EUROPEAN STANDARD **EN 50159-2**

NORME EUROPÉENNE

EUROPÄISCHE NORM March 2001

ICS 35.240.60; 45.020

English version

Railway applications - Communication, signalling and processing systems Part 2: Safety related communication in open transmission systems

Applications ferroviaires - Systèmes de signalisation, de télécommunication et de traitement Partie 2: Communication de sécurité sur des systèmes de transmission ouverts

Bahnanwendungen - Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme Teil 2: Sicherheitsrelevante Kommunikation in offenen Übertragungssystemen

CENELEC

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

Central Secretariat: rue de Stassart 35, B - 1050 Brussels

Ref. No. EN 50159-2:2001 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.

The text of the draft was submitted to the formal vote and was approved by CENELEC as EN 50159-2 on 2000-01-01.

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)	2001-10-01
– latest date by which the national standards conflicting with the EN have to be withdrawn	(dow)	2003-01-01

Annexes designated "informative" are given for information only.
In this standard, annexes A, B, C and D are informative.

Contents

Introduction

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

The safety requirements for a data communication system depend on its characteristics which can be known or not. In order to reduce the complexity of the approach to demonstrate the safety of the system two classes of transmission systems have been considered. The first class consists of the ones over which the safety system designer has some degree of control. It is the case of the closed transmission systems whose safety requirements are defined in EN 50159-1. The second class, named open transmission system, consists of all the systems whose characteristics are unknown or partly unknown. This standard defines the safety requirements addressed to the transmission through open transmission systems.

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

This standard is closely related to EN 50159-1 "Safety-related communication in closed transmission systems" and ENV 50129 "Safety related electronic systems for signalling".

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

Cross-acceptance, aimed at generic approval and not at specific applications, is required in the same way as for ENV 50129 "Safety related electronic systems for signalling".

1 Scope

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

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

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

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

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

This standard does not specify:

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

2 Normative references

This European Standard incorporates by dated or undated reference, provisions from other publications. These normative references are cited at appropriate places in the text and the publications are listed hereafter. For dated references, subsequent amendments to or revisions of these publications apply to this European Standard only when incorporated in it by amendment or revision. For undated references the latest edition of the publication referred to applies.

EN 50126	Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)
EN 50128	Railway applications - Communications, signalling and processing systems - Software for railway control and protection systems
ENV 50129	Railway applications - Safety related electronic systems for signalling

3 Definitions

For the purpose of this standard, the following definitions apply:

3.1
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*

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

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

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

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

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

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

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

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

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

3.6.1
data corruption
the alteration of data

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3.6.4.4
source and destination identifier
an identifier is assigned to each entity. This identifier can be a name, number or arbitrary bit pattern. This identifier will be used for the safety-related transmission. Usually the identifier is added to the user data

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

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

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

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

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

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

3.10.1

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

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

3.11
hazard
a condition that can lead to an accident

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

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

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

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

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

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

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

3.14.4
message stream
an ordered set of messages

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

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

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

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

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

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

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

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

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

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

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

3.15
process

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

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

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

3.16
safety
freedom from unacceptable levels of risk

3.16.1
safety-related
carries responsibility for safety

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

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

3.17
transmission system
a service used by the application to communicate *message streams* between a number of participants, who may be sources or sinks of information

3.17.1
closed transmission system
a fixed number or fixed maximum number of participants linked by a transmission system with well known and fixed properties, and where the risk of *unauthorised* access is considered negligible

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

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

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

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

4 Reference architecture

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

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

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

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

- Elements which read, store, process or re-transmit data produced and presented by users of the transmission system in accordance with a program not known to the user. The number of the users is generally unknown, safety-related and non safety-related equipment and equipment which are 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.

The open transmission system may be subject to the following:

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

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

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

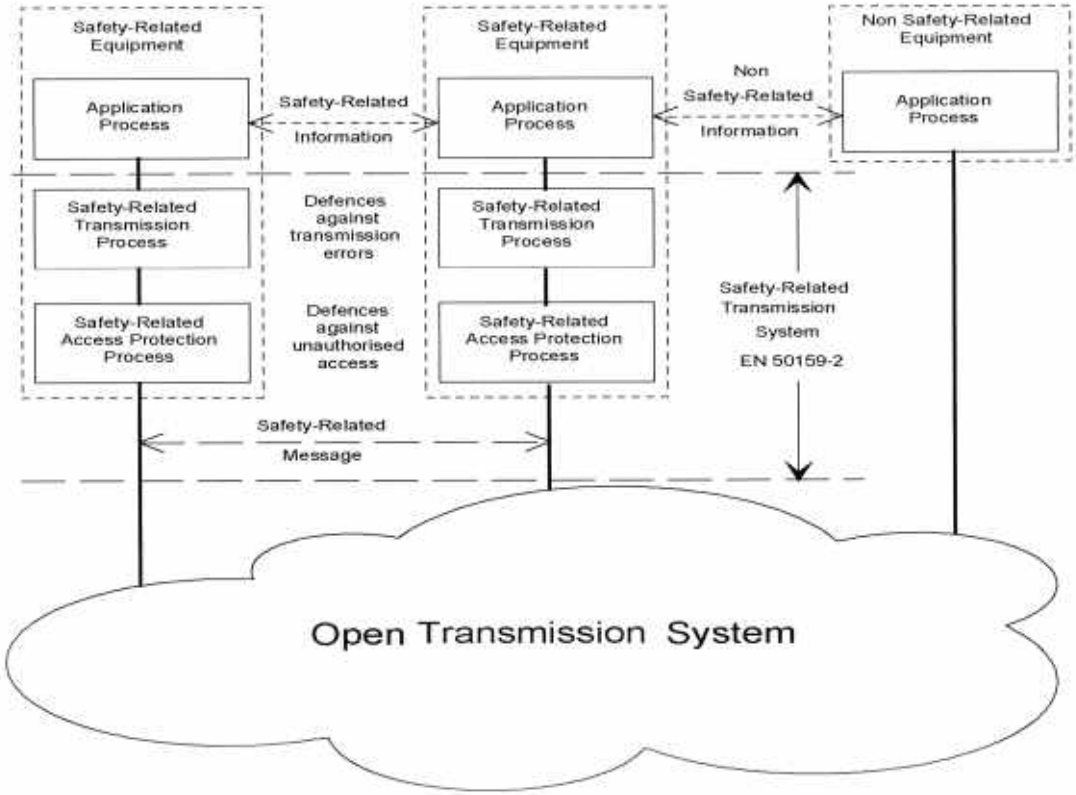

Figure 1 - Structure of safety-related system using a non trusted transmission system

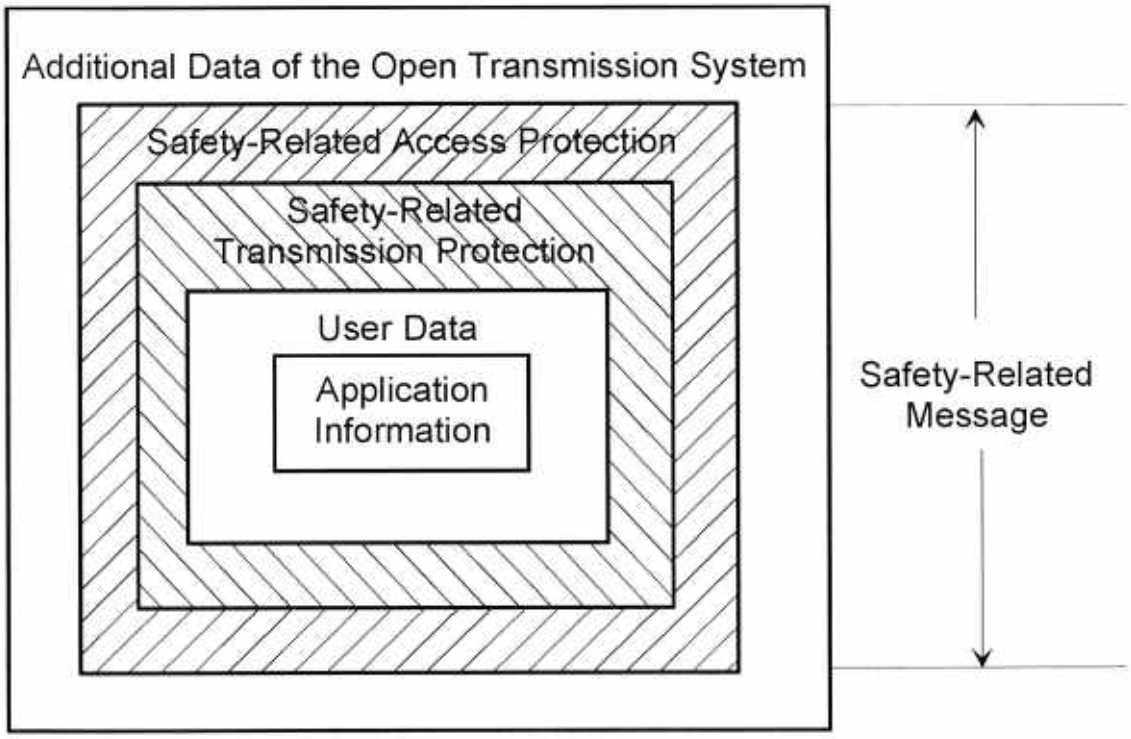

Figure 2 - Model of a safety-related message

5 Threats to the transmission system

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

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

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

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

The corresponding threats are:

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

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

6 Requirements for defences

6.1 Introduction

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

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

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

- 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.

6.2 General requirements

1) Adequate defences shall be provided against all identified threats to the safety of systems using open communication networks. Any threats which are not to be assumed shall be agreed with the safety authority and/or railway authority and shall be put into the safety-related application conditions. Annex D derives a possible list of threats, to be used as guidance.

2) Detailed requirements for the defences needed for the application shall take into account:

   - the level of risk (frequency/consequence) identified for each particular threat, and
   - the safety integrity level of the data and process concerned.

   Annex A (guidelines for defences) gives guidance on the selection of currently known techniques to give defence against threats. Issues of effectiveness addressed in this annex should be carefully considered when the defence is chosen.

3) The requirements for the defences needed shall be included in the system requirements specification and in the system safety requirements specification for the application, and shall form input to the "assurance of correct operation" portion of the safety case for the application.

4) All defences shall be implemented according to the requirements defined in ENV 50129. This implies that the defences:

   - shall be implemented completely within the safety-related transmission equipment of the system, or
   - may include access protection measures not implemented within the safety-related equipment. In this case, the continued correct functioning of the access protection processes shall be checked with adequate safety-related techniques for the application.

5) Mandatory requirements for particular defences are given in the following sections. They apply when the particular defence is used.

6) Other defences than those described in this standard may be used, provided that analysis of their effectiveness against threats is included in the safety case.

7) The safety case, as described in ENV 50129 shall include:

   - analysis of each defence used in the safety transmission system,
   - the safety reaction in case of a detected transmission error.

6.3 Specific defences

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

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

6.3.1 Sequence number

6.3.1.1 Introduction

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

6.3.1.2 Requirements

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

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

6.3.2 Time stamp

6.3.2.1 Introduction

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

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

6.3.2.2 Requirements

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

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

6.3.3 Time-out

6.3.3.1 Introduction

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

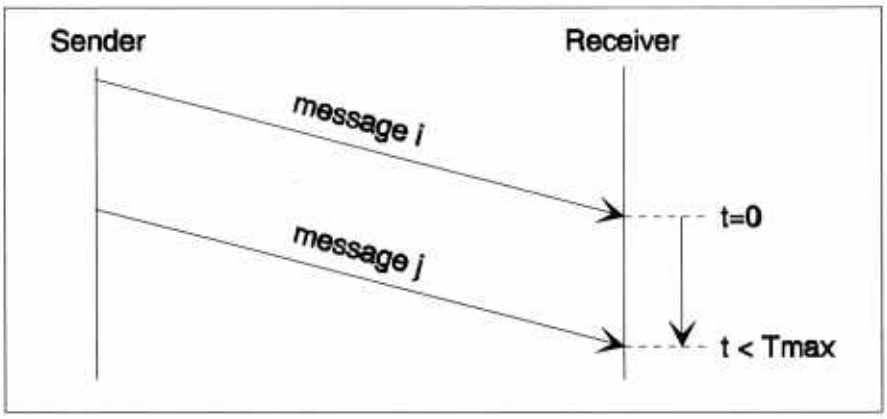

Figure 3 - Cyclic transmission of messages

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

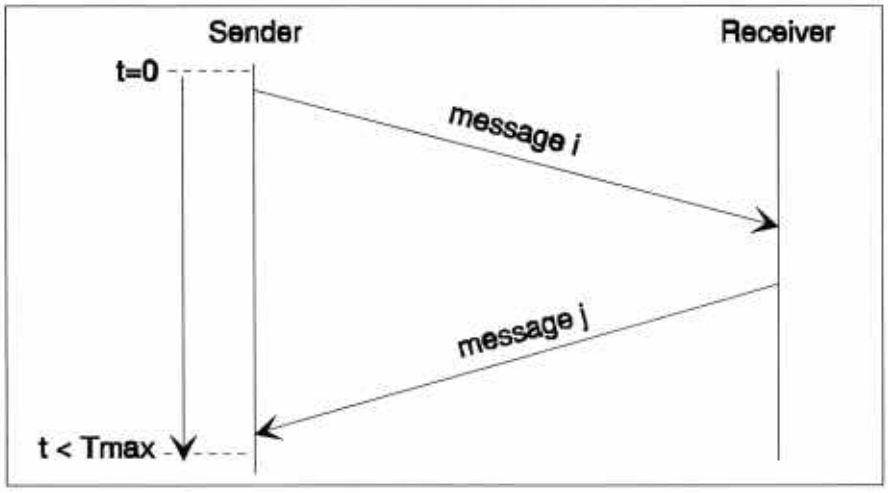

Figure 4 - Bi-directional transmission of messages

6.3.3.2 Requirements

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

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

6.3.4 Source and destination identifiers

6.3.4.1 Introduction

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

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

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

6.3.4.2 Requirements

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

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

6.3.5 Feedback message

6.3.5.1 Introduction

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

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

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

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

6.3.5.2 Requirements

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

6.3.6 Identification procedure

6.3.6.1 Introduction

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

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

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

Two types of identification procedure can be distinguished:

- bi-directional identification

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

- dynamic identification procedures

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

6.3.6.2 Requirements

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

6.3.7 Safety code

6.3.7.1 Introduction

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

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

6.3.7.2 Requirements

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

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

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

6.3.8 Cryptographic techniques

6.3.8.1 Introduction

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

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

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

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

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

6.3.8.2 Requirements

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

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

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

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

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

7 Applicability of defences against threats

7.1 Introduction

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

7.2 Threats/defences matrix

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

Table 1 - Threats/defences matrix

Threats	Defences							
	Sequence number	Time stamp	Time-out	Source and destination identifiers	Feed-back message	Identification procedure	Safety code	Cryptographic techniques
Repetition	X	X						
Deletion	X							
Insertion	X			X [2]	X [1]	X [1]		
Resequence	X	X						
Corruption							X [3]	X
Delay		X	X					
Masquerade					X [1]	X [1]		X [3]

1) Application dependent

2) Only applicable for source identifier
Will only detect insertion from invalid source
If unique identifiers cannot be determined because of unknown users, a cryptographic technique shall be used, see 6.3.8.

3) See 7.3 and A.2.

7.3 Choice and use of safety code and cryptographic techniques

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

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

Guidance on these issues is given in A.2.

Annex A (informative)

Guideline for defences

A.1 Applications of time stamps

A time stamp can be used for different purposes:

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

   Constraints:

   - If an absolute time stamp is used, the time in the entities needs to be 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.

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

   Constraints:

   - If the time granularity is too coarse, the sequencing properties of events can be indeterminate. In such cases the information shall be complemented with sequence numbers
   - The order of messages is affected by network routing of messages and time delays in the network.
   - Absence of messages will not be detected if a dialogue communication procedure is not provided.

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

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

   Constraints:

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

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

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

   Constraints:

   - The procedure shall handle interruption due to initialisation or fault conditions.
   - The procedure will not guarantee authentication of the messages.

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

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

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

   c) checking the correct order of messages;

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

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

Constraints:

- If the time granularity is too coarse, the sequencing properties of events can be indeterminate. In such cases the information shall be complemented with sequence numbers.
- Double time stamping may require knowledge about the round-trip transmission delays if the application considers case 1 above.

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

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

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

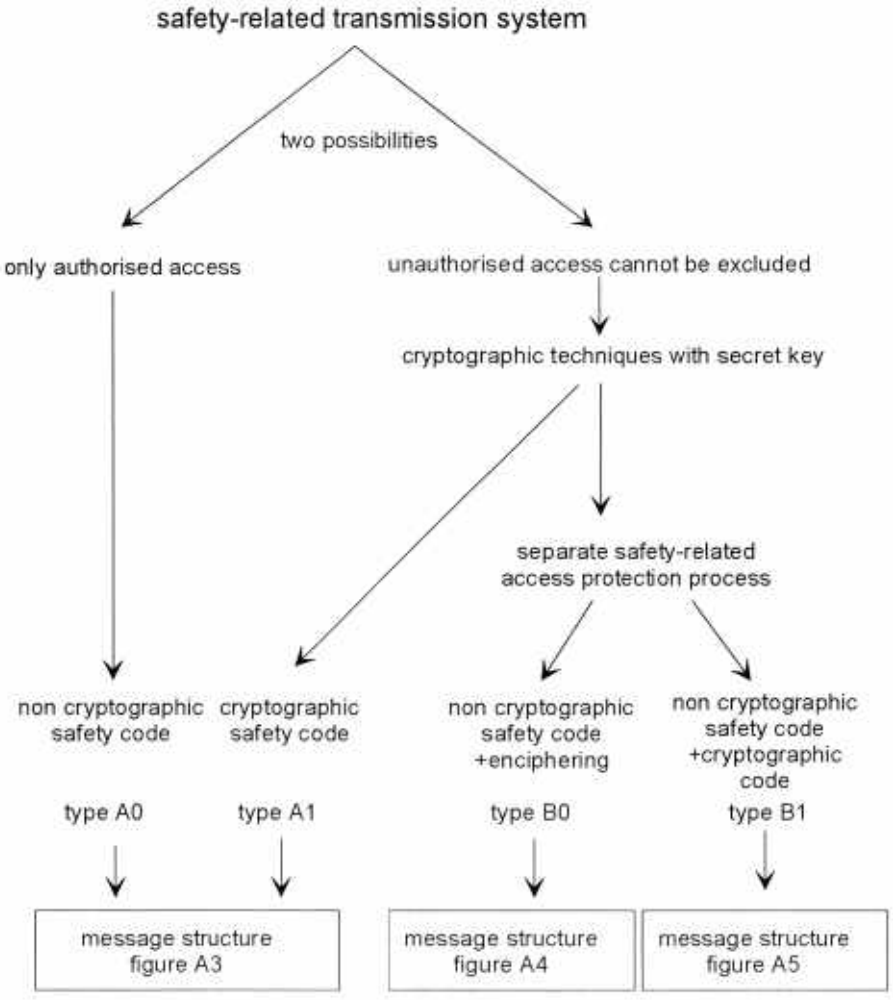

Figure A.1 - Classification of the safety-related transmission system

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

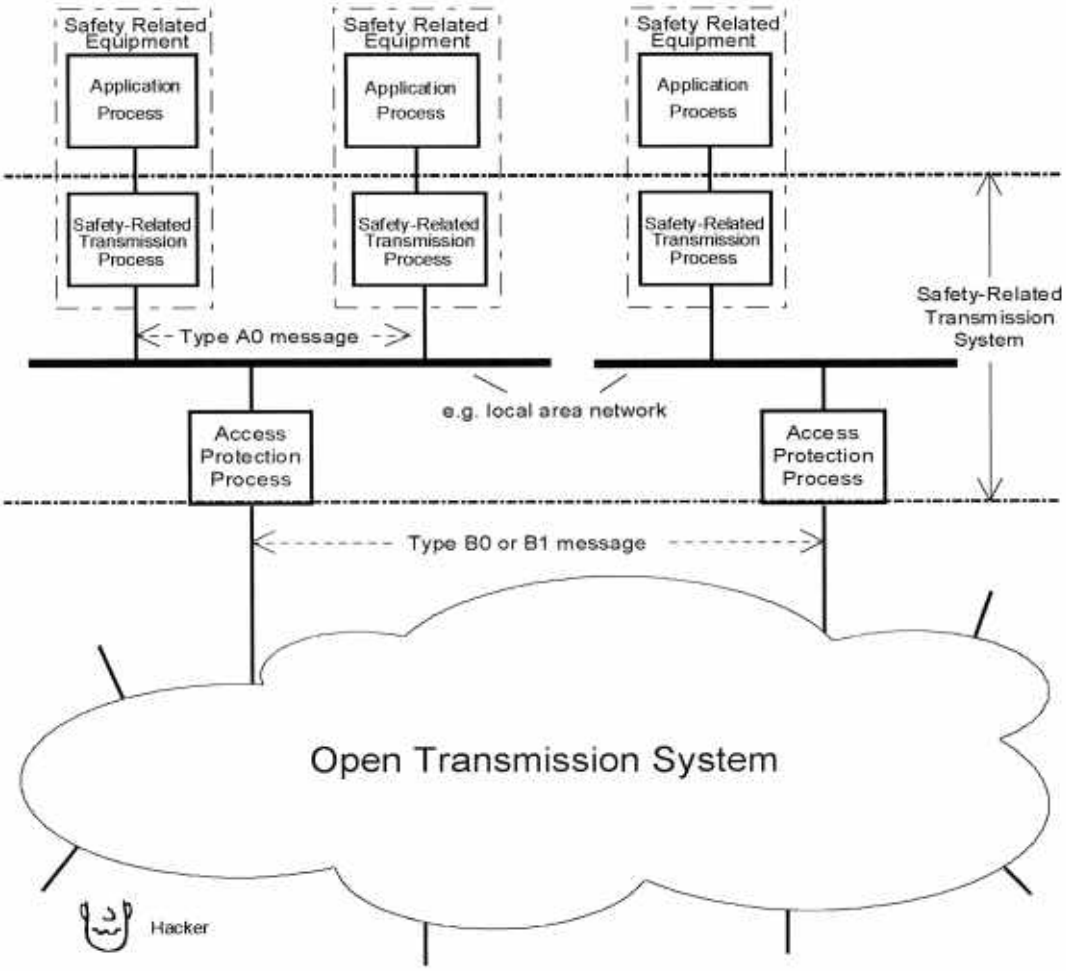

Figure A.2 - Use of a separate access protection layer

The access protection process can be performed by different modes:

1) enciphering of the messages;

2) adding a cryptographic code

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

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

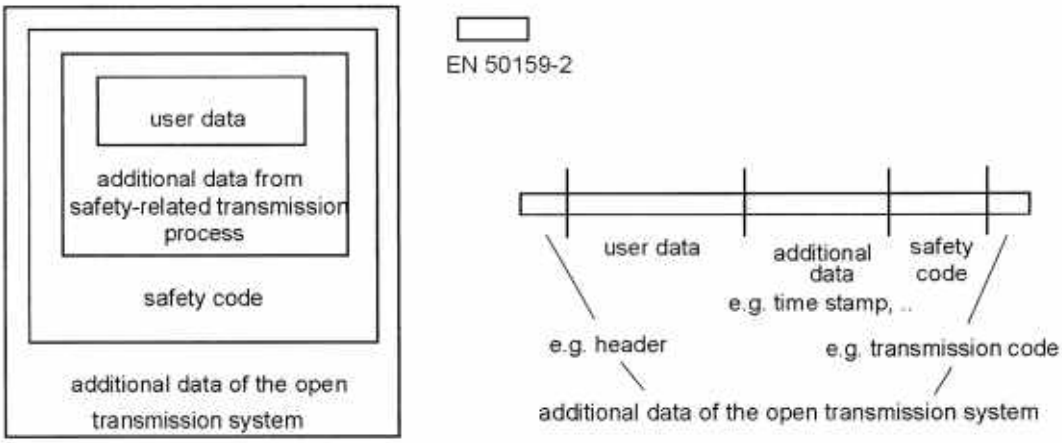

Figure A.3 - Model of message representation within the transmission system (type A0, A1)

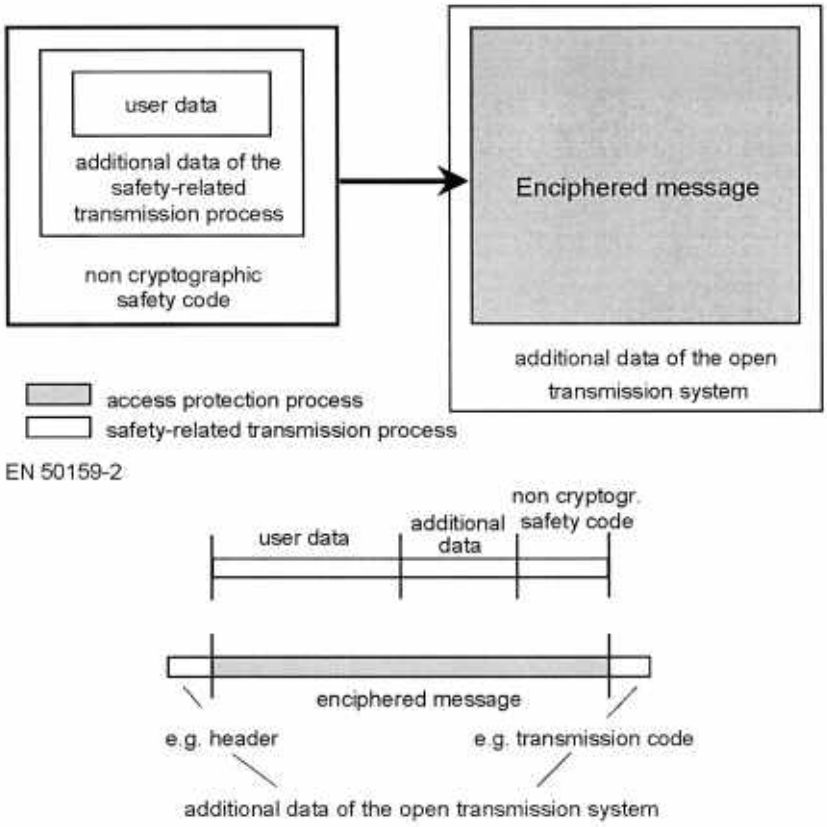

Figure A.4 - Model of message representation within the transmission system (type B0)

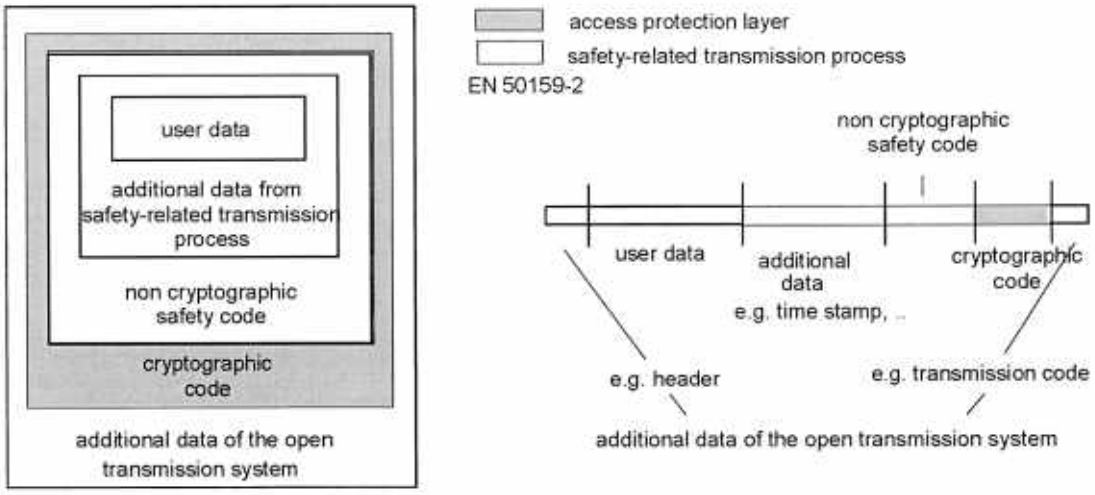

Figure A.5 - Model of message representation within the transmission system (type B1)

A.2.1 Safety code

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

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

If 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.

A.2.1.1 Main block codes

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

Linear block codes

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

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 up to *d-1* bit errors are detected to 100%. Because of their linearity the codes can also be tested for systematic error detection capability.

Cyclic block codes (CRC)

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

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

In certain applications the cyclic nature of the code can be exploited to avoid the danger of false code word 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.

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 the average, half of the bits in the hash value. Given a hash value, it is computationally unfeasible to find the input data that hash to that value (one-wayness property) and, given the input data, it is computationally unfeasible to find another input data that hash to the same value (collision property for weak hash functions) and it is computationally unfeasible to find any couple of input data that hash to the same value (collision property for strong hash functions).

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

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

Digital signatures

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

Cryptographic block codes

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

A.2.1.2 Recommendations for the application of safety codes

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

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

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

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

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

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

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

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

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

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

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

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

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

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

A.2.2 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 the rules of the international standard ISO/IEC 9979, but the registration itself does not guarantee the strength of the algorithms.

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

Annex B (informative)

Bibliography

EN 50159-1	Railway applications - Communication, signalling and processing systems Part 1: Safety-related communication in closed transmission systems
ISO/IEC 11770	Information technology -- Security techniques -- Key management Part 1: Framework (1996) Part 2: Mechanisms using symmetric techniques (1996) Part 3: Mechanisms using asymmetric techniques (1999)
ISO/IEC 9796:1991	Information technology - Security techniques - Digital signatures scheme giving message recovery
ISO/IEC 9797:1994	Information technology -- Security techniques -- Data integrity mechanism using a cryptographic check function employing a block cipher algorithm
ISO/IEC 9979:1999	Information technology -- Security techniques -- Procedures for the registration of cryptographic algorithms
ISO/IEC 10116:1991	Information technology -- Security techniques -- Modes of operation for an n-bit block cipher
ISO/IEC 10118	Information technology -- Security techniques -- Hash-functions Part 1: General (2000) Part 2: Hash-functions using an *n*-bit block cipher (2000)
[TBaum]	A. Tanenbaum: Distributed Systems, Pretince Hall 1995
[A155]	UIC/ORE A155.1 Report RP 4, September 1984: Survey of available measures for protection of safety information during transmission (also available in German and French)
[DES]	FIPS PUB 46, 15.1.1977: Specifications for the Data Encryption Standard
[Peterson]	W.Wesly Peterson: Error correction Codes, M.I.T. Press, 1967
[Schneier]	Bruce Schneier: Applied Cryptography, J. Wiley & Sons, Inc, 2nd edition 1995
[Rivest]	R. Rivest: The MD4 Message-Digest Algorithm, 4/92, published within Internet
[Davies]	D.W. Davies and W.L. Price: Security for Computer Networks, 2. edition, J. Wiley & Sons, Chichester

Annex C (informative)

Guidelines for use of the standard

C.1 Scope/purpose

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

C.2 Classification of transmission systems

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

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

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

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

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

Table C.1 - Classes of open transmission systems

Type	Main characteristics	Examples	Comments
Class 1	All properties are known and invariable during the life time Single user group	Proprietary local networks, PROFIBUS, MVB (multi purpose vehicle bus proposed by IEC) invariable during life time	Use EN 50159-1
Class 2	Some properties are known and invariable during the life time Limited extension Limited storage Single user group	same as class 1 but the possibility exists that the transmission system could be substituted by an other transmission system during the life time	-
Class 3	Some properties are known and invariable during the life time Limited extension Nearly unlimited storage Known multiple users groups	LAN	-
Class 4	Properties are unknown and/or variable during the life time Only using trusted networks (Known) multiple users groups	WAN belonging to the railways	-
Class 5	Properties are unknown and/or variable during the life time Sometimes using non trusted networks Multiple users groups	Use of public telephone network at unpredictable times	e.g. remote diagnostic of interlocking systems
Class 6	Properties are unknown and/or variable during the life time Use of public telecommunication network Misuse remote Multiple users groups	Public telephone network	-
Class 7	Properties are unknown and/or variable during the life time Use of public telecommunication network Misuse frequently	Internet	-

Relationship between class of transmission system and the threats.

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

Table C.2 - Threat/class relationship

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

Legend:
- : Threat can be neglected
+ : Threat existent, but rare; weak countermeasures sufficient
++ : Threat existent; strong countermeasures required

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

C.3 Procedure

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

These steps are identified below:

Application
↓
Hazard analysis
↓
Risk reduction
↓
Allocation of SIL and quantitative targets
↓
Safety Requirements Specifications

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

C.3.1 Application

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

C.3.2 Hazard analysis

Qualitative hazard analysis of the system (as required by EN 50126) must identify the top-level hazard(s) which can arise as a result of failures of the sending and receiving equipment, or of the transmission link itself. This analysis must consider operational or other external conditions which could expose the system to the hazard. For each threat to the system, the possibility of including a defence in the system design can be included.

C.3.3 Risk reduction

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

C.3.4 Allocation of SIL and quantitative targets

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

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

C.3.5 Safety requirements specifications (SRS)

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

C.4 Example

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

C.4.1 Application

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

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

C.4.2 Hazard analysis

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

1) Reception of an incorrect (wrong-side) message on-board a train could result in the train entering an occupied section, and colliding with another train.

2) Delay in receiving an emergency stop message could result in a train colliding with an obstruction on the track.

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

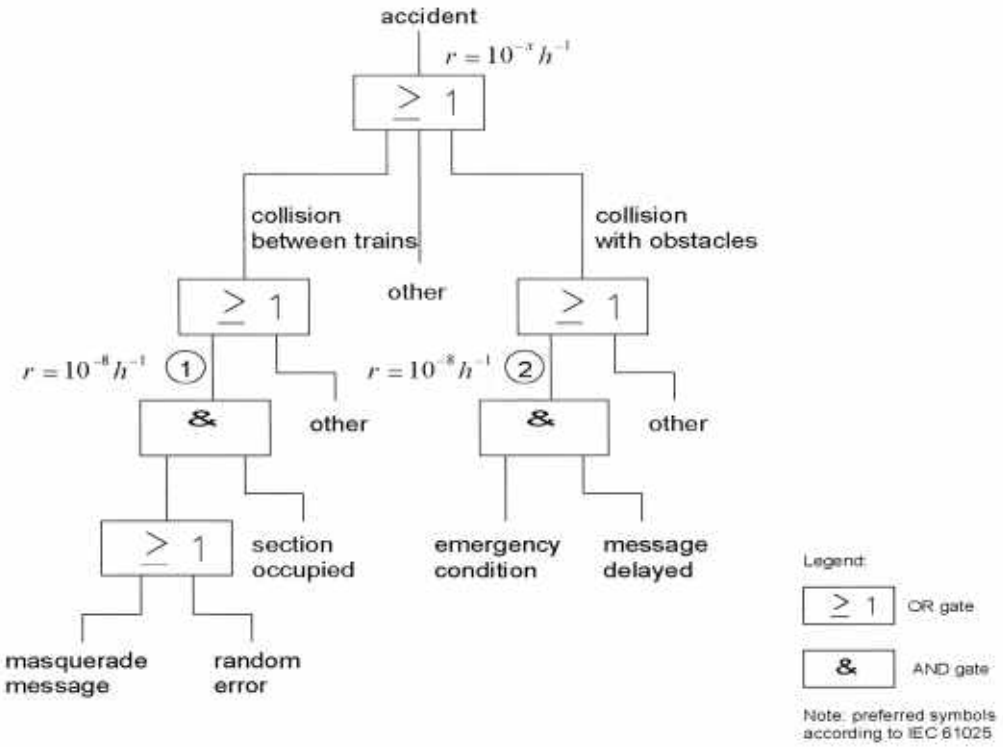

Figure C.1 - Fault tree for the hazard "accident"

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

Cases 1 and 2 will be considered in detail.

C.4.3 Case 1

Risk reduction

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

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

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

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

Introducing this defence into the portion of the fault tree for this case, the following results:

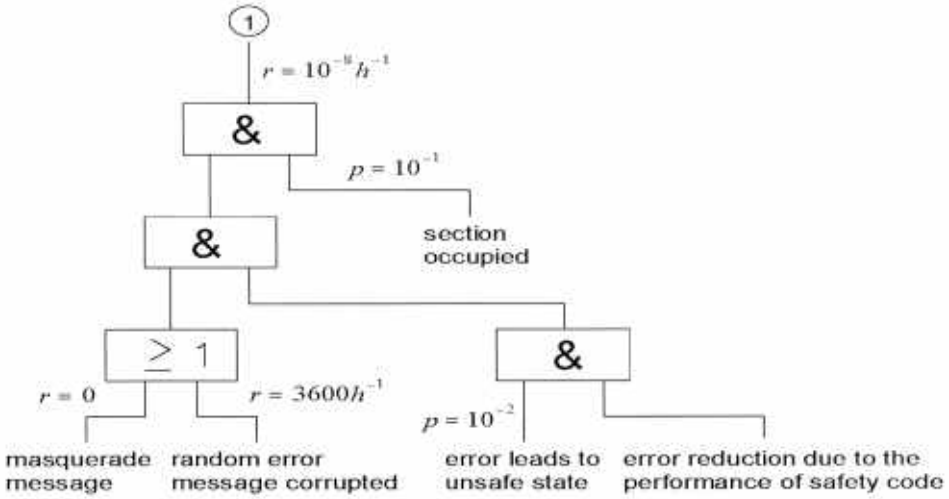

Figure C.2 - Fault tree for case 1

Considering quantitative safety targets, it must 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. 3600 messages per hour), it is clear that the safety code for the message must guarantee a probability of undetected error of less than $3 \cdot 10^{-9}$ per message, or the frequency of this kind of events shall not exceed $10^{-5} h^{-1}$.

SIL allocation and quantified target

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

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

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

C.4.4 Case 2

Risk reduction

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

Suppose that, using a public radio network shared with an uncontrolled number of other users, no maximum message delay is guaranteed, and delay must 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 results:

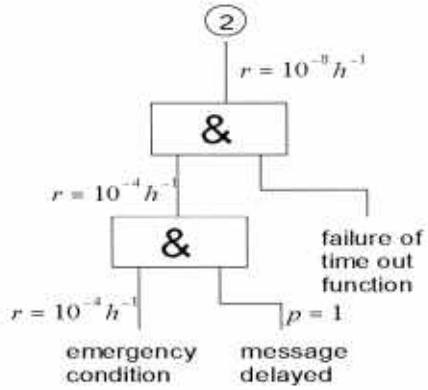

Figure C.3 - Fault tree for case 2

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

SIL allocation and quantified target

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

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

Annex D (informative)

Threats on open transmission systems

D.1 System view

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

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

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

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

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

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

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

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

1) one at a *system/user application* level, treating with the implementation of the system, independently from the transmission field; an example is the deletion, that can turn out to be absolutely not dangerous if the system has been designed in such a way that deleted messages do not represent a hazard;

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

3) one at a *physical* level, an example is the shielding in order to avoid the corruption due to an electromagnetic interference.

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

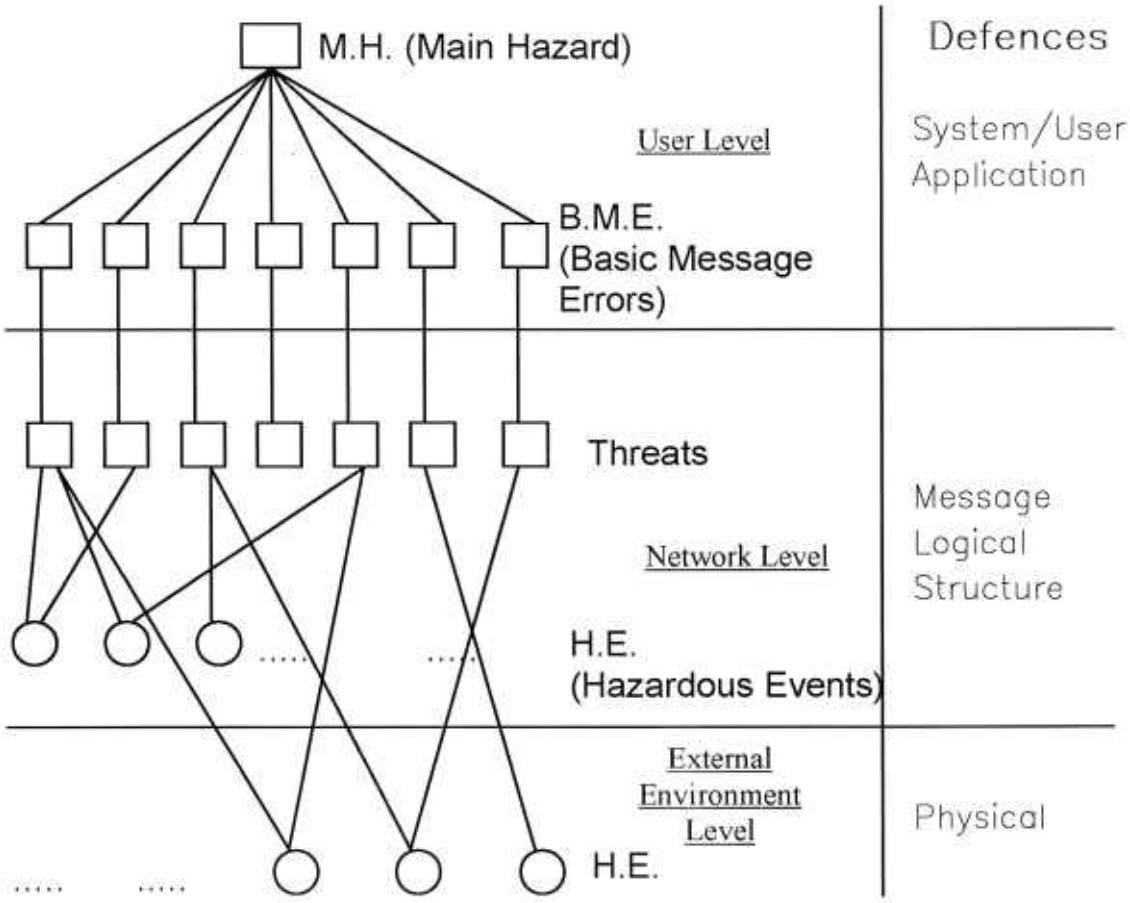

Figure D.1 - Hazard tree

D.2 Derivation of the basic message errors

The message is the main subject of the whole analysis, so the communication process has been studied from the point of view of the receiver. A message can be defined as "*useful information originated by a source to be delivered within a time Δt 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: resequencing has taken place;
- for a message in the stream it took longer than nominal Δt to reach the receiver: delay has taken place;
- the message has been modified: corruption has taken place;
- the receiver believes that the sender of a message is another than the real one: masquerade has taken place.

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

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

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

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

D.3 Threats

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

Let A-B and C-D be the two couples of 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.

Repetition

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

or

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

Deletion

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

or

- a message is deleted due to a hardware failure.

Insertion

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

or

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

Resequencing

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

or

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

Corruption

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

or

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

Delay

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

or

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

Masquerade

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

or

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

D.4 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 the deep knowledge of the application to which it is related, in order to perform also a proper risk assessment.

D.4.1 Structured methods for hazardous events identification

In the following, the analysis starts from the consideration that the examined case is dealing with a network interacting with the external environment. These two entities are structured in sub-entities (underlined in Figure D.2) that can be considered as the causes of the possible hazardous events to the 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 D.2 represent the causes of hazards: for each cause the corresponding generated hazardous events are identified. This way to proceed makes it also easier, once defined the probability of a single cause, the allocation of probability for each hazardous event produced.

In the following each cause is split into one number of possible Hazardous Events; this splitting is not exhaustive: during the Hazard Analysis some other Hazardous Events might be taken into account depending on the specific application.

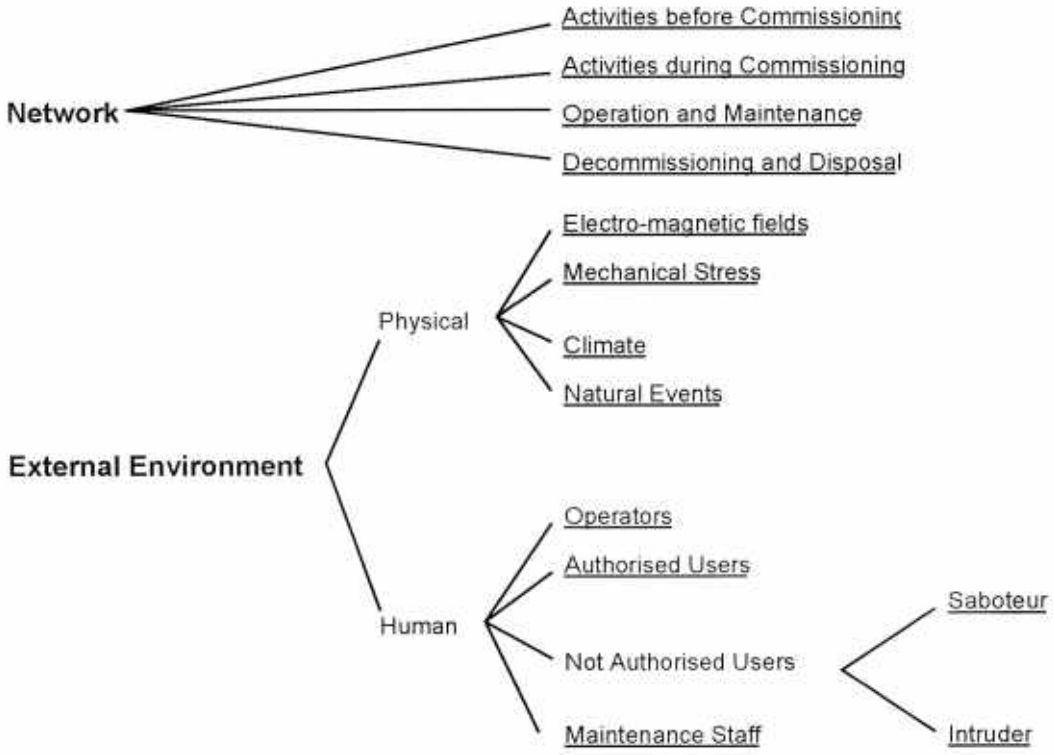

Figure D.2 - Causes of threats

D.4.1.1 Network

The phases of network life-cycle can be defined according to 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: are related to the commissioning of the system
- operation and maintenance;
- decommissioning and disposal.

Activities before commissioning

Errors during this phase can lead to:

- HW systematic failure;
- SW systematic failure.

Activities during commissioning

Errors during this phase can lead to:

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

Operation and maintenance

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

Loss of performance

- HW random failure;
- HW ageing.

Maintenance

- use of not calibrated instruments;
- use of not suited instruments;
- incorrect HW replacement;
- incorrect SW upgrading or replacement.

Modification

- fading effects;
- human mistakes[1)].

Decommissioning and disposal

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

D.4.1.2 External environment

Electro-magnetic fields

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

Mechanical stress

- HW random failures;
- HW ageing.

---

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

Climate

- thermal noise;
- HW ageing;
- HW random failures;
- fading effects.

Natural events

- magnetic storm;
- fire;
- earthquake;
- lightning.

Operators

- human mistakes[1)]

Authorised users

- human mistakes[1)];
- overloading of transmission system.

Maintenance staff

- use of not calibrated instruments;
- use of not suited instruments;
- incorrect HW replacement;
- human mistakes[1)];
- incorrect SW upgrading or replacement.

Saboteur[2)]

- wires tapping;
- HW damage or breaking;I
- not authorised SW modifications.

Intruder[2)]

- monitoring of channels;
- transmission of not authorised messages.

D.4.2 Relationship hazardous events - threats

Referring to D.1, each threat can be seen as the set of hazardous events which generate it. Starting from the hazardous events identified in the previous subclause, the next step consists in building a relationship between them and the threats outlined in D.3 by means of a bottom-up method[3)]. The goal is that of verifying that no extra threat comes out, in order to prove the validity of the undertaken approach. The relationship threats-hazardous events can be represented by the Table D.1.

---

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

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

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

D.5 Conclusions

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

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

Table D.1 - Relationship between hazardous events - threats

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

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

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

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

FINAL DRAFT
prEN 50159-1

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

June 1998

ICS 35.240.60;45.020

Descriptors: Railway equipment, information interchange, telecommunication, data processing, data transfer, message, safety

English version

Railway applications - Communication, signalling and processing systems
Part 1: Safety-related communication in closed transmission systems

Applications ferroviaires - Systèmes de signalisation, de télécommunication et de traitement
Partie 1: Communication en sécurité utilisant des systèmes de transmission fermée

Bahnanwendungen - Telekommunikationstechnik, Signaltechnik und Datenvearbeitungssysteme
Teil 1: Sicherheitsrelevante Kommunikation in geschlossenen Übertragungssystemen

This draft European Standard is submitted to CENELEC members for formal vote.

It has been drawn up by SC 9XA of Technical Committee CENELEC TC 9X.

If this draft becomes a European Standard, 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.

This draft European Standard was established by CENELEC 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, Czech Republic, Denmark, Finland, France, Germany, Greece, Iceland, Ireland, Italy, Luxembourg, Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and United Kingdom.

CENELEC

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

Central Secretariat: rue de Stassart 35, B - 1050 Brussels

Foreword

This draft European Standard was prepared by SC 9XA, Communication, signalling and processing systems, of CENELEC Technical Committee 9X, Electrical and electronic applications for railways. It is submitted to the formal vote.

The following dates are proposed:

- latest date by which the existence of the EN has to be announced at national level	(doa)	1999-07-01
- latest date by which the EN has to be implemented at national level by publication of an identical national standard or by endorsement	(dop)	2000-01-01
- latest date by which the national standards conflicting with the EN have to be withdrawn	(dow)	2000-01-01

This standard is in close relation to prEN 50128, prEN 50129 and prEN 50159-2.

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

Annexes designated "informative" are given for information only.
In this standard, annex A is informative.

Contents

Introduction

This European Standard deals with safety-related communication between safety-related equipment using a closed transmission system. For those transmission systems which cannot be considered as closed, EN 50159-2 shall be applied.

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

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

- to detect errors
- to initiate a safety reaction

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

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

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

1 Scope

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

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

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

This standard is not applicable to existing systems which had already been accepted prior to the release of this standard. However, as far as is reasonably practicable, this standard shall be applied to modifications and extensions to existing systems, subsystems and equipment.

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

1 Only approved access is permitted.
2 There is a known maximum number of connectable participants.
3 The transmission media is known and fixed.

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

In particular this standard does not define:

- The transmission system.
- The equipment connected to the transmission system.
- Specific solutions (e.g. for interoperability).
- Which kinds of data are safety-related and which aren't.

2 Normative References

This European Standard incorporates by dated or undated reference, provisions from other publications. These normative references are cited at appropriate places in the text and the publications are listed hereafter. For dated references, subsequent amendments to or revisions of these publications apply to this European Standard only when incorporated in it by amendment or revision. For undated references the latest edition of the publication referred to applies.

EN 50126 (*) Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)

EN 50128 (*) Railway applications - Software for railway control and protection systems

EN 50129 (**) Railway applications - Safety related electronic systems for signalling

(*) In preparation.
(**) In preparation, use ENV 50129:1998.

3 Definitions

For the purpose of this standard, the following definitions apply:

3.1 Authenticity

The state in which information is valid and known to have originated from the stated source.

3.2 Closed transmission system

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

3.3 CRC

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

3.4 EMI

Electromagnetic Interference

3.5 Integrity

The state in which information is complete and correct and not altered or corrupted.

3.6 Message

Information which is transmitted from a sender (data source) to one or more receivers (data sink)

3.7 Non-trusted

No specific precautions towards safety

3.8 Safe fall back state

Safe state of a safety-related equipment or system as a deviation from the fault-free state and as a result of a safety reaction leading to a reduced functionality of safety-related functions, possibly also of non safety-related functions.

3.9 Safety code

Redundant data included in a message to permit data corruptions to be detected by redundancy checks

3.10 Safety reaction

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

3.11 Transmission code

Redundant information, added to the safety and non safety message of the non trusted transmission system in order to ensure the integrity of the message during the transmission.

3.12 Transmission system

A service used by the application to communicate message streams between a number of participants, who may be sources or sinks of information.

3.13 User data

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

4 Reference Architecture

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

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

The safety-related transmission system is defined as:

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

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

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

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

Pr1 The transmission system is closed.

Pr2 The number of pieces of connectable equipment - either safety-related or not - to the transmission system has to be known and fixed. As the safety of the safety-related transmission system depends on this parameter, the maximum number of participants allowed to communicate together shall be put into the safety requirement specification as a precondition[1]

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

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

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

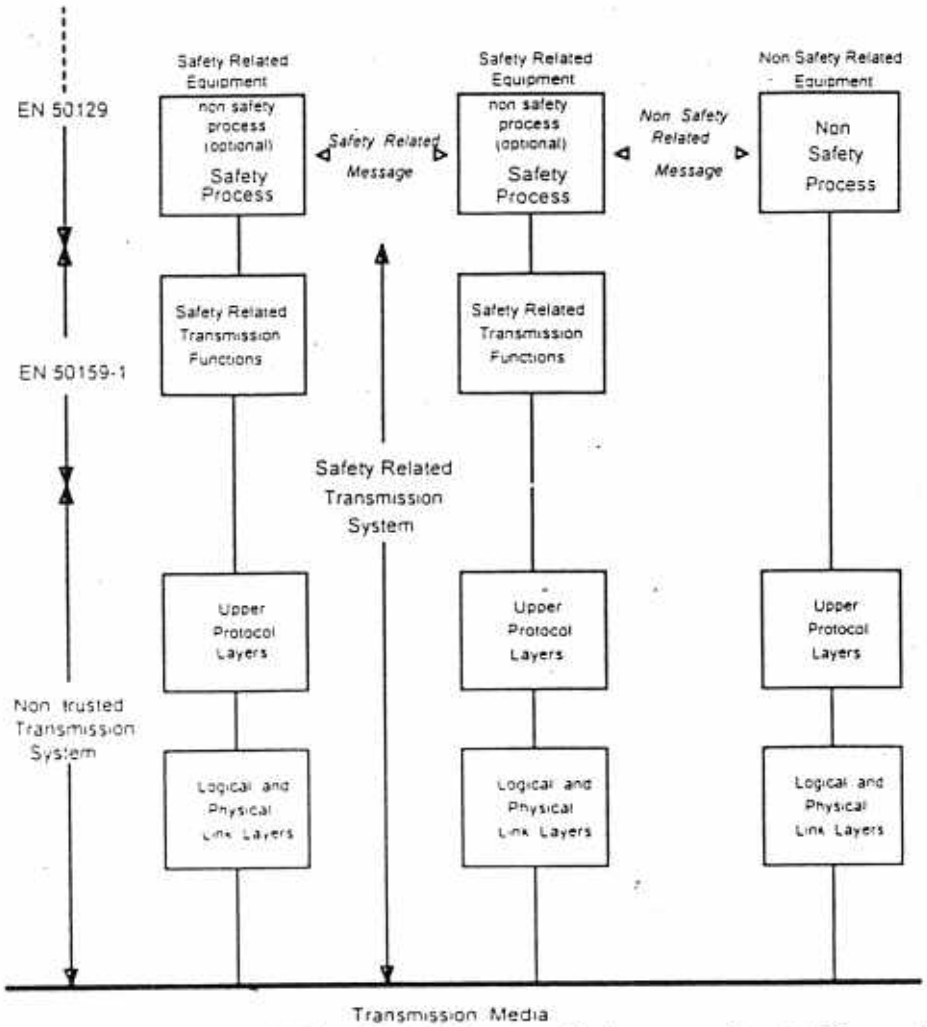

Figure 1: Structure of Safety-Related System Using a non Trusted Transmission System

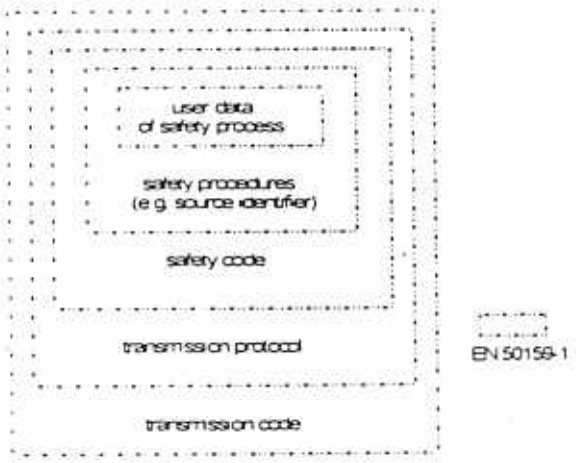

Figure 2: Model of Message Representation on the Transmission Media

5 Relation Between the Characteristics of the Transmission System and Safety Procedures

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

5.1 Functional Integrity Requirement

This mandatory analysis consists of the functional hazard analysis.

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

- Erroneous information (transmitter identity error, type error, value error),
- Time errors (data delayed too long, sequencing error).

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

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

P1 Detect transmitter identifier error
P2 Detect data type error
P3 Detect data value error
P4 Detect out dated data or data not received in due time
P5 Detect the loss of communication after a predefined delay
P6 Ensure the functional independence of the safety-related transmission functions and the used layers of the non-trusted transmission system

5.2 Safety Integrity Requirements

The six following requirements shall be fulfilled

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

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

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

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

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

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

These safety requirements are detailed in the

- Safety Procedure Requirements (qualitative precautions see chapter 6)
- Safety Code Requirements(quantitative precautions see chapter 7)

6 Safety Procedure Requirements

6.1 General

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

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

a) Safety-related equipment with safety-related equipment (see 6.1).
b) Safety-related equipment with non safety-related equipment (see 6.2).
c) Non safety-related equipment with non safety-related equipment (see 6.3).

6.2 Communication between Safety-Related Equipment

Authenticity, Integrity and Correct Time of Data shall be ensured.

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

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

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

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

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

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

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

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

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

6.3 Communication between Safety-Related and non Safety-Related Equipment

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

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

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

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

R13 Safety-related and non safety-related messages shall have different structures achieved by applying a safety code to safety-related messages. This safety code shall be capable of protecting the system to the required safety integrity level (see Safety Target Chapter 7) that a non safety-related message changes to safety-related one.

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

6.4 Communication between non Safety-Related Equipment

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

7 Safety Code Requirements

7.1 General Requirements

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

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

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

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

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

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

Requirements:

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

- Interrupted transmission line
- All bits logical 0
- All bits logical 1
- Message inversion
- Synchronisation slip (in case of serial transmission)

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

- Random errors
- Burst errors
- Systematic errors, e.g. repeated error patterns
- combinations of the above

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

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

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

7.2 Safety Target

Given the safety integrity level for the entire system, of which the safety-related communication system is a part, the hazardous failure rate for the entire system R_H shall be derived according to the procedures given in EN 50126[2] and EN 50129[3].

7.3 Length of Safety Code

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

Annex A (informative)

Length of safety code

This paragraph gives simple formulae for calculating the length of the safety code. The justification for these formulae is given in the report „Safety Analysis for a Closed Transmission System" CLC/SC9XA/WG2(Sec) 122. 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 3.

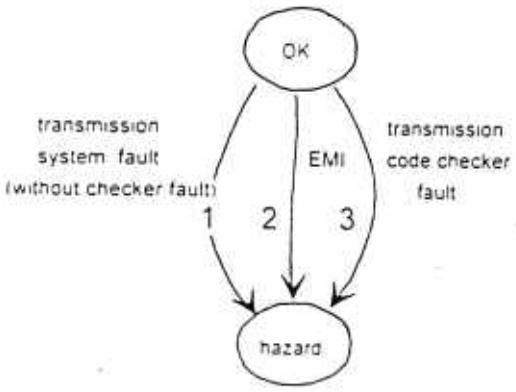

Figure 3: Basic error model

There are three ways in which a hazard may be created

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

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

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

The following definitions are given

R_H Hazardous failure rate of the complete transmission system

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

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

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

note When the non-trusted transmission systems contain no transmission coding mechanisms then $P_{UT} = 1$ has to be asumed

t_M Maximum frequency of messages for one receiver

t_W Frequency of wrong (corrupted) messages

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

k_1 Factor for hardware faults including safety margin

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

m Safety factor included within k_1

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

With these definitions the following inequations have to be fulfilled:

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

$$p_{UT} \cdot p_{US} \cdot f_W \leq R_{H2} \quad \text{(EMI)} \qquad (2)\ ^{4}$$

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

The sum of all three rates shall not exceed R_H:

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

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

$$k_1 \geq n \cdot m.$$

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

The maximum frequency of wrong messages f_W shall be estimated

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

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

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

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

where b denotes the number of redundancy bits

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

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

---

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

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

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

The following derivation is given for information only:

- If a hardware fault occurs, in only 1 of 10000 cases the transmission code checker fails undetected.
- In this case the average duration (without EMI) of this state is $T = MTBF_{HW} = \frac{1}{R_{HW}}$

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

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

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

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

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

This formula can be used as a rough estimation of the probability of undetected faults. This is valid for a large class of codes (e.g. BCH-codes, cryptographic codes,..) under realistic assumptions. Nevertheless it has to be domonstrated that the properness[5] of the chosen code is fulfilled.

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

[5] Properness means that the relation between bit error probability and probability of undetected error is monotone.