



IEC 61784-3-1

Edition 1.0 2007-12

INTERNATIONAL STANDARD

**Industrial communication networks – Profiles –
Part 3-1: Functional safety fieldbuses – Additional specifications for CPF 1**

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

PRICE CODE **XB**

ICS 35.100.05 25.040.40

ISBN 2-8318-9398-4

CONTENTS

FOREWORD.....	6
INTRODUCTION.....	8
1 Scope.....	11
2 Normative references	11
3 Terms, definitions, symbols, abbreviated terms and conventions	12
3.1 Terms and definitions	12
3.1.1 Common terms and definitions	12
3.1.2 CPF 1: Additional terms and definitions	16
3.2 Symbols and abbreviated terms.....	17
3.2.1 Common symbols and abbreviated terms	17
3.2.2 CPF 1: Additional symbols and abbreviated terms	18
3.3 Conventions	18
3.3.1 State Diagrams.....	18
3.3.2 Use of colors in figures.....	19
4 Overview of FSCP 1/1 (FOUNDATION Fieldbus™ SIS)	20
4.1 General.....	20
4.2 Key concepts of FSCP 1/1.....	21
4.2.1 Black channel.....	21
4.2.2 Connection key.....	21
4.2.3 Cross-check	21
4.2.4 FSCP 1/1.....	21
4.2.5 Programmable electronic system.....	21
4.2.6 Queuing delays	21
4.2.7 Redundancy	22
4.2.8 SIL environment	22
4.3 Key components of FSCP 1/1	22
4.3.1 Overview	22
4.3.2 Black channel	22
4.4 Relationship to the ISO OSI basic reference model	23
5 General	23
5.1 External documents providing specifications for the profile.....	23
5.2 Safety functional requirements	23
5.2.1 Requirements for functional safety.....	23
5.2.2 Functional constraints.....	24
5.2.3 Device manufacturer requirements	24
5.3 Safety measures	25
5.3.1 Sequence number	25
5.3.2 Time stamp	25
5.3.3 Time expectation	25
5.3.4 Connection authentication	25
5.3.5 Data integrity assurance.....	25
5.3.6 Redundancy with cross checking	25
5.3.7 Different data integrity assurance systems	25
5.3.8 Relationships between errors and safety measures	25
5.4 Safety communication layer structure	26
5.4.1 Network topology and device connectivity.....	26

5.4.2	Device architecture.....	26
5.5	Relationships with FAL (and DLL, PhL)	27
5.5.1	General	27
5.5.2	Data Types.....	28
6	Safety communication layer services.....	28
6.1	Application Process (AP).....	28
6.1.1	Overview	28
6.1.2	Network visible objects	29
6.1.3	Application layer interface	29
6.1.4	Object dictionary	29
6.1.5	Application program directory	29
6.2	Function block application processes	29
6.2.1	General	29
6.2.2	Function block model.....	29
6.2.3	Application process	32
6.3	Device to device communications.....	34
6.3.1	General	34
6.3.2	Client/server.....	34
6.3.3	Publisher/subscriber	35
6.3.4	Report distribution	35
6.3.5	FBAP operation in a linking device	35
6.3.6	System management kernel protocol (SMK) communications	35
6.4	Profiles.....	35
6.4.1	General	35
6.4.2	FSCP 1/1 profile	35
6.5	Device descriptions	36
6.6	Common file formats	37
6.7	Configuration information	37
6.7.1	Overview	37
6.7.2	Level 1 configuration: manufacturer device definition.....	37
6.7.3	Level 2 configuration: network definition	37
6.7.4	Level 3 configuration: distributed application definition	37
6.7.5	Level 4 configuration: device configuration	37
7	Safety communication layer protocol	37
7.1	Safety PDU format	37
7.1.1	General	37
7.1.2	Safety communication layer CRC	38
7.1.3	Black channel time synchronization monitoring.....	38
7.1.4	Sequence number	38
7.1.5	Virtual header.....	39
7.1.6	Connection key.....	39
7.1.7	Redundancy and cross-check	40
7.2	Protocol extensions for use in safety-related systems.....	40
7.2.1	Overview	40
7.2.2	Publisher-subscriber interactions	40
7.2.3	Client-server interactions.....	46
7.2.4	Time synchronization.....	51
7.2.5	Device start-up	52
7.3	Communications entity	52

7.3.1	General	52
7.3.2	Network management	52
7.3.3	FMS	52
7.3.4	H1 stack	52
8	Safety communication layer management	53
8.1	Overview	53
8.2	SMK communications	53
8.3	FMS services	53
8.4	SMK services	53
8.4.1	General	53
8.4.2	Address assignment	53
8.4.3	Time synchronization	53
8.5	Safety communication layer configuration and start-up	53
8.5.1	H1 configuration and start-up	53
8.5.2	FSCP 1/1 FBAP	54
8.5.3	Testing	54
9	System requirements	54
9.1	Indicators and switches	54
9.2	Installation guidelines	54
9.3	Safety function response time	54
9.4	Duration of demands	55
9.5	Constraints for calculation of system characteristics	55
9.5.1	Message rate	55
9.5.2	SIL level	55
9.6	Maintenance	55
9.7	Safety manual	55
10	Certification	55
Annex A (informative)	Additional information for functional safety communication profiles of CPF 1	56
A.1	Hash function calculation	56
A.2	Fault conditions arising from locations beyond the output function block	58
	Bibliography	60
Table 1	– Example state transition table	19
Table 2	– Safety measures and possible communication errors	26
Table 3	– Data types used within FSCP 1/1	28
Table 4	– Fault state behaviour	31
Table 5	– Publisher states	41
Table 6	– Publisher state table - Received transitions	42
Table 7	– Publisher state table - Internal transitions	42
Table 8	– Subscriber states	44
Table 9	– Subscriber state table - Received transitions	45
Table 10	– Subscriber state table - Internal transitions	45
Table 11	– Server states during read operations	47
Table 12	– Received transitions for a FSCP 1/1 Server during read operations	48
Table 13	– States of a FSCP 1/1 server during write operations	49

Table 14 – Received transitions for a FSCP 1/1 Server during write operations	50
Table A.1 – Fault conditions arising from locations beyond the output function block	59

Figure 1 – Relationships of IEC 61784-3 with other standards (machinery)	8
Figure 2 – Relationships of IEC 61784-3 with other standards (process)	9
Figure 3 – Example state diagram	19
Figure 4 – Use of colors in figures	19
Figure 5 – Scope of FSCP 1/1	20
Figure 6 – FSCP 1/1 architecture (H1)	22
Figure 7 – Black channel	23
Figure 8 – FSCP 1/1 in system architecture	26
Figure 9 – FSCP 1/1 H1 device	27
Figure 10 – FSCP 1/1 protocol layers	27
Figure 11 – Relationship between FSCP 1/1 and the other layers of IEC 61784-1 type 1	28
Figure 12 – Key write-lock	30
Figure 13 – Password write-lock	30
Figure 14 – Example of FSCP 1/1 communication	34
Figure 15 – Example of device description	36
Figure 16 – Safety PDU showing virtual content	41
Figure 17 – Safety PDU showing duplication of data and addition of CRC	41
Figure 18 – State transition diagram for a FSCP 1/1 Publisher	42
Figure 19 – Safety PDU showing duplication of data and addition of CRC	43
Figure 20 – Safety PDU showing virtual content	43
Figure 21 – State transition diagram for a FSCP 1/1 subscriber	44
Figure 22 – Safety PDU showing virtual content	46
Figure 23 – Safety PDU showing virtual content with sub index	46
Figure 24 – Safety PDU showing duplication of data, addition of sequence number and CRC	47
Figure 25 – State transition diagram for a FSCP 1/1 Server during read operations	47
Figure 26 – Safety PDU showing duplication of data and addition of sequence number and CRC	48
Figure 27 – Example of FSCP 1/1 write	49
Figure 28 – Example of FSCP 1/1 write with sub index	49
Figure 29 – State transition diagram for a FSCP 1/1 Server during write operations	50
Figure 30 – Safety PDU showing duplication of data and CRC	51
Figure 31 – Example of safety function response time components	54

INTERNATIONAL ELECTROTECHNICAL COMMISSION

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES

Part 3-1: Functional safety fieldbuses – Additional specifications for CPF 1

FOREWORD

- 1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
- 2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
- 3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
- 4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
- 5) IEC provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with an IEC Publication.
- 6) All users should ensure that they have the latest edition of this publication.
- 7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
- 8) Attention is drawn to the normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.

The International Electrotechnical Commission (IEC) draws attention to the fact that it is claimed that compliance with this document may involve the use of patents concerning the functional safety communication profiles for family 1 as follows, where the [xx] notation indicates the holder of the patent right:

US 99 824	[FF]	System and method for implementing safety instrumented systems in a fieldbus architecture
-----------	------	---

IEC takes no position concerning the evidence, validity and scope of these patent rights.

The holders of these patents rights have assured the IEC that they are willing to negotiate licences under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statements of the holders of these patent rights are registered with IEC.

Information may be obtained from:

[FF]	Fieldbus Foundation
	9005 Mountain Ridge Drive
	Bowie Bldg. - Suite 190
	Austin, TX 78759-5316
	Tel: +1 512 794 8890

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights other than those identified above. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 61784-3-1 has been prepared by subcommittee 65C: Industrial networks, of IEC technical committee 65: Industrial process measurement, control and automation.

The text of this standard is based on the following documents:

FDIS	Report on voting
65C/470/FDIS	65C/481/RVD

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

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

The committee has decided that the contents of this publication will remain unchanged until the maintenance result date indicated on the IEC web site under "<http://webstore.iec.ch>" in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

The list of all parts of the IEC 61784-3 series, under the general title *Industrial communication networks – Profiles – Functional safety fieldbuses*, can be found on the IEC website.

INTRODUCTION

The IEC 61158 fieldbus standard together with its companion standards IEC 61784-1 and IEC 61784-2 defines a set of communication protocols that enable distributed control of automation applications. Fieldbus technology is now considered well accepted and well proven. Thus many fieldbus enhancements are emerging, addressing not yet standardized areas such as real time, safety-related and security-related applications.

This standard explains the relevant principles for functional safety communications with reference to IEC 61508 series and specifies several safety communication layers (profiles and corresponding protocols) based on the communication profiles and protocol layers of IEC 61784-1, IEC 61784-2 and the IEC 61158 series. It does not cover electrical safety and intrinsic safety aspects.

Figure 1 shows the relationships between this standard and relevant safety and fieldbus standards in a machinery environment.

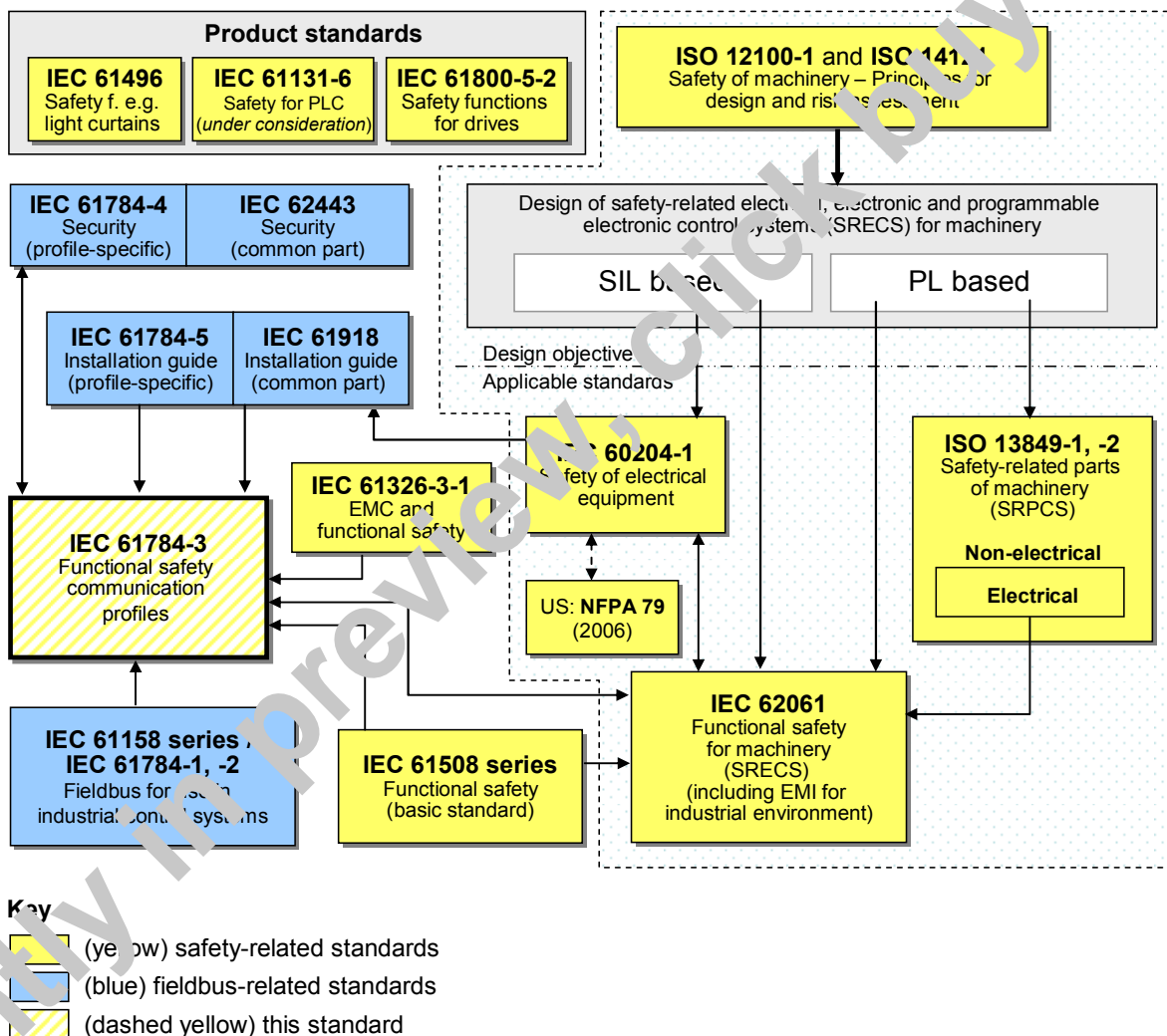
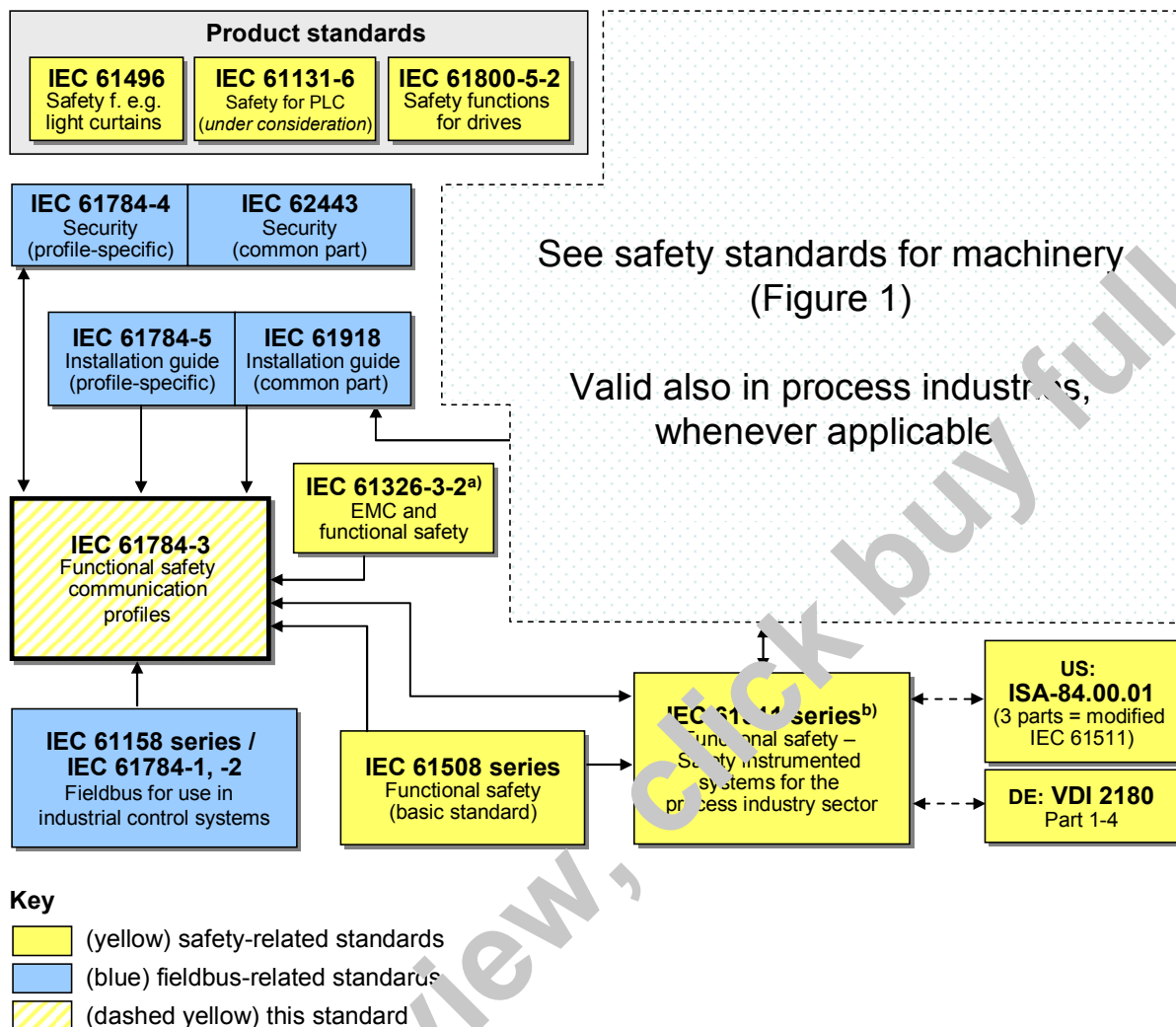


Figure 1 – Relationships of IEC 61784-3 with other standards (machinery)

Figure 2 shows the relationships between this standard and relevant safety and fieldbus standards in a process environment.



^a For specified electromagnetic environments; otherwise IEC 61326-3-1.

^b EN ratified.

Figure 2 – Relationships of IEC 61784-3 with other standards (process)

Safety communication layers which are implemented as parts of safety-related systems according to IEC 61508 series provide the necessary confidence in the transportation of messages (information) between two or more participants on a fieldbus in a safety-related system, or sufficient confidence of safe behaviour in the event of fieldbus errors or failures.

Safety communication layers specified in this standard do this in such a way that a fieldbus can be used for applications requiring functional safety up to the Safety Integrity Level (SIL) specified by its corresponding functional safety communication profile.

The resulting SIL claim of a system depends on the implementation of the selected functional safety communication profile within this system – implementation of a functional safety communication profile in a standard device is not sufficient to qualify it as a safety device.

This standard describes

- basic principles for implementing the requirements of IEC 61508 series for safety-related data communications, including possible transmission faults, remedial measures and considerations affecting data integrity;
- individual description of functional safety profiles for several communication profile families in IEC 61784-1 and IEC 61784-2;
- safety layer extensions to the communication service and protocols sections of the IEC 61158 series.

Currently in preview, click buy full version

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES

Part 3-1: Functional safety fieldbuses – Additional specifications for CPF 1

1 Scope

This part of the IEC 61784-3 series specifies a safety communication layer (services and protocol) based on CPF 1 of IEC 61784-1 and IEC 61158 Type 1 and 9. It identifies the principles for functional safety communications defined in IEC 61784-3 that are relevant for this safety communication layer.

NOTE 1 It does not cover electrical safety and intrinsic safety aspects. Electrical safety relates to hazards such as electrical shock. Intrinsic safety relates to hazards associated with potentially explosive atmospheres.

This part¹ defines mechanisms for the transmission of safety-relevant messages among participants within a distributed network using fieldbus technology in accordance with the requirements of IEC 61508 series for functional safety. These mechanisms may be used in various industrial applications such as process control, manufacturing automation and machinery.

This part provides guidelines for both developers and assessors of compliant devices and systems.

NOTE 2 The resulting SIL claim of a system depends on the implementation of the selected functional safety communication profile within this system – implementation of a functional safety communication profile according to this part in a standard device is not sufficient to qualify it as a safety device.

2 Normative references

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

IEC 61131-2, *Programmable controllers – Part 2: Equipment requirements and tests*

IEC 61158-2, *Industrial communication networks – Fieldbus specifications – Part 2: Physical layer specification and service definition*

IEC 61158-3-1, *Industrial communication networks – Fieldbus specifications – Part 3-1: Data-link layer service definition – Type 1 elements*

IEC 61158-4-1, *Industrial communication networks – Fieldbus specifications – Part 4-1: Data-link layer protocol specification – Type 1 elements*

IEC 61158-5-5, *Industrial communication networks – Fieldbus specifications – Part 5-5: Application layer service definition – Type 5 elements*

IEC 61158-5-9, *Industrial communication networks – Fieldbus specifications – Part 5-9: Application layer service definition – Type 9 elements*

IEC 61158-6-5, *Industrial communication networks – Fieldbus specifications – Part 6-5: Application layer protocol specification – Type 5 elements*

¹ In the following pages of this standard, “this part” will be used for “this part of the IEC 61784-3 series”.

IEC 61158-6-9, *Industrial communication networks – Fieldbus specifications – Part 6-9: Application layer protocol specification – Type 9 elements*

IEC 61508 (all parts), *Functional safety of electrical/electronic/programmable electronic safety-related systems*

IEC 61511 (all parts), *Functional safety – Safety instrumented systems for the process industry sector*

IEC 61784-1, *Industrial communication networks – Profiles – Part 1: Fieldbus profiles*

IEC 61784-3, *Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions*

IEC 61918, *Industrial communication networks – Installation of communication networks in industrial premises*

IEC 62280-1:2002, *Railway applications – Communication, signalling and processing systems – Part 1: Safety-related communication in closed transmission systems*