IEC 61784-3

Edition 4.0 2024-04

INTERNATIONAL STANDARD

NORME INTERNATIONALE

AMENDMENT 1
AMENDEMENT 1

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

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

IEC 61784-3:2021-02/AMD1:2024-04(en-fr)

IEC 61784-3

Edition 4.0 2024-04

INTERNATIONAL STANDARD

NORME INTERNATIONALE

AMENDMENT 1
AMENDEMENT 1

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

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

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 25.040.40, 35.100.05

ISBN978-2-8322-8279-3

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.

INTERNATIONAL ELECTROTECHNICAL COMMISSION

____

INDUSTRIAL COMMUNICATION NETWORKS – PROFILES –

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

AMENDMENT 1

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC 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) IEC draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). IEC takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, IEC had not received notice of (a) patent(s), which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at https://patents.iec.ch. IEC shall not be held responsible for identifying any or all such patent rights.

Amendment 1 to IEC 61784-3:2021 has been prepared by subcommittee 65C: Industrial networks, of IEC technical committee 65: Industrial-process measurement, control and automation.

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

Draft	Report on voting
65C/1284/FDIS	65C/1291/RVD

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

The language used for the development of this Amendment is English.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement, available at www.iec.ch/members_experts/refdocs. The main document types developed by IEC are described in greater detail at www.iec.ch/publications/.

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 webstore.iec.ch in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn, or
- revised.

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.

3 Terms, definitions, symbols, abbreviated terms and conventions

3.1 Terms and definitions

Add the following new term and definition:

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

3.2 Symbols and abbreviated terms

3.2.1 Abbreviated terms

Add, at the end of the list, the following new abbreviated term:

UDS uniformly distributed segment

5.4.1 General

Replace, at the beginning of the sentence, "5.4.9" *with* "5.4.8".

5.4.9 Different data integrity assurance systems

Delete this subclause.

5.5 Typical relationships between errors and safety measures

Replace, at the beginning of the second paragraph, "Actual protection of a measure against errors" *with* "The effectiveness of a measure against errors".

Table 1 − Overview of the effectiveness of the various measures on the possible errors

Replace Table 1 (both title and contents) with the following new title and table:

Table 1 – Typical relationships between errors and safety measures

Communication errors	Safety measures						
	Sequence number (see 5.4.2)	Time stamp (see 5.4.3)	Time expectation (see 5.4.4)	Connection authentication (see 5.4.5)	Feedback message (see 5.4.6)	Data integrity assurance (see 5.4.7)	Redundancy with cross checking (see 5.4.8)
Corruption (see 5.3.2)					X [d]	X	X
Unintended repetition (see 5.3.3)	X	X					
Incorrect sequence (see 5.3.4)	X	X					
Loss (see 5.3.5)	X				X		
Unacceptable delay (see 5.3.6)		X	X [b]				
Insertion (see 5.3.7)	X [e]	X [e]		X [a]	X		
Masquerade (see 5.3.8)	X	X		X	X [d]	X	X
Addressing (see 5.3.9)				X			

NOTE Table adapted from IEC 62280:2014, Table 1.

[a] Only for sender identification. Detects only insertion of an invalid source.

[b] Required in all cases.

[c] Void

[d] Effective only if feedback message includes original data or information about the original data, and if the receiver only acts on the data after acknowledging of the feedback message.

[e] Effective only if the sequence numbers or time stamps of the source entities are different.

5.8.5.2.5 Contribution of masquerade errors (RR_M)

Add, at the end of the first paragraph, the following new sentence:

This Equation (3) assumes the SPDU structure differs from the structure of non-safety PDUs in terms of location of the fields of uniqueness.

5.8.6.3 Residual error probability for data integrity RP_I

Add, at the end of the subclause, the following new note:

NOTE Annex I complements Annex B by providing a comprehensive data integrity model using CRC-based error checking.

5.8.12.1 General

Replace, in Note 1 and Note 3, "IEC 62061:2005, 6.11.2.3" *with* "IEC 62061:2021, 6.7.3 and IEC 62061:2021, 6.7.4"*.*

5.12 Safety manual

Add, at the end of the subclause, the following new text and table:

Table 5 lists the summary of topics to be added in the safety manual of products implementing IEC 61784-3-x, if relevant.

Table 5 – Topics for the safety manual of products implementing IEC 61784-3-x

#	Item	Reference	Notes
1	Safety function decomposition PFH, PFDavg	5.1 and 5.8.10	Guidance on the calculations of the PFH or PFDavg for a safety function shall be provided.
2	FSCP installation aspects	5.7	If the safe behaviour of an FSCP or its provided PFH and PFDavg values depend on prerequisites made for the underlying communication channel, these prerequisites should be mentioned in the manual.
		5.8.4	Potential prerequisites include, but are not limited to: • maximum number of safe network endpoints; • maximum number of non-safe network endpoints; • maximum number of network devices (routers, switches); • maximum or minimum safety PDU and non-safety PDU rates; • watchdog time. Where appropriate, it should be explained in the manual how the end user can verify whether the prerequisites are fulfilled or not.
3	Installation guideline	5.11	The requirements for installation of equipment using the communication technologies specified in IEC 61784-3 are specified in IEC 61918 and IEC 61784-5-x.
4	Authenticity	5.8.7.1	According to 5.8.7.1, authenticity requirements shall be met during all communication phases in 5.6 for which connection authentication is relevant. If automatic authenticity checks are not possible for certain phases (e.g. at first-time connection establishment), this shall be documented.
5	Configuration and parameterization	5.8.12.1	Systematic configuration and parameterization errors can only be safely prevented by verification and validation. The safety manuals shall provide the necessary instructions. (Relevant information see IEC 62061:2021, 6.7.3, 6.7.4 and ISO 13849-1:2015, 4.6.4)
6	Electrical safety	5.10.1	The safety manual shall specify the constraints required of the devices connected in a functional safety communication system, whether safety devices or non-safety devices, including active network elements.
7	Security	5.9	Security shall be considered for safety-related applications that include functional safety communication systems. Security of industrial automation and control systems (IACS) is addressed in IEC 62443 (all parts).
8	Safety function response time (SFRT)	D.4.6	Maximum safety function response time specified by the manufacturer and time required to complete a safety-related reaction shall not be exceeded, even in the presence of errors and failures.

15 Communication Profile Family 18 (SafetyNET p™ Fieldbus) – Profiles for functional safety

Delete this clause and Footnote 14.

Add, after Annex H, the following new informative Annex I:

Annex I
(informative)

Comprehensive safety communication channel data integrity model using CRC-based error checking

I.1 Overview

Annex I contains a black channel model for data integrity calculations based on binary symmetric channel in addition to data corruption faults affecting multiple contiguous bits.

For data integrity calculations of safety communication channels, application of the binary symmetric channel (BSC) model alone is useful for evaluating comparisons of CRC-based error checking efficacy. However, it is not sufficient for modeling several data corruption error types.

Annex B recommends use of the BSC model unless a different model can be proven more applicable for a particular functional safety communications protocol (FSCP). This recommendation has a history based on a recognition that alternative models were generally complex and difficult to calculate, and further, using a sufficiently conservative upper limit for bit error probability P_e results in sufficiently conservative values for residual error probability RP_I that can be used to evaluate the relative effectiveness of CRC-based error checking implementations.

This Annex I describes a comprehensive data corruption model which is more applicable than BSC alone for evaluating the data integrity of FSCPs. In addition to single bit error probability (BSC), this comprehensive model accounts for faults that affect multiple data bits with a single fault occurrence. These multiple-bit data faults are a prevalent type of data corruption fault affecting black channels.

This comprehensive data corruption model adds to the BSC model yet is no more complicated to calculate because, like BSC, it uses binary distribution. Further, it demonstrates that using BSC alone, with an upper limit of 10^{-2} for P_e is not sufficiently conservative for evaluating the residual error probability of data corruption errors for FSCPs unless the associated black channel is shown to exhibit only BSC type errors.

I.2 Basic principles

Although the BSC model accounts for some data corruption errors, a number of data error types, where multiple contiguous bits are affected by a single fault, are not addressed with BSC alone.

For example, there are data corruption errors that do not follow the BSC model (see [81]):

- burst errors;
- overwrite errors;
- shift errors;

- message length errors;
- bit slipping errors;
- masquerade errors;
- data errors before bit de-stuffing;
- data errors before symbol decoding;
- data errors before decompression;
- data errors before error correction;
- data errors before decryption.

To account for these multiple-bit error types, a comprehensive channel model for data integrity calculations is needed.

I.3 General case

A comprehensive model has been developed (see [81]) that considers the aforementioned multiple-bit data corruption error cases by applying approximation modeling using uniformly distributed segments (UDS) and superimposes this with the BSC model.

The UDS model treats data corruption errors as affected segments of bits within which the error patterns are uniformly distributed. All possible combinations of affected segment lengths, positions, and bit values occur with equal probability.

In accordance with mathematical analysis, the UDS model is described by means of a binomial distribution with probability parameter p up to 0,5. This UDS model is superimposed with the BSC model (also using binomial distribution) with probability parameter p as described in Annex B (using bit error probability P_e) up to the limit p_{max}^{BSC}.

NOTE 1 p represents a parameter of the binomial distribution for the UDS model, in contrast to its meaning in the BSC model, where, for example, a P_e of 0,5 implies a case where on average one out of two bits is erroneous.

The comprehensive data corruption residual error probability RP_I is given by Equation (I.1).

$$RP_I \leq \max_{0 \leq p \leq p_{max}^{BSC}} RP_I^{Binom}(p) \times (1 - P(f^{UDS})) + \max_{0 \leq p \leq 0,5} RP_I^{Binom}(p) \times P(f^{UDS}) \qquad (I.1)$$

where

RP_I	is the comprehensive data corruption residual error probability;
p_{max}^{BSC}	is the upper limit of the BSC bit error probability;
RP_I^{Binom}	is the residual error probability with binomial distribution;
$P(f^{UDS})$	is the probability of occurrence of a fault causing UDS errors.

In the first summand, a maximum bit error probability (usually 10^{-2}) of the BSC applies. Both summands contain the probability of occurrence of a fault causing UDS errors $P(f^{UDS})$. The worst-case value of 1 shall be used for $P(f^{UDS})$ as shown in Clause I.4. However, FSCPs may specify instead their own values if sufficient proof is provided.

NOTE 2 Actual methods of proof for $P(f^{UDS})$ of less than 1 are beyond the scope of IEC 61784-3.