



BSI Standards Publication

Industrial communication networks – Profiles

Part 3: Functional safety fieldbuses – General rules
and profile definitions (IEC 61784-3:2016)

National foreword

This British Standard is the UK implementation of EN 61784-3:2016, including amendment A1:2017. It is identical to IEC 61784-3:2016, including amendment 1:2017. It supersedes BS EN 61784-3:2016, which will be withdrawn on 8 September 2020.

The text of IEC amendment 1:2017 has been provided in its entirety at the beginning of this document. BSI's policy of providing consolidated content remains unchanged; however, in the interest of expediency, in this instance BSI have chosen to collate the relevant content at the beginning of this document.

The UK participation in its preparation was entrusted to Technical Committee AMT/7, Industrial communications: process measurement and control, including fieldbus.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2018
Published by BSI Standards Limited 2018

ISBN 978 0 580 91195 8

ICS 35.100.05; 25.040.40

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 September 2016.

Amendments/corrigenda issued since publication

Date	Text affected
31 March 2018	Implementation of IEC amendment 1:2017 with CENELEC endorsement A1:2017

English Version

Industrial communication networks - Profiles -
Part 3: Functional safety fieldbuses -
General rules and profile definitions
(IEC 61784-3:2016)

Réseaux de communication industriels - Profils -
Partie 3: Bus de terrain de sécurité fonctionnelle -
Règles générales et définitions de profils
(IEC 61784-3:2016)

Industrielle Kommunikationsnetze - Profile -
Teil 3: Funktional sichere Übertragung bei Feldbussen -
Allgemeine Regeln und Festlegungen für Profile
(IEC 61784-3:2016)

This European Standard was approved by CENELEC on 2016-06-17. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

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

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

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



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

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

European foreword

The text of document 65C/840/FDIS, future edition 3 of IEC 61784-3, prepared by SC 65C "Industrial networks" of IEC/TC 65 "Industrial-process measurement, control and automation" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN 61784-3:2016.

The following dates are fixed:

- latest date by which the document has to be implemented at national level by publication of an identical national standard or by endorsement (dop) 2017-03-17
- latest date by which the national standards conflicting with the document have to be withdrawn (dow) 2019-06-17

This document supersedes EN 61784-3:2010.

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

Endorsement notice

The text of the International Standard IEC 61784-3:2016 was approved by CENELEC as a European Standard without any modification.

In the official version, for Bibliography, the following notes have to be added for the standards indicated:

IEC 60204-1	NOTE	Harmonized as EN 60204-1.
IEC 61131-2:2007	NOTE	Harmonized as EN 61131-2:2007 (not modified).
IEC 61131-6	NOTE	Harmonized as EN 61131-6.
IEC 61496	NOTE	Harmonized in EN 61496 series.
IEC 61496-1	NOTE	Harmonized as EN 61496-1.
IEC 61508-4:2010	NOTE	Harmonized as EN 61508-4:2010 (not modified).
IEC 61508-5:2010	NOTE	Harmonized as EN 61508-5:2010 (not modified).
IEC 61511	NOTE	Harmonized in EN 61511 series.
IEC 61800-5-2	NOTE	Harmonized as EN 61800-5-2.
IEC 62061:2005	NOTE	Harmonized as EN 62061:2005 (not modified).
IEC/TR 62685	NOTE	Harmonized as CLC/TR 62685.

ISO 10218-1	NOTE	Harmonized as EN ISO 10218-1.
ISO 12100	NOTE	Harmonized as EN ISO 12100.
ISO 13849	NOTE	Harmonized in EN ISO 13849 series.
ISO 13849-1:2015	NOTE	Harmonized as EN ISO 13849-1:2015 (not modified).

English Version

Industrial communication networks - Profiles -
Part 3: Functional safety fieldbuses - General rules
and profile definitions
(IEC 61784-3:2016/A1:2017)

Réseaux de communication industriels - Profils -
Partie 3: Bus de terrain de sécurité fonctionnelle - Règles
générales et définitions de profils
(IEC 61784-3:2016/A1:2017)

Industrielle Kommunikationsnetze - Profile -
Teil 3: Funktional sichere Übertragung bei Feldbussen -
Allgemeine Regeln und Festlegungen für Profile
(IEC 61784-3:2016/A1:2017)

This amendment A1 modifies the European Standard EN 61784-3:2016; it was approved by CENELEC on 2017-09-08. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this amendment the status of a national standard without any alteration.

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

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

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



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

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

European foreword

The text of document 65C/879/FDIS, future IEC 61784-3:2016/A1, prepared by SC 65C "Industrial networks", of IEC/TC 65 "Industrial-process measurement, control and automation" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN 61784-3:2016/A1:2017.

The following dates are fixed:

- latest date by which the document has to be (dop) 2018-06-08
implemented at national level by
publication of an identical national
standard or by endorsement
- latest date by which the national (dow) 2020-09-08
standards conflicting with the
document have to be withdrawn

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

Endorsement notice

The text of the International Standard IEC 61784-3:2016/A1:2017 was approved by CENELEC as a European Standard without any modification.

Annex ZA

(normative)

Normative references to international publications with their corresponding European publications

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

NOTE 1 When an International Publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

NOTE 2 Up-to-date information on the latest versions of the European Standards listed in this annex is available here: www.cenelec.eu.

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
IEC 61000-6-7	-	Electromagnetic compatibility (EMC) - Part 6-7: Generic standards - Immunity requirements for equipment intended to perform functions in a safety-related system (functional safety) in industrial locations	EN 61000-6-7	-
IEC 61010-2-201	2013	Safety requirements for electrical equipment for measurement, control and laboratory use -	EN 61010-2-201	2013
-	-	Part 2-201: Particular requirements for control equipment	+ AC	2013
IEC 61158	series	Industrial communication networks - Fieldbus specifications	EN 61158	series
IEC 61326-3-1	-	Electrical equipment for measurement, control and laboratory use - EMC requirements - Part 3-1: Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions (functional safety) - General industrial applications	EN 61326-3-1	-
IEC 61326-3-2	-	Electrical equipment for measurement, control and laboratory use - EMC requirements - Part 3-2: Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions (functional safety) - Industrial applications with specified electromagnetic environment	EN 61326-3-2	-
IEC 61508	series	Functional safety of electrical/electronic/programmable electronic safety-related systems	EN 61508	series

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
IEC 61508-1	2010	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1: General requirements	EN 61508-1	2010
IEC 61508-2	-	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems	EN 61508-2	-
IEC 61784-1	-	Industrial communication networks - Profiles - Part 1: Fieldbus profiles	EN 61784-1	-
IEC 61784-2	-	Industrial communication networks - Profiles - Part 2: Additional fieldbus profiles for real-time networks based on ISO/IEC 8802-3	EN 61784-2	-
IEC 61784-3-1	-	Industrial communication networks - Profiles - Part 3-1: Functional safety fieldbuses - Additional specifications for CPF 1	EN 61784-3-1	-
IEC 61784-3-2	-	Industrial communication networks - Profiles - Part 3-2: Functional safety fieldbuses - Additional specifications for CPF 2	EN 61784-3-2	-
IEC 61784-3-3	-	Industrial communication networks - Profiles - Part 3-3: Functional safety fieldbuses - Additional specifications for CPF 3	EN 61784-3-3	-
IEC 61784-3-6	-	Industrial communication networks - Profiles - Part 3-6: Functional safety fieldbuses - Additional specifications for CPF 6	EN 61784-3-6	-
IEC 61784-3-8	-	Industrial communication networks - Profiles - Part 3-8: Functional safety fieldbuses - Additional specifications for CPF 8	EN 61784-3-8	-
IEC 61784-3-12	-	Industrial communication networks - Profiles - Part 3-12: Functional safety fieldbuses - Additional specifications for CPF 12	EN 61784-3-12	-
IEC 61784-3-13	-	Industrial communication networks - Profiles - Part 3-13: Functional safety fieldbuses - Additional specifications for CPF 13	EN 61784-3-13	-
IEC 61784-3-14	-	Industrial communication networks - Profiles - Part 3-14: Functional safety fieldbuses - Additional specifications for CPF 14	EN 61784-3-14	-

EN 61784-3:2016

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
IEC 61784-3-17	- ¹⁾	Industrial communication networks - Profiles - Part 3-17: Functional safety fieldbuses - Additional specifications for CPF 17	-	-
IEC 61784-3-18	-	Industrial communication networks - Profiles - Part 3-18: Functionnal safety fieldbuses - Additional specifications for CPF 18	EN 61784-3-18	-
IEC 61784-5	series	Industrial communication networks - Profiles - Part 5: Installation of fieldbuses	EN 61784-5	series
IEC 61918 (mod)	2013	Industrial communication networks - Installation of communication networks in industrial premises	EN 61918	2013
-	-		+ AC	2014
IEC 62443	series	Industrial communication networks - Network and system security	EN 62443	series

1) To be published.

INTERNATIONAL STANDARD

NORME INTERNATIONALE



AMENDMENT 1
AMENDEMENT 1

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

**Réseaux de communication industriels – Profils –
Partie 3: Bus de terrain de sécurité fonctionnelle – Règles générales et
définitions de profils**

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 25.040.40; 35.100.05

ISBN 978-2-8322-4585-9

**Warning! Make sure that you obtained this publication from an authorized distributor.
Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.**

FOREWORD

This amendment has been prepared by subcommittee 65C: Industrial networks, of IEC technical committee 65: Industrial-process measurement, control and automation.

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

FDIS	Report on voting
65C/879/FDIS	65C/886/RVD

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

The committee has decided that the contents of this amendment and the base publication will remain unchanged until the stability date indicated on the IEC website 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.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

This Amendment 1 discusses the concepts of implicit data safety mechanisms for use in functional safety communications protocols (FSCPs) as specified in IEC 61784-3:2016.

3 Terms, definitions, symbols, abbreviated terms and conventions

3.1 Terms and definitions

Add the following new terms and definitions 3.1.56 and 3.1.57:

3.1.56

explicit data

data that is transmitted

3.1.57

implicit data

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

[SOURCE: IEC 62280:2014, 3.1.25]

3.2 Symbols and abbreviated terms

Add two new Subclauses 3.2.1 and 3.2.2, as specified below.

3.2.1 Abbreviated terms

Move the existing list of symbols and abbreviated terms to this new Subclause 3.2.1.

Delete “Pe” and “RP” from the existing list of abbreviated terms. Add, in alphabetical order, in the list of abbreviated terms the following new abbreviated terms:

A-code Authenticity code

T-code Timeliness code

3.2.2 Symbols

Add, in this new Subclause 3.2.2 the following list of symbols:

A_k	Weight distribution of the code: number of valid codewords having k bits set to “one”
e	Bit length of explicit data
err_{impl}	Bitwise disjunction of $impl_S$ and $impl_R$
$expl$	Explicit data
$expl_R$	Explicit data in the receiver
$expl_S$	Explicit data in the sender
FCS_C	Frame check sequence calculated in the receiver
FCS_R	Frame check sequence received
FCS_S	Frame check sequence sent
i	Bit length of implicit data
ID	Incorrect delivery
$impl_R$	Implicit data in the receiver
$impl_S$	Implicit data in the sender

n	Bit length of SPDU
P_e	Bit error probability
P_{ID}	Probability of incorrect delivery
r	Bit length of FCS (degree of generator polynomial)
RP	Residual error probability

Add, after Annex F, the following new informative Annex G:

Annex G (informative)

Implicit data safety mechanisms for IEC 61784-3 functional safety communication profiles (FSCPs)

G.1 Overview

Annex G discusses the concepts of implicit data safety mechanisms for use in functional safety communications protocols (FSCPs) as specified in this standard. Implicit data is that which is not explicitly transmitted in a PDU. Instead, the implicit data values are known by both the sender (source) and the receiver (sink). Implicit data values are validated by the value of one or more transmitted frame check sequence(s) (FCS) which are calculated using an overall data string comprised of the implicit data string appended with the explicit data string. Because the implicit data is not transmitted, the load on the transmission media is reduced.

Today, the FSCPs that use implicit data mechanisms do so in order to communicate complete or partial timeliness codes (T-codes) and/or authenticity codes (A-codes), see Annex E. These FSCPs also use cyclic redundancy check (CRC) algorithms for the frame check sequence (FCS) exclusively. Therefore, Annex G is limited to the analysis of implicitly transmitted T-codes and A-codes using CRC-algorithms.

According to Clause E.8, with regard to implicit data, "Due to the various possible approaches generic formulae cannot be provided. It is up to the individual FSCP to prove sufficient residual error probabilities." In the hope of advancing IEC 61784-3 for the next edition and beyond, the subject of this new Annex G is to improve the understanding of formulating models for the residual error probabilities of FSCPs using CRC-algorithms to implicitly transmit T-codes and A-codes when a single FCS code is used by the protocol.

Presented in Annex G are two formulae examples, applicable for two special cases, and from which a better understanding is promoted for the development of additional (specific and general) formulae.

Also presented is a summation method generally applicable when conditional weight distributions for implicit data error patterns are known and can be quantified in a way either leading to a closed-form solution, or suitable for iterative summation with a reasonably bounded execution time.

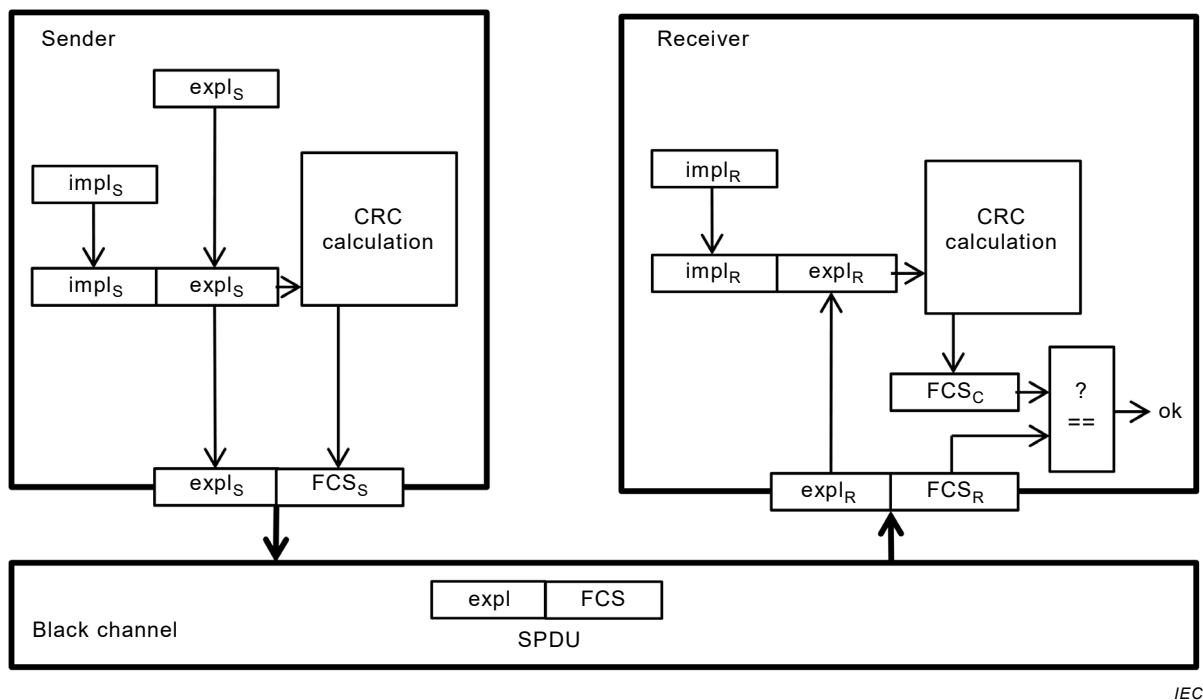
G.2 Basic principles

Calculations in Annex G also use the binary symmetric channel (BSC) model as specified in Annex B.

NOTE 1 Although it does not take into account burst errors, the BSC model with a sufficiently conservative bit error probability is so far the most practical known for use in probability calculations needed for the determination of the FSCP residual error rate.

Figure G.1 shows the basic principle of an FSCP using single FCS protection mechanisms involving implicit data. In the sender, a CRC-checksum over the implicit data $impl_S$ concatenated with the explicit data $expl_S$ is generated, resulting in a frame check sequence FCS_S . When multiple FCS codes are used in an FSCP format, the calculation shall be done for each FCS code. While $expl_S$ and FCS_S are explicitly transmitted over the black channel, $impl_S$ is not transmitted, but impacts the value of the FCS_S . Therefore, it can only contain data whose value is already known to the receiver. Implicit data is used to detect e.g. SPDUs which were misdirected in either space ("authentication error") or time ("timeliness error"). This is accomplished by deriving the implicit data from the A-code (e.g. connection identifier) and/or the T-code (e.g. sequence number) of an SPDU.

NOTE 2 Initialization details are addressed in F.12.1.



Key Symbols are specified in 3.2.2

Figure G.1 – FSCP with implicit transmission of authenticity and/or timeliness codes

When the SPDU comprising $expl$ and FCS is delivered to the FSCP-layer in the receiver, it may contain transmission errors, i.e. the value delivered may differ from the value sent. For discrimination, the symbols $expl_R$ and FCS_R are used in the receiver.

The expected value of the implicit data is called $impl_R$. In the error free case, this expectation is identical to $impl_S$. In case of, for example, a misdirected SPDU, $impl_R$ and $impl_S$ may differ.

The receiver generates one or more frame check sequence(s) FCS_C by building a CRC-checksum over the concatenation of $impl_R$ and $expl_R$. When each FCS_C is identical to its corresponding FCS_R , it is assumed that no error occurred. Otherwise an error has been detected.

The lengths of the bitstrings for a single FCS are defined as follows:

- r length of FCS (degree of generator-polynomial);
- i length of implicit data (it is assumed that $i \geq r$);
- e length of explicit data;
- n length of SPDU, with $n = e + r$.

G.3 Problem statement: constant values for implicit data

In FSCPs using implicit data, the CRC-check in the receiver is used for both the detection of data integrity errors as well as the detection of mis-directed or mis-timed SPDUs. Therefore, it may happen that the CRC-mechanism becomes “overburdened” by multiple simultaneous errors, resulting in an increase of the overall residual error probability. This is exemplified in the following scenario in Figure G.2.

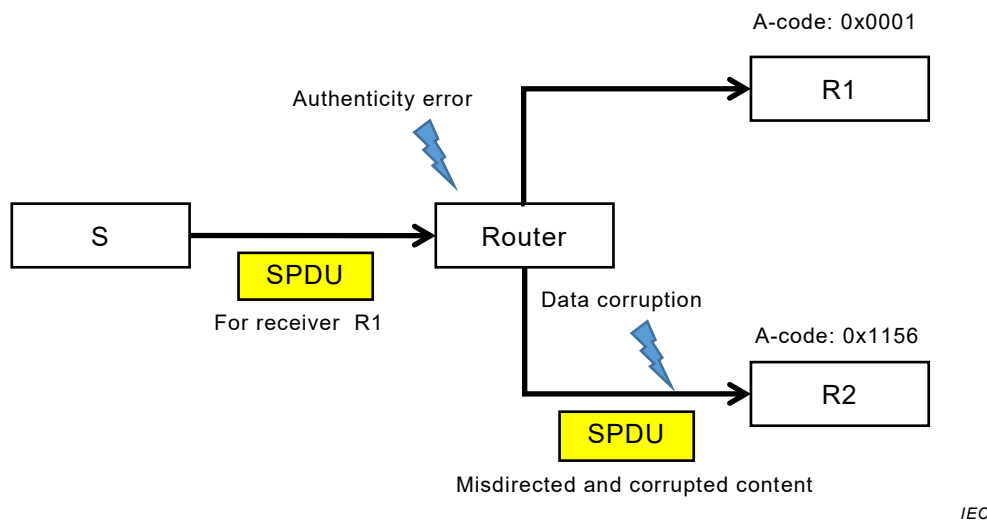


Figure G.2 – Example of an incorrect transmission with multiple error causes

The scenario assumes a sender S sending SPDUs to receiver R1 and receiver R2, using a black channel containing a router. The implicit data used comprises a single field containing an authenticity-code (A-code) of length 16 bits, identifying the receiver (see Figure E.4). For each SPDU sent from S to R1, the A-code of R1 is used as implicit data, and similarly the A-code of R2 for SPDUs sent from S to R2. It is further assumed that the following errors can occur during the transmission of an SPDU.

- Authenticity error: Due to a fault within the router, the SPDU is delivered to the incorrect receiver (receiver R2 instead of receiver R1 or vice versa). Thus, the implicit authenticity code impl_S used to calculate the FCS_S in the sender is unequal to the expected authenticity code impl_R in the receiver.
- Data corruption: Due to for example interference or noise on the transmission media, the content of the SPDU is corrupted (expl and/or FCS).

It is further assumed that the black channel itself does not detect any of these errors. Therefore, the errors, and possibly a combination of errors shall be detected by the check within the safety layer of the receiver. The error pattern err_{impl} caused by the authenticity error is defined by the bit-wise exclusive disjunction (XOR) of the A-codes in use. In this case with only two receivers, this error pattern is constant. The error pattern err_{expl} is defined as the bit-wise exclusive disjunction (XOR) of expl_S and expl_R . It is modelled by a BSC (see Annex B).

Figure G.3 shows the residual error probabilities for different parameters when using the proper generator polynomial $x^{16}+x^{14}+x^{11}+x^{10}+x^9+x^7+x^5+x^3+x+1$ (0x14EAB) of degree 16.

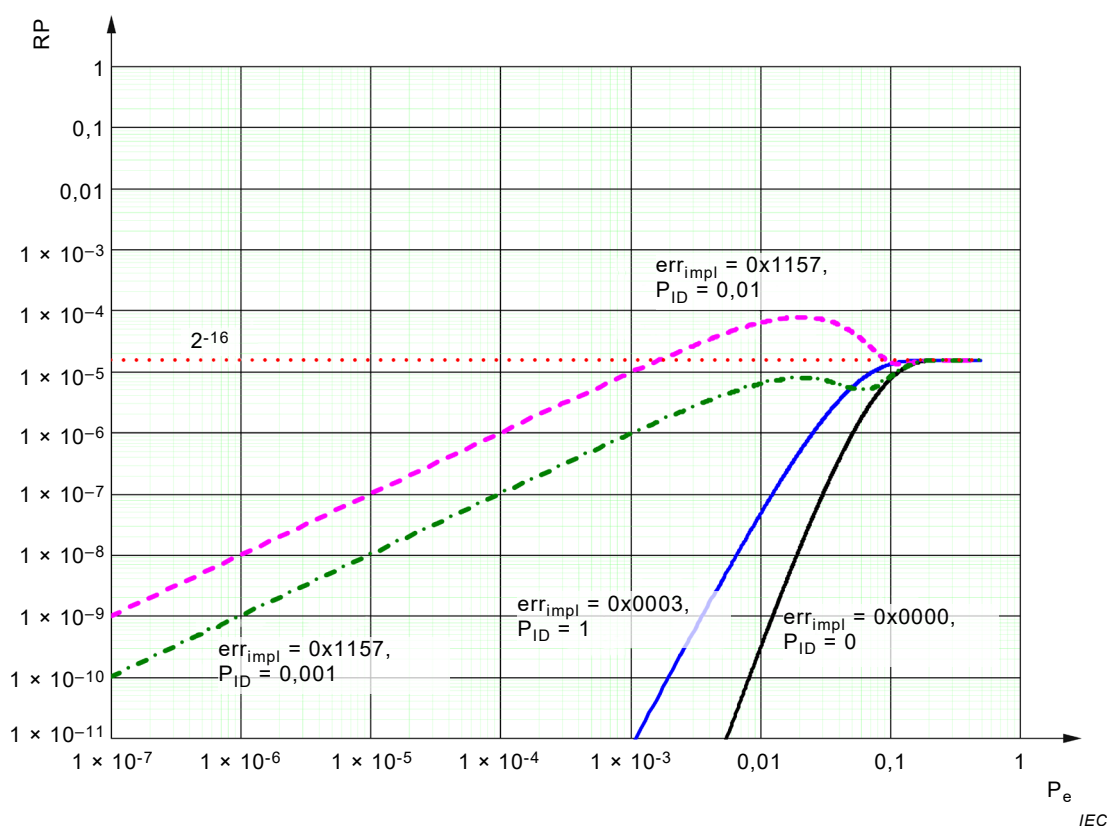


Figure G.3 – Impact of errors in implicit data on the residual error probability

Figure G.3 is based on data which was generated by a brute force algorithm checking all possible error patterns. In addition to the generator polynomial, the following input data was used in the algorithm:

P_{ID} probability of incorrect delivery (here: addressing error);

err_{impl} constant error pattern caused by an addressing error (bitwise disjunction of the A-codes).

It is important to note that the residual error probability does not only depend on p and P_{ID} , but also on the constant err_{impl} and hence on the values of the A-codes chosen during commissioning.

The curve for $P_{ID} = 0$ (solid black) proves the properness of the generator polynomial. In this case of no errors in implicit data, the residual error probability is always below the limit 2^{-16} and the curve is monotonically increasing.

The dashed purple curve and the dotted-dashed green curve show the characteristics when using A-codes resulting in an err_{impl} of 0x1157 (for example the A-codes 0x0001 and 0x1156). The residual error probability is no longer monotonically increasing but has a maximum greater than 2^{-16} . For $P_{ID} = 10^{-3}$, the corresponding curve (dotted-dashed green) does not pass the limit of 2^{-16} . However, if P_{ID} is set to 10^{-2} (dashed purple), the maximum is greater (worse) than the limit 2^{-16} . As a consequence the limit 2^{-r} cannot be used as an approximation even if the generator polynomial has proven properness for the case $P_{ID} = 0$.

The green and purple curve is only observed for certain rare values of err_{impl} . For most other values of err_{impl} , the curves are below the limit even for a probability of occurrence $P_{ID} = 1$. As an example, the curve for $err_{impl} = 0x0003$ (e.g. A-codes equal to 0x0001 and 0x0002) shows this characteristics (solid blue).

Conclusion: When using implicit transmission mechanisms, the residual error probability is not necessarily bounded by 2^{-r} . This bound is only valid if the FSCP provides additional mechanisms such as the ones shown in the following clauses.

NOTE Improper bounding of an FCS would not necessarily lead to insufficient residual error when other FSCP specific protocol measures are combined in the error detection scheme.

G.4 RP for FSCPs with random, uniformly distributed err_{impl}

G.4.1 General

Clause G.4 investigates the case of a random err_{impl} taking each possible value with equal probability ("uniform distribution"). As seen in Clause G.3 where err_{impl} is constant, this assumption is not always justified and shall be provably guaranteed by the design of the respective FSCP.

As already defined earlier, err_{impl} is the bitwise exclusive disjunction (XOR) between the implicit data impl_S used in the sender of the erroneous packet, and the expected value for the implicit data impl_R in the receiver. Clearly, if impl_S and impl_R are uniformly distributed, independent random variables, also err_{impl} is uniformly distributed, i.e. takes each possible value with equal possibility. However, because errors can be assumed to happen at 'random' points of time, it is also possible to achieve a uniformly distributed err_{impl} if impl_S and impl_R are non-random variables. In order to validate whether err_{impl} follows a uniform distribution, statistical checks such as the Chi-Square-Test or the Kolmogoroff-Smirnoff-Test can be used, (see for example [35]).

NOTE 1 err_{impl} being a uniformly distributed random variable, it does not require that all possible values are observed with equal frequency during a finite interval of time. It is therefore not always possible to evaluate a random number generator by simply counting the number of occurrences within a limited time interval.

Depending on the design of the FSCP, there are two reasonable variants of the assumption " err_{impl} is uniformly distributed":

- a) err_{impl} takes each value out of $[0; 2^i - 1]$ with probability 2^{-i} ;
- b) err_{impl} takes each value out of $[1; 2^i - 1]$ with probability $1/(2^i - 1)$.

NOTE 2 There is a slight difference in the two variants: in the second variant, a value of $\text{err}_{\text{impl}} = 0$ means that the SPDU was delivered correctly, as an incorrectly delivered SPDU will always result in a value $\text{err}_{\text{impl}} \neq 0$. In the first variant, a value of $\text{err}_{\text{impl}} = 0$ does not necessarily imply a correct delivery.

In the second case, measures shall be implemented to ensure that each SPDU is assigned a unique value for implicit data. Hence, the error pattern in case of a misdirected SPDU can never become zero. In the first case, no such measures are implemented and hence the error pattern 'zero' may occur. Clearly, such an error cannot be detected in the receiver unless there are additional detectable data integrity errors or other FSCP specific checks.

In the following, the two variants are shown separately.

Other and perhaps more detailed models are beyond the scope of this document. For example, it is possible to eliminate data error patterns with demonstrated certainty of detection by the CRC polynomial.

EXAMPLE Examples of these data error patterns include: Hamming distances less than the minimum Hamming distance for the CRC polynomial over the data block length; burst errors of length r ; odd number of bit errors; and others.

Subclause G.4.2 shows an example where the implicit data field is at least as long as the FCS and the implicit data values are randomly generated in such a way that A-codes are not guaranteed unique for each endpoint, T-codes are not guaranteed unique for each SPDU time, and the combinations of A-code and T-code are not guaranteed unique.

Subclause G.4.3 shows an example where the implicit data field is exactly as long as the FCS and A-codes and T-codes are guaranteed unique for each endpoint and SPDU time. In actual application, additional terms may be necessary to account for exceptions such as T-code wrap around.

Clause G.5 shows a summation method for general applicability when conditional weight distributions for implicit data error patterns are known and can be quantified.

G.4.2 Uniform distribution within the interval $[0;2^i-1]$, $i \geq r$

This case applies in particular to FSCPs that use random number generators to derive implicit data values.

At a coarse-grained level, two main types of errors can be discriminated:

- Incorrect content of an SPDU, i. e. data integrity errors;
- Incorrect delivery of an SPDU, i.e. the SPDU is delivered to the wrong receiver or at the wrong instance of time.

In combination, the following disjoint cases can be discriminated:

- Case 1. CC: No error (correct delivery, and correct explicit data);
- Case 2. IC: Incorrect delivery, and correct explicit data;
- Case 3. CI: Correct delivery, and incorrect explicit data;
- Case 4. II: Incorrect delivery, and incorrect data.

The residual error probabilities RP_2 , RP_3 , and RP_4 for each of the cases 2, 3, and 4 are calculated from the following parameters:

P_{ID} is the “probability of incorrect delivery”, i.e. the probability that due to for example an authenticity or timeliness error an SPDU is erroneously delivered to the FSCP;

NOTE 1 The event “incorrect delivery” can result in an $err_{impl} \neq 0$. However, due to the uniform distribution within $[0;2^r-1]$ the case $err_{impl} = 0$ can also occur.

P_{IED} is the probability of incorrect explicit data, i.e. the probability that data corruption occurs;

P_{IC} is the probability that an error is not detected in the receiver under the condition that case 2 occurs;

P_{CI} is the probability that an error is not detected in the receiver under the condition that case 3 occurs;

P_{II} is the probability that an error is not detected in the receiver under the condition that case 4 occurs;

RP_I is the residual error probability for data corruption as defined in Annex F.

R_{CRC} is the residual error probability for CRC polynomials as defined in Equation B.3.

NOTE 2 $RP_I \leq R_{CRC}$ because other safety measures than CRC can further reduce the value of RP_I .

r is the length of the FCS, identical to the degree of the CRC polynomial;

i is the length of the implicit data, with $i \geq r$;

n is the number of bits of the SPDU.

Because the events IC, CI, and II are disjoint, the overall residual error probability can be obtained by building the sum of the respective RP_x values.

In general, RP_x is calculated by:

$RP_x = P(\text{“error case x takes place”}) \times P(\text{“error case x is not detectable”}).$

This leads to the formulae for cases 2, 3 and 4 detailed in the following paragraphs.

Case 2 (IC)

$$\begin{aligned} RP_2 &= P_{ID} \times (1 - P_{IED}) \times P_{IC} \\ &= P_{ID} \times (1 - P_{IED}) \times 2^{-r} \end{aligned}$$

Explanations on P_{IC} :

- If $i > r$, this probability is 2^{-r} , because
 - by assumption, the bitwise disjunction of $impl_S$ and $impl_R$ is uniformly distributed in the interval $[0; 2^i - 1]$;
 - therefore, the bitwise disjunction of $FCS_S = FCS_R$ and FCS_C is uniformly distributed in the interval $[0; 2^r - 1]$;
 - therefore, the probability that the bitwise disjunction of FCS_R and FCS_C equals zero is 2^{-r} ;
 - therefore, the probability that FCS_R is equal to FCS_C is 2^{-r} .
- If $i = r$, this probability is 2^{-r} , because
 - FCS_R is equal to FCS_C , if and only if $err_{impl} = 0$, because the length of err_{impl} does not exceed the degree of the CRC polynomial. CRC-codes detect all burst errors of length less than or equal to r ;
 - the probability that $err_{impl} = 0$ is 2^{-r} because of the uniform distribution in the interval $[0; 2^r - 1]$.

Case 3 (CI)

$$\begin{aligned} RP_3 &= (1 - P_{ID}) \times P_{IED} \times P_{CI} \\ &= (1 - P_{ID}) \times RP_I \\ &\leq (1 - P_{ID}) \times 2^{-r} \text{ for proper polynomials.} \end{aligned}$$

Case 4 (II)

$$\begin{aligned} RP_4 &= P_{ID} \times P_{IED} \times P_{II} \\ &= P_{ID} \times P_{IED} \times 2^{-r} \end{aligned}$$

Explanations:

- Due to the assumptions, err_{impl} takes all values from $[0; 2^i - 1]$ with equal probability.
- Hence, each bit of err_{impl} takes the value 0 or 1 with equal probability 0,5.
- Because CRC-codes are linear codes, and because $|err_{impl}| \geq r$, each bit of err_{impl} determines the result of one bit in the bitwise exclusive disjunction of FCS_R and FCS_C .
- Hence, the bits in the bitwise exclusive disjunction of FCS_R and FCS_C can be treated as independent random variables, each taking the values 0 and 1 with equal probability 0,5.
- The bitwise exclusive disjunction of FCS_R and FCS_C is a uniformly distributed random variable, taking all values from $[0; 2^r - 1]$ with equal probability.
- The probability that the bitwise exclusive disjunction of FCS_R and FCS_C equals zero is 2^{-r} .
- The probability that FCS_C is identical to FCS_R is 2^{-r} .

In summary, the residual error probability of an FSCP using implicit mechanisms for the detection of timeliness and authenticity error (guaranteeing that the error in the implicit data is uniformly distributed in the interval $[0; 2^i - 1]$) can be calculated using the following formula:

$$\begin{aligned}
 RP_{TOTAL} &= RP_2 + RP_3 + RP_4 \\
 &= (P_{ID} \times (1 - P_{IED}) \times 2^{-r}) + ((1-P_{ID}) \times P_{IED} \times P_{CI}) + (P_{ID} \times P_{IED} \times 2^{-r}) \\
 &= (P_{ID} \times 2^{-r}) + ((1-P_{ID}) \times P_{IED} \times P_{CI}) \\
 &= (P_{ID} \times 2^{-r}) + ((1-P_{ID}) \times RP_I)
 \end{aligned}$$

Explanation:

- Cases 2 to 4 are disjoint events.

In case of a proper polynomial, the following applies:

$$\begin{aligned}
 RP_{TOTAL} &= RP_2 + RP_3 + RP_4 \\
 &= (P_{ID} \times (1 - P_{IED}) \times 2^{-r}) + ((1-P_{ID}) \times P_{IED} \times P_{CI}) + (P_{ID} \times P_{IED} \times 2^{-r}) \\
 &\leq (P_{ID} \times (1 - P_{IED}) \times 2^{-r}) + ((1-P_{ID}) \times 2^{-r}) + (P_{ID} \times P_{IED} \times 2^{-r}) \\
 &\leq 2^{-r}
 \end{aligned}$$

Explanations:

- Cases 2 to 4 are disjoint events.
- This upper bound of RP_{TOTAL} is independent of the values of P_{IED} and P_{ID} .

G.4.3 Uniform distribution in the interval $[1;2^r-1]$, $i = r$

For this variant, it is assumed $i = r$, i.e. the length of the implicit data is exactly the degree of the CRC polynomial, and that err_{impl} is uniformly distributed within the interval $[1;2^r-1]$. In contrast to the variant shown in G.4.2, err_{impl} is always unequal to 0 in case of an incorrect delivery.

The following cases of error combinations can be discriminated:

- Case 1. CC: No error (correct delivery, and correct explicit data);
- Case 2. IC: Incorrect delivery, and correct explicit data;
- Case 3. CI: Correct delivery, and incorrect explicit data;
- Case 4. II: Incorrect delivery, and incorrect data.

The residual error probabilities RP_2 , RP_3 , and RP_4 for each of the cases 2, 3, and 4 are calculated from the following parameters:

P_{ID} is the “probability of incorrect delivery”, i.e. the probability that due to for example an authenticity or timeliness error an SPDU is erroneously delivered to the FSCP;

NOTE Due to the uniform distribution within $[1;2^r-1]$, $err_{impl} \neq 0$ is guaranteed. Hence, the event “incorrect delivery” is equivalent to the event “incorrect implicit data” in this case.

P_{IED} is the probability of incorrect explicit data, i.e. the probability that data corruption occurs;

P_{IC} is the probability that an error is not detected in the receiver under the condition that case 2 occurs;

P_{CI} is the probability that an error is not detected in the receiver under the condition that case 3 occurs;

P_{II} is the probability that an error is not detected in the receiver under the condition that case 4 occurs;

$P_{EIC(i)}$ is the probability that the error pattern in the explicit data err_{expl} complements the error pattern in the implicit data err_{impl} making the error undetectable, under the condition that “ $err_{impl} = i$ ”;

r is the length of the implicit data and the length of the FCS (degree of the CRC polynomial);

n is the number of bits in the SPDU.

Because the events IC, CI, and II are disjoint, the overall residual error probability can be obtained by building the sum of the respective RP_x values.

In general, RP_x is calculated by:

$$RP_x = P(\text{"error case x takes place"}) \times P(\text{"error case x is not detectable"}).$$

This leads to the formulae for cases 2, 3 and 4 detailed in the following paragraphs.

Case 2 (IC)

$$\begin{aligned} RP_2 &= P_{ID} \times (1 - P_{IED}) \times P_{IC} \\ &= 0 \end{aligned}$$

Explanation:

- Errors of type 2 are always detected, because the length of err_{impl} does not exceed r . CRC-codes detect all burst errors of length less than or equal to r . Hence P_{IC} is equal to 0 in this case.

Case 3 (CI)

$$\begin{aligned} RP_3 &= (1 - P_{ID}) \times P_{IED} \times P_{CI} \\ &= (1 - P_{ID}) \times RP_I \\ &\leq (1 - P_{ID}) \times 2^{-r} \text{ for proper polynomials.} \end{aligned}$$

Case 4 (II)

$$\begin{aligned} RP_4 &= P_{ID} \times P_{IED} \times P_{II} \\ &\approx P_{ID} \times P_{IED} \times 2^{-r} \end{aligned}$$

Explanations:

$$\begin{aligned} \bullet \quad P_{II} &= \sum_{i=1}^{2^r-1} P\{err_{impl} = i\} \times P_{EIC}(i) \\ &= \sum_{i=1}^{2^r-1} \frac{1}{2^r-1} \times P_{EIC}(i) \\ &= \frac{1}{2^r-1} \times \sum_{i=1}^{2^r-1} P_{EIC}(i) \\ &= \frac{1}{2^r-1} \text{ (because for all possible } err_{expl} \text{ there is exactly one matching } err_{impl}) \\ &\approx 2^{-r} \end{aligned}$$

In summary, the residual error probability of an FSCP using implicit mechanisms for the detection of timeliness and authenticity error guaranteeing that the error in the implicit data is uniformly distributed in the interval $[1; 2^r-1]$, can be calculated using the following formula:

$$\begin{aligned} RP_{TOTAL} &= RP_2 + RP_3 + RP_4 \\ &= (P_{ID} \times (1 - P_{IED}) \times 2^{-r}) + ((1 - P_{ID}) \times P_{IED} \times P_{CI}) + (P_{ID} \times P_{IED} \times 2^{-r}) \\ &= (P_{ID} \times 2^{-r}) + ((1 - P_{ID}) \times P_{IED} \times P_{CI}) \end{aligned}$$

$$= (P_{ID} \times 2^{-r}) + ((1-P_{ID}) \times RP_I)$$

Explanation:

- Cases 2 to 4 are disjoint events.

G.5 General case

The calculations presented in G.4.2 and G.4.3 are only valid under the assumption of a uniform distribution of err_{impl} and with certain restrictions on the length of the implicit data field. In the general case, RP_{TOTAL} can be calculated as follows, if the conditional weight distribution of the code is known for each possible value of err_{impl} .

$$RP_{TOTAL} = P_{ID} \times \sum_{j=0}^{2^i-1} R\{err_{impl} = j\} \times R\{FCS_C = FCS_R \mid err_{impl} = j\} + (1 - P_{ID}) \times P_{re}^{CRC, BSC}$$

where

$R\{err_{impl} = j\}$ is the probability that the error pattern in implicit data has the value j (under the condition that there is a misdirected SPDU);

$R\{FCS_C = FCS_R \mid err_{impl} = j\}$ is the probability that no error is indicated for the given CRC-polynomial and code length, under the condition that the error pattern in implicit data has the value j ;

$P_{re}^{CRC, BSC}$ is the residual error probability for the given CRC-polynomial and code length without implicit data.

$P_{re}^{CRC, BSC}$ and $R\{FCS_C = FCS_R \mid err_{impl} = j\}$ are given by:

$$P_{re}^{CRC, BSC} = \sum_{k=1}^n A_k(err_{impl} = 0) \times P_e^k \times (1 - P_e)^{n-k}$$

$$R\{FCS_C = FCS_R \mid err_{impl} = j\} = \sum_{k=0}^n A_k(err_{impl} = j) \times P_e^k \times (1 - P_e)^{n-k}$$

where

$A_k(err_{impl} = j)$ is the weight distribution of the code under the condition that the error pattern in the implicit data takes the value j .

Explanations:

- $R\{FCS_C = FCS_R \mid err_{impl} = 0\} = P_{re}^{CRC, BSC} + (1 - P_e)^n$.

G.6 Calculation of P_{ID}

If both the T-code and the A- code are implicit, P_{ID} can be calculated as follows:

$$P_{ID} = \min\left(\frac{R_T + R_A}{v}, 1\right)$$

where

P_{ID} is the probability that due to for example an authenticity or timeliness error an SPDU is erroneously delivered to the FSCP;

R_T is the rate of occurrence for incorrect sequence safety PDUs (see F.5.2.4);

R_A is the rate of occurrence for misdirected safety PDUs (see F.5.2.3);

v is the maximum number of SPDU samples by the SCL ("sample rate") per hour (see F.5.2.2).

Explanation:

- Due to approximation, $R_T + R_A$ may become greater than one. In this case, the value 1 shall be used for P_{ID} .

If only the T-code is implicit, P_{ID} can be calculated as follows:

$$P_{ID} = \frac{R_T}{v}$$

If only the A-code is implicit, P_{ID} can be calculated as follows:

$$P_{ID} = \frac{R_A}{v}$$

Calculation of the total residual error rate

According to F.10.1, the total residual error rate is calculated by (see Equation (F.6)):

$$\lambda_{SC} = RR_T + RR_A + RR_I + RR_M$$

Alternatively, the following formula can be used:

$$\lambda_{SC} = v \times RP_{TOTAL}$$

Bibliography

Add, at the end of Bibliography, the following new reference:

- [35] D. KNUTH, *The Art of Computer Programming, Volume 2: Seminumerical Algorithms*, 3rd Edition, Addison-Wesley, 1997

CONTENTS

FOREWORD.....	7
0 Introduction	9
0.1 General.....	9
0.2 Transition from Edition 2 to extended assessment methods in Edition 3.....	11
0.3 Patent declaration	12
1 Scope.....	13
2 Normative references.....	13
3 Terms, definitions, symbols, abbreviated terms and conventions.....	15
3.1 Terms and definitions	15
3.2 Symbols and abbreviated terms.....	22
4 Conformance.....	23
5 Basics of safety-related fieldbus systems	23
5.1 Safety function decomposition	23
5.2 Communication system	24
5.2.1 General	24
5.2.2 IEC 61158 fieldbuses	24
5.2.3 Communication channel types	25
5.2.4 Safety function response time	25
5.3 Communication errors	26
5.3.1 General	26
5.3.2 Corruption.....	26
5.3.3 Unintended repetition	26
5.3.4 Incorrect sequence	26
5.3.5 Loss	27
5.3.6 Unacceptable delay.....	27
5.3.7 Insertion	27
5.3.8 Masquerade.....	27
5.3.9 Addressing.....	27
5.4 Deterministic remedial measures	27
5.4.1 General	27
5.4.2 Sequence number	27
5.4.3 Time stamp.....	27
5.4.4 Time expectation.....	28
5.4.5 Connection authentication	28
5.4.6 Feedback message	28
5.4.7 Data integrity assurance.....	28
5.4.8 Redundancy with cross checking	28
5.4.9 Different data integrity assurance systems.....	29
5.5 Typical relationships between errors and safety measures	29
5.6 Communication phases	30
5.7 FSCP implementation aspects	31
5.8 Data integrity considerations	31
5.8.1 Calculation of the residual error rate.....	31
5.8.2 Total residual error rate and SIL	33
5.9 Relationship between functional safety and security.....	34
5.10 Boundary conditions and constraints.....	35

5.10.1	Electrical safety	35
5.10.2	Electromagnetic compatibility (EMC)	35
5.11	Installation guidelines	36
5.12	Safety manual	36
5.13	Safety policy	36
6	Communication Profile Family 1 (FOUNDATION™ Fieldbus) – Profiles for functional safety	37
7	Communication Profile Family 2 (CIP™) and Family 16 (SERCOS®) – Profiles for functional safety	37
8	Communication Profile Family 3 (PROFIBUS™, PROFINET™) – Profiles for functional safety	37
9	Communication Profile Family 6 (INTERBUS®) – Profiles for functional safety	38
10	Communication Profile Family 8 (CC-Link™) – Profiles for functional safety	38
10.1	Functional Safety Communication Profile 8/1	38
10.2	Functional Safety Communication Profile 8/2	39
11	Communication Profile Family 12 (EtherCAT™) – Profiles for functional safety	39
12	Communication Profile Family 13 (Ethernet POWERLINK™) – Profiles for functional safety	40
13	Communication Profile Family 14 (EPA®) – Profiles for functional safety	40
14	Communication Profile Family 17 (RAPIEnet™) – Profiles for functional safety	40
15	Communication Profile Family 18 (SafetyNET p™ Fieldbus) – Profiles for functional safety	41
Annex A	(informative) Example functional safety communication models	42
A.1	General	42
A.2	Model A (single message, channel and FAL, redundant SCLs)	42
A.3	Model B (full redundancy)	42
A.4	Model C (redundant messages, FALs and SCLs, single channel)	43
A.5	Model D (redundant messages and SCLs, single channel and FAL)	43
Annex B	(normative) Safety communication channel model using CRC-based error checking	45
B.1	Overview	45
B.2	Channel model for calculations	45
B.3	Bit error probability P_e	46
B.4	Cyclic redundancy checking	47
B.4.1	General	47
B.4.2	Considerations concerning CRC polynomials	48
Annex C	(informative) Structure of technology-specific parts	50
Annex D	(informative) Assessment guideline	52
D.1	Overview	52
D.2	Channel types	52
D.2.1	General	52
D.2.2	Black channel	52
D.2.3	White channel	52
D.3	Data integrity considerations for white channel approaches	53
D.3.1	General	53
D.3.2	Models B and C	53
D.3.3	Models A and D	54
D.4	Verification of safety measures	55

D.4.1	General	55
D.4.2	Implementation	55
D.4.3	"De-energize to trip" principle	55
D.4.4	Safe state	55
D.4.5	Transmission errors	55
D.4.6	Safety reaction and response times	55
D.4.7	Combination of measures	56
D.4.8	Absence of interference	56
D.4.9	Additional fault causes (white channel)	56
D.4.10	Reference test beds and operational conditions	56
D.4.11	Conformance tester	56
Annex E	(informative) Examples of implicit vs. explicit FSCP safety measures	57
E.1	General	57
E.2	Example fieldbus message with safety PDUs	57
E.3	Model with completely explicit safety measures	57
E.4	Model with explicit A-code and implicit T-code safety measures	58
E.5	Model with explicit T-code and implicit A-code safety measures	58
E.6	Model with split explicit and implicit safety measures	59
E.7	Model with completely implicit safety measures	60
E.8	Addition to Annex B – impact of implicit codes on properness	60
Annex F	(informative) Extended models for estimation of the total residual error rate	61
F.1	Applicability	61
F.2	General models for black channel communications	61
F.3	Identification of generic safety properties	62
F.4	Assumptions for residual error rate calculations	62
F.5	Residual error rates	63
F.5.1	Explicit and implicit mechanisms	63
F.5.2	Residual error rate calculations	63
F.6	Data integrity	65
F.6.1	Probabilistic considerations	65
F.6.2	Deterministic considerations	65
F.7	Authenticity	66
F.7.1	General	66
F.7.2	Residual error rate for authenticity (RR_A)	67
F.8	Timeliness	68
F.8.1	General	68
F.8.2	Residual error rate for timeliness (RR_T)	70
F.9	Masquerade	71
F.9.1	General	71
F.9.2	Other terms used to calculate residual error rate for masquerade rejection (RR_M)	71
F.10	Calculation of the total residual error rates	71
F.10.1	Based on the summation of the residual error rates	71
F.10.2	Based on other quantitative proofs	72
F.11	Total residual error rate and SIL	72
F.12	Configuration and parameterization for an FSCP	73
F.12.1	General	73
F.12.2	Configuration and parameterization change rate	75
F.12.3	Residual error rate for configuration and parameterization	75

Bibliography	76
Figure 1 – Relationships of IEC 61784-3 with other standards (machinery).....	9
Figure 2 – Relationships of IEC 61784-3 with other standards (process)	10
Figure 3 – Transition from Edition 2 to Edition 3 assessment methods	11
Figure 4 – Safety communication as a part of a safety function	24
Figure 5 – Example model of a functional safety communication system	25
Figure 6 – Example of safety function response time components	26
Figure 7 – Conceptual FSCP protocol model	31
Figure 8 – FSCP implementation aspects	31
Figure 9 – Example application 1 (m=4)	33
Figure 10 – Example application 2 (m = 2).....	33
Figure 11 – Zones and conduits concept for security according to IEC 62443.....	35
Figure A.1 – Model A	42
Figure A.2 – Model B	43
Figure A.3 – Model C	43
Figure A.4 – Model D	44
Figure B.1 – Communication channel with perturbation	45
Figure B.2 – Binary symmetric channel (BSC)	46
Figure B.3 – Example of a block with a message part and a CRC signature	47
Figure B.4 – Block codes for error detection	48
Figure B.5 – Proper and improper CRC polynomials	49
Figure D.1 – Basic Markov model.....	54
Figure E.1 – Example safety PDUs embedded in a fieldbus message.....	57
Figure E.2 – Model with completely explicit safety measures	57
Figure E.3 – Model with explicit A-code and implicit T-code safety measures	58
Figure E.4 – Model with explicit T-code and implicit A-code safety measures	59
Figure E.5 – Model with split explicit and implicit safety measures	59
Figure E.6 – Model with completely implicit safety measures	60
Figure F.1 – Black channel from an FSCP perspective.....	61
Figure F.2 – Model for authentication considerations	66
Figure F.3 – Fieldbus and internal address errors	67
Figure F.4 – Example of slowly increasing message latency	69
Figure F.5 – Example of an active network element failure.....	70
Figure F.6 – Example application 1 (m = 4)	72
Figure F.7 – Example application 2 (m = 2)	72
Figure F.8 – Example of configuration and parameterization procedures for FSCP	74
Table 1 – Overview of the effectiveness of the various measures on the possible errors.....	30
Table 2 – Definition of items used for calculation of the residual error rates	32
Table 3 – Typical relationship of residual error rate to SIL.....	34
Table 4 – Typical relationship of residual error on demand to SIL.....	34
Table 5 – Overview of profile identifier usable for FSCP 6/7	38

Table B.1 – Example dependency $d_{\min}$ and block bit length n	48
Table C.1 – Common subclause structure for technology-specific parts	50
Table F.1 – Typical relationship of residual error rate to SIL	73
Table F.2 – Typical relationship of residual error on demand to SIL.....	73

INTERNATIONAL ELECTROTECHNICAL COMMISSION

**INDUSTRIAL COMMUNICATION NETWORKS –
PROFILES –****Part 3: Functional safety fieldbuses –
General rules and profile definitions**

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 itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
- 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.

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

This third edition cancels and replaces the second edition published in 2010. This edition constitutes a technical revision.

This edition includes the following significant technical changes with respect to the previous edition:

- clarifications and additional explanations for requirements, updated references;
- deletion of technical overviews of profiles (Clauses 6 to 13), and associated dedicated subclauses for terms, definitions, symbols and abbreviations;
- addition of profiles for Communication Profile Families 8, 17 and 18 (Clauses 10, 14, 15);
- clarifications of models in Annex A;