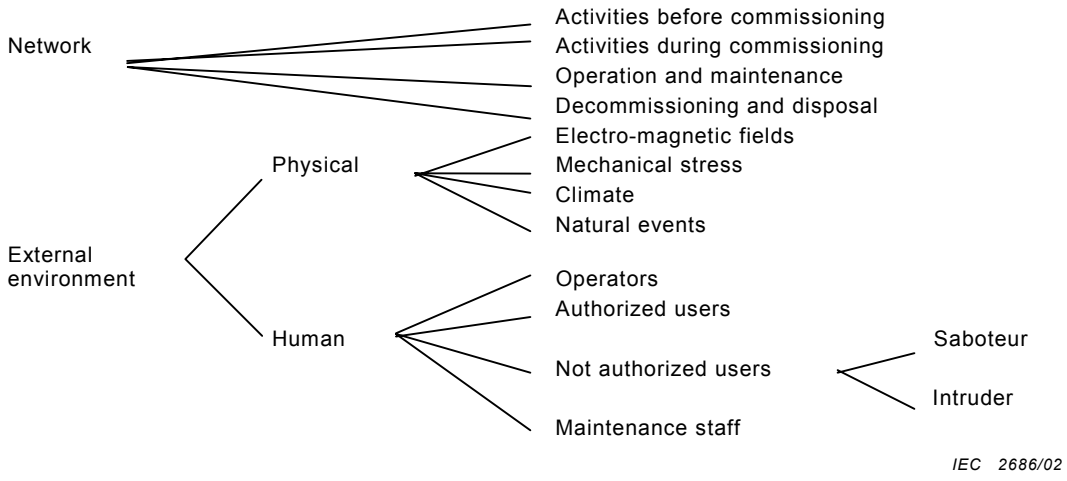



**Figure D.2 – Causes of threats**

#### D.4.1.1 Network

The phases of network life-cycle can be defined according to IEC 62278. For the scope of this annex (i.e. identification of hazardous events arising from ”errors” in each phase), they can be grouped together in the following way:

- concept, system definition and application condition, risk analysis, system requirements, apportionment of system requirements, design and implementation, manufacture: all these phases are related to activities before the commissioning of the system;
- installation, system validation and system acceptance: are related to the commissioning of the system
- operation and maintenance;
- decommissioning and disposal.

**Activités avant la mise en état de fonctionnement**

Des erreurs durant cette phase peuvent conduire à

- des défaillances systématiques matérielles;
- des défaillances systématiques logicielles.

**Activités pendant la mise en état de fonctionnement**

Des erreurs durant cette phase peuvent conduire à

- de la diaphonie;
- des ruptures de connexions;
- des désalignements d'antenne;
- des erreurs de câblage.

**Fonctionnement et maintenance**

Durant cette phase du cycle de vie, des événements dangereux peuvent surgir à la fois de la baisse en performance des composants du système et d'erreurs durant les réparations et les modifications.

**Perte de performance**

- Défaillance aléatoire matérielle
- Vieillissement du matériel.

**Maintenance**

- Utilisation d'instruments non calibrés
- Utilisation d'instruments inadéquats
- Remplacement incorrect de matériel
- Mise à niveau ou remplacement incorrect de logiciel.

**Modification**

- Effets de fading
- Erreurs humaines [5].

**Retrait du service et dépose**

Il n'est pas envisagé que des événements dangereux liés aux erreurs de communication puissent se produire durant cette phase du cycle de vie du réseau.

### D.4.1.2 Environnement extérieur

**Champs électromagnétiques**

- Induction électromagnétique
- Diaphonie (avec le câblage extérieur ou les liens radio).

---

5 Elles dépendent du type particulier d'application et ne peuvent donc pas être spécifiées à ce niveau de l'analyse.

**Activities before commissioning**

Errors during this phase can lead to

- HW systematic failure;
- SW systematic failure.

**Activities during commissioning**

Errors during this phase can lead to

- cross-talk;
- wires breaking;
- antennas misalignment;
- cabling errors.

**Operation and maintenance**

During this phase of life, hazardous events can arise both from loss of performance of system components and from errors during repair and/or modifications.

**Loss of performance**

- HW random failure
- HW ageing.

**Maintenance**

- Use of not calibrated instruments
- Use of not suited instruments
- Incorrect HW replacement
- Incorrect SW upgrading or replacement.

**Modification**

- Fading effects
- Human mistakes[4].

**Decommissioning and disposal**

It is not envisaged that hazardous events related to communication errors can arise during this phase of the network life cycle.

#### D.4.1.2 External environment

**Electro-magnetic fields**

- EMI
- cross-talk (with external cabling or radio links).

4 They depend from the particular type of application and cannot therefore be specified at this level of analysis.

**Contraintes mécaniques**

- Défaillances aléatoires matérielles
- Vieillissement du matériel.

**Climat**

- Bruit thermique
- Vieillissement du matériel
- Défaillances aléatoires matérielles
- Effets de fading.

**Evénements naturels**

- Orage magnétique
- Feu
- Tremblement de terre
- Foudre.

**Opérateurs**

- Erreurs humaines [6].

**Utilisateurs autorisés**

- Erreurs humaines [6]
- Surcharge du système de transmission.

**Equipe de maintenance**

- Utilisation d'instruments non calibrés
- Utilisation d'instruments inadéquats
- Remplacement incorrect de matériel
- Erreurs humaines [6]
- Mise à niveau ou remplacement incorrect de logiciel.

**Saboteur [7]**

- Ecoute
- Dommage matériel
- Modifications indues de logiciel.

**Intrus [7]**

- Surveillance des canaux
- Transmission de messages non autorisés.

---

6 Elles dépendent du type particulier d'application et ne peuvent donc pas être spécifiées à ce niveau de l'analyse.

7 La différence entre un saboteur et un intrus est que le premier ne fait pas attention à ce qui passe sur la ligne, son objectif n'étant que de modifier le réseau, alors que le second ne modifie pas le réseau mais l'utilise pour en tirer un avantage.

**Mechanical stress**

- HW random failures
- HW ageing.

**Climate**

- Thermal noise
- HW ageing
- HW random failures
- Fading effects.

**Natural events**

- Magnetic storm
- Fire
- Earthquake
- Lightning.

**Operators**

- Human mistakes[5].

**Authorized users**

- Human mistakes[5]
- Overloading of transmission system.

**Maintenance staff**

- Use of not calibrated instruments
- Use of not suited instruments
- Incorrect HW replacement
- Human mistakes[5]
- Incorrect SW upgrading or replacement.

**Saboteur**[6]

- Wires tapping
- HW damage or breaking
- Not authorized SW modifications.

**Intruder**[6]

- Monitoring of channels
- Transmission of not authorized messages.



---

5 They depend from the particular type of application and cannot therefore be specified at this level of analysis.

6 The difference between a saboteur and an intruder is that the first does not care of what is on the line, his aim is only to modify the network, whilst the second does not alter the network, he utilises it in order to gain some advantage.

### D.4.2 Relations entre événements dangereux et menaces

En se référant à l'article D.1, chaque menace peut être vue comme un ensemble d'événements dangereux qui la génère. Partant des événements dangereux identifiés dans le paragraphe qui précède, l'étape suivante consiste à bâtir une relation entre ces derniers et les menaces exposées dans l'article D.3 au moyen d'une méthode de type *bottom-up* [8] (de bas en haut).

Le but est de vérifier qu'il n'en résulte aucune menace supplémentaire afin de prouver la validité de l'approche entreprise. La relation entre événements dangereux et menaces peut être représentée par le tableau D.1.

Ainsi qu'on peut le constater, aucune menace supplémentaire n'a été découverte après analyse de chaque événement dangereux; cela prouve que la liste de l'article D.3 est exhaustive.

(Il doit être clair que le tableau D.1 ne considère que les effets primaires de chaque événement dangereux, c'est-à-dire que d'autres relations peuvent être identifiées.)

## D.5 Conclusions

On a identifié deux approches différentes pour déduire un ensemble de menaces possibles sur une transmission de sécurité dans un réseau de communications ouvert. La première est une méthode de type *top-down* partant du danger principal et s'achevant avec la classification de tous les événements dangereux possibles conduisant à ce danger. La seconde part de la définition des deux entités principales du système considéré (c'est-à-dire le réseau et l'environnement extérieur) afin de classer les causes possibles des événements dangereux liés à ce système; ces événements sont ensuite rapportés aux menaces qu'ils génèrent.

Ces deux analyses convergent vers le même ensemble de menaces prouvant ainsi la validité du travail.

---

[8] De manière générale, une telle méthode *bottom-up* est utilisée durant l'analyse du dossier de sécurité pour évaluer les menaces causées par tous les événements dangereux (HE) liés à l'application particulière considérée.

### D.4.2 Relationship between hazardous events – threats

Referring to clause D.1, each threat can be seen as the set of hazardous events which generate it. Starting from the hazardous events identified in the previous subclause, the next step consists in building a relationship between them and the threats outlined in D.3 by means of a bottom-up method[7].

The goal is that of verifying that no extra threat comes out, in order to prove the validity of the undertaken approach. The relationship threats-hazardous events can be represented by the Table D.1.

As it can be seen, no extra threat has been discovered after analyzing each hazardous event; this proves the fact that the list of D.3 is exhaustive.

(It has to be clear that table D.1 considers, for each hazardous event, only the primary effects, i.e. other relationships can be identified).

## D.5 Conclusions

Two different approaches for deriving the set of possible threats to a safety-related transmission in an open communication system have been identified. The first one is a top-down method starting from the main hazard and ending with the classification of all the possible hazardous events leading to the hazard. The second one starts from the definition of the two main entities of the considered system (i.e. the network and the external environment) in order to classify all the possible causes of the hazardous events related to that system; these events are then referred to the threat(s) they generate.

The two analyses converge to the same set of threats, proving therefore the validity of the work.



---

7 Generally speaking, during the safety case analysis such a bottom-up method should be used to evaluate the threats which are caused by all the H.E. related to the particular application.

**Tableau D.1 – Relations entre événements dangereux et menaces**

| Evénements dangereux | Menaces | | | | | | |
|---|---|---|---|---|---|---|---|
| | Répétition | Suppression | Insertion | Réséquencement | Corruption | Retard | Mascarade |
| Défaillances systématiques matérielles | X | X | X | X | X | X | X [1)] |
| Défaillances systématiques logicielles | X | X | X | X | X | X | X [1)] |
| Diaphonie | | X | X | | X | | X [1)] |
| Rupture de connexion | | X | | | X | X | |
| Désalignement d'antennes | | X | | | X | | |
| Erreur de câblage | | X | X | | X | X | X [1)] |
| Défaillances aléatoires matérielles | X | X | X | X | X | X | X [1)] |
| Vieillissement du matériel | X | X | X | X | X | X | X [1)] |
| Utilisation d'instruments non calibrés | X | X | X | X | X | X | X [1)] |
| Utilisation d'instruments inadéquats | X | X | X | X | X | X | X [1)] |
| Remplacement incorrect de matériel | X | X | X | X | X | X | X [1)] |
| Effets de *fading* | | X | | X | X | X | |
| Induction électromagnétique | | X | | | X | | |
| Erreurs humaines | X | X | X | X | X | X | X [1)] |
| Bruit thermique | | X | | | X | | |
| Orage magnétique | | X | | | X | X | |
| Feu | | X | | | X | X | |
| Tremblement de terre | | X | | | X | X | |
| Foudre | | X | | | X | X | |
| Surcharge du système de transmission | | X | | | | X | |
| Ecoute | X | X | X | X | X | X | X [1)] |
| Dommage matériel | | X | | | X | X | |
| Modifications indues de logiciel | X | X | X | X | X | X | X [2)] |
| Transmission de messages non autorisés | X | | X | | | | X [2)] |
| Surveillance des canaux [3)] | | | | | | | |

[1)] Dans ce cas, un message correct est délivré à un mauvais destinataire, par exemple suite à un mauvais routage; une contre-mesure possible est la spécification de l'adresse de l'émetteur.

[2)] Au cas où le message est frauduleux depuis le début, une forte défense est nécessaire, par exemple l'emploi d'une clé.

[3)] L'absence de menace pour l'événement dangereux (HE) «surveillance des canaux» est compréhensible; le secret, en fait, est une exigence du système: cela concerne l'application particulière considérée.

**Table D.1 – Relationship between hazardous events – threats**

| Hazardous events | Threats | | | | | | |
|---|---|---|---|---|---|---|---|
| | Repetition | Deletion | Insertion | Rese-quencing | Corruption | Delay | Masque-rade |
| HW systematic failure | X | X | X | X | X | X | X [1)] |
| SW systematic failure | X | X | X | X | X | X | X [1)] |
| Cross-talk | | X | X | | X | | X [1)] |
| Wires breaking | | X | | | X | X | |
| Antennas misalignment | | X | | | X | | |
| Cabling errors | | X | X | | X | X | X [1)] |
| HW random failures | X | X | X | X | X | X | X [1)] |
| HW ageing | X | X | X | X | X | X | X [1)] |
| Use of not calibrated instruments | X | X | X | X | X | X | X [1)] |
| Use of not suited instruments | X | X | X | X | X | X | X [1)] |
| Incorrect HW replacement | X | X | X | X | X | X | X [1)] |
| Fading effects | | X | | X | X | X | |
| EMI | | X | | | X | | |
| Human mistakes | X | X | X | X | X | X | X [1)] |
| Thermal noise | | X | | | X | | |
| Magnetic storm | | X | | | X | X | |
| Fire | | X | | | X | X | |
| Earthquake | | X | | | X | X | |
| Lightning | | X | | | X | X | |
| Overloading of transmission system | | X | | | | X | |
| Wires tapping | X | X | X | X | X | X | X [1)] |
| HW damage or breaking | | X | | | X | X | |
| Not authorized SW modifications | X | X | X | X | X | X | X [2)] |
| Transmission of not authorised messages | X | | X | | | | X [2)] |
| Monitoring of channels [3)] | | | | | | | |

1) In this case, a correct message is delivered to the wrong receiver due, for instance, to a misrouting; a possible countermeasure is the specification of the sender address.

2) In this case, the message is fraudulent from the beginning; a strong defence is needed, for example the use of a key.

3) It makes sense that there is no threat for the hazardous event ”monitoring of channels”; the secrecy, in fact, is a system requirement: it has to do with the particular application.

**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 2-8318-6679-0


**ICS 45.060**

Typeset and printed by the IEC Central Office
GENEVA, SWITZERLAND