BS EN IEC 61784-3:2021+A1:2024



BSI Standards Publication

Industrial communication networks — Profiles

Part 3: Functional safety fieldbuses — General rules and profile definitions

Documents
Document Sharing Hub

Full document details: BS EN IEC 61784-3:2021+A1:2024

National foreword

This British Standard is the UK implementation of EN IEC 61784-3:2021+A1:2024. It is identical to IEC 61784-3:2021, incorporating amendment 1:2024. It supersedes BS EN IEC 61784-3:2021, which is withdrawn.

The start and finish of text introduced or altered by amendment is indicated in the text by tags. Tags indicating changes to IEC text carry the number of the IEC amendment. For example, text altered by IEC amendment 1 is indicated by A1 A1.

The UK participation in its preparation was entrusted to Technical Committee GEL/65, Measurement and control.

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

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

© The British Standards Institution 2024
Published by BSI Standards Limited 2024

ISBN 978 0 539 26502 6

ICS 25.040.40; 35.100.05

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 31 March 2021.

Amendments/corrigenda issued since publication

Date	Text affected
31 May 2024	Implementation of IEC amendment 1:2024 with CENELEC endorsement A1:2024

AVA Documents
Document Sharing Hub

Full document details: BS EN IEC 61784-3:2021+A1:2024

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN IEC 61784-3:2021+A1

May 2024

ICS 25.040.40; 35.100.05

Supersedes EN 61784-3:2016 and all of its amendments and corrigenda (if any)

English Version

Industrial communication networks - Profiles - Part 3: Functional safety fieldbuses - General rules and profile definitions (IEC 61784-3:2021)

Réseaux de communication industriels - Profils - Partie 3: Bus de terrain de sécurité fonctionnelle - Règles générales et définitions de profils (IEC 61784-3:2021)

Industrielle Kommunikationsnetze - Profile - Teil 3: Funktional sichere Übertragung bei Feldbussen - Allgemeine Regeln und Festlegungen für Profile (IEC 61784-3:2021)

This European Standard was approved by CENELEC on 2021-03-23. 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, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, 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: Rue de la Science 23, B-1040 Brussels

© 2021 CENELEC All rights of exploitation in any form and by any means reserved worldwide for CENELEC Members.

Ref. No. EN IEC 61784-3:2021 E

Documents
Document Sharing Hub

Full document details: BS EN IEC 61784-3:2021+A1:2024

European foreword

The text of document 65C/1067/FDIS, future edition 4 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 IEC 61784-3:2021.

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) 2021-12-23
- latest date by which the national standards conflicting with the document have to be withdrawn (dow) 2024-03-23

This document supersedes EN 61784-3:2016 and all of its amendments and corrigenda (if any).

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 61784-3:2021 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 61000-1-2	NOTE	Harmonized as EN 61000-1-2
IEC 61131-6	NOTE	Harmonized as EN 61131-6
IEC 61158-2:2014	NOTE	Harmonized as EN 61158-2:2014 (not modified)
IEC 61158-3-1	NOTE	Harmonized as EN 61158-3-1
IEC 61158-3-2	NOTE	Harmonized as EN 61158-3-2
IEC 61158-3-3	NOTE	Harmonized as EN 61158-3-3
IEC 61158-3-8	NOTE	Harmonized as EN 61158-3-8
IEC 61158-3-12	NOTE	Harmonized as EN IEC 61158-3-12
IEC 61158-3-13	NOTE	Harmonized as EN 61158-3-13
IEC 61158-3-14	NOTE	Harmonized as EN 61158-3-14
IEC 61158-3-18	NOTE	Harmonized as EN 61158-3-18
IEC 61158-3-19	NOTE	Harmonized as EN IEC 61158-3-19
IEC 61158-3-21	NOTE	Harmonized as EN IEC 61158-3-21
IEC 61158-3-22	NOTE	Harmonized as EN 61158-3-22
IEC 61158-4-1	NOTE	Harmonized as EN 61158-4-1
IEC 61158-4-2	NOTE	Harmonized as EN IEC 61158-4-2
IEC 61158-4-3	NOTE	Harmonized as EN IEC 61158-4-3
IEC 61158-4-8	NOTE	Harmonized as EN 61158-4-8
IEC 61158-4-12	NOTE	Harmonized as EN IEC 61158-4-12
IEC 61158-4-13	NOTE	Harmonized as EN 61158-4-13
IEC 61158-4-14	NOTE	Harmonized as EN 61158-4-14
IEC 61158-4-18	NOTE	Harmonized as EN 61158-4-18
IEC 61158-4-19	NOTE	Harmonized as EN IEC 61158-4-19

AVA Documents
Document Sharing Hub

Full document details: BS EN IEC 61784-3:2021+A1:2024

IEC 61158-4-21	NOTE	Harmonized as EN IEC 61158-4-21
IEC 61158-4-22	NOTE	Harmonized as EN 61158-4-22
IEC 61158-5-2	NOTE	Harmonized as EN IEC 61158-5-2
IEC 61158-5-3	NOTE	Harmonized as EN 61158-5-3
IEC 61158-5-5	NOTE	Harmonized as EN 61158-5-5
IEC 61158-5-8	NOTE	Harmonized as EN 61158-5-8
IEC 61158-5-9	NOTE	Harmonized as EN 61158-5-9
IEC 61158-5-10	NOTE	Harmonized as EN IEC 61158-5-10
IEC 61158-5-12	NOTE	Harmonized as EN IEC 61158-5-12
IEC 61158-5-13	NOTE	Harmonized as EN 61158-5-13
IEC 61158-5-14	NOTE	Harmonized as EN 61158-5-14
IEC 61158-5-18	NOTE	Harmonized as EN 61158-5-18
IEC 61158-5-19	NOTE	Harmonized as EN IEC 61158-5-19
IEC 61158-5-21	NOTE	Harmonized as EN IEC 61158-5-21
IEC 61158-5-22	NOTE	Harmonized as EN 61158-5-22
IEC 61158-5-23	NOTE	Harmonized as EN IEC 61158-5-23
IEC 61158-6-2	NOTE	Harmonized as EN IEC 61158-6-2
IEC 61158-6-3	NOTE	Harmonized as EN IEC 61158-6-3
IEC 61158-6-5	NOTE	Harmonized as EN 61158-6-5
IEC 61158-6-8	NOTE	Harmonized as EN 61158-6-8
IEC 61158-6-9	NOTE	Harmonized as EN 61158-6-9
IEC 61158-6-10	NOTE	Harmonized as EN IEC 61158-6-10
IEC 61158-6-12	NOTE	Harmonized as EN IEC 61158-6-12
IEC 61158-6-13	NOTE	Harmonized as EN 61158-6-13
IEC 61158-6-14	NOTE	Harmonized as EN 61158-6-14
IEC 61158-6-18	NOTE	Harmonized as EN 61158-6-18
IEC 61158-6-19	NOTE	Harmonized as EN IEC 61158-6-19
IEC 61158-6-21	NOTE	Harmonized as EN IEC 61158-6-21
IEC 61158-6-22	NOTE	Harmonized as EN 61158-6-22
IEC 61158-6-23	NOTE	Harmonized as EN IEC 61158-6-23
IEC 61496 (series)	NOTE	Harmonized as EN IEC 61496 (series)
IEC 61496-1	NOTE	Harmonized as EN IEC 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 (series)	NOTE	Harmonized as 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 62061:2005/A1:2012	NOTE	Harmonized as EN 62061:2005/A1:2013 (not modified)
IEC 62061:2005/A2:2015	NOTE	Harmonized as EN 62061:2005/A2:2015 (not modified)
ISO 10218-1	NOTE	Harmonized as EN ISO 10218-1
ISO 13849 (series)	NOTE	Harmonized as EN ISO 13849 (series)
ISO 13849-1:2015	NOTE	Harmonized as EN ISO 13849-1:2015 (not modified)

AVA Documents
Document Sharing Hub

Full document details: BS EN IEC 61784-3:2021+A1:2024

European foreword to amendment A1

The text of document 65C/1284/FDIS, future IEC 61784-3/AMD1, 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 IEC 61784-3:2021/A1:2024.

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) 2025-02-24
- latest date by which the national standards conflicting with the document have to be withdrawn (dow) 2027-05-24

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.

Any feedback and questions on this document should be directed to the users' national committee. A complete listing of these bodies can be found on the CENELEC website.

Endorsement notice

The text of the International Standard IEC 61784-3:2021/AMD1:2024 was approved by CENELEC as a European Standard without any modification.

In the official version, for Bibliography, the following note has to be added for the standard indicated:

IEC 62061:2021 NOTE Approved as EN IEC 62061:2021 (not modified)

Documents
Document Sharing Hub

Full document details: BS EN IEC 61784-3:2021+A1:2024

Annex ZA
(normative)

Normative references to international publications with their corresponding European publications

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

NOTE 1 Where 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.

Publication	Year	Title	EN/HD	Year
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	-	Safety requirements for electrical equipment for measurement, control, and laboratory use - Part 2-201: Particular requirements for control equipment	EN IEC 61010-2-201	-
IEC 61158	series	Industrial communication networks - Fieldbus specifications	EN IEC 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 IEC 61326-3-2	-
IEC 61508	series	Functional safety of electrical /electronic/programmable electronic safety-related systems	EN 61508	series

Documents
Document Sharing Hub

Full document details: BS EN IEC 61784-3:2021+A1:2024

Publication	Year	Title	EN/HD	Year
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 IEC 61784-1	-
IEC 61784-2	-	Industrial communication networks - Profiles - Part 2: Additional fieldbus profiles for real-time networks based on ISO/IEC/IEEE 8802-3	EN IEC 61784-2	-
IEC 61784-3	series	Industrial communication networks - Profiles - Part 3: Functional safety fieldbuses	-	-
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	-

AVA Documents
Document Sharing Hub

Full document details: BS EN IEC 61784-3:2021+A1:2024

Publication	Year	Title	EN/HD	Year
IEC 61784-3-17	-	Industrial communication networks - Profiles - Part 3-17: Functional safety fieldbuses - Additional specifications for CPF 17	EN 61784-3-17	-
IEC 61784-3-18	-	Industrial communication networks - Profiles - Part 3-18: Functional 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	2018	Industrial communication networks - Installation of communication networks in industrial premises	EN IEC 61918	2018
-	-		EN IEC 61918:2018 /AC:2019-03	2019
IEC 62443	series	Security for industrial process measurement and control - Network and system security	-	-

Documents
Document Sharing Hub

Full document details: BS EN IEC 61784-3:2021+A1:2024

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
INTRODUCTION to Amendment 1 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
3.2.1 Abbreviated terms 22
3.2.2 Symbols 23
4 Conformance 23
5 Basics of safety-related fieldbus systems 24
5.1 Safety function decomposition 24
5.2 Communication system 25
5.2.1 General 25
5.2.2 IEC 61158 fieldbuses 25
5.2.3 Communication channel types 25
5.2.4 Safety function response time 26
5.3 Communication errors 26
5.3.1 General 26
5.3.2 Corruption 26
5.3.3 Unintended repetition 27
5.3.4 Incorrect sequence 27
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 28
5.4.1 General 28
5.4.2 Sequence number 28
5.4.3 Time stamp 28
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 29
〈A1〉 *Text deleted* 〈A1〉
5.5 Typical relationships between errors and safety measures 29
5.6 Communication phases 30
5.7 FSCP implementation aspects 31
5.8 Models for estimation of the total residual error rate 31
5.8.1 Applicability 31
5.8.2 General models for black channel communications 32

AVA Documents Document Sharing Hub

Full document details: BS EN IEC 61784-3:2021+A1:2024

5.8.3 Identification of generic safety properties 32
5.8.4 Assumptions for residual error rate calculations 33
5.8.5 Residual error rates 34
5.8.6 Data integrity 36
5.8.7 Authenticity 37
5.8.8 Timeliness 39
5.8.9 Masquerade 42
5.8.10 Calculation of the total residual error rates 42
5.8.11 Total residual error rate and SIL 44
5.8.12 Configuration and parameterization for an FSCP 44
5.9 Relationship between functional safety and security 46
5.10 Boundary conditions and constraints 46
5.10.1 Electrical safety 46
5.10.2 Electromagnetic compatibility (EMC) 47
5.11 Installation guidelines 47
5.12 Safety manual 47
5.13 Safety policy 48
6 Communication Profile Family 1 (FOUNDATION™ Fieldbus) – Profiles for functional safety 49
7 Communication Profile Family 2 (CIP™) and Family 16 (SERCOS®) – Profiles for functional safety 49
8 Communication Profile Family 3 (PROFIBUS™, PROFINET™) – Profiles for functional safety 49
9 Communication Profile Family 6 (INTERBUS®) – Profiles for functional safety 50
10 Communication Profile Family 8 (CC-Link™) – Profiles for functional safety 50
10.1 Functional Safety Communication Profile 8/1 50
10.2 Functional Safety Communication Profile 8/2 51
11 Communication Profile Family 12 (EtherCAT™) – Profiles for functional safety 51
12 Communication Profile Family 13 (Ethernet POWERLINK™) – Profiles for functional safety 51
13 Communication Profile Family 14 (EPA®) – Profiles for functional safety 51
14 Communication Profile Family 17 (RAPIEnet™) – Profiles for functional safety 52
〈A1〉 *Text deleted* 〈A1〉
Annex A (informative) Example functional safety communication models 53
A.1 General 53
A.2 Model A (single message, channel and FAL, redundant SCLs) 53
A.3 Model B (full redundancy) 53
A.4 Model C (redundant messages, FALs and SCLs, single channel) 54
A.5 Model D (redundant messages and SCLs, single channel and FAL) 54
Annex B (normative) Safety communication channel model using CRC-based error checking 56
B.1 Overview 56
B.2 Channel model for calculations 56
B.3 Bit error probability Pe 57
B.4 Cyclic redundancy checking 58
B.4.1 General 58
B.4.2 Requirements for methods to calculate R_{CRC} 58
Annex C (informative) Structure of technology-specific parts 60
Annex D (informative) Assessment guideline 63

AVA Documents Document Sharing Hub
Full document details: BS EN IEC 61784-3:2021+A1:2024

D.1 Overview 63
D.2 Channel types 63
D.2.1 General 63
D.2.2 Black channel 63
D.2.3 White channel 63
D.3 Data integrity considerations for white channel approaches 64
D.3.1 General 64
D.3.2 Models B and C 64
D.3.3 Models A and D 65
D.4 Verification of safety measures 65
D.4.1 General 65
D.4.2 Implementation 66
D.4.3 Default safety action 66
D.4.4 Safe state 66
D.4.5 Transmission errors 66
D.4.6 Safety reaction and response times 66
D.4.7 Combination of measures 66
D.4.8 Absence of interference 67
D.4.9 Additional fault causes (white channel) 67
D.4.10 Reference test beds and operational conditions 67
D.4.11 Conformance tester 67
Annex E (informative) Examples of implicit vs. explicit FSCP safety measures 68
E.1 General 68
E.2 Example fieldbus message with safety PDUs 68
E.3 Model with completely explicit safety measures 68
E.4 Model with explicit A-code and implicit T-code safety measures 69
E.5 Model with explicit T-code and implicit A-code safety measures 69
E.6 Model with split explicit and implicit safety measures 70
E.7 Model with completely implicit safety measures 71
E.8 Addition to Annex B – impact of implicit codes on properness 71
Annex F (informative) Legacy models for estimation of the total residual error rate 72
F.1 General 72
F.2 Calculation of the residual error rate 72
F.3 Total residual error rate and SIL 74
Annex G (informative) Implicit data safety mechanisms for IEC 61784-3 functional safety communication profiles (FSCPs) 75
G.1 Overview 75
G.2 Basic principles 75
G.3 Problem statement: constant values for implicit data 76
G.4 RP for FSCPs with random, uniformly distributed err_{impl} 79
G.4.1 General 79
G.4.2 Uniform distribution within the interval $[0;2^i-1]$, $i \geq r$ 80
G.4.3 Uniform distribution in the interval $[1;2^r-1]$, $i = r$ 82
G.5 General case 84
G.6 Calculation of P_{ID} 84
Annex H (informative) Residual error probability for example CRC codes (tables for verification of calculation methods) 86
H.1 Overview 86
H.2 Example of a 32-bit CRC 86

AVA Documents Document Sharing Hub

Full document details: BS EN IEC 61784-3:2021+A1:2024

H.3 Example of a 16-bit CRC 91
H.4 Conclusion 95
Annex I (informative) Comprehensive safety communication channel data integrity model using CRC-based error checking 97
I.1 Overview 97
I.2 Basic principles 97
I.3 General case 98
I.4 Upper estimation 98
Bibliography 100

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 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 – Black channel from an FSCP perspective 32
Figure 10 – Model for authentication considerations 37
Figure 11 – Fieldbus and internal address errors 38
Figure 12 – Example of slowly increasing message latency 40
Figure 13 – Example of an active network element failure 41
Figure 14 – Example application 1 (m = 4) 43
Figure 15 – Example application 2 (m = 2) 43
Figure 16 – Example of configuration and parameterization procedures for FSCP 45
Figure A.1 – Model A 53
Figure A.2 – Model B 54
Figure A.3 – Model C 54
Figure A.4 – Model D 55
Figure B.1 – Binary symmetric channel (BSC) 56
Figure B.2 – Block codes for error detection 57
Figure B.3 – Example of a block with a message part and a CRC signature 58
Figure B.4 – Proper and improper CRC polynomials 59
Figure D.1 – Basic Markov model 65
Figure E.1 – Example safety PDUs embedded in a fieldbus message 68
Figure E.2 – Model with completely explicit safety measures 68
Figure E.3 – Model with explicit A-code and implicit T-code safety measures 69
Figure E.4 – Model with explicit T-code and implicit A-code safety measures 70
Figure E.5 – Model with split explicit and implicit safety measures 70
Figure E.6 – Model with completely implicit safety measures 71
Figure F.1 – Example application 1 (m = 4) 73
Figure F.2 – Example application 2 (m = 2) 74
Figure G.1 – FSCP with implicit transmission of authenticity and/or timeliness codes 76

AVA Documents Document Sharing Hub
Full document details: BS EN IEC 61784-3:2021+A1:2024

Figure G.2 – Example of an incorrect transmission with multiple error causes 77
Figure G.3 – Impact of errors in implicit data on the residual error probability 78
Figure H.1 – Residual error probabilities (example of a 32-bit CRC – result 1) 88
Figure H.2 – Residual error probabilities (example of a 32-bit CRC – result 2) 88
Figure H.3 – Residual error probabilities (example of a 32-bit CRC – result 3) 89
Figure H.4 – Residual error probabilities (example of a 32-bit CRC – result 4) 89
Figure H.5 – Residual error probabilities (example of a 32-bit CRC – result 5) 90
Figure H.6 – Residual error probabilities (example of a 32-bit CRC – result 6) 90
Figure H.7 – Residual error probabilities (example of a 16-bit CRC – result 1) 93
Figure H.8 – Residual error probabilities (example of a 16-bit CRC – result 2) 93
Figure H.9 – Residual error probabilities (example of a 16-bit CRC – result 3) 94
Figure H.10 – Residual error probabilities (example of a 16-bit CRC – result 4) 94
Figure H.11 – Residual error probabilities (example of a 16-bit CRC – result 5) 95
Figure H.12 – Example 1 of improper polynomial 95
Figure H.13 – Example 2 of improper polynomial 96

〈A1〉 Table 1 – Typical relationships between errors and safety measures ..... 30 〈A1〉
Table 2 – Typical relationship of residual error rate to SIL 44
Table 3 – Typical relationship of residual error on demand to SIL 44
〈A1〉 Table 5 – Topics for the safety manual of products implementing IEC 61784-3-x ..... 47 〈A1〉
Table 4 – Overview of profile identifier usable for FSCP 6/7 50
Table B.1 – Example dependency d_{min} and block bit length n 57
Table C.1 – Common subclause structure for technology-specific parts 60
Table F.1 – Definition of items used for calculation of the residual error rates 73
Table F.2 – Typical relationship of residual error rate to SIL 74
Table F.3 – Typical relationship of residual error on demand to SIL 74
Table H.1 – Residual error probabilities (R_{CRC1}) for example CRC32 polynomial 87
Table H.2 – Residual error probabilities (R_{CRC2}) for example CRC16 polynomial 92

AVA Documents
Document Sharing Hub

Full document details: BS EN IEC 61784-3:2021+A1:2024

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.
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 assumptions)

AVA Documents
Document Sharing Hub

Full document details: BS EN IEC 61784-3:2021+A1:2024

- 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 RCRC.

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.

Documents
Document Sharing Hub

Full document details: BS EN IEC 61784-3:2021+A1:2024

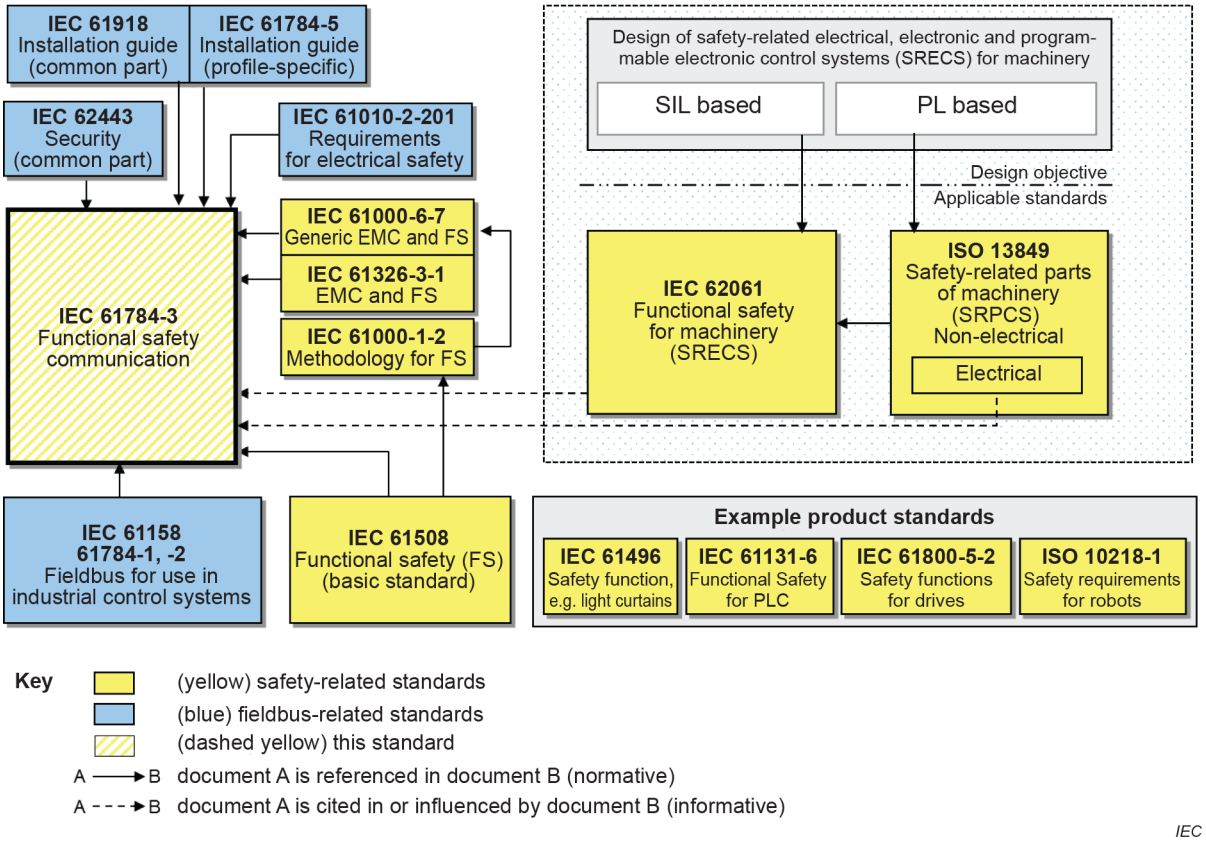
0 Introduction

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.

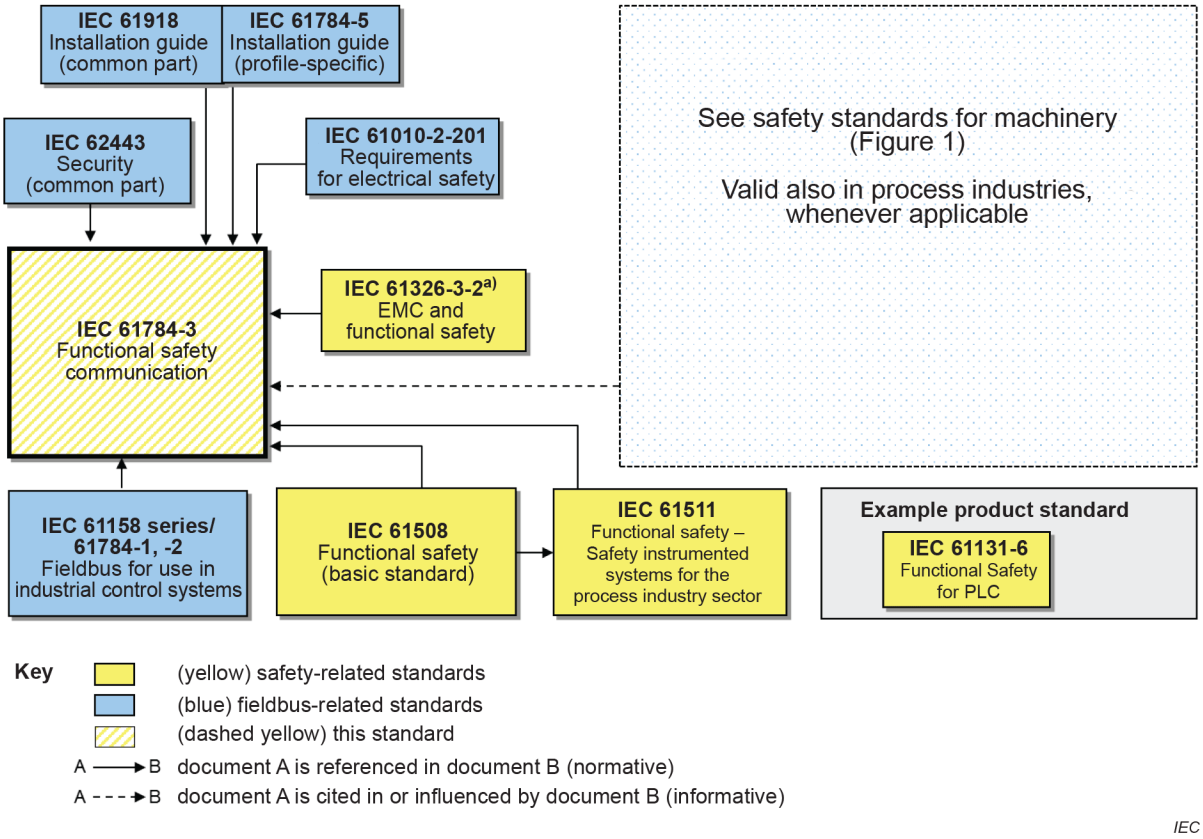


NOTE IEC 62061 specifies the relationship between PL (Category) and SIL.

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

Documents
Document Sharing Hub
Full document details: BS EN IEC 61784-3:2021+A1:2024

Figure 2 shows the relationships between IEC 61784-3 (all parts) and relevant safety and fieldbus standards in a process environment.



[a] For specified electromagnetic environments; otherwise IEC 61326-3-1 or IEC 61000-6-7.

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

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

Safety communication layers specified in IEC 61784-3 (all parts) do this in such a way that a fieldbus can be used for applications requiring functional safety up to the Safety Integrity Level (SIL) specified by its corresponding functional safety communication profile.

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

IEC 61784-3 (all parts) describes:

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

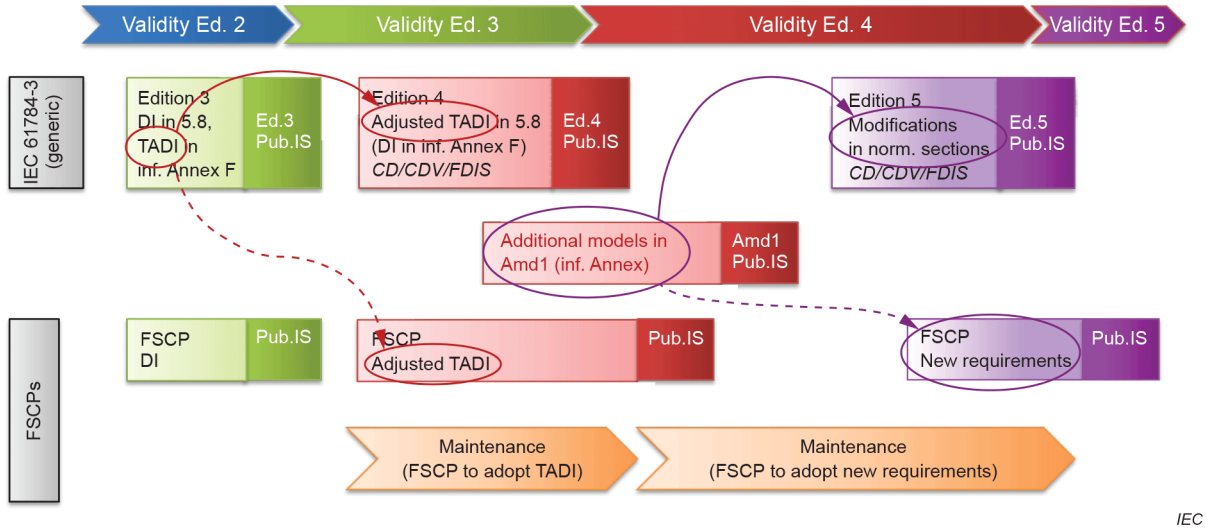
Documents
Document Sharing Hub
Full document details: BS EN IEC 61784-3:2021+A1:2024

0.2 Use of extended assessment methods in Edition 4

This edition of the generic part of IEC 61784-3 (all parts) includes extended models for use when estimating the total residual error rate for an FSCP. This value can be used to determine if the FSCP meets the requirements of functional safety applications up to a given SIL. These extended models for qualitative and quantitative safety determination methods are detailed in Annex E and 5.8.

Upon publication of this new edition of the generic part, FSCPs shall be assessed using the methods from this Edition 4, based on the extended models specified in 5.8 (derived from a modified version of Annex F of Edition 3). The informative Annex F contains the legacy models for reference purpose only.

Figure 3 shows the transitions from original assessment methods of Edition 2 to extended assessment methods in this Edition 4 and the future Edition 5.



Key

DI Data Integrity

TADI Timeliness, Authenticity, Data Integrity

Figure 3 – Transitions from Ed. 2 to Ed. 4 and future Ed. 5 assessment methods

0.3 Patent declaration

The International Electrotechnical Commission (IEC) draws attention to the fact that it is claimed that compliance with this document may involve the use of patents concerning functional safety communication profiles for families 1, 2, 3, 6, 8, 12, 13, 14, 17 and 18 given in IEC 61784-3-1, IEC 61784-3-2, IEC 61784-3-3, IEC 61784-3-6, IEC 61784-3-8, IEC 61784-3-12, IEC 61784-3-13, IEC 61784-3-14, IEC 61784-3-17 and IEC 61784-3-18.

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

The holders of these patent rights have assured IEC that they are willing to negotiate licences under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statements of the holders of these patent rights are registered with IEC. Information may be obtained from the patent database available at http://patents.iec.ch.

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

Documents
Document Sharing Hub
Full document details: BS EN IEC 61784-3:2021+A1:2024

INTRODUCTION to Amendment 1

This Amendment 1 discusses the concepts of a comprehensive channel model for data integrity calculations for functional safety communications protocols (FSCPs) as specified in IEC 61784-3:2021. The comprehensive channel model addresses data corruption error types where multiple contiguous bits are affected by a single fault.

It also reviews typical relationships between the possible errors and the various safety measures which can be implemented.

Documents
Document Sharing Hub

Full document details: BS EN IEC 61784-3:2021+A1:2024

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES –

Part 3: Functional safety fieldbuses – General rules and profile definitions

1 Scope

This part of the IEC 61784-3 series explains some common principles that can be used in the transmission of safety-relevant messages among participants within a distributed network which use fieldbus technology in accordance with the requirements of IEC 61508 (all parts)[1] for functional safety. These principles are based on the black channel approach. They can be used in various industrial applications such as process control, manufacturing automation and machinery.

This part and the IEC 61784-3-x parts specify several functional safety communication profiles based on the communication profiles and protocol layers of the fieldbus technologies in IEC 61784-1, IEC 61784-2 and IEC 61158 (all parts). These functional safety communication profiles use the black channel approach, as defined in IEC 61508. These functional safety communication profiles are intended for implementation in safety devices exclusively.

NOTE 1 Other safety-related communication systems meeting the requirements of IEC 61508 (all parts) can exist that are not included in IEC 61784-3 (all parts).

NOTE 2 It does not cover electrical safety and intrinsic safety aspects. Electrical safety relates to hazards such as electrical shock. Intrinsic safety relates to hazards associated with potentially explosive atmospheres.

All systems are exposed to unauthorized access at some point of their life cycle. Additional measures need to be considered in any safety-related application to protect fieldbus systems against unauthorized access. IEC 62443 (all parts) will address many of these issues; the relationship with IEC 62443 (all parts) is detailed in a dedicated subclause of this document.

NOTE 3 Implementation of a functional safety communication profile according to this document in a device is not sufficient to qualify it as a safety device, as defined in IEC 61508 (all parts).

NOTE 4 The resulting SIL claim of a system depends on the implementation of the selected functional safety communication profile within this system.

NOTE 5 Annex C explains the numbering scheme used for the technology-specific parts (IEC 61784-3-x) as well as their common general structure.

NOTE 6 Annex D provides a guideline for the assessment and test of safety communication profiles as well as safety-related devices using these profiles.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 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*

[1] In the following pages of this document, "IEC 61508" will be used for "IEC 61508 (all parts)".

Documents
Document Sharing Hub
Full document details: BS EN IEC 61784-3:2021+A1:2024

IEC 61010-2-201, *Safety requirements for electrical equipment for measurement, control and laboratory use – Part 2-201: Particular requirements for control equipment*

IEC 61158 (all parts), *Industrial communication networks – Fieldbus specifications*

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*

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*

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

IEC 61508-1:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements*

IEC 61508-2, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*

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

IEC 61784-2, *Industrial communication networks – Profiles – Part 2: Additional fieldbus profiles for real-time networks based on ISO/IEC/IEEE 8802-3*

IEC 61784-3 (all parts), *Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses*

IEC 61784-3-1, *Industrial communication networks – Profiles – Part 3-1: Functional safety fieldbuses – Additional specifications for CPF 1*

IEC 61784-3-2, *Industrial communication networks – Profiles – Part 3-2: Functional safety fieldbuses – Additional specifications for CPF 2*

IEC 61784-3-3, *Industrial communication networks – Profiles – Part 3-3: Functional safety fieldbuses – Additional specifications for CPF 3*

IEC 61784-3-6, *Industrial communication networks – Profiles – Part 3-6: Functional safety fieldbuses – Additional specifications for CPF 6*

IEC 61784-3-8, *Industrial communication networks – Profiles – Part 3-8: Functional safety fieldbuses – Additional specifications for CPF 8*

IEC 61784-3-12, *Industrial communication networks – Profiles – Part 3-12: Functional safety fieldbuses – Additional specifications for CPF 12*

IEC 61784-3-13, *Industrial communication networks – Profiles – Part 3-13: Functional safety fieldbuses – Additional specifications for CPF 13*

IEC 61784-3-14, *Industrial communication networks – Profiles – Part 3-14: Functional safety fieldbuses – Additional specifications for CPF 14*

IEC 61784-3-17, *Industrial communication networks – Profiles – Part 3-17: Functional safety fieldbuses – Additional specifications for CPF 17*

Documents
Document Sharing Hub

Full document details: BS EN IEC 61784-3:2021+A1:2024

IEC 61784-3-18, *Industrial communication networks – Profiles – Part 3-18: Functional safety fieldbuses – Additional specifications for CPF 18*

IEC 61784-5 (all parts), *Industrial communication networks – Profiles – Part 5: Installation of fieldbuses*

IEC 61918:2018, *Industrial communication networks – Installation of communication networks in industrial premises*

IEC 62443 (all parts), *Industrial communication networks – Network and system security*

3 Terms, definitions, symbols, abbreviated terms and conventions

3.1 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at http://www.electropedia.org/
- ISO Online browsing platform: available at http://www.iso.org/obp

NOTE Italics are used in the definitions to highlight terms which are themselves defined in 3.1.

3.1.1
absolute time stamp
time stamp referenced to a global time which is common for a group of devices using a *fieldbus*

[SOURCE: IEC 62280:2014, 3.1.1, modified – use of "devices" and "fieldbus" instead of "entities" and "transmission system"]

3.1.2
active network element
network element containing electrically and/or optically active components that allows extension of the network

Note 1 to entry: Examples of active network elements are repeaters and switches.

[SOURCE: IEC 61918:2018, 3.1.2]

3.1.3
bit error probability
Pe
probability for a given bit to be received with the incorrect value

3.1.4
black channel
defined communication system containing one or more elements without evidence of design or validation according to IEC 61508

Note 1 to entry: This definition expands the usual meaning of channel to include the system that contains the channel.

3.1.5
bridge
abstract device that connects multiple network segments along the data link layer

Documents
Document Sharing Hub
Full document details: BS EN IEC 61784-3:2021+A1:2024

3.1.6
closed communication system
fixed number or fixed maximum number of participants linked by a communication system with well-known and fixed properties, and where the risk of unauthorized access is considered negligible

[SOURCE: IEC 62280:2014, 3.1.6, modified – transmission replaced by communication]

3.1.7
communication channel
logical connection between two end-points within a *communication system*

3.1.8
communication system
arrangement of hardware, software and propagation media to allow the transfer of *messages* (ISO/IEC 7498-1 application layer) from one application to another

3.1.9
connection
logical binding between two application objects within the same or different devices

3.1.10
Cyclic Redundancy Check
CRC
<value> redundant data derived from, and stored or transmitted together with, a block of data in order to detect data corruption

<method> procedure used to calculate the redundant data

Note 1 to entry: Terms "CRC code" and "CRC signature", and labels such as CRC1, CRC2, may also be used in this document to refer to the redundant data.

Note 2 to entry: See also [71], [72][2].

3.1.11
defined communication system
defined channel
fixed number or fixed maximum number of participants linked by a fieldbus based communication system with well-known and fixed properties, such as installation conditions, electromagnetic immunity, industrial (active) network elements, and where the risk of unauthorized access is reduced to a tolerated level according to the lifecycle model of IEC 62443 (all parts), using for example zones and conduits

3.1.12
device
physical entity connected to the fieldbus composed of communication element and possibly other functional elements

[SOURCE: IEC 61158-2:2014, 3.1.13, modified – Note to entry and some details have been deleted.]

2 Figures in square brackets refer to the bibliography.

Documents
Document Sharing Hub
Full document details: BS EN IEC 61784-3:2021+A1:2024

3.1.13
diversity
different means of performing a required function

Note 1 to entry: Diversity may be achieved by different physical methods or different design approaches.

[SOURCE: IEC 61508-4:2010, 3.3.7]

3.1.14
DLPDU
DEPRECATED: frame
Data Link Protocol Data Unit

3.1.15
error
discrepancy between a computed, observed or measured value or condition and the true, specified or theoretically correct value or condition

Note 1 to entry: Errors may be due to design mistakes within hardware/software and/or corrupted information due to electromagnetic interference and/or other effects.

Note 2 to entry: Errors do not necessarily result in a failure or a fault.

[SOURCE: IEC 61508-4:2010, 3.6.11, modified – notes added]

3.1.16
explicit code
code for safety measure that is actually transmitted within the SPDU and is known to the sender and receiver

3.1.17
explicit data
data that is transmitted

Note 1 to entry: Explicit data is defined in contrast to implicit data.

3.1.18
failure
termination of the ability of a functional unit to perform a required function or operation of a functional unit in any way other than as required

Note 1 to entry: Failure may be due to an *error* (for example, problem with hardware/software design or message disruption).

[SOURCE: IEC 61508-4:2010, 3.6.4, modified – notes and figures replaced]

3.1.19
fault
abnormal condition that may cause a reduction in, or loss of, the capability of a functional unit to perform a required function

Note 1 to entry: IEC 60050-191:1990, 191-05-01 defines "fault" as a state characterized by the inability to perform a required function, excluding the inability during preventive maintenance or other planned actions, or due to lack of external resources.

[SOURCE: IEC 61508-4:2010, 3.6.1, modified – figure reference deleted]

3.1.20
fieldbus
communication system based on serial data transfer and used in industrial automation or process control applications

AVA Documents
Document Sharing Hub

Full document details: BS EN IEC 61784-3:2021+A1:2024

3.1.21
fieldbus system
system using a *fieldbus* with connected devices

3.1.22
Frame Check Sequence
FCS
redundant data derived from a block of data within a DLPDU (frame), using a hash function, and stored or transmitted together with the block of data, in order to detect data corruption

Note 1 to entry: An FCS can be derived using for example a CRC or other hash function.

Note 2 to entry: See also [71], [72].

3.1.23
functional safety communication profile
FSCP
technology specification for the implementation of an SCL

3.1.24
hash function
(mathematical) function that maps values from a (possibly very) large set of values into a (usually) smaller range of values

Note 1 to entry: Hash functions can be used to detect data corruption.

Note 2 to entry: Common hash functions include parity, checksum or CRC.

3.1.25
hazard
potential source of harm

Note 1 to entry: The term includes danger to persons arising within a short time scale (for example, fire and explosion) and also those that have a long-term effect on a person's health (for example, release of a toxic substance).

[SOURCE: IEC 61508-4:2010, 3.1.2 and ISO/IEC Guide 51:2014, definition 3.2]

3.1.26
implicit code
code for safety measure that is not transmitted within the SPDU but is known to the sender and receiver

3.1.27
implicit data
additional data that is not transmitted but is known to the sender and receiver, and used in the encoding and decoding of the message/SPDU

Note 1 to entry: Implicit data is defined in contrast to explicit data.

[SOURCE: IEC 62280:2014, 3.1.25, modified – addition of ", and used in the encoding and decoding of the message/SPDU" and of Note 1 to entry]

3.1.28
master
communication entity able to initiate and schedule communication activities by other stations which may be masters or slaves

Documents
Document Sharing Hub
Full document details: BS EN IEC 61784-3:2021+A1:2024

3.1.29
message

<information theory and communication theory> ordered sequence of characters (usually octets) intended to convey information

[SOURCE: ISO/IEC 2382:2015, 2123205, modified – insertion of "(usually octets)", deletion of notes and source]

3.1.30
message sink
information sink
part of a *communication system* in which *messages* are considered to be received

[SOURCE: ISO/IEC 2382:2015, 2123207, modified – deletion of notes and source]

3.1.31
message source
information source
part of a *communication system* from which *messages* are considered to originate

[SOURCE: ISO/IEC 2382:2015, 2123206, modified – deletion of notes and source]

3.1.32
performance level
PL
discrete level used to specify the ability of safety-related parts of control systems to perform a safety function under foreseeable conditions

[SOURCE: ISO 13849-1:2015, 3.1.23]

3.1.33
redundancy
existence of more than one means for performing a required function or for representing information

[SOURCE: IEC 61508-4:2010, 3.4.6, modified – example and notes deleted]

3.1.34
relative time stamp
time stamp referenced to the local clock of an entity

Note 1 to entry: In general, there is no relationship to clocks of other entities.

[SOURCE: IEC 62280:2014, 3.1.43]

3.1.35
residual error probability
RP
probability of an error undetected by the SCL safety measures

3.1.36
residual error rate
statistical rate at which the SCL safety measures fail to detect errors

3.1.37
risk
combination of the probability of occurrence of harm and the severity of that harm

Note 1 to entry: For more discussion on this concept see Annex A of IEC 61508-5:2010.

Documents
Document Sharing Hub

Full document details: BS EN IEC 61784-3:2021+A1:2024

[SOURCE: IEC 61508-4:2010, 3.1.6, and ISO/IEC Guide 51:2014, definition 3.9, modified – different note]

3.1.38
safety communication channel
SC
communication channel starting at the top of the SCL of the source and ending at the top of the SCL of the sink

Note 1 to entry: It can be modelled as two SCLs connected by a black channel or a defined communication system, or a defined channel.

3.1.39
safety communication layer
SCL
communication layer above the FAL that includes all necessary additional measures to ensure safe transmission of data in accordance with the requirements of IEC 61508

3.1.40
safety connection
connection that utilizes the safety protocol for communications transactions

3.1.41
safety data
data transmitted across a safety network using a safety protocol

Note 1 to entry: The safety communication layer does not ensure safety of the data itself, only that the data is transmitted safely.

3.1.42
safety device
device designed in accordance with IEC 61508 and which implements the functional safety communication profile

3.1.43
safety function
function to be implemented by an E/E/PE safety-related system or other risk reduction measures, that is intended to achieve or maintain a safe state for the EUC, in respect of a specific hazardous event

[SOURCE: IEC 61508-4:2010, 3.5.1, modified – references and example deleted]

3.1.44
safety function response time
worst case elapsed time following an actuation of a safety sensor connected to a fieldbus, until the corresponding safe state of its safety actuator(s) is achieved in the presence of errors or failures in the safety function

Note 1 to entry: This concept is introduced in 5.2.4 and addressed by the functional safety communication profiles defined in this document.

3.1.45
safety integrity level
SIL
discrete level (one out of a possible four), corresponding to a range of safety integrity values, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest

Note 1 to entry: The target failure measures (see IEC 61508-4:2010, 3.5.17) for the four safety integrity levels are specified in Tables 2 and 3 of IEC 61508-1:2010.

AVA Documents Document Sharing Hub

Full document details: BS EN IEC 61784-3:2021+A1:2024

Note 2 to entry: Safety integrity levels are used for specifying the safety integrity requirements of the safety functions to be allocated to the E/E/PE safety-related systems.

Note 3 to entry: A safety integrity level (SIL) is not a property of a system, subsystem, element or component. The correct interpretation of the phrase "SIL n safety-related system" (where n is 1, 2, 3 or 4) is that the system is potentially capable of supporting safety functions with a safety integrity level up to n.

[SOURCE: IEC 61508-4:2010, 3.5.8]

3.1.46
safety measure
measure to control possible communication *errors* that is designed and implemented in compliance with the requirements of IEC 61508

Note 1 to entry: In practice, several safety measures are combined to achieve the required safety integrity level.

Note 2 to entry: Communication errors and related safety measures are detailed in 5.3 and 5.4.

3.1.47
safety PDU
SPDU
PDU transferred through the safety communication channel

Note 1 to entry: The SPDU may include more than one copy of the safety data using differing coding structures and hash functions together with explicit parts of additional protections such as a key, a sequence count, or a time stamp mechanism.

Note 2 to entry: Redundant SCLs may provide two different versions of the SPDU for insertion into separate fields of the fieldbus frame.

3.1.48
safety-related application
programs designed in accordance with IEC 61508 to meet the SIL requirements of the application

3.1.49
safety-related system
system performing *safety functions* according to IEC 61508

3.1.50
slave
communication entity able to receive messages and send them in response to another communication entity which may be a master or a slave, but not to initiate communication activities

3.1.51
spurious trip
trip caused by the safety system without a process demand

3.1.52
time stamp
time information included in a *message*

3.1.53
uniform distribution
probability distribution where all values from a finite set are equally likely to occur

Note 1 to entry: For a field of bit length i the probability of occurrence of a particular field value is 2^{-i} since the sum of all probabilities of occurrence is equal to 1.

Documents
Document Sharing Hub
Full document details: BS EN IEC 61784-3:2021+A1:2024

3.1.54
white channel
defined communication system in which all relevant hardware and software elements are designed, implemented and validated according to IEC 61508

Note 1 to entry: This definition expands the usual meaning of channel to include the system that contains the channel.

〈A1〉 **3.1.55**
uniformly distributed segment
UDS
segment of a message consisting of contiguous bits within which error patterns are uniformly distributed 〈A1〉

3.2 Symbols and abbreviated terms

3.2.1 Abbreviated terms

A-code	Authenticity code	
BSC	Binary Symmetric Channel	(see Clause B.2)
CP	Communication Profile	[IEC 61784-1]
CPF	Communication Profile Family	[IEC 61784-1]
CRC	Cyclic Redundancy Check	
DLL	Data Link Layer	[ISO/IEC 7498-1]
DLPDU	Data Link Protocol Data Unit	
EMC	Electromagnetic Compatibility	
EMI	Electromagnetic Interference	
EUC	Equipment Under Control	[IEC 61508-4:2010]
E/E/PE	Electrical/Electronic/Programmable Electronic	[IEC 61508-4:2010]
FAL	Fieldbus Application Layer	[IEC 61158-5 (all parts)]
FCS	Frame Check Sequence	
FIT	Failure In Time (equals 10^{-9} failure per hour)	
FS	Functional Safety	
FSCP	Functional Safety Communication Profile	
IACS	Industrial Automation and Control System	
MTBF	Mean Time Between Failures	
MTTF	Mean Time To Failure	
NSR	Non Safety Related	
PDU	Protocol Data Unit	[ISO/IEC 7498-1]
PELV	Protective Extra Low Voltage	[IEC 61010-2-201]
PES	Programmable Electronic System	[IEC 61508-4:2010]
PFD_{avg}	Average probability of dangerous Failure on Demand	[IEC 61508-4:2010]
PFH	Average frequency of dangerous failure [h^{-1}] per hour	[IEC 61508-4:2010]
PhL	Physical Layer	[ISO/IEC 7498-1]
PL	Performance Level	[ISO 13849-1]
PLC	Programmable Logic Controller	
SC	Safety Communication Channel	
SCL	Safety Communication Layer	
SELV	Safety Extra Low Voltage	[IEC 61010-2-201]
SIS	Safety Instrumented Systems	

AVA Documents Document Sharing Hub

Full document details: BS EN IEC 61784-3:2021+A1:2024

SIL	Safety Integrity Level	[IEC 61508-4:2010]
SMS	Security Management System	[IEC 62443 (all parts)]
SPDU	Safety PDU	
SR	Safety Related	
T-code	Timeliness code	
A1 UDS	uniformly distributed segment A1	

3.2.2 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

4 Conformance

Each functional safety communication profile within IEC 61784-3 (all parts) is based on communication profiles of IEC 61784-1 or IEC 61784-2 and protocol layers of IEC 61158 (all parts).

A statement of conformance to a Functional Safety Communication Profile (FSCP) of IEC 61784-3 (all parts) shall be stated as either

conformance to IEC 61784-3:20xx FSCP n/m <Type>

or

conformance to IEC 61784-3 (Ed.y.z) FSCP n/m <Type>

where the Type within the angle brackets < > is optional and the angle brackets are not to be included.

Alternatively, a statement of conformance may be stated as either

conformance to IEC 61784-3-N:20xx

or

Documents
Document Sharing Hub
Full document details: BS EN IEC 61784-3:2021+A1:2024

conformance to IEC 61784-3-N (Ed.y.z)

where N is the family number assigned to the corresponding CPF.

Conformance to a IEC 61784-3-N part means that all mandatory requirements of the corresponding FSCP(s) for the particular device, system or application shall be fulfilled.

Product standards shall not include any Conformity Assessment aspects (including QM provisions), either normative or informative, other than provisions for product testing (evaluation and examination).

5 Basics of safety-related fieldbus systems

5.1 Safety function decomposition

According to IEC 61508, a risk analysis will define safety functions. These safety functions can be decomposed to parts that contribute to the overall safety function (for example, Sensor(s) – Safety communication channel – PES(s) – Safety communication channel – Actuator(s)).

The communication system itself in this document performs transmission of safety data. To simplify system calculations, it is recommended that any logical connection of the safety communication channels of a safety function does not consume more than 1 % of the maximum PFH or PFD_{avg} of the target SIL for which the functional safety communication profile is designed (see Figure 4 and 5.8.11).

The overall PFH and PFD_{avg} of each safety device shall incorporate the PFH and PFD_{avg} of the logical connection. The PFD_{avg} shall be provided if the FSCP is also used for low demand mode applications according to IEC 61508.

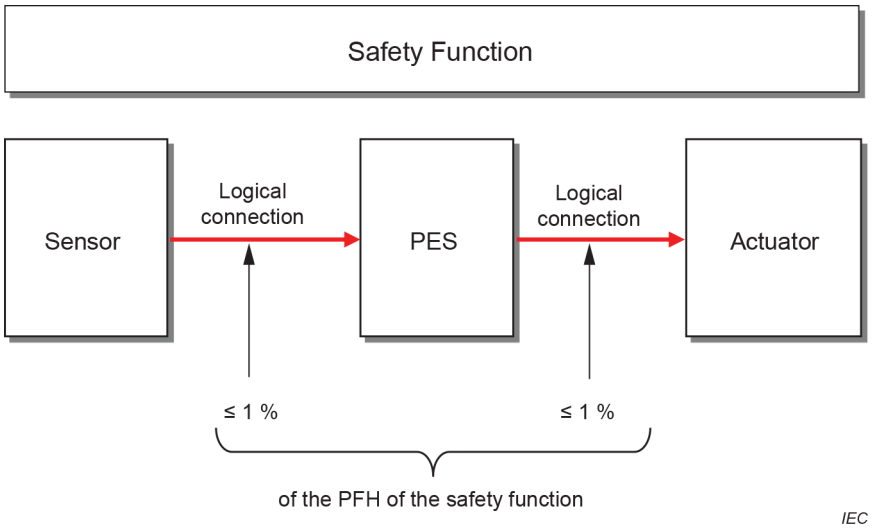


Figure 4 – Safety communication as a part of a safety function

Alternatively, the PFH / PFD_{avg} of the communication can be calculated for the whole safety function. In this case, the PFH / PFD_{avg} of the safety communication needs to be considered only once.

In any case, the safety manual for this FSCP shall provide guidance on the calculations of the PFH or PFD_{avg} for a safety function (see 5.8.10).

Documents
Document Sharing Hub
Full document details: BS EN IEC 61784-3:2021+A1:2024

5.2 Communication system

5.2.1 General

The following information is used to provide a common understanding of technology and terms.

5.2.2 IEC 61158 fieldbuses

While IEC 61508 is not restricting the use of communication technologies, this document focuses on the use of fieldbus based functional safety communication systems. Figure 5 shows an example model of the use of functional safety communications with a fieldbus based on the black channel approach.

When using IEC 61158 based fieldbus structures without modifications in the definition of each communication layer, all the measures necessary to implement transmission of safety data in accordance with the requirements of IEC 61508 shall be performed by an additional "safety communication layer", positioned as shown in Figure 5.

The safety communication layer includes suitable services and protocol to encode safety data into safety PDUs and pass them to the black channel and to receive safety PDUs from the black channel and decode them to extract safety data.

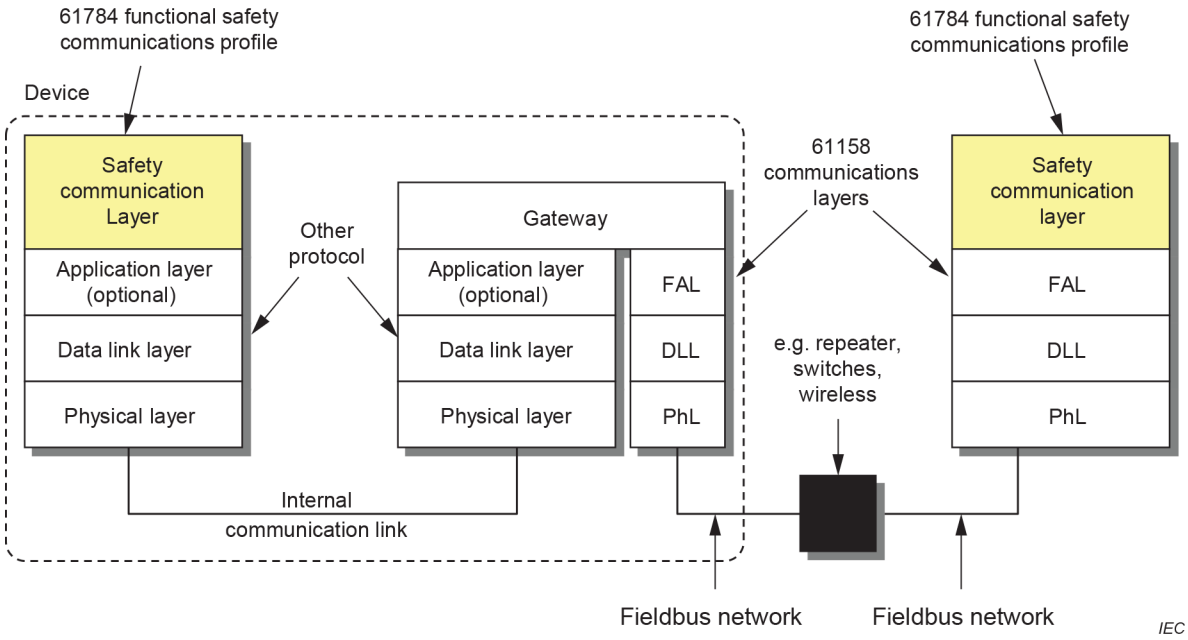


Figure 5 – Example model of a functional safety communication system

While implementation of the Fieldbus Application Layer (FAL) is required for functional safety communication systems according to this document, the Application Layer may be omitted for communication links internal to a device (for example with a gateway).

Functions that are not safety-related may bypass the SCL and access the FAL directly.

5.2.3 Communication channel types

IEC 61508 uses the concepts of the "black channel" or "white channel" to define the requirements of the base fieldbus for transmission of safety data. This document specifies functional safety communication profiles that use the black channel approach.

Documents
Document Sharing Hub
Full document details: BS EN IEC 61784-3:2021+A1:2024

In this context, a safety communication channel is defined to start at the top of the safety communication layer of the source and stop at the top of the safety communication layer of the sink (see Figure 5). The black channel includes everything between the safety communication layers.

5.2.4 Safety function response time

The safety function response time is the worst case elapsed time following an actuation of a safety sensor (for example switch, pressure transmitter, light curtain) connected to a fieldbus, until the corresponding safe state of its safety actuator(s) (for example relay, valve, drive) is achieved in the presence of errors or failures in the safety function.

Calculation of the safety function response time is specified in the profile specific parts of IEC 61784-3 (all parts).

Empirical measurements may only serve as a plausibility check of the worst case calculation.

The demand (actuation) on a safety function is caused either by an analogue signal crossing a threshold or a digital signal changing state.

Figure 6 shows an example of typical components making up a safety function response time.

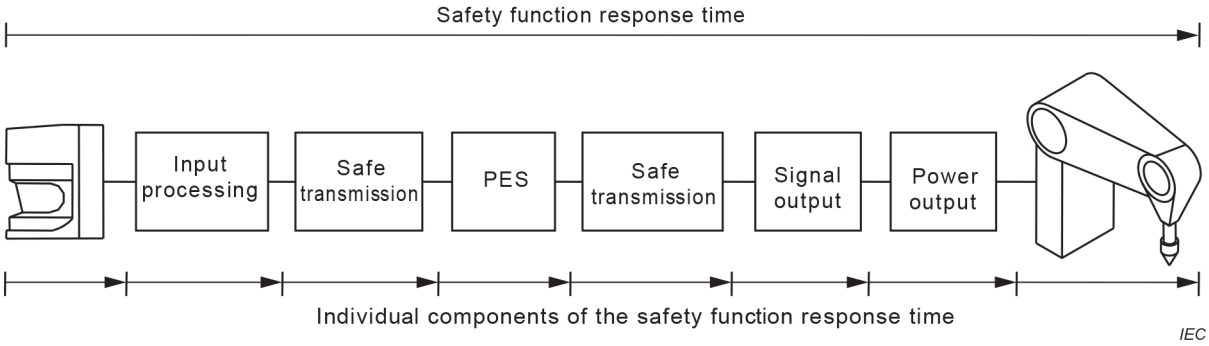


Figure 6 – Example of safety function response time components

Individual functional safety communication profiles may have a different set of components, but all relevant components shall be accounted for in the safety function response time.

5.3 Communication errors

5.3.1 General

Subclauses 5.3.2 to 5.3.9 specify possible communication errors. Additional notes are provided to indicate the typical behaviour of a black channel.

5.3.2 Corruption

Messages may be corrupted due to errors within a bus participant, due to errors on the transmission medium, or due to message interference.

NOTE 1 Message error during transfer is a normal event for any standard communication system; such events are detected at receivers with high probability by use of a hash function and the message is ignored.

NOTE 2 Most communication systems include protocols for recovery from message errors, so these messages will not be classed as 'Loss' until recovery or repetition procedures have failed or are not used.

NOTE 3 If the recovery or repetition procedures take longer than a specified deadline, a message is classed as 'Unacceptable delay'.

AVA Documents Document Sharing Hub

Full document details: BS EN IEC 61784-3:2021+A1:2024

NOTE 4 In the very low probability event that multiple errors result in a new message with correct message structure (for example addressing, length, hash function such as CRC, etc.), the message will be accepted and processed further. Evaluations based on a message sequence number or a time stamp can result in fault classifications such as Unintended repetition, Incorrect sequence, Unacceptable delay, Insertion.

5.3.3 Unintended repetition

Due to an error, fault or interference, messages are repeated.

NOTE 1 Repetition by the sender is a normal procedure when an expected acknowledgment/response is not received from a target station, or when a receiver station detects a missing message and asks for it to be resent.

NOTE 2 Some fieldbuses use redundancy to send the same message multiple times or via multiple alternate routes to increase the probability of good reception.

5.3.4 Incorrect sequence

Due to an error, fault or interference, the predefined sequence (for example natural numbers, time references) associated with messages from a particular source is incorrect.

NOTE 1 This "incorrect sequence" error is also referred to as "out-of-sequence" error.

NOTE 2 Fieldbus systems can contain elements that store messages (for example FIFOs in switches, bridges, routers) or use protocols that can alter the sequence (for example by allowing messages with high priority to overtake those with lower priority).

NOTE 3 When multiple sequences are active, such as messages from different source entities or reports relating to different object types, these sequences are monitored separately, and errors can be reported for each sequence.

5.3.5 Loss

Due to an error, fault or interference, a message or acknowledgment is not received.

5.3.6 Unacceptable delay

Messages may be delayed beyond their permitted arrival time window, for example due to errors in the transmission medium, congested transmission lines, interference, or due to bus participants sending messages in such a manner that services are delayed or denied (for example FIFOs in switches, bridges, routers).

5.3.7 Insertion

Due to a fault or interference, a message is received that relates to an unexpected or unknown source entity.

NOTE These messages are additional to the expected message stream, and because they do not have expected sources, they cannot be classified as Correct, Unintended repetition, or Incorrect sequence.

5.3.8 Masquerade

Due to a fault or interference, a message from a non-safety related source is interpreted in such a way that it appears to originate from a valid safety related source entity. Non-safety related data would therefore be received by a safety related participant, which then treats it as safety related.

NOTE Communication systems used for safety-related applications can use additional checks to detect Masquerade, such as authorised source identities and passphrases or cryptography.

5.3.9 Addressing

Due to a fault or interference, a safety related message is delivered to the incorrect safety related participant, which then treats reception as correct. This includes the so-called loopback error case, where the sender receives back its own sent message.

Documents
Document Sharing Hub
Full document details: BS EN IEC 61784-3:2021+A1:2024