# *Republic of Bulgaria*

## EDICT OF GOVERNMENT

In order to promote public education and public safety, equal justice for all, a better informed citizenry, the rule of law, world trade and world peace, this legal document is hereby made available on a noncommercial basis, as it is the right of all humans to know and speak the laws that govern them.

EN 50159:2010: Railway applications - Communication, signalling and processing systems -- Part 1: Safety-related communication in closed transmission systems [Required by Directive 2008/57/EC]

BLANK PAGE


Декември 2010

БЪЛГАРСКИ ИНСТИТУТ ЗА СТАНДАРТИЗАЦИЯ

**БЪЛГАРСКИ СТАНДАРТ**

# БДС EN 50159

ICS: 45.020, 35.240.60

Заменя:
БДС EN 50159-1:2004; БДС EN 50159-2:2004.

## Железопътна техника. Системи за съобщения, сигнализация и обработка на данни. Съобщения, свързани със сигурността в предавателни системи

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

**Европейският стандарт EN 50159:2010 има статут на български стандарт от 2010-12-17.**

Този стандарт е официалното издание на Българския институт за стандартизация на английски език на европейския стандарт EN 50159:2010.

66 стр.



Национален № за позоваване:БДС EN 50159:2010

## НАЦИОНАЛЕН ПРЕДГОВОР

Този стандарт е подготвен с участието на БИС/ТК 70 "Железопътен транспорт".

Следват 64 страници на EN 50159:2010.

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

# EN 50159

September 2010

ICS 35.240.60; 45.020

Supersedes EN 50159-1:2001, EN 50159-2:2001

English version

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

Applications ferroviaires - Systèmes de signalisation, de télécommunication et de traitement - Communication de sécurité sur des systèmes de transmission

Bahnanwendungen - Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme - Sicherheitsrelevante Kommunikation in Übertragungssystemen

This European Standard was approved by CENELEC on 2010-09-01. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the Central Secretariat or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the Central Secretariat has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and the United Kingdom.

CENELEC

European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

**Management Centre: Avenue Marnix 17, B - 1000 Brussels**



Ref. No. EN 50159:2010 E

## Foreword

This European Standard was prepared by SC 9XA, Communication, signalling and processing systems, of Technical Committee CENELEC TC 9X, Electrical and electronic applications for railways. It was submitted to the formal vote and was approved by CENELEC as EN 50159 on 2010-09-01.

This document supersedes EN 50159-1:2001 and EN 50159-2:2001.

The contents of both standards have been merged; the informative Annex E gives a mapping between these previous editions and the present document.

This European Standard is closely related to EN 50129:2003.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN and CENELEC shall not be held responsible for identifying any or all such patent rights.

The following dates were fixed:

| | | |
|---|---|---|
| – latest date by which the EN has to be implemented at national level by publication of an identical national standard or by endorsement | (dop) | 2011-09-01 |
| – latest date by which the national standards conflicting with the EN have to be withdrawn | (dow) | 2013-09-01 |

This draft European Standard has been prepared under a mandate given to CENELEC by the European Commission and the European Free Trade Association and covers essential requirements of EC Directives 96/48/EC (HSR), recast by EC Directives 2008/57/EC (RAIL). See Annex ZZ.

# Contents

**Figures**



**Tables**

## Introduction

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

The transmission system considered in this standard, which serves the transfer of information between different locations, has in general no particular preconditions to satisfy. It is from the safety point of view not trusted, or not fully trusted.

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

Although the RAM aspects are not considered in this standard it is recommended to keep in mind that they are a major aspect of the global safety.

The safety requirements depend on the characteristics of the transmission system. In order to reduce the complexity of the approach to demonstrate the safety of the system, transmission systems have been classified into three categories:

– Category 1 consists of systems which are under the control of the designer and fixed during their lifetime;

– Category 2 consists of systems which are partly unknown or not fixed, however unauthorised access can be excluded;

– Category 3 consists of systems which are not under the control of the designer, and where unauthorised access has to be considered.

The first category was covered by EN 50159-1:2001, the others by EN 50159-2:2001.

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

# 1 Scope

This European Standard is applicable to safety-related electronic systems using for digital communication purposes a transmission system which was not necessarily designed for safety-related applications and which is

– under the control of the designer and fixed during the lifetime, or

– partly unknown or not fixed, however unauthorised access can be excluded, or

– not under the control of the designer, and also unauthorised access has to be considered.

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

This standard gives the basic requirements needed to achieve safety-related communication between safety-related equipment connected to the transmission system.

This European Standard is applicable to the safety requirement specification of the safety-related equipment connected to the transmission system, in order to obtain the allocated safety integrity requirements.

Safety requirements are generally implemented in the safety-related equipment, designed according to EN 50129. In certain cases these requirements may be implemented in other equipment of the transmission system, as long as there is control by safety measures to meet the allocated safety integrity requirements.

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

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

This European Standard does not specify

– the transmission system,

– equipment connected to the transmission system,

– solutions (e.g. for interoperability),

– which kind of data are safety-related and which are not.

A safety-related equipment connected through an open transmission system can be subjected to many different IT security threats, against which an overall program has to be defined, encompassing management, technical and operational aspects.

In this European Standard however, as far as IT security is concerned, only intentional attacks by means of messages to safety-related applications are considered.

This European Standard does not cover general IT security issues and in particular it does not cover IT security issues concerning

– ensuring confidentiality of safety-related information,

– preventing overloading of the transmission system.

## 2 Normative references

The following 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.

CLC/TR / EN 50126 series, *Railway applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)*

EN 50129:2003, *Railway applications – Communication, signalling and processing systems – Safety related electronic systems for signalling*

## 3 Terms, definitions and abbreviations

### 3.1 Terms and definitions

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

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

**3.1.2**
**access protection**
processes designed to prevent unauthorised access to read or to alter information, either within user safety-related systems or within the transmission system

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

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

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

**3.1.6**
**closed transmission system**
fixed number or fixed maximum number of participants linked by a transmission system with well known and fixed properties, and where the risk of unauthorised access is considered negligible

**3.1.7**
**communication**
transfer of information between applications

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

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

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

NOTE By knowing the output data, it is impossible within a reasonable time to calculate the input data without knowledge of the key. It is also impossible within a reasonable time to derive the key from the output data, even if the input data are known.

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

**3.1.12**
**data**
part of a message which represents some information (see also user data, additional data, redundant data)

**3.1.13**
**data corruption**
alteration of data

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

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

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

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

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

**3.1.19**
**failure**
deviation from the specified performance of a system

NOTE A failure is the consequence of a fault or an error in the system.

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

NOTE A fault can be random or systematic.

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

**3.1.22**
**hacker**
person trying deliberately to bypass access protection

**3.1.23**
**hazard**
condition that can lead to an accident

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

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

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

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

**3.1.28**
**integrity**
state in which information is complete and not altered

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

NOTE 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.

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

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

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

NOTE By the whole message is meant also any implicit data of the message which is not sent to the transmission system.

**3.1.33**
**message enciphering**
transformation of bits by using a cryptographic technique within a message, in accordance with an algorithm controlled by keys, to render casual reading of data more difficult. Does not provide protection against data corruption

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

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

**3.1.36**
**message stream**
ordered set of messages

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

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

**3.1.39**
**random failure**
failure that occurs randomly in time

**3.1.40**
**redundancy check**
type of check that a predefined relationship exists between redundant data and user data within a message, to prove message integrity

**3.1.41**
**redundant data**
additional data, derived, by a safety-related transmission function, from the user data

**3.1.42**
**relative time stamp**
time stamp referenced to the local clock of an entity. In general there is no relationship to clocks of other entities

**3.1.43**
**repeated message**
type of message error in which a single message is received more than once

**3.1.44**
**re-sequenced message**
type of message error in which the order of messages in the message stream is changed

**3.1.45**
**safe fall back state**
safe state of a safety-related equipment or system as a deviation from the fault-free state and as a result of a safety reaction leading to a reduced functionality of safety-related functions, possibly also of non safety-related functions

**3.1.46**
**safety**
freedom from unacceptable levels of risk

**3.1.47**
**safety case**
documented demonstration that the product complies with the specified safety requirements

**3.1.48**
**safety code**
redundant data included in a safety-related message to permit data corruptions to be detected by the safety-related transmission function

**3.1.49**
**safety integrity level**
number which indicates the required degree of confidence that a system will meet its specified safety functions with respect to systematic failures

**3.1.50**
**safety reaction**
safety-related protection taken by the safety process in response to an event (such as a failure of the transmission system), which may lead to a safe fall back state of the equipment

**3.1.51**
**safety-related**
carries responsibility for safety

**3.1.52**
**safety-related transmission function**
function incorporated in the safety-related equipment to ensure authenticity, integrity, timeliness and sequence of data

**3.1.53**
**sequence number**
additional data field containing a number that changes in a predefined way from message to message

**3.1.54**
**source and destination identifier**
identifier which is assigned to each entity. This identifier can be a name, number or arbitrary bit pattern. This identifier will be used for the safety-related communication. Usually the identifier is added to the user data

**3.1.55**
**systematic failure**
failure that occurs repeatedly under some particular combination of inputs, or under some particular environmental condition

**3.1.56**
**threat**
potential violation of safety

**3.1.57**
**time stamp**
information concerning time of transmission attached to a message by the sender

**3.1.58**
**timeliness**
state in which information is available at the right time according to requirements

**3.1.59**
**transmission code**
redundant information, added to the safety and non safety message of the non-trusted transmission system in order to ensure the integrity of the message during transmission

**3.1.60**
**transmission system**
service used by the application to communicate message streams between a number of participants, who may be sources or sinks of information

**3.1.61**
**trusted**
which has properties used as evidence to support the safety demonstration

**3.1.62**
**unauthorised access**
situation in which user information or information within the transmission system is accessed and/or changed by unauthorised persons or hackers

**3.1.63**
**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

**3.1.64**
**valid message**
message whose form meets in all respects the specified user requirements

**3.1.65**
**validity**
state of meeting in all respects the specified user requirements

## 3.2 Abbreviations

For the purpose of this document, the following abbreviations apply.

| | |
|---|---|
| BCH | Bose, Ray-Chaudhuri, Hocquenghem Code |
| B.M.E. | Basic Message Errors |
| BSC | Binary Symmetric Channel |
| CAN | Controller Area Network |
| CRC | Cyclic Redundancy Check |
| EC | European Community |
| ECB | Electronic CodeBook mode |
| EMI | Electromagnetic Interference |
| FTA | Fault Tree Analysis |
| GPRS | General Packet Radio Service |
| GSM-R | Global System for Mobile communication – Railways |
| H.E. | Hazardous Events |
| HW | Hardware |
| IT | Information Technology |
| LAN | Local Area Network |
| MAC | Message Authentification Code |
| MDC | Manipulation Detection code |
| MD4, MD5 | Message Digest algorithms |
| M.H. | Main Hazard |
| MTBF | Mean Time Between Failures |
| MVB | Multi-purpose Vehicle Bus |
| PROFIBUS | Process Field Bus |
| QSC | q-nary symmetric channel |
| RAMS | Reliability, Availability, Maintainability and Safety |
| SIL | Safety Integrity Level |
| SR | Safety Related |

| | |
|---|---|
| SRS | Safety Requirements Specifications |
| SW | Software |
| TX | Transmission |
| UTC | Universal Coordinated Time |
| WAN | Wide Area Network |
| Wi-Fi | Wireless Fidelity |

# 4 Reference architecture

This European Standard defines the safety requirements for the safe communication between safety-related equipment via a transmission system, which can either be closed or open. Both, safety-related and non safety-related equipment can be connected to the transmission system. This clause describes possible configurations of the safety-related communication in transmission systems including the definition of involved functional blocks. Particular requirements to be fulfilled by these blocks are specified in further clauses.

A combined view – open and closed transmission system – of the principal architecture is shown in Figure 1, where all communication elements are linked according to the information flow to exchange safety-related information between safety-related equipment. The reference architecture also shows a non-safety-related interface which is not always present. A typical use could be for diagnostic messages routed to a maintenance centre.

Besides the source and destination of safety-related communication the reference architecture deals with a safety-related communication system, which can be divided into

– safety-related transmission functions incorporated in the safety-related equipment. These functions ensure authenticity, integrity, timeliness and sequence of data,

– safety-related cryptographic techniques which protect the safety-related message. These can either be realised by incorporating them in the safety-related equipment or having them outside of the safety-related equipment but checked by safety techniques. These techniques protect the safety-related message in a Category 3 transmission system and are not needed in the case of a Category 1 or 2 transmission system,

– a non safety-related, open or closed transmission system which may itself include transmission protection functions and/or access protection functions.

The characteristics of closed transmission systems (Category 1) are as follows:

– the number of pieces of connectable equipment – either safety-related or not – to the transmission system is known and fixed;

– the risk of unauthorized access is considered negligible;

– the physical characteristics of the transmission system (e.g. transmission media, environment according to design hypothesis, etc.) are fixed and unchanged during the life cycle of the system.

The open transmission system (Category 2 and/or 3) 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, and 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 open transmission system, in accordance with a program not known to the user;

– other users of the transmission system, not known to the safety-related application designer, sending unknown amounts of information, in unknown formats.

The open transmission system of Category 3 may be subject to unauthorised access to the transmission system for malicious purposes.

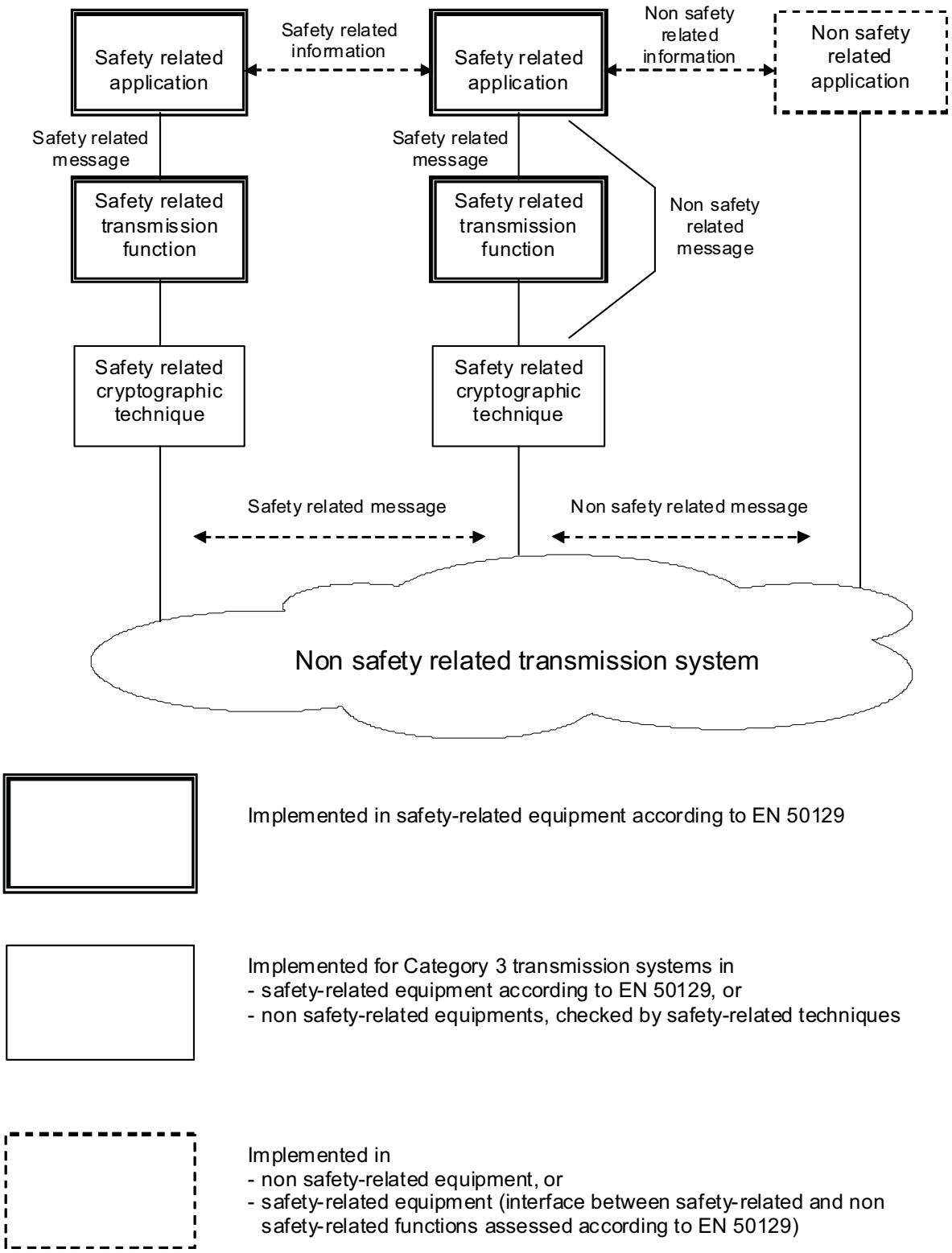



**Figure 1 – Reference architecture for safety-related communication**

The reference architecture is not intended to restrict implementations; different structures are possible, see examples in the informative Annex C and in particular Clause C.5 for non safety-related messages.

# 5 Threats to the transmission system

The main hazard to safety-related communication is the failure to obtain a valid message in terms of authenticity, integrity, sequence and timeliness at the receiving end. This standard considers threats to these message properties arising from the transmission system. Threats to the safety-related equipment shall be considered in accordance with EN 50129.

However, meeting the requirements of this standard does not give protection against intentional or unintentional misuse coming from authorised sources. It is necessary for the safety case to address these aspects.

Further information, with guidelines on threat analysis and safety case, is included in informative Annex A. It shall be emphasised that an analysis shall be made for each project, so although the methodology for message errors of Annex A can be included, it will not on its own necessarily be complete.

Hazardous events identified may include the following:

– systematic failure;
– broken wires;
– cabling errors;
– antenna misalignment;
– performance loss;
– HW random failure and ageing;
– human error;
– maintenance error;
– EMI;
– cross-talk;
– thermal noise;
– fading effects;
– overloading of transmission system;
– magnetic storm;
– fire;
– earthquake;
– lightning

as well as deliberately-caused events such as

– wire-tapping,
– damage or unauthorised change to HW,
– unauthorised change to SW,
– monitoring of channels,
– transmission of unauthorised messages.

However, although there can be a wide range of hazardous events, the basic message errors, which form the threats to the transmission system, are one of the following:

– repetition;
– deletion;
– insertion;
– re-sequencing;
– corruption;

– delay;

– masquerade.

Table A.1 suggests which threats to the transmission system can be caused by each type of hazardous event. Having identified the hazardous events – not protected by other means – that can occur for a particular system, the table can be used as a guide to identify the threats to be considered for that system.

Table A.1 does not contain probabilities of occurrence; this shall be part of analysis of threats.

# 6 Classification of transmission systems

## 6.1 General

This clause defines the process to be used to classify all transmission systems, identifying the threats relevant for such systems that affect the choice of defences for inclusion in the safety application.

## 6.2 General aspects of classification

There are many factors which can influence the threats to a safety-related communication system.

For example it is possible that transmission services can be obtained by the signalling system user from private or public telecommunications service providers. Under such service provision contracts, the responsibility of the service provider for guaranteeing performance of the transmission system can be limited.

Therefore the significance of threats (and hence the requirements for defences) depend on the extent of control exercised by the user over the transmission system, 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 re-sequencing of messages);

– the consistency of the performance of the system over its life (e.g. as changes to the system, 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.

Following these issues three categories of transmission systems can be defined.

## 6.3 Criteria for the classification of transmission systems

### 6.3.1 Criteria for Category 1 transmission systems

A transmission system can be considered to be of Category 1 if the following preconditions are fulfilled.

**Pr1** The number of pieces of connectable equipment – either safety-related or not – to the transmission system is known and fixed. As the safety-related communication depends on this parameter, the maximum number of participants allowed to communicate together shall be put into the safety requirement specification as a precondition. The configuration of the system shall be defined/ embedded in the safety case. Any subsequent change to that configuration shall be preceded by a review of their effects on the safety case.

**Pr2** The characteristics of the transmission system (e.g. transmission media, environment under worst case conditions, etc.) are known and fixed. They shall be maintained during the life cycle of the system. If major parameters which were used in the safety case are to be changed, all safety-related aspects shall be reviewed.

**Pr3** The risk of unauthorised access to the transmission system shall be negligible.

If a transmission system satisfies all the above preconditions, it may be considered as **Category 1** and a closed system and, if so, it shall comply with a generally reduced set of processes and requirements given in Clause 7.

#### 6.3.2 Criteria for Category 2 transmission systems

If a transmission system does not satisfy the preconditions 1 or 2 (Pr1 or Pr2) of 6.3.1, but fulfils precondition 3 (Pr3) it shall be considered as **Category 2** and an open system, and shall be assessed with a more comprehensive set of processes and requirements given in Clause 7.

#### 6.3.3 Criteria for Category 3 transmission systems

If a transmission system does not satisfy the precondition 3 (Pr3) of 6.3.1 it shall be considered as **Category 3** and an open system, and shall be assessed with the full set of processes and requirements given in Clause 7.

### 6.4 Relationship between transmission systems and the threats

The significance of threats to the safety-related communication system shall be assessed according to the extent of control exercised by the user over the transmission system.

The threats identified in Clause 5 are applicable to all the transmission systems categories with the exception of masquerade, which is only applicable to open transmission systems.

In Annex B an example of classification of transmission systems is given in Table B.1 and an example of threat/category relationship is given in Table B.2.

The applicability of Clause 7 depends on the category of the transmission system.

## 7 Requirements for defences

### 7.1 Preface

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.

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

– message authenticity;

– message integrity;

– message timeliness;

– message sequence.

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.

A number of architectural issues shall be considered by the particular application and justified in the Safety Case, for example

– conditions for claiming and maintaining the compliance with preconditions of Category 1 or 2 transmission systems,

– criteria for the separation among transmission systems of different categories,

– robustness of transmission systems against denial of service resulting from flooding attacks, e.g. need of firewalls.

With reference to h), the scope of this standard excludes general IT security issues:

– only attacks during the operational phase are considered;

– only attacks by means of messages to safety-related applications are addressed here .

However, a complete access protection policy should consider

– procedural and maintenance aspects of access protection,

– vulnerability of software not part of the safety-related application,

– confidentiality of information.

## 7.2 General requirements

**7.2.1** Adequate defences shall be provided against all identified threats to the safety of systems using an open or closed transmission system. Any assumptions of threats which are to be ignored shall be justified and recorded in the safety case. Annex A derives a possible list of threats, to be used as guidance.

**7.2.2** In case of communication between safety-related and non safety-related applications via the same transmission system the following requirements apply:

– the safety defences implemented in the safety-related transmission functions shall be demonstrated as being functionally independent from defences used by the non safety-related functions;

– the safety-related and non safety-related messages shall have different structures achieved by applying a safety code to safety-related messages. This safety code shall be capable of protecting the system to the required safety integrity (see 7.3.7) so that a non safety-related message cannot be corrupted into a safety-related one.

**7.2.3** 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 C 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.

**7.2.4** 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.

**7.2.5** All defences shall be implemented according to the requirements defined in EN 50129. This implies that the defences

– shall be implemented completely in the safety-related transmission equipment (with the possible exception of some cryptographic architectures, see 7.3.8 and Clause C.2),

– shall be functionally independent from the layers used in the non-trusted transmission system.

**7.2.6** Mandatory requirements for particular defences are given in the following subclauses. They apply when the particular defence is used.

**7.2.7** 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.

**7.2.8** The evidence of functional and technical safety shall follow the same process as specified in EN 50129, including

– an overall error model,

– a functional specification based on analysis of the overall error model,

– analysis of each defence used in the safety-related communication,

– the safety reaction in case of a detected transmission error,

– a safety integrity requirement specification and SIL allocation.

**7.2.9** Subclause 7.3 defines a comprehensive set of defences. However for Category 1 transmission systems, the following reduced set is sufficient, still maintaining the fundamental safety services:

– source and/or destination identifiers (in case of more than one sender and/or more than one receiver);

– sequence number and/or time stamps to the extent needed by the application; and

– a safety code.

## 7.3 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 C.

### 7.3.1 Sequence number

#### 7.3.1.1 Preface

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.

#### 7.3.1.2 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 initialisation and roll-over of the sequence number;

– the provision for recovery following interruption of the sequence of the messages.

### 7.3.2 Time stamp

#### 7.3.2.1 Preface

When an entity receives information, the meaning of the information is often time-related. The degree of dependence between information and time can 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 Clause C.1.

#### 7.3.2.2 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 coordinated time) or any other global clock);

– the synchronism of the timers in the various entities;

– the time delay between originating the information and adding a time stamp to it;

– the time delay between checking the time stamp and using the information.

### 7.3.3 Time-out

#### 7.3.3.1 Preface

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.

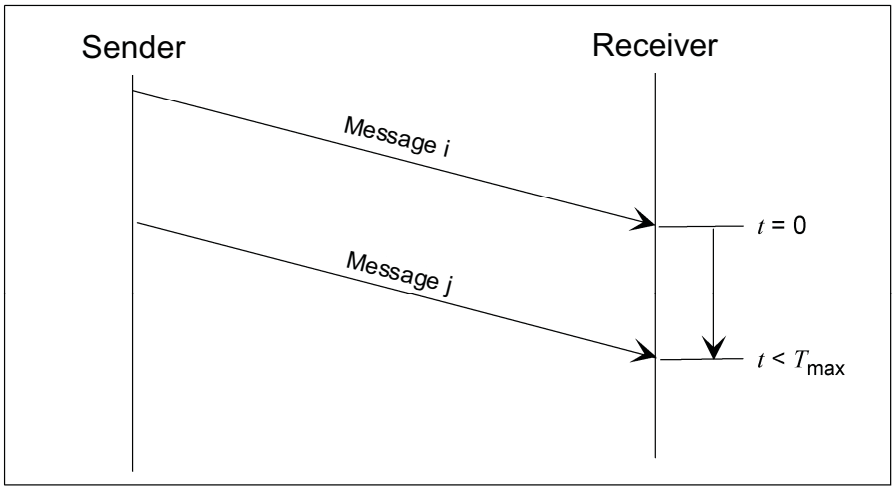



**Figure 2 – Cyclic transmission of messages**

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.

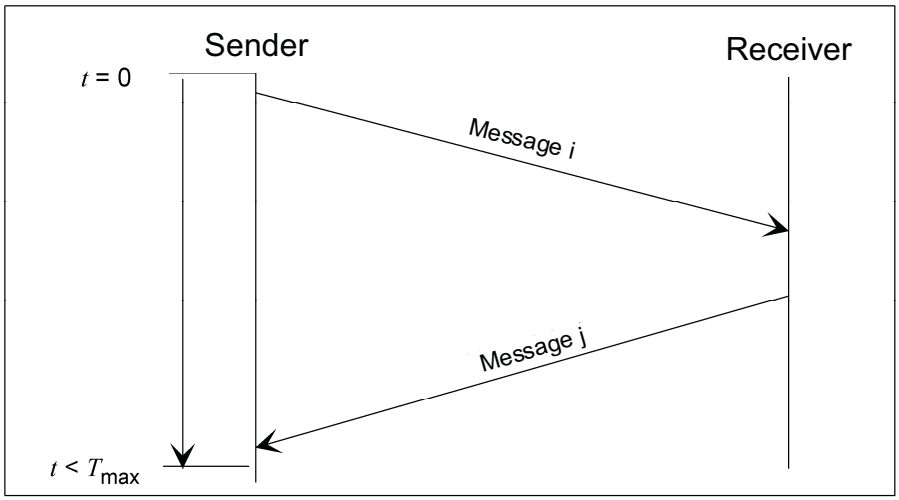



**Figure 3 – Bi-directional transmission of messages**

#### 7.3.3.2 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.

### 7.3.4 Source and destination identifiers

#### 7.3.4.1 Preface

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 unidirectional or broadcast communications.

– 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 unidirectional or broadcast communications. Destination identifiers can be chosen to identify individual destinations, or groups of users.

#### 7.3.4.2 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.

### 7.3.5 Feedback message

#### 7.3.5.1 Preface

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 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 synchronisation of clocks in sending and receiving equipment;

– by facilitating dynamic checking procedures between parties.

#### 7.3.5.2 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.

### 7.3.6 Identification procedure

#### 7.3.6.1 Preface

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

Open transmission systems can 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.

#### 7.3.6.2 Requirements

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

### 7.3.7 Safety code

#### 7.3.7.1 Preface

In transmission systems, in general, transmission codes are used to detect bit and/or burst errors, and/or to improve the transmission quality by error-correction techniques. Even though these transmission codes can be very efficient, they can fail because of hardware faults, external influences or systematic errors.

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

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

– the capability for detection of expected systematic types of message corruption;

– the probability of detection of random types of message corruption.

NOTE The safety code can be a combination of different codes, e.g. a linear code combined with a constant value.

Guidance for selection of safety codes is given in Clause C.3.

#### 7.3.7.2 Requirements

**7.3.7.2.1** The safety code shall be different from the transmission code. This difference can be gained

– either by using different algorithms, or

– by using different configuration parameters (e.g. polynomials) for the same algorithms. If both codes are based on a CRC, the polynomials shall be different. If both polynomials have common factors, their contribution to the performance of the safety code shall be neglected in the safety analysis.

NOTE In the case of a closed transmission system, the designer can simply choose a safety code which is different to the transmission code, because he has full knowledge about the transmission system. In the case of an open transmission system, this requirement can be fulfilled by using a safety code which is not used by commercial transmission systems.

**7.3.7.2.2** The safety code shall detect

– transmission errors, e.g. caused by EMI,

– systematic errors caused by hardware failures within the non-trusted transmission system.

NOTE Failures which would mimic the safety code cannot adequately be detected. Therefore the safety code has to be more complex than the expected failures. Hence it can be assumed that a hardware failure in the non-trusted transmission system cannot generate a valid safety code.

**7.3.7.2.3** To fulfil the required safety integrity it is necessary that the safety code is sufficient complex, e.g. based on a CRC, to detect and act on typical faults and errors. The analysis shall at least include:

– interrupted transmission line;

– all bits logical 0;

– all bits logical 1;

– message inversion;

– synchronisation slip (in case of serial transmission);

– random errors;

– burst errors;

– systematic errors, e.g. repeated error patterns;

– combinations of the above.

**7.3.7.2.4** The probabilistic analysis of the performance of the safety code shall be compatible with the safety target. A model of the failure modes shall be provided and all assumptions made for the calculations shall be verified and validated.

The probability of undetected errors of linear codes is often calculated by using the binary symmetric channel (BSC) model (see Clause C.4). In the case the non binary code is used, the q-nary symmetrical channel (QSC) can be more suitable. This standard recommends limiting this probability to the worst case value calculated by these models.

NOTE The BSC is well suited for random errors as caused by EMI. But simple random errors are usually eliminated by the non-trusted transmission system. Therefore, if an error is detected by the safety code, usually many bits in the safety-related message are disturbed. Because no simple models are available for these cases, this standard recommends not using lower probabilities of undetected errors than the worst case value achieved by the application of the BSC for bit error rate less than one half (see Clause C.4).

An example of a simplified model for a closed transmission system is given in Clause C.4 (informative).

### 7.3.8 Cryptographic techniques

#### 7.3.8.1 Preface

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

This is usually the case when safety-related communication uses

– a public network,

– a radio transmission system,

– a transmission system with connections to public networks.

Against intentional attacks by means of messages to safety-related applications, the safety-related messages shall be protected with cryptographic techniques.

This requirement, aimed at avoiding masquerade from unauthorized senders, can be met by one of the following solutions:

1) use a safety code able to provide cryptographic protection;

2) encipher the messages after the safety code has been applied;

3) add a cryptographic code to the safety code.

These techniques can be combined with the safety encoding mechanism or provided separately. Annex C 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.

#### 7.3.8.2 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 (e.g. symmetric or asymmetric),
  - key characteristics (e.g. fixed or session-based),
  - justification of selected key length,
  - frequency of key update,
  - physical storage of keys,

– technical choice of cryptographic architectures, including
  - checking the correct functioning (before and during the operational phase) of the cryptographic processes when they are implemented outside the safety-related equipment,

– 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 may be applied over additional data that is not transmitted but is known to the sender and receiver (implicit data).

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

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

## 7.4 Applicability of defences

### 7.4.1 Preface

The defences outlined in 7.3 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 each defined possible threat.

### 7.4.2 Threats/defences matrix

The Xs in Table 1 indicate that a defence can provide protection against the corresponding threat. The defences in Table 1 can be expanded in accordance with 7.2.7.

**Table 1 – Threats/Defences matrix**

| Threats | Defences | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | **Sequence number** | **Time stamp** | **Time-out** | **Source and destination identifiers** | **Feed-back message** | **Identification procedure** | **Safety code** | **Cryptographic techniques** |
| Repetition | X | X | | | | | | |
| Deletion | X | | | | | | | |
| Insertion | X | | | X [a] | X [b] | X [b] | | |
| Re-sequence | X | X | | | | | | |
| Corruption | | | | | | | X [c] | X |
| Delay | | X | X | | | | | |
| Masquerade | | | | | X [b] | X [b] | | X [c] |

[a] 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 7.3.8.

[b] Application dependent.

[c] See 7.4.3 and Clause C.2.

### 7.4.3 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 C.2.

# Annex A
(informative)

# Threats on open transmission systems

## A.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 can arise either in normal conditions (i.e. without failures) or abnormal conditions (i.e. following failures of the transmission system).

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 A.1), into three separate levels:

– the user level;

– the network level;

– the external environment level.

These levels follow a top-down approach, starting from the *main hazard* (M.H.), which is the failure to obtain a valid message in terms of authenticity, integrity, sequence and timeliness at the receiving 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* (B.M.E.), intended as a classification of all possible message failure modes, has been 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 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* (H.E.), which can be present at both the network and the external environment level. The same hazardous event can obviously be related to different threats.

Splitting the analysis into different levels also provides the possibility of (at least) three levels of defences:

a) one at a system/user application level, dealing with system implementation independently from the transmission field; an example is deletion, that can be non-dangerous if the system has been designed so that deleted messages do not represent a hazard;

b) one regarding the message logical structure; for example all the possible codes that can be applied to the message, or specific countermeasures such as sequence numbers, time stamps, etc.;

c) one at a physical level; an example is shielding to avoid corruption due to electromagnetic interference.

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

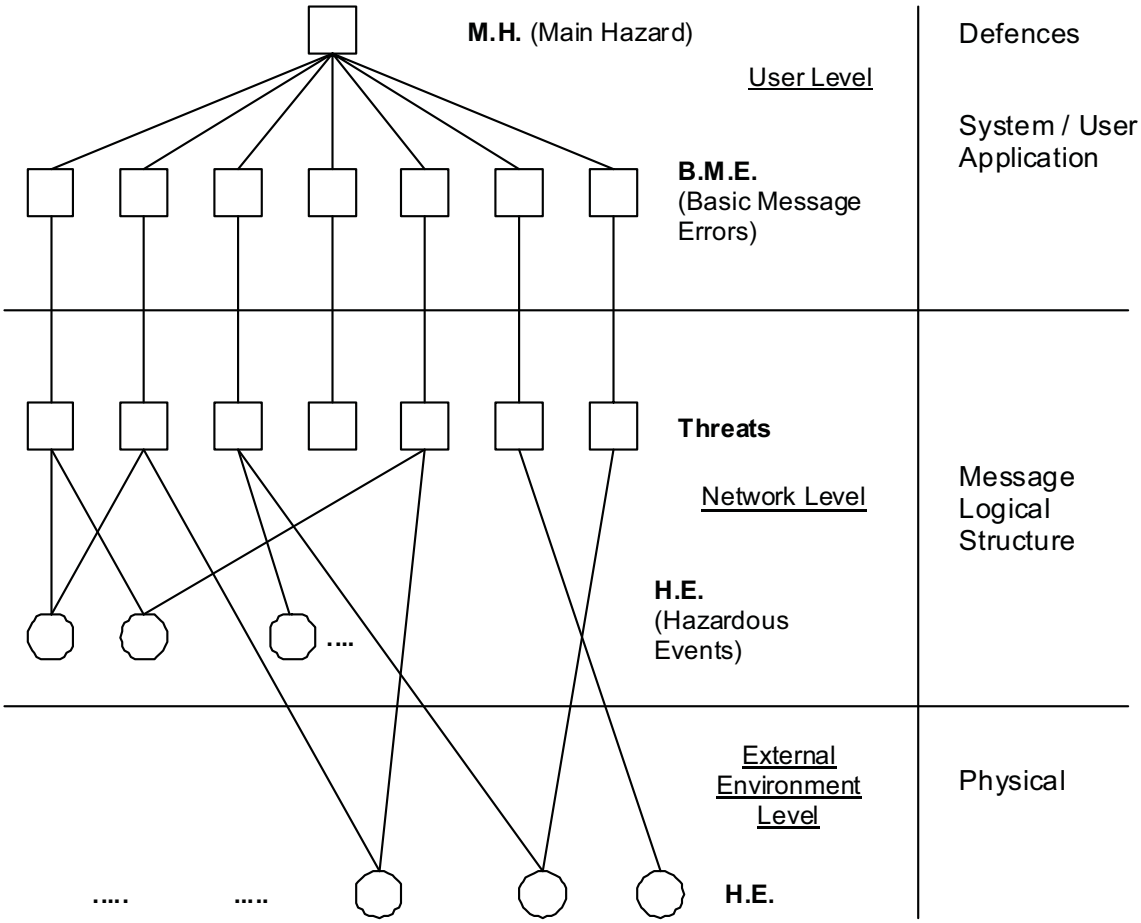



**Figure A.1 – Hazard tree**

## A.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.

**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: re-sequencing 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 different from 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 *re-sequenced, delayed, corrupted, masqueraded message*.

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

– repeated message;

– deleted message;

– inserted message;

– re-sequenced 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.

## A.3 Threats

Being the basic message errors the ones specified in Clause A.2, the derivation of the corresponding threats is straightforward.

Let A, B and C be three authorised 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 example and are therefore not exhaustive.

### A.3.1 Repetition

– X copies a message [‘Maximum speed: 250 km/h’] and replays it in an inappropriate situation [while train is in a slow speed track section],

or

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

### A.3.2 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.

### A.3.3 Insertion

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

or

– an authorised third party C involuntarily inserts a message in between the information flow from A to B (or the same happens due to a network error).

### A.3.4 Re-sequencing

– 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.

### A.3.5 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.

### A.3.6 Delay

– The transmission system is overloaded by the normal traffic (e.g. because of wrong design or an accidentally 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.

### A.3.7 Masquerade

– A and B communicate safety-related data,

and

– X pretends towards A to be B or towards B to be A (or both) to get access to the safety-related data or to be regarded as a legal user of the system.

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

The approach that will be outlined hereafter is an example and is not the only one that can be followed. A complete Hazard Analysis needs in depth knowledge of the application to which it is related, in order to perform a proper risk assessment.

### A.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 A.2) that can be considered as the causes of the possible hazardous events to the analysed 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 A.2 represent the causes of hazards: for each cause the corresponding generated hazardous events are identified. This way of proceeding also makes it easier, once the probability of a single cause is defined, to allocate the probability for each hazardous event produced.

In the following each cause is split into a 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.

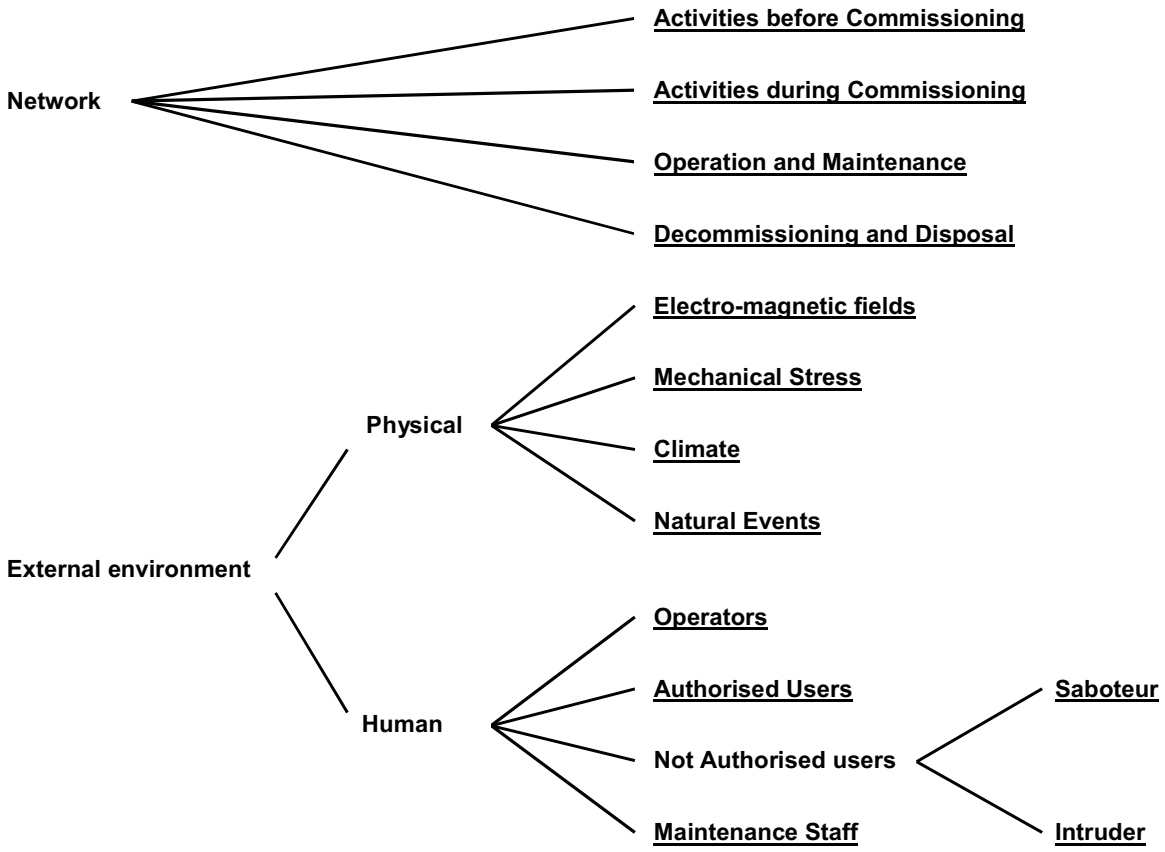



**Figure A.2 – Causes of threats**

### A.4.1.1 Network

The phases of network life-cycle can be defined according to EN 50126. 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: these are related to the commissioning of the system;

– operation and maintenance;

– decommissioning and disposal.

#### A.4.1.1.1 Activities before commissioning

Errors during this phase can lead to

– HW systematic failure,

– SW systematic failure.

#### A.4.1.1.2 Activities during commissioning

Errors during this phase can lead to

– cross-talk,

– wires breaking,

– antenna misalignment,

– cabling errors.

#### A.4.1.1.3 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.

#### A.4.1.1.4 Maintenance

– Use of uncalibrated instruments;

– use of unsuitable instruments;

– incorrect HW replacement;

– incorrect SW upgrading or replacement.

#### A.4.1.1.5 Modification

– Fading effects;

– human mistakes [1)].

#### A.4.1.1.6 Decommissioning and disposal

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

### A.4.1.2 External environment

#### A.4.1.2.1 Electro-magnetic fields

– EMI;

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

#### A.4.1.2.2 Mechanical stress

– HW random failures;

– HW ageing.

---

[1)] They depend on the particular type of application and cannot therefore be specified at this level of analysis.

#### A.4.1.2.3 Climate

– Thermal noise;
– HW ageing;
– HW random failures;
– fading effects.

#### A.4.1.2.4 Natural events

– Magnetic storm;
– fire;
– earthquake;
– lightning.

#### A.4.1.2.5 Operators

– Human mistakes [1)].

#### A.4.1.2.6 Authorised users

– Human mistakes [1)];
– overloading of transmission system.

#### A.4.1.2.7 Maintenance staff

– Use of uncalibrated instruments;
– use of unsuitable instruments;
– incorrect HW replacement;
– human mistakes [1)];
– incorrect SW upgrading or replacement.

#### A.4.1.2.8 Saboteur [2)]

– Wire tapping;
– HW damage or breaking;
– unauthorised SW modifications.

#### A.4.1.2.9 Intruder [2)]

– Monitoring of channels;
– transmission of unauthorised messages.

[2)] The difference between a saboteur and an intruder is that the first does not care 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.

### A.4.2 Relationship hazardous events – threats

Referring to Clause A.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 Clause A.3 by means of a bottom-up method [3)]. The goal is that of verifying that no extra threat is found, in order to prove the validity of the approach undertaken. The relationship threats-hazardous events can be represented by Table A.1.

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

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

## A.5 Conclusions

Two different approaches for deriving the set of possible threats to safety-related communication in transmission systems 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, therefore proving the validity of the work.

3) 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.

**Table A.1 – Relationship between hazardous events and threats**

| Hazardous events | Threats | | | | | | |
|---|---|---|---|---|---|---|---|
| | Repetition | Deletion | Insertion | Re-sequencing | Corruption | Delay | Masquerade |
| HW systematic failure | X | X | X | X | X | X | |
| SW systematic failure | X | X | X | X | X | X | |
| Cross-talk | | X | X | | X | | |
| Wires breaking | | X | | | X | X | |
| Antenna misalignment | | X | | | X | | |
| Cabling errors | | X | X | | X | X | |
| HW random failures | X | X | X | X | X | X | |
| HW ageing | X | X | X | X | X | X | |
| Use of uncalibrated instruments | X | X | X | X | X | X | |
| Use of unsuitable instruments | X | X | X | X | X | X | |
| Incorrect HW replacement | X | X | X | X | X | X | |
| Fading effects | | X | | X | X | X | |
| EMI | | X | | | X | | |
| Human mistakes | X | X | X | X | X | X | |
| Thermal noise | | X | | | X | | |
| Magnetic storm | | X | | | X | X | |
| Fire | | X | | | X | X | |
| Earthquake | | X | | | X | X | |
| Lightning | | X | | | X | X | |
| Overloading of TX system | | X | | | | X | |
| Wire tapping | X | X | X | X | X | X | |
| HW damage or breaking | | X | | | X | X | |
| Unauthorised SW modifications | X | X | X | X | X | X | X [a] |
| Transmission of unauthorised messages | X | | X | | | | X [a] |
| Monitoring of channels [b] | | | | | | | |

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

[b] Unauthorised monitoring of SR messages is not considered to be a directly hazardous event; the hazard to system safety arises from “transmission of unauthorised messages” resulting from unauthorised monitoring. Confidentiality of application data is a separate system requirement outside the scope of this standard.

# Annex B
(informative)

# Categories of transmission systems

## B.1 Categories of transmission systems

Subclause 6.3 identifies three categories of transmission system:

– Category 1 – Closed transmission systems, where all essential properties of the system are under the control of the safety-related system designer, and a simplified set of safety requirements can be defined;

– Category 2 – Open transmission systems where, although the transmission is not fully under the control of the safety-related system designer, the risk of malicious attack can be considered negligible;

– Category 3 – Open transmission systems where there is opportunity for malicious attack, and cryptographic defence measures are required.

The following Table B.1 gives some further guidance on how actual transmission systems that can be encountered in safety-related applications may relate to the above three categories, on the basis of the characteristics of the technology they use, and key features of their configuration.

It is not possible to be precise about purely hypothetical example systems, but the main characteristics listed in the table may guide users of this standard towards determining whether a particular system should be regarded as a Category 1, 2 or 3 system for the purposes of analysis.

**Table B.1 – Categories of transmission systems**

| Category | Main characteristics | Example transmission systems |
|---|---|---|
| Category 1 | Designed for known and fixed maximum number of participants.<br>All properties of the transmission system are known and invariable during the lifetime of the system.<br>Negligible opportunity for unauthorised access. | Close air-gap transmission (e.g. track balise to train antenna).<br>Proprietary serial bus internal to the safety-related system (e.g. PROFIBUS, CAN, MVB (multi purpose vehicle bus defined by IEC)).<br>Industry-standard LAN connecting different equipment (safety-related and non safety-related) within a single system, subject to fulfilment and maintenance of the preconditions. |
| Category 2 | Properties are unknown, partially unknown or variable during the lifetime of the system.<br>Limited scope for extension of user group.<br>Known user group or groups.<br>Negligible opportunity for unauthorised access (networks are trusted).<br>Occasional use of non-trusted networks. | Proprietary serial bus internal to the safety-related system (e.g. PROFIBUS, MVB), but with the possibility that the transmission system could be reconfigured or substituted by another transmission system during the lifetime.<br>Industry-standard LAN connecting different systems (safety-related and non safety-related) within a controlled and limited area.<br>WAN belonging to the railway, connecting different systems (safety-related and non safety-related) at various locations.<br>Switched circuit in public telephone network, used occasionally and at unpredictable times (e.g. dial-up remote diagnostic of an interlocking system).<br>Leased permanent point-to-point circuit in public telecom network.<br>Radio transmission system with restricted access (e.g. use of wave guides or leaky cables with a link budget limiting the possibility of reception to a close transceiver only, or using a proprietary scheme of modulation, impossible to reproduce with off the shelf or affordable lab equipment). |
| Category 3 | Properties are unknown, partially unknown or variable during the lifetime of the system.<br>Unknown multiple users groups.<br>Significant opportunity for unauthorised access. | Packet switched data in public telephone network.<br>Internet.<br>Circuit switched data radio (e.g. GSM-R).<br>Packet switched data radio (e.g. GPRS).<br>Short range broadcast radio (e.g. Wi-fi).<br>Radio transmission systems without restrictions. |

## B.2 Relationship between the category of transmission systems and threats

The following Table B.2 shows a rough assignment of the threats to each of the categories of transmission system defined above.

**Table B.2 – Threat/Category relationship**

| Category | Repetition | Deletion | Insertion | Re-sequence | Corruption | Delay | Masquerade |
|---|---|---|---|---|---|---|---|
| Cat. 1 | + | + | + | + | ++ | + | - |
| Cat. 2 | ++ | ++ | ++ | + | ++ | ++ | - |
| Cat. 3 | ++ | ++ | ++ | ++ | ++ | ++ | ++ |

**Key**

- \- Threat can be neglected.
- \+ Threat exists, but rare; weak countermeasures sufficient.
- ++ Threat exists; strong countermeasures required.

NOTE This matrix of threats is only a guide – analysis will always be necessary to determine whether countermeasures are required and to what degree. Each threat will be dependent on network type, application and configuration.

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

# Annex C
(informative)

# Guideline for defences

## C.1 Applications of time stamps

A time stamp can be used for different purposes.

a) 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 synchronised. 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.

b) 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 should 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.

c) 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).

   Constraint:

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

d) 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 should handle interruption due to initialisation or fault conditions;

   – the procedure will not guarantee authentication of the messages.

e) To create a procedure called double time stamping [A155]. This procedure inherits the properties of a combination of cases b), c) and d). 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

   – creating a logical clock from the partners' local clock and relative time stamps from the own local clock (and organising a clock synchronisation between the two entities),

   – relating events to the relative time stamps including network delay,

   – checking the correct order of messages,

   – 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 should be complemented with sequence numbers;

   – double time stamping could require knowledge about the round-trip transmission delays if the application considers case a) above.

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

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

Although the transmission system could be unknown or variable during its lifetime, in most cases one can determine whether malicious attacks to safety-related messages can be excluded or not. This distinction is very useful because in case of the possibility of these malicious attacks, cryptographic mechanisms with secret keys are demanded. It is recommended to make this distinction at an early stage to limit the amount of safety-related functionality. If there is the possibility of unauthorised access, a separate access protection layer can be applied (Type B0 or B1) or the protection is provided by the safety related transmission function using cryptographic mechanisms (Type A1) and in this case the term "cryptographic safety code" is used in the following text.

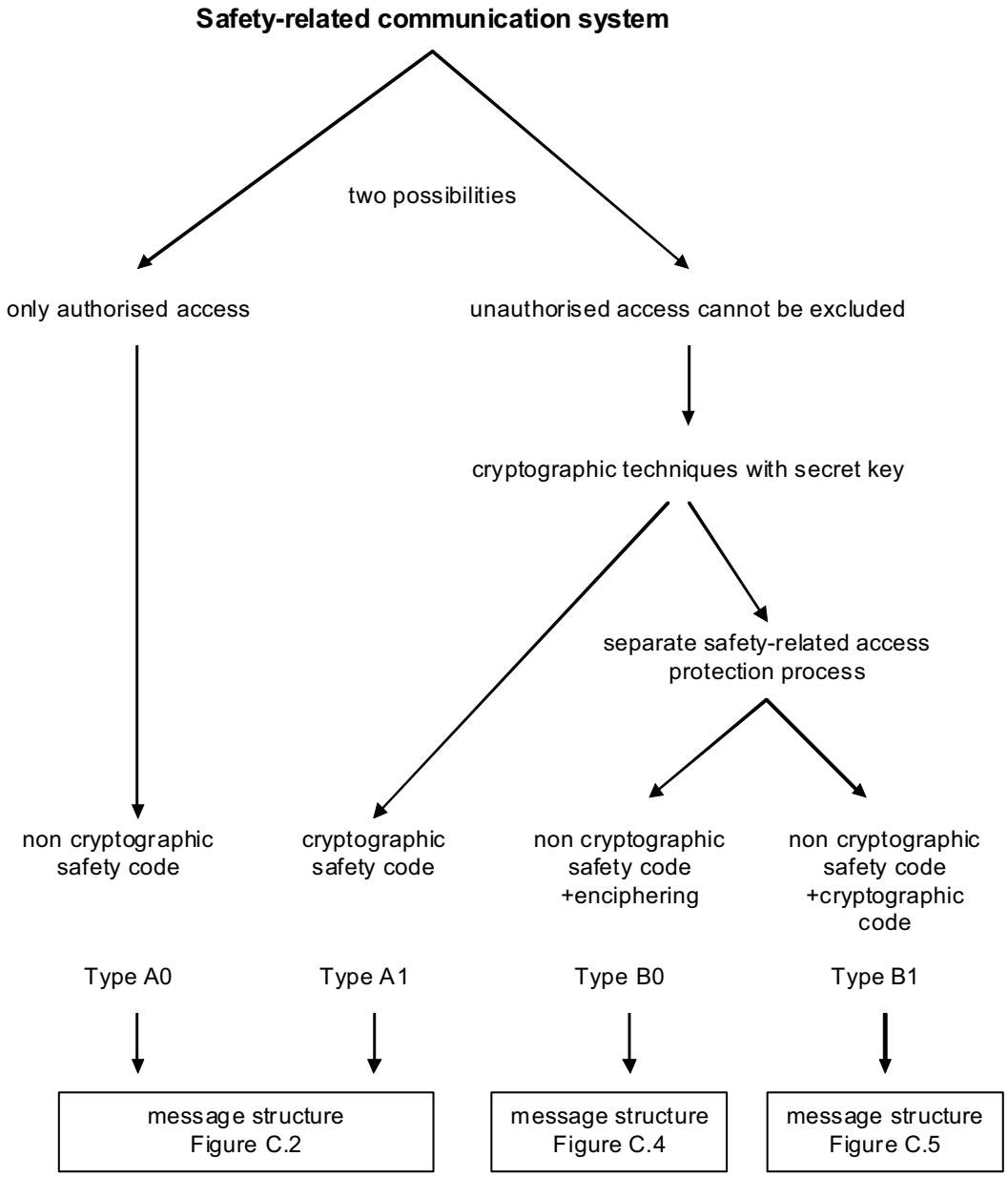



**Figure C.1 – Classification of the safety-related communication system**

The principles of message structures for message Types A0 and A1 are depicted in Figure C.2.

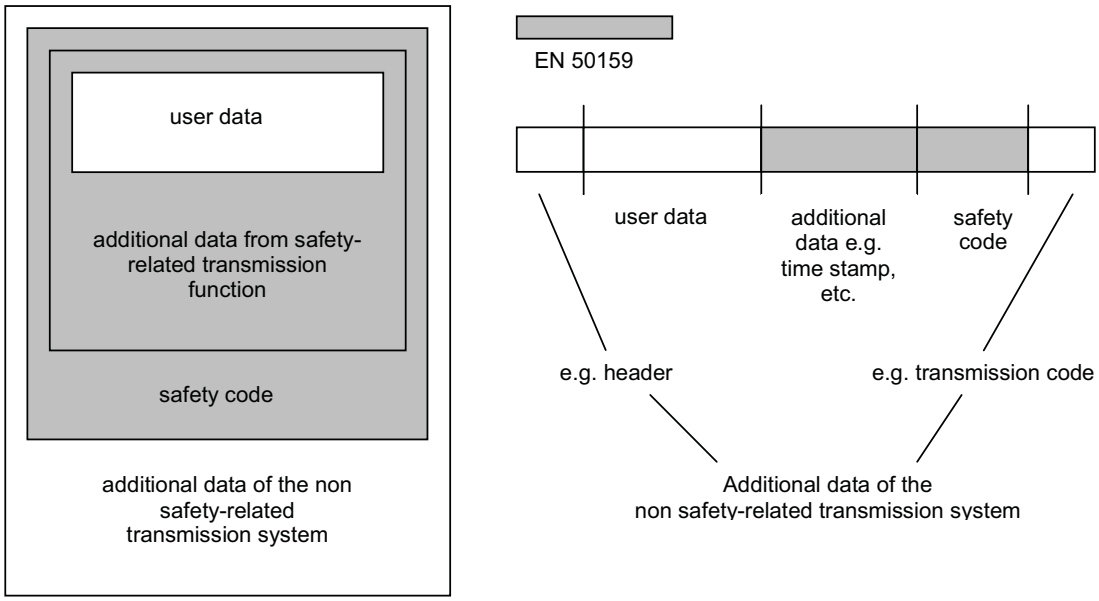



**Figure C.2 – Model of message representation within the transmission system (Type A0, A1)**

Separate access protection layers are useful, in those cases where groups of safety-related computers which are connected by a local area network (LAN), have to communicate over open transmission systems (see Figure C.3). An implicit assumption behind the model depicted in Figure C.3 is that the LANs can be classified as Category 2. The cryptographic hardware and software can be concentrated at the unique entry point to the open transmission system. Other interfaces to the open transmission system should be excluded. The cryptographic functions can be combined with gateway functions which are normally required when a LAN is connected to a, for example, wide area network.

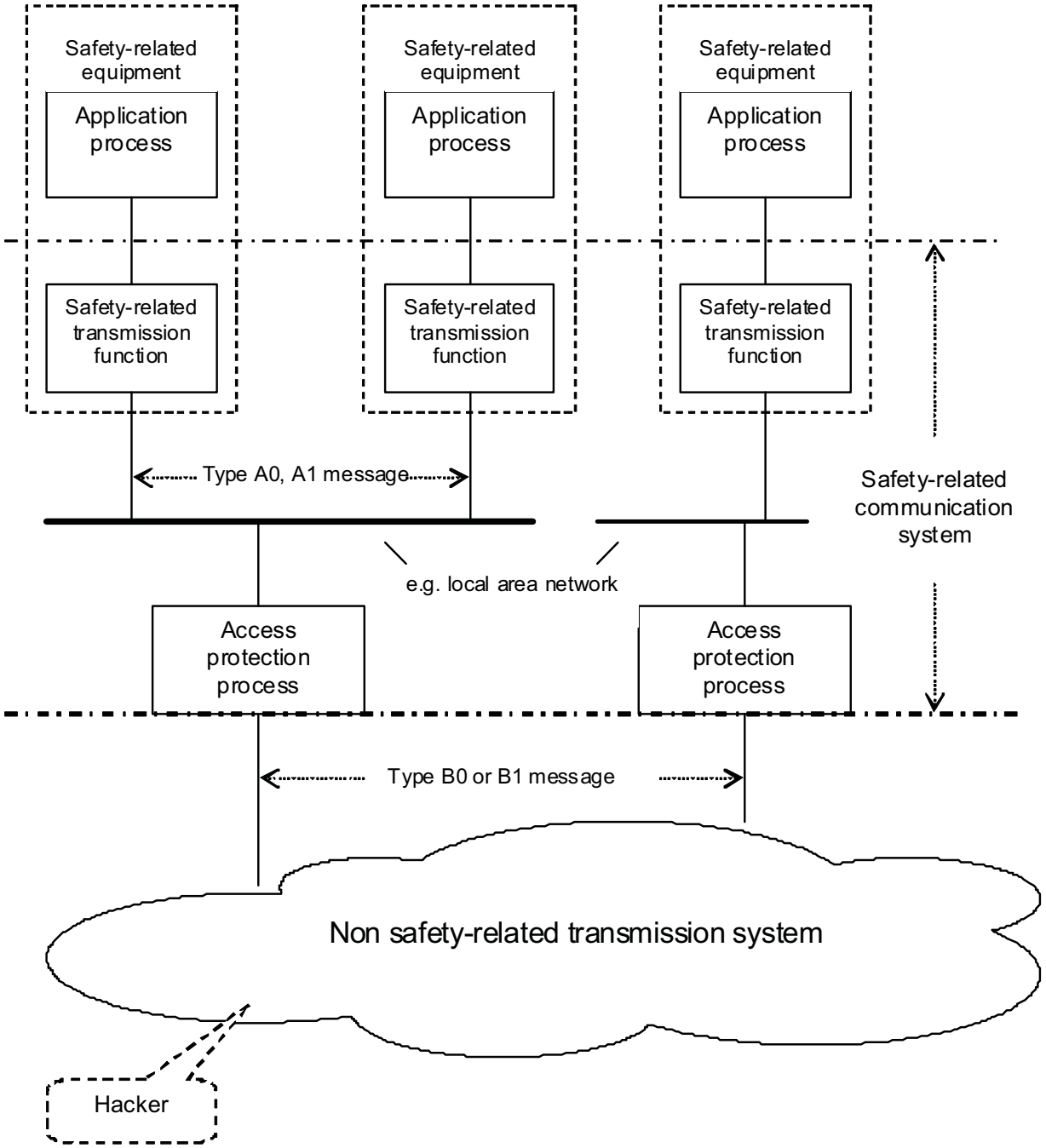



**Figure C.3 – Use of a separate access protection layer**

The access protection process can be performed by different modes:

a) enciphering of the messages;

b) 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 7.2. Note that failures of the access protection process should be considered.

The principles of message structures for message Types B0 and B1 are depicted in Figures C.4 and C.5.

These examples show the cryptographic protection being applied immediately after the safety code. In other examples it can be applied at lower levels (e.g. transport or network).

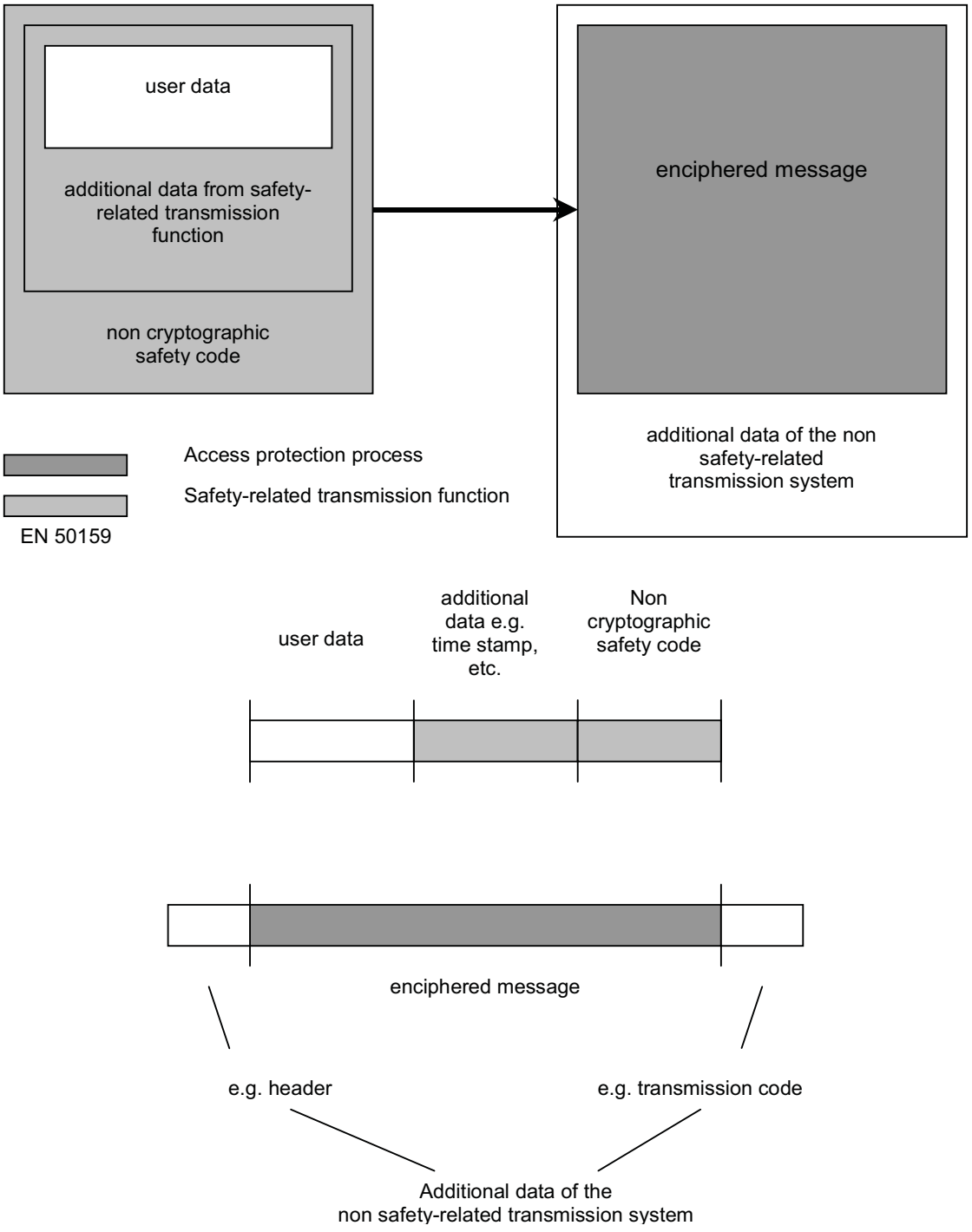



**Figure C.4 – Model of message representation within the transmission system (Type B0)**

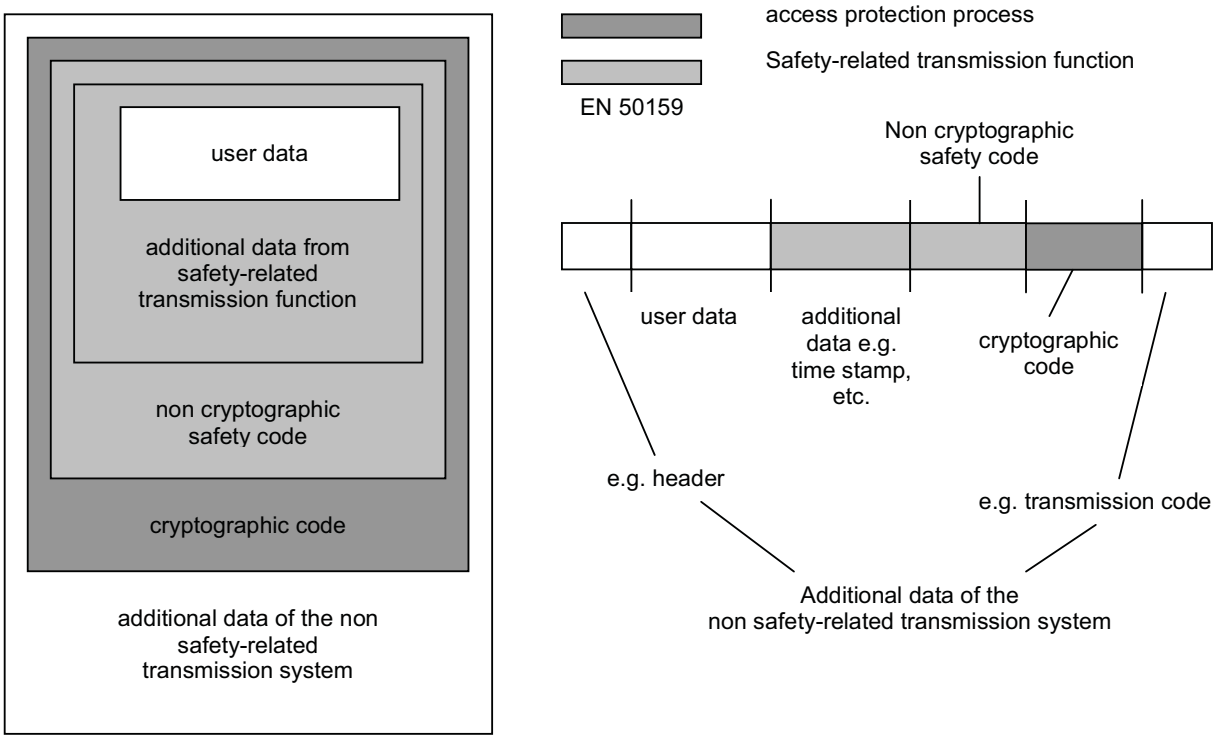



**Figure C.5 – Model of message representation within the transmission system (Type B1)**

## C.3 Safety code

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

If unauthorised access to the transmission system can be excluded, the safety code has to detect all kinds of random and systematic bit errors. Note, that usually the 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 transmission system delivers an invalid message, either the disturbance on the transmission channel was so great that the transmission code failed, or a failure has occurred. In either case, it should be considered that residual bit errors are not random, and can have any Hamming weight [Peterson].

If unauthorised 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.

### C.3.1 Main block codes

The following subclauses briefly describe some block codes and their main characteristics. See [Peterson] for more detail.

#### C.3.1.1 Linear block codes

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

Most of the codes in use for error control are linear binary codes. Non-binary codes are also used, e.g. 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 errors up to *d-1* wrong symbols are fully detected. Because of their linearity the codes can be tested for systematic transmission error detection capability.

The useful models are binary symmetric channel (BSC) and q-nary symmetric channel (QSC). The codes can also be tested for systematic transmission error detection.

#### C.3.1.2 Cyclic block codes

A linear block code is cyclic if every cyclic shift of a code word is also a code word. A cyclic code 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. A cyclic code with *c* redundant symbols detects all burst errors up to the length *c*.

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

#### C.3.1.3 Hash block codes

Hash codes can be linear or non-linear. 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 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 two sets 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 a cryptographic protection over the entire safety-related message including the hash value is applied.

#### C.3.1.4 Digital signatures

A digital signature is 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].

#### C.3.1.5 Cryptographic block codes

Cryptographic block codes are a kind of non-linear hash block code based on cryptographic algorithms. The advantage is that they can protect against malicious attack if they are based on keys. The most well known code is the message authentication code MAC that is standardised in ISO/IEC 9797-1 and ISO/IEC 9797-2.

### C.3.2 Recommendations for the application of safety codes

Examples for the assessment of diverse basic techniques are given in Table C.1.

**Table C.1 – Assessment of the safety encoding mechanisms [4)]**

| Type [a] | Reference, see Clause 2 & Bibliography | Type of safety-related communication system, see Figure C.1 | | | |
|---|---|---|---|---|---|
| | | **A0** | **A1** | **B0** [b] | **B1** [b] |
| CRC [c] | [Peterson] | R | US [d] | - [e] | R |
| MAC [c] | ISO/IEC 9797-1 & 2 | R | HR | R | R |
| Hash code [c] | ISO/IEC 10118-2 | R | US [d] | HR | HR |
| Digital signature [c] | ISO/IEC 9796-2 & 3 | R | R | R | R |

**Key**

| | |
|---|---|
| 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 '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. |

| | |
|---|---|
| [a] | Other safety measures are possible but not considered here. |
| [b] | Non cryptographic safety code only. Cryptographic techniques to be considered separately. |
| [c] | The error detection capability is similar for the same number of redundancy bits. |
| [d] | Secret key demanded, cannot be performed by this mechanism. |
| [e] | If stream ciphering techniques are used then applying a CRC as safety code is unsuitable. 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 $p_{UE} = 2^{-c}$, where c denotes the number of redundancy bits.

### C.3.3 Cryptographic techniques

When using ciphering techniques, standardised modes of operation are recommended, e.g. 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 [AES] are recommended.

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

## C.4 Length of safety code

This annex is applicable for Category 1 only, i.e. closed transmission systems, since the given formulae are based on specific assumptions on the transmission system.

In fact the model described here relies partly on the error detecting and managing mechanisms of the transmission systems. Usually, under fault free conditions, the error detecting mechanism of the transmission system detects and counteracts all transmission errors. In this case the safety code will not detect any errors. Nevertheless, the transmission system itself or its error detecting mechanism can fail because of hardware failures, or some transmission errors are so high that they are not detected. In all these cases the safety code has to detect those failures.

Using this model leads to lower safety integrity requirements for the safety code in comparison to models neglecting the error detecting capabilities of the transmission system. On the other hand, the transmission system is now fixed and cannot be exchanged for another one without adapting the safety case. This model can be (and should be if necessary) modified for systems ignoring their error detecting mechanisms or the influences coming from the hardware failure rate.

This annex gives simple formulae for calculating the length of the safety code. Fulfilling the given requirements guarantees that the safety target will be reached.

The basic model for calculating the length of the safety code is shown in Figure C.6.

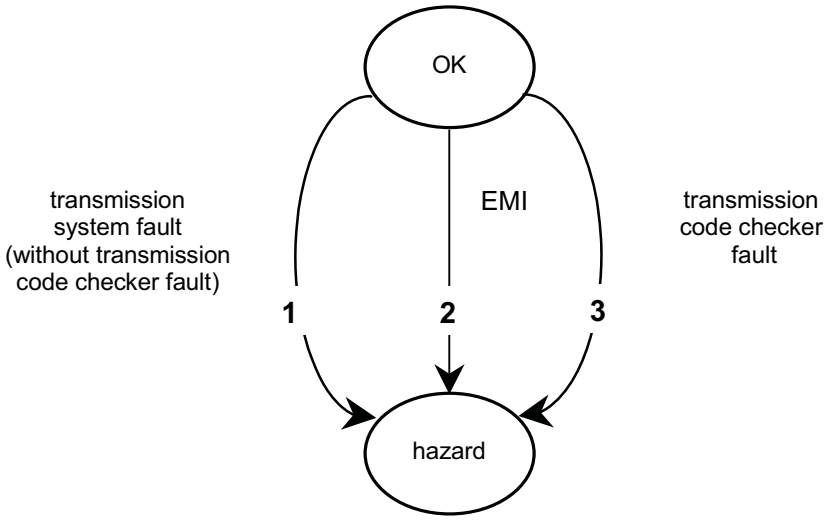



**Figure C.6 – Basic error model**

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

1. the transmission hardware fails, so the messages are corrupted;

2. bit errors arise due to EMI and are not detected by the transmission coding;

3. faults occur in the transmission code checker, such that every corrupted message could be passed from the non-trusted transmission system to the safety-related equipment.

The following definitions are given:

$R_{\mathrm{H}}$ Target hazardous failure rate of the complete transmission system

$R_{\mathrm{H1}}$ Hazardous failure rate of hardware faults without transmission code checker

$R_{\mathrm{H2}}$ Hazardous failure rate of EMI

$R_{H3}$ Hazardous failure rate of transmission code checker

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

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

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

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

$f_M$ Maximum frequency of messages for one receiver

$f_W$ Frequency of wrong (corrupted) messages

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

$k_1$ Factor for hardware faults including safety margin

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

$m$ Safety factor included within $k_1$

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

With these definitions the following equations have to be evaluated:

$$R_{HW} \times p_{US} \times k_1 = R_{H1} \quad (1)$$

$$p_{UT} \times p_{US} \times f_W = R_{H2} \quad [5] \quad (2)$$

$$k_2 \times p_{US} \times \frac{1}{T} = R_{H3} \quad (3)$$

The sum of all three rates should not exceed $R_H$:

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

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

$$k_1 \geq n \times m$$

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

The maximum frequency of wrong messages $f_W$ should be estimated

– either by the worst case estimation $f_W = f_M$,

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

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

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

By using proper or good CRC [6] the maximum value of $p_{UT}$ may be estimated as

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

where b denotes the number of redundancy bits.

If other codes are used, e.g. a combination of two codes, the worst case block error probability using the model of “binary symmetric channel" [7] should be taken.

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

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

NOTE The following derivation is given for information only.

- If a hardware fault occurs, in only 1 of 10 000 cases the transmission code checker fails undetected.
- In this case the average duration (without EMI) of this state is

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

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

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

Equation (3) leads to a minimum time interval, in which only one error detected by the safety code is allowed. If such a mechanism is not used, the safe fall back state shall be entered immediately after the first detected error, otherwise other measures against possible error conditions shall be introduced.

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

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

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

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

NOTE This mechanism relies on the fact that common cause failures affecting the two messages are negligible.

## C.5 Communication between safety-related and non safety-related applications

An example of communication between non safety-related applications and safety-related applications is shown in Figure C.7.

---

[6] Properness means that the relation between bit error probability (less than one half) and probability of undetected error is monotone. Goodness means that the probability of undetected error has its absolute maximum at the bit error probability of one half. See e.g. Wolf, J. K., Michelson, A. M. und Levesque, A. H.: "On the probability of undetected error for linear block codes", IEEE COM-30, 1982, 317-324; Dodunekova R., Dodunekov S. M.: "Sufficient conditions for good and proper detecting codes", IEEE Trans. Inform. Theory, vol. 43. pp. 2023-2026, Nov. 1997.

[7] Binary symmetric channel: With probability p a received bit is falsified (0→1 and 1→0). Each bit is independent from each other.

Within trusted networks (Category 1 and 2) non safety-related applications can communicate over the same transmission media used by safety-related applications. For requirements therefore, see 7.2.

In this example the non-safety-related message is also protected by cryptographic techniques when passing through a Category 3 transmission system.

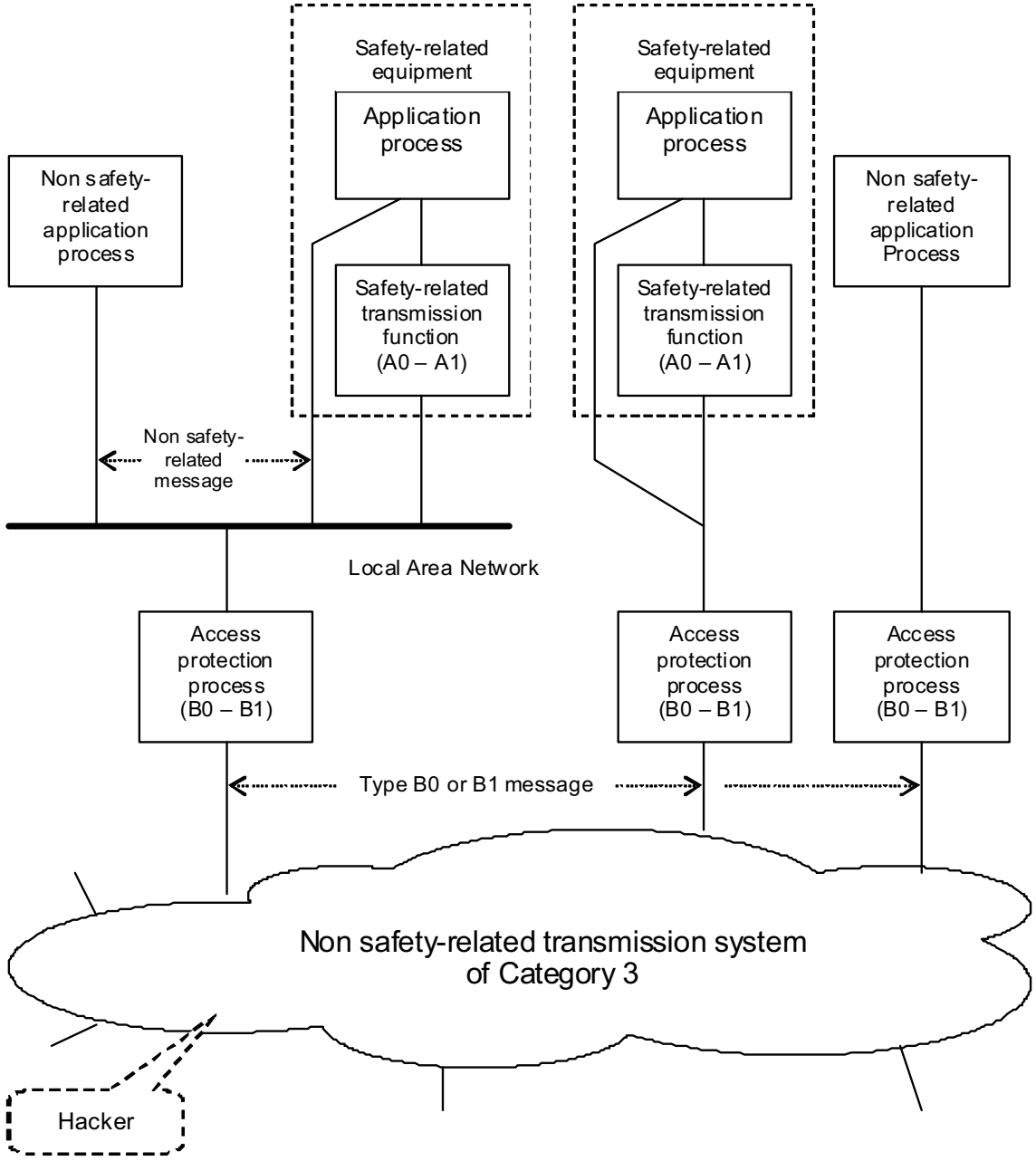



**Figure C.7 – Communication between non safety-related and safety-related applications**

# Annex D
(informative)

# Guidelines for use of the standard

## D.1 Procedure

A number of distinct steps can be identified to carry out the system design activities covered by EN 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 details in the following subclauses.

### D.1.1 Application

The system designer shall 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 qualitative parameters and non-functional parameters) for the system shall also be defined (by the user or the safety authority).

### D.1.2 Hazard analysis

Qualitative hazard analysis of the system (as required by EN 50126) shall 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 shall 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.

### D.1.3 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.

### D.1.4 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 EN 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 EN 50129, and the rate of occurrence of unsafe failures due to random faults can be calculated.

### D.1.5 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 shall be recorded in the SRS for the system.

## D.2 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.

### D.2.1 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.

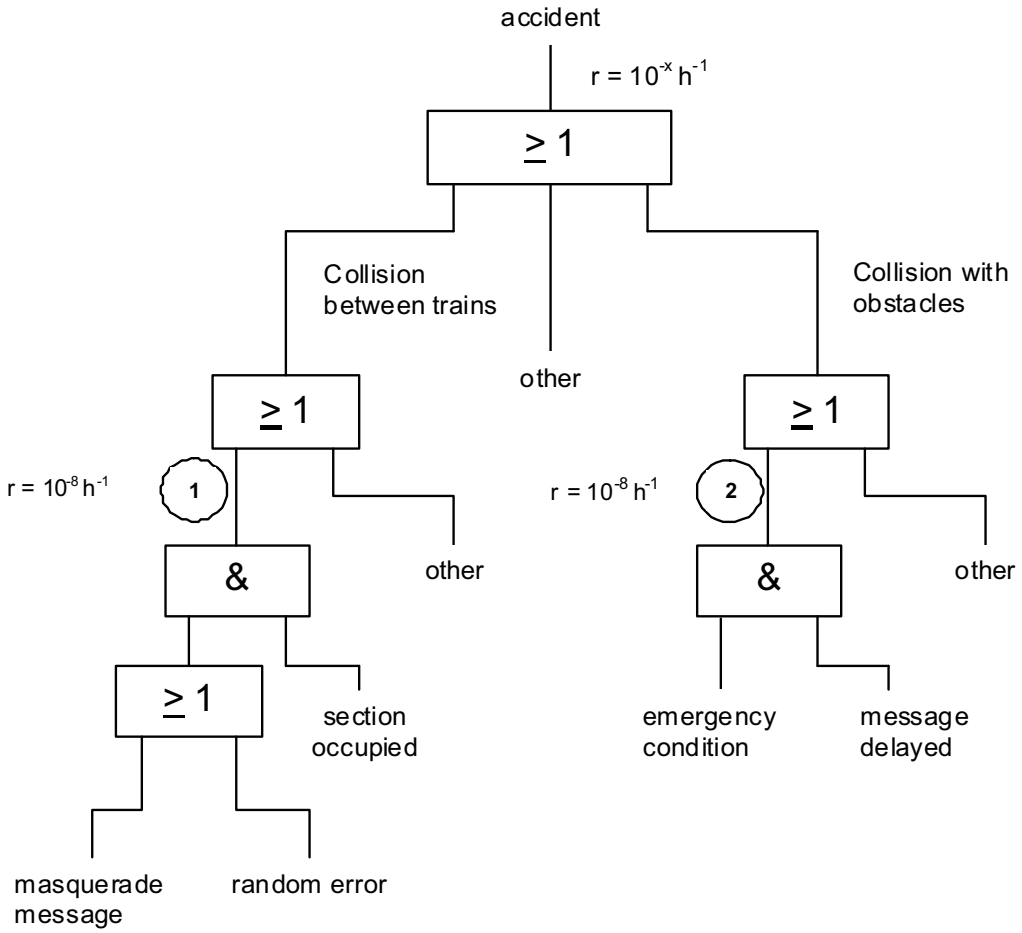
### D.2.2 Hazard analysis

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

a) 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;

b) 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 D.1), as an example of one method of performing the hazard analysis.




**Key**

| | |
|---|---|
| ≥ 1 | OR gate |
| & | AND gate |
| 1 | Fault tree for case 1 (see Figure D.2) |
| 2 | Fault tree for case 2 (see Figure D.3) |
| r | Tolerable hazard rate |

NOTE Preferred symbols according to EN 61025.

**Figure D.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.

## D.2.3 Case 1

### D.2.3.1 Risk reduction

If a message to a train is corrupted due to random errors, it can 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, the following Figure D.2 results:

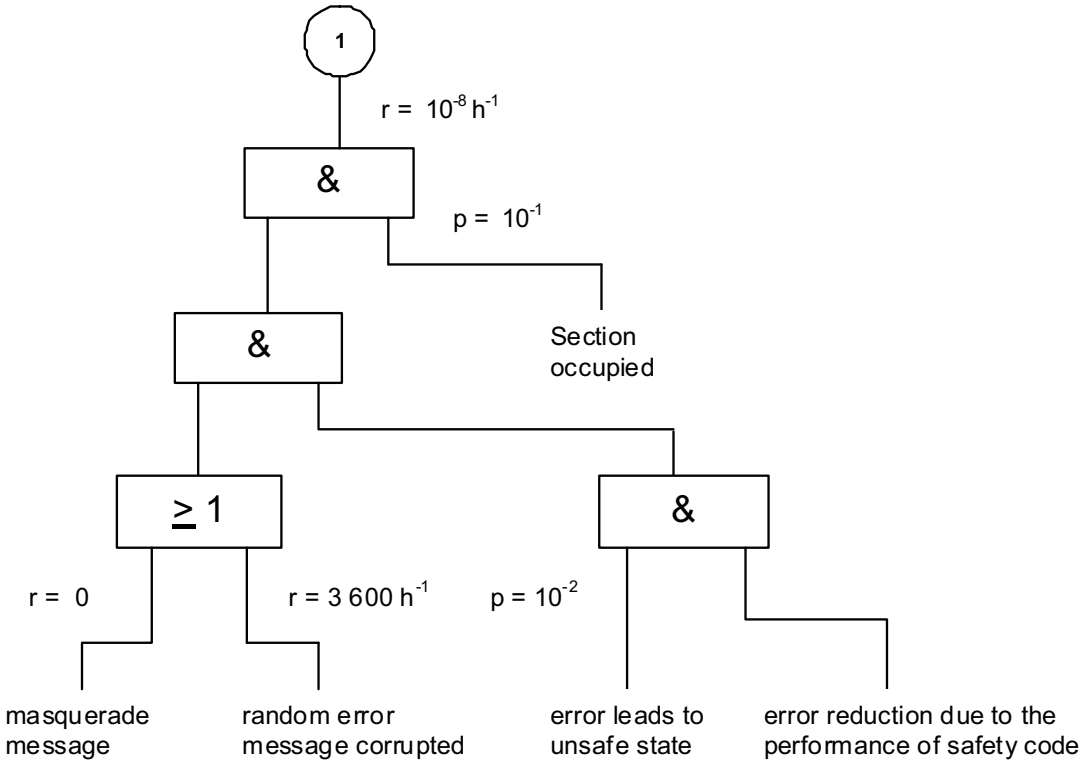



**Figure D.2 – Fault tree for case 1**

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 authorise 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 shall guarantee a probability of undetected error of less than $3 \times 10^{-9}$ per message, or the frequency of this kind of events should not exceed $10^{-5}$ $h^{-1}$.

#### D.2.3.2 SIL allocation and quantified target

According to EN 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 communication system”.

The designer of the system shall 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. For example, for infrequent transmission of short messages, the likelihood of deliberate attempts to create accidents could be 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.

### D.2.4 Case 2

#### D.2.4.1 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, the following Figure D.3 results:

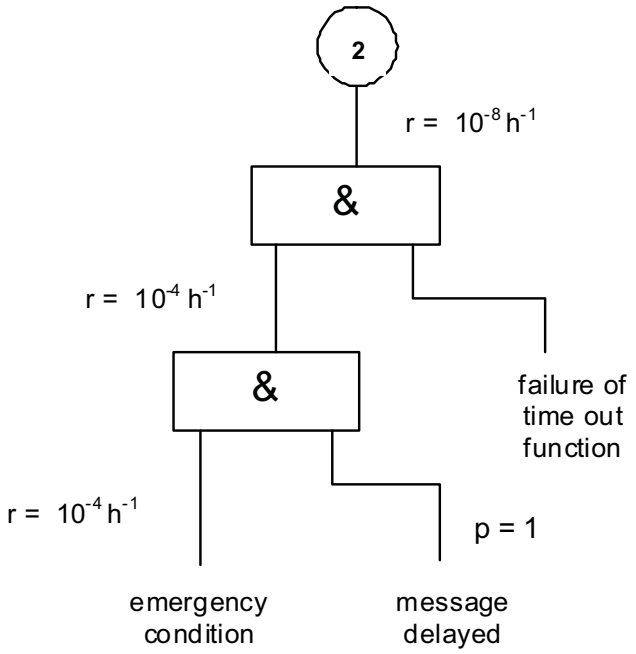



**Figure D.3 – Fault tree for case 2**

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.

#### D.2.4.2 SIL allocation and quantified target

Reference to EN 50129 indicates how to achieve the required SIL.

The implementation of this function shall therefore be designed using techniques suggested in EN 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).

# Annex E
(informative)

## Mapping from previous standards

This European Standard is the result of revision and merging of the previous standards EN 50159-1:2001 and EN 50159-2:2001. Primarily only corrections and improvements were carried out. Some new parts were necessary due to consistency reasons.

Tables E.1 and E.2 show the mapping of the (sub)clauses and annexes of the previous standards to the (sub)clauses and annexes of EN 50159:201X.

These should facilitate the traceability in case of maintenance and/or extensions of systems once approved according to the previous standards and furthermore the understanding of the new standard.

The reference in the tables is only from the previous standards to the new, but not vice versa.

**Table E.1 – Mapping from EN 50159-1:2001 into EN 50159:201X**

| (Sub)clause of EN 50159-1:2001 | | Informative / Normative | (Sub)clause of EN 50159:201X | | Unchanged / Modified |
|---|---|---|---|---|---|
| Introduction | | Inf. | Introduction | | E |
| 1 | Scope | Nor. | 1 | Scope | E |
| 2 | Normative references | Nor. | 2 | Normative references | E |
| 3 | Definitions | Nor. | 3 | Terms, definitions and abbreviations | E |
| 4 | Reference architecture | Nor. | 4 | Reference architecture | T |
| | Pr1 | Nor. | 6.3.1 | Pr3 | E |
| | Pr2 | Nor. | 6.3.1 | Pr1 | E |
| | Pr3 | Nor. | 6.3.1 | Pr2 | E |
| 5 | Relation between the characteristics of the transmission system and safety procedures | Nor. | 7.2.8 | | E |
| 5.1 | Functional integrity requirement (text up to P1) | Nor. | Not used | | |
| | P1 to P5 | Nor. | 7.1 | Preface | T |
| | P6 | Nor. | 7.2.5 | | E |
| 5.2 | Safety integrity requirements R1 to R6 | Nor. | 7.2 | General requirements | T |
| 6.1 | General | Nor. | Not used | | |
| 6.2 | Communication between safety-related equipment | Nor. | 7.1 and 7.2 | | T |
| 6.3 | Communication between safety-related and non safety-related equipment | Nor. | 7.2.2 | | E |
| | | | 7.3.7.2.1 | | E |
| 6.4 | Communication between non safety-related equipment | Nor. | Not used | | |
| 7.1 | General requirements | Nor. | 7.3.7.2.3 | | E |
| 7.2 | Safety target | Nor. | 7.2.5 | | T |
| 7.3 | Length of safety code | Nor. | 7.3.7.2.4 | | E |
| Annex A | Length of safety code | Inf. | C.4 | Length of safety code | U |

**Key**

Inf. Informative

Nor. Normative

U (unchanged) includes:
Changes of references and changes of terminology to achieve consistency of the whole standard.

E (editorial changes) includes:
No change of contents, only rearrangements and improvements.

T (technical changes) includes:
Contents either moved to other (sub)clauses or changed.

**Table E.2 – Mapping from EN 50159-2:2001 into EN 50159:201X**

| (Sub)clause of EN 50159-2:2001 | | Informative / Normative | (Sub)clause of EN 50159:201X | | Unchanged / Modified |
|---|---|---|---|---|---|
| Introduction | | Inf. | Introduction | | E |
| 1 | Scope | Nor. | 1 | Scope | E |
| 2 | Normative references | Nor. | 2 | Normative references | E |
| 3 | Definitions | Nor. | 3 | Terms, definitions and abbreviations | E |
| 4 | Reference architecture | Nor. | 4 | Reference architecture | T |
| 5 | Threats to the transmission system | Nor. | 5 | Threats to the transmission system | U |
| 6.1 | Introduction | Nor. | 7.1 | Preface | U |
| 6.2 | General requirements | Nor. | 7.2 | General requirements | T |
| 6.3 | Specific defences | Nor. | 7.3 | Specific defences | U |
| 6.3.1 | Sequence number | Nor. | 7.3.1 | Sequence number | U |
| 6.3.2 | Time stamp | Nor. | 7.3.2 | Time stamp | U |
| 6.3.3 | Time-out | Nor. | 7.3.3 | Time-out | U |
| 6.3.4 | Source and destination identifiers | Nor. | 7.3.4 | Source and destination identifiers | U |
| 6.3.5 | Feedback message | Nor. | 7.3.5 | Feedback message | U |
| 6.3.6 | Identification procedure | Nor. | 7.3.6 | Identification procedure | U |
| 6.3.7 | Safety code | Nor. | 7.3.7 | Safety code | T |
| 6.3.8 | Cryptographic techniques | Nor. | 7.3.8 | Cryptographic techniques | T |
| 7.1 | Introduction | Nor. | 7.4.1 | Preface | U |
| 7.2 | Threats/defences matrix | Nor. | 7.4.2 | Threats/defences matrix | U |
| 7.3 | Choice and use of safety code and cryptographic techniques | Nor. | 7.4.3 | Choice and use of safety code and cryptographic techniques | U |
| A.1 | Applications of time stamps | Inf. | C.1 | Applications of time stamps | U |
| A.2 | Choice and use of safety codes and cryptographic techniques | Inf. | C.2 | Choice and use of safety codes and cryptographic techniques | T |
| Bibliography | | Inf. | Bibliography | | T |
| C.1 | Scope/purpose | Inf. | 6.1 | General | T |
| C.2 | Classification of transmission systems | Inf. | 6.2 | General aspects of classification | T |
| | | | Annex B | Categories of transmission system | T |
| C.3 | Procedure | Inf. | D.1 | Procedure | U |
| C.4 | Example | Inf. | D.2 | Example | U |
| Annex D | Threats on open transmission systems | Inf. | Annex A | Threats on open transmission systems | E |

**Key**

Inf. Informative

Nor. Normative

U (unchanged) includes:
Changes of references and changes of terminology to achieve consistency of the whole standard.

E (editorial changes) includes:
No change of contents, only rearrangements and improvements.

T (technical changes) includes:
Contents either moved to other (sub)clauses or changed.

# Annex ZZ
(informative)

## Coverage of Essential Requirements of EC Directives

This European Standard has been prepared under a mandate given to CENELEC by the European Commission and the European Free Trade Association and within its scope the standard covers all relevant essential requirements as given in Annex III of the EC Directive 2008/57/EC.

Compliance with this standard provides one means of conformity with the specified essential requirements of the Directive concerned.

WARNING: Other requirements and other EC Directives may be applicable to the products falling within the scope of this standard.

# Bibliography

EN 61025, *Fault Tree Analysis (FTA)* (IEC 61025)

ISO/IEC 9796-2:2002, *Information technology – Security techniques – Digital signatures scheme giving message recovery – Part 2: Integer factorization based mechanisms*

ISO/IEC 9796-3:2006, *Information technology – Security techniques – Digital signatures scheme giving message recovery – Part 3: Discrete logarithm based mechanisms*

ISO/IEC 9797-1:1999, *Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher*

ISO/IEC 9797-2:2002, *Information technology – Security techniques – Message Authentication Codes (MACs) – Part 2: Mechanisms using a dedicated hash-function*

ISO/IEC 9979:1999 [8)], *Information technology – Security techniques – Procedures for the registration of cryptographic algorithms*

ISO/IEC 10116:2006, *Information technology – Security techniques – Modes of operation for an n-bit block cipher*

ISO/IEC 10118-1:2000, *Information technology – Security techniques – Hash-functions – Part 1: General*

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

ISO/IEC 10118-3:2004, *Information technology – Security techniques – Hash-functions – Part 3: Dedicated Hash-functions*

ISO/IEC 10118-4:1998, *Information technology – Security techniques – Hash-functions – Part 4: Hash-functions using modular arithmetic*

ISO/IEC 11770-1:1996, *Information technology – Security techniques – Key management – Part 1: Framework*

ISO/IEC 11770-2:2008, *Information technology – Security techniques – Key management – Part 2: Mechanisms using symmetric techniques*

ISO/IEC 11770-3:2008, *Information technology – Security techniques – Key management – Part 3: Mechanisms using asymmetric techniques*

UIC 738, *Processing and transmission of safety information*

[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)

[AES] FIPS PUB 197, 26.11.2001: *Advanced Encryption Standard*

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

[Peterson] W.Wesley Peterson, *Error correction Codes*, M.I.T. Press, 1967

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

8) Withdrawn

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

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

Wolf, J. K., Michelson, A. M. und Levesque, A. H., *On the probability of undetected error for linear block codes*

IEEE COM-30, Dodunekova R., Dodunekov S. M., *Sufficient conditions for good and proper detecting codes,*1982, 317-324

IEEE Trans. Inform. Theory, vol. 43. pp. 2023-2026, Nov. 1997