

INTERNATIONAL STANDARD

NORME INTERNATIONALE

**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**



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2016 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'IEC ou du Comité national de l'IEC du pays du demandeur. Si vous avez des questions sur le copyright de l'IEC ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de l'IEC de votre pays de résidence.

IEC Central Office
3, rue de Varembe
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
info@iec.ch
www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

IEC Catalogue - webstore.iec.ch/catalogue

The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

IEC publications search - www.iec.ch/searchpub

The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee,...). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and also once a month by email.

Electropedia - www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing 20 000 terms and definitions in English and French with equivalent terms in 15 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary

65 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

IEC Customer Service Centre - webstore.iec.ch/csc

If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: csc@iec.ch.

A propos de l'IEC

La Commission Electrotechnique Internationale (IEC) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications IEC

Le contenu technique des publications IEC est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Catalogue IEC - webstore.iec.ch/catalogue

Application autonome pour consulter tous les renseignements bibliographiques sur les Normes internationales, Spécifications techniques, Rapports techniques et autres documents de l'IEC. Disponible pour PC, Mac OS, tablettes Android et iPad.

Recherche de publications IEC - www.iec.ch/searchpub

La recherche avancée permet de trouver des publications IEC en utilisant différents critères (numéro de référence, texte, comité d'études,...). Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

IEC Just Published - webstore.iec.ch/justpublished

Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et aussi une fois par mois par email.

Electropedia - www.electropedia.org

Le premier dictionnaire en ligne de termes électroniques et électriques. Il contient 20 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans 15 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

Glossaire IEC - std.iec.ch/glossary

65 000 entrées terminologiques électrotechniques, en anglais et en français, extraites des articles Termes et Définitions des publications IEC parues depuis 2002. Plus certaines entrées antérieures extraites des publications des CE 37, 77, 86 et CISPR de l'IEC.

Service Clients - webstore.iec.ch/csc

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: csc@iec.ch.

INTERNATIONAL STANDARD

NORME INTERNATIONALE



**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 978-2-8322-3238-5

**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.**

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

Withdrawn

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;

- Annex B changed from informative to normative;
- addition of a new informative Annex E describing models for explicit and implicit FSCP mechanisms;
- addition of a new informative Annex F introducing an extended model for estimation of the total residual error rate;
- updates in parts for CPF 1, CPF 2, CPF 3, CPF 8, CPF 13 (details provided in the parts);
- addition of a new part for CPF 17.

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

FDIS	Report on voting
65C/840/FDIS	65C/848/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.

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

The committee has decided that the contents of this 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.