

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 © 2021 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
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 corrigendum or an amendment might have been published.

IEC publications search - webstore.iec.ch/advsearchform

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 It also gives information on projects, replaced and withdrawn publications.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 once a month by email.

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: sales@iec.ch.

IEC online collection - oc.iec.ch

Discover our powerful search engine and read freely all the publications previews. With a subscription you will always have access to up to date content tailored to your needs.

Electropedia - www.electropedia.org

The world's leading online dictionary on electrotechnology, containing more than 22 000 terminological entries in English and French, with equivalent terms in 18 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

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.

Recherche de publications IEC -

webstore.iec.ch/advsearchform

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 une fois par mois par email.

Service Clients - webstore.iec.ch/csc

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

IEC online collection - oc.iec.ch

Découvrez notre puissant moteur de recherche et consultez gratuitement tous les aperçus des publications. Avec un abonnement, vous aurez toujours accès à un contenu à jour adapté à vos besoins.

Electropedia - www.electropedia.org

Le premier dictionnaire d'électrotechnologie en ligne au monde, avec plus de 22 000 articles terminologiques en anglais et en français, ainsi que les termes équivalents dans 16 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

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 978-2-8322-9268-6

**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 Use of extended assessment methods in Edition 4.....	11
0.3 Patent declaration.....	11
1 Scope.....	12
2 Normative references	12
3 Terms, definitions, symbols, abbreviated terms and conventions	14
3.1 Terms and definitions.....	14
3.2 Symbols and abbreviated terms	21
3.2.1 Abbreviated terms	21
3.2.2 Symbols	22
4 Conformance.....	22
5 Basics of safety-related fieldbus systems	23
5.1 Safety function decomposition	23
5.2 Communication system	23
5.2.1 General	23
5.2.2 IEC 61158 fieldbuses.....	24
5.2.3 Communication channel types	24
5.2.4 Safety function response time.....	25
5.3 Communication errors.....	25
5.3.1 General	25
5.3.2 Corruption	25
5.3.3 Unintended repetition	26
5.3.4 Incorrect sequence	26
5.3.5 Loss	26
5.3.6 Unacceptable delay	26
5.3.7 Insertion	26
5.3.8 Masquerade	26
5.3.9 Addressing	26
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	27
5.4.5 Connection authentication	27
5.4.6 Feedback message.....	27
5.4.7 Data integrity assurance	27
5.4.8 Redundancy with cross checking	28
5.4.9 Different data integrity assurance systems.....	28
5.5 Typical relationships between errors and safety measures.....	28
5.6 Communication phases	29
5.7 FSCP implementation aspects	30
5.8 Models for estimation of the total residual error rate	30
5.8.1 Applicability	30
5.8.2 General models for black channel communications.....	31

5.8.3	Identification of generic safety properties.....	31
5.8.4	Assumptions for residual error rate calculations.....	32
5.8.5	Residual error rates	33
5.8.6	Data integrity.....	35
5.8.7	Authenticity.....	36
5.8.8	Timeliness	38
5.8.9	Masquerade.....	41
5.8.10	Calculation of the total residual error rates	41
5.8.11	Total residual error rate and SIL	43
5.8.12	Configuration and parameterization for an FSCP	43
5.9	Relationship between functional safety and security	45
5.10	Boundary conditions and constraints.....	45
5.10.1	Electrical safety	45
5.10.2	Electromagnetic compatibility (EMC)	46
5.11	Installation guidelines	46
5.12	Safety manual.....	46
5.13	Safety policy	46
6	Communication Profile Family 1 (FOUNDATION™ Fieldbus) – Profiles for functional safety	47
7	Communication Profile Family 2 (CIP™) and Family 16 (SERCOS®) – Profiles for functional safety	47
8	Communication Profile Family 3 (PROFIBUS™, PROFINET™) – Profiles for functional safety	48
9	Communication Profile Family 6 (INTERBUS®) – Profiles for functional safety	48
10	Communication Profile Family 8 (CC-Link™) – Profiles for functional safety	49
10.1	Functional Safety Communication Profile 8/1	49
10.2	Functional Safety Communication Profile 8/2	49
11	Communication Profile Family 12 (EtherCAT™) – Profiles for functional safety.....	49
12	Communication Profile Family 13 (Ethernet POWERLINK™) – Profiles for functional safety	50
13	Communication Profile Family 14 (EPA®) – Profiles for functional safety.....	50
14	Communication Profile Family 17 (RAPIEnet™) – Profiles for functional safety.....	50
15	Communication Profile Family 18 (SafetyNET p™ Fieldbus) – Profiles for functional safety	51
Annex A (informative)	Example functional safety communication models	52
A.1	General.....	52
A.2	Model A (single message, channel and FAL, redundant SCLs).....	52
A.3	Model B (full redundancy)	52
A.4	Model C (redundant messages, FALs and SCLs, single channel).....	53
A.5	Model D (redundant messages and SCLs, single channel and FAL).....	53
Annex B (normative)	Safety communication channel model using CRC-based error checking	55
B.1	Overview.....	55
B.2	Channel model for calculations	55
B.3	Bit error probability P_e	56
B.4	Cyclic redundancy checking.....	57
B.4.1	General	57
B.4.2	Requirements for methods to calculate R_{CRC}	57
Annex C (informative)	Structure of technology-specific parts.....	59

Annex D (informative) Assessment guideline	62
D.1 Overview.....	62
D.2 Channel types.....	62
D.2.1 General	62
D.2.2 Black channel.....	62
D.2.3 White channel.....	62
D.3 Data integrity considerations for white channel approaches	63
D.3.1 General	63
D.3.2 Models B and C	63
D.3.3 Models A and D	64
D.4 Verification of safety measures	64
D.4.1 General	64
D.4.2 Implementation.....	65
D.4.3 Default safety action	65
D.4.4 Safe state	65
D.4.5 Transmission errors	65
D.4.6 Safety reaction and response times	65
D.4.7 Combination of measures	65
D.4.8 Absence of interference.....	66
D.4.9 Additional fault causes (white channel).....	66
D.4.10 Reference test beds and operational conditions.....	66
D.4.11 Conformance tester	66
Annex E (informative) Examples of implicit vs. explicit TSCP safety measures.....	67
E.1 General.....	67
E.2 Example fieldbus message with safety PDUs	67
E.3 Model with completely explicit safety measures	67
E.4 Model with explicit A-code and implicit T-code safety measures.....	68
E.5 Model with explicit T-code and implicit A-code safety measures.....	68
E.6 Model with split explicit and implicit safety measures	69
E.7 Model with completely implicit safety measures	70
E.8 Addition to Annex E – Impact of implicit codes on properness	70
Annex F (informative) Logarithmic models for estimation of the total residual error rate	71
F.1 General.....	71
F.2 Calculation of the residual error rate	71
F.3 Total residual error rate and SIL	73
Annex G (informative) Implicit data safety mechanisms for IEC 61784-3 functional safety communication profiles (FSCPs).....	74
G.1 Overview.....	74
G.2 Basic principles.....	74
G.3 Problem statement: constant values for implicit data	75
G.4 RP for FSCPs with random, uniformly distributed err_{impl}	78
G.4.1 General	78
G.4.2 Uniform distribution within the interval $[0;2^i-1]$, $i \geq r$	79
G.4.3 Uniform distribution in the interval $[1;2^r-1]$, $i = r$	81
G.5 General case	83
G.6 Calculation of P_{ID}	83
Annex H (informative) Residual error probability for example CRC codes (tables for verification of calculation methods)	85
H.1 Overview.....	85

H.2	Example of a 32-bit CRC.....	85
H.3	Example of a 16-bit CRC.....	90
H.4	Conclusion.....	94
	Bibliography.....	96
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	– Transitions from Ed. 2 to Ed. 4 and future Ed. 5 assessment methods.....	11
Figure 4	– Safety communication as a part of a safety function.....	23
Figure 5	– Example model of a functional safety communication system.....	24
Figure 6	– Example of safety function response time components.....	25
Figure 7	– Conceptual FSCP protocol model.....	30
Figure 8	– FSCP implementation aspects.....	30
Figure 9	– Black channel from an FSCP perspective.....	31
Figure 10	– Model for authentication considerations.....	36
Figure 11	– Fieldbus and internal address errors.....	37
Figure 12	– Example of slowly increasing message latency.....	39
Figure 13	– Example of an active network element failure.....	40
Figure 14	– Example application 1 (m = 4).....	42
Figure 15	– Example application 2 (m = 2).....	42
Figure 16	– Example of configuration and parameterization procedures for FSCP.....	44
Figure A.1	– Model A.....	52
Figure A.2	– Model B.....	53
Figure A.3	– Model C.....	53
Figure A.4	– Model D.....	54
Figure B.1	– Binary symmetric channel (BSC).....	55
Figure B.2	– Block codes for error detection.....	56
Figure B.3	– Example of a block with a message part and a CRC signature.....	57
Figure B.4	– Proper and improper CRC polynomials.....	58
Figure D.1	– Basic Man-ov model.....	64
Figure E.1	– Example safety PDUs embedded in a fieldbus message.....	67
Figure E.2	– Model with completely explicit safety measures.....	67
Figure E.3	– Model with explicit A-code and implicit T-code safety measures.....	68
Figure E.4	– Model with explicit T-code and implicit A-code safety measures.....	69
Figure E.5	– Model with split explicit and implicit safety measures.....	69
Figure E.6	– Model with completely implicit safety measures.....	70
Figure F.1	– Example application 1 (m = 4).....	72
Figure F.2	– Example application 2 (m = 2).....	73
Figure G.1	– FSCP with implicit transmission of authenticity and/or timeliness codes.....	75
Figure G.2	– Example of an incorrect transmission with multiple error causes.....	76
Figure G.3	– Impact of errors in implicit data on the residual error probability.....	77
Figure H.1	– Residual error probabilities (example of a 32-bit CRC – result 1).....	87
Figure H.2	– Residual error probabilities (example of a 32-bit CRC – result 2).....	87

Figure H.3 – Residual error probabilities (example of a 32-bit CRC – result 3)	88
Figure H.4 – Residual error probabilities (example of a 32-bit CRC – result 4)	88
Figure H.5 – Residual error probabilities (example of a 32-bit CRC – result 5)	89
Figure H.6 – Residual error probabilities (example of a 32-bit CRC – result 6)	89
Figure H.7 – Residual error probabilities (example of a 16-bit CRC – result 1)	92
Figure H.8 – Residual error probabilities (example of a 16-bit CRC – result 2)	92
Figure H.9 – Residual error probabilities (example of a 16-bit CRC – result 3)	93
Figure H.10 – Residual error probabilities (example of a 16-bit CRC – result 4)	93
Figure H.11 – Residual error probabilities (example of a 16-bit CRC – result 5)	94
Figure H.12 – Example 1 of improper polynomial	94
Figure H.13 – Example 2 of improper polynomial	95
Table 1 – Overview of the effectiveness of the various measures on the possible errors	29
Table 2 – Typical relationship of residual error rate to SIL	43
Table 3 – Typical relationship of residual error on demand to SIL	43
Table 4 – Overview of profile identifier usable for FSCP 6/7	48
Table B.1 – Example dependency d_{min} and block bit length n	56
Table C.1 – Common subclause structure for technology-specific parts	59
Table F.1 – Definition of items used for calculation of the residual error rates	72
Table F.2 – Typical relationship of residual error rate to SIL	73
Table F.3 – Typical relationship of residual error on demand to SIL	73
Table H.1 – Residual error probabilities (R_{CRC1}) for example CRC32 polynomial	86
Table H.2 – Residual error probabilities ($R_{C1}, C2$) for example CRC16 polynomial	91

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, issue 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.
- 9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

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 fourth edition cancels and replaces the third edition, published in 2016 and its Amendment 1, published in 2017. This edition constitutes a technical revision.

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

- Contents of previous Annex F were corrected based on feedback from peer review and subsequent analysis (in particular deletion of RP_U for data integrity, reduction of the Equation for RR_A , and clarifications on the values of RP_I and R_T).
- Additional assumptions for residual error rate calculations, clarification of assumption a).

- After correction, contents of previous Annex F were exchanged with the contents of previous Subclause 5.8.
- Contents of Subclause 5.9 on security replaced by a simple reference to IEC 62443 in accordance with Guide 120.
- Changes in Annex B: Dependency of this Annex B with the BSC model has been highlighted. First two paragraphs and figure in Clause B.2 have been deleted because of little relevance. The approximation Equation (B.4) has been deleted due to obsolescence, based on the observations that the CRC shall be anyway explicitly calculated in order to prove properness, and that it may produce optimistic results. Guidance for calculation of R_{CRC} in B.4.2 has been reviewed.
- Changes in Annex D: Formula D.1 was changed from an approximation to a proper Equation, with some adjustments, and contents of D.4.3 were clarified (default safety action).
- New informative Annex H, providing additional guidance for the calculation of $R_{C,C}$.

The text of this International Standard is based on the following documents:

FDIS	Report on voting
65C/1067/FDIS	65C/1072/RVD

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

This document 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 document will remain unchanged until the stability date indicated on the IEC website under "<http://webstore.iec.ch>" in the data related to the specific document. At this date the document 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.

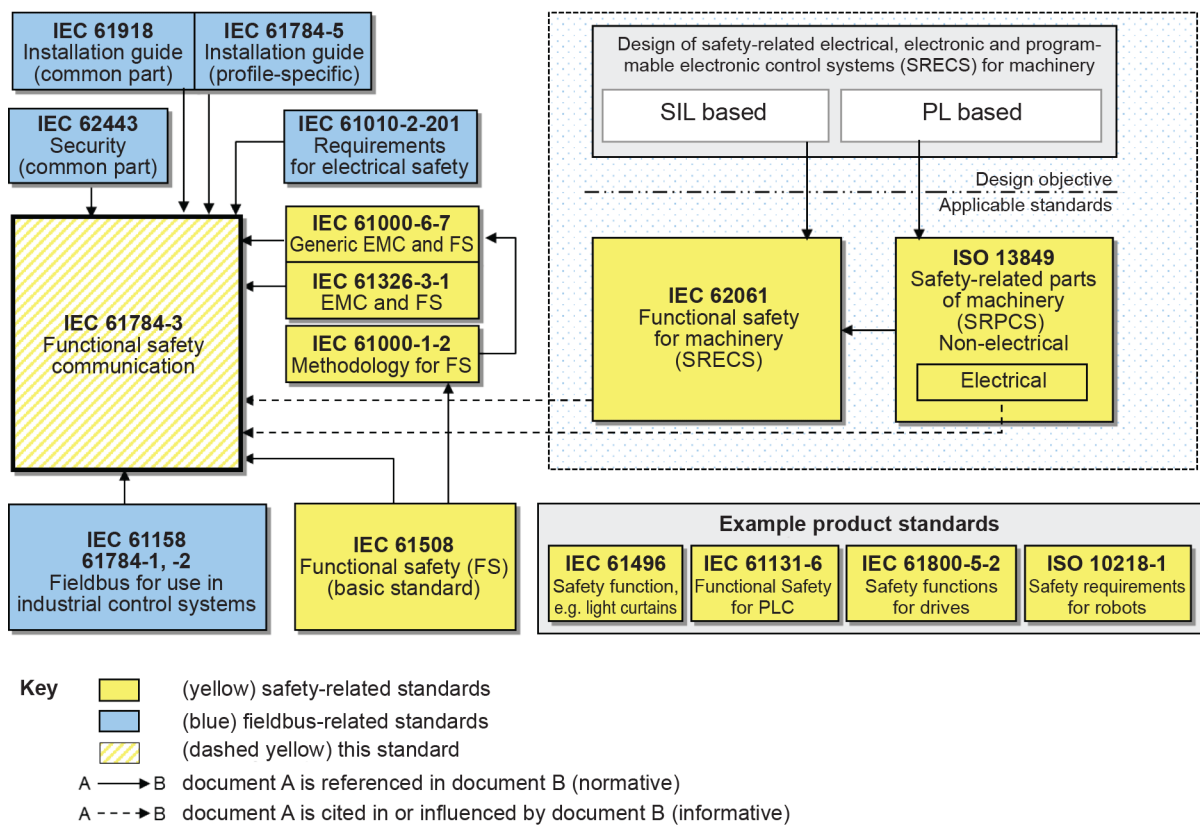
0 Introduction

0.1 General

The IEC 61158 (all parts) 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, fieldbus enhancements continue to emerge, addressing applications for areas such as real time and safety-related applications.

IEC 61784-3 (all parts) explains the relevant principles for functional safety communications with reference to IEC 61508 (all parts) 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 IEC 61158 (all parts). It does not cover electrical safety and intrinsic safety aspects. It also does not cover security aspects, nor does it provide any requirements for security.

Figure 1 shows the relationships between IEC 61784-3 (all parts) and relevant safety and fieldbus standards in a machinery environment.



IEC

NOTE IEC 62061 specifies the relationship between PL (Category) and SIL.

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