

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

IECNORM.COM : Click to view the PDF of IEC 61784-3:2021/AMD1:2024



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2024 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 Secretariat
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 It also gives information on projects, replaced and withdrawn publications.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 Products & Services Portal - products.iec.ch

Discover our powerful search engine and read freely all the publications previews, graphical symbols and the glossary. 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 22 500 terminological entries in English and French, with equivalent terms in 25 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 Products & Services Portal - products.iec.ch

Découvrez notre puissant moteur de recherche et consultez gratuitement tous les aperçus des publications, symboles graphiques et le glossaire. 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 22 500 articles terminologiques en anglais et en français, ainsi que les termes équivalents dans 25 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

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 5.8.4	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. 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 $p_{\max}^{\text{BSC}}$.

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).

$$RP_I \leq \max_{0 \leq p \leq p_{\max}^{\text{BSC}}} RP_I^{\text{Binom}}(p) \times (1 - P(f^{\text{UDS}})) + \max_{0 \leq p \leq 0.5} RP_I^{\text{Binom}}(p) \times P(f^{\text{UDS}}) \quad (\text{I.1})$$

where

RP_I is the comprehensive data corruption residual error probability;

$p_{\max}^{\text{BSC}}$ is the upper limit of the BSC bit error probability;

RP_I^{Binom} is the residual error probability with binomial distribution;

$P(f^{\text{UDS}})$ 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 $P(f^{\text{UDS}})$. The worst-case value of 1 shall be used for $P(f^{\text{UDS}})$ 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 $P(f^{\text{UDS}})$ of less than 1 are beyond the scope of IEC 61784-3.

I.4 Upper estimation

For cases where the probability of occurrence for UDS errors $P(f^{UDS})$ is not known, the upper estimation of comprehensive data corruption residual error probability RP_I is applied, given by Equation (I.2).

$$RP_I \leq \max_{0 \leq p \leq 0,5} RP_I^{\text{Binom}}(p) \quad (\text{I.2})$$

NOTE Equation (I.2) is the equivalent of an application of the BSC calculation with P_e up to 0,5.

Bibliography

Renumber Footnote 15 as Footnote 14.

Replace the existing reference [63] to IEC 62061:2005, IEC 62061:2005/AMD1:2012 and IEC 62061:2005/AMD2:2015 with the following new reference:

- [63] IEC 62061:2021, *Safety of machinery – Functional safety of safety-related control systems*

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

- [81] SCHILLER F, et.al., *Enhancement of Safety Communication Model – Preserving the Black Channel Concept*, *Automatisierungstechnik*, vol. 70, no. 1, pp. 38-52. <https://doi.org/10.1515/auto-2021-0098>, De Gruyter, 2022

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

**RÉSEAUX DE COMMUNICATION INDUSTRIELS –
PROFILS –****Partie 3: Bus de terrain de sécurité fonctionnelle –
Règles générales et définitions de profils****AMENDEMENT 1****AVANT-PROPOS**

- 1) La Commission Électrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. À cet effet, l'IEC – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de l'IEC"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. L'IEC collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
- 2) Les décisions ou accords officiels de l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
- 3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
- 4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
- 5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
- 6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
- 7) Aucune responsabilité ne doit être imputée à l'IEC, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de l'IEC, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de l'IEC ou de toute autre Publication de l'IEC, ou au crédit qui lui est accordé.
- 8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
- 9) L'IEC attire l'attention sur le fait que la mise en application du présent document peut entraîner l'utilisation d'un ou de plusieurs brevets. L'IEC ne prend pas position quant à la preuve, à la validité et à l'applicabilité de tout droit de brevet revendiqué à cet égard. À la date de publication du présent document, l'IEC n'a pas reçu notification qu'un ou plusieurs brevets pouvaient être nécessaires à sa mise en application. Toutefois, il y a lieu d'avertir les responsables de la mise en application du présent document que des informations plus récentes sont susceptibles de figurer dans la base de données de brevets, disponible à l'adresse <https://patents.iec.ch>. L'IEC ne saurait être tenue pour responsable de l'identification de ces droits de propriété en tout ou partie.

L'Amendement 1 de l'IEC 61784-3:2021 a été établi par le sous-comité 65C: Réseaux industriels, du comité d'études 65 de l'IEC: Mesure, commande et automation dans les processus industriels.

Le texte de cet Amendement est issu des documents suivants:

Projet	Rapport de vote
65C/1284/FDIS	65C/1291/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à son approbation.

La langue employée pour l'élaboration de cet Amendement est l'anglais.

Ce document a été rédigé selon les Directives ISO/IEC, Partie 2, il a été développé selon les Directives ISO/IEC, Partie 1 et les Directives ISO/IEC, Supplément IEC, disponibles sous www.iec.ch/members_experts/refdocs. Les principaux types de documents développés par l'IEC sont décrits plus en détail sous www.iec.ch/publications/.

Une liste de toutes les parties de la série IEC 61784-3, publiées sous le titre général *Réseaux de communication industriels – Profils – Bus de terrain de sécurité fonctionnelle*, se trouve sur le site web de l'IEC.

Le comité a décidé que le contenu de ce document ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous webstore.iec.ch dans les données relatives au document recherché. À cette date, le document sera

- reconduit,
- supprimé, ou
- révisé.

INTRODUCTION de l'Amendement 1

Le présent Amendement 1 traite des concepts d'un modèle de canal complet pour les calculs d'intégrité des données pour les protocoles de communications de sécurité fonctionnelle (FSCP) tels qu'ils sont spécifiés dans l'IEC 61784-3:2021. Le modèle de canal complet traite des types d'erreurs de corruption de données où plusieurs bits contigus sont affectés par un premier défaut.

Il examine également les relations typiques entre les erreurs possibles et les différentes mesures de sécurité qui peuvent être mises en œuvre.

3 Termes, définitions, symboles, abréviations et conventions

3.1 Termes et définitions

Ajouter le nouveau terme suivant et sa définition:

3.1.55

segment uniformément réparti

UDS

segment d'un message constitué de bits contigus à l'intérieur desquels les configurations d'erreurs sont uniformément réparties

3.2 Symboles et termes abrégés

3.2.1 Termes abrégés

Ajouter, à la fin de la liste, la nouvelle abréviation suivante:

UDS (uniformly distributed segment) segment uniformément réparti

5.4.1 Généralités

Remplacer, au milieu de la phrase, "5.4.9" par "5.4.8".

5.4.9 Différents systèmes d'assurance d'intégrité des données

Supprimer ce paragraphe.

5.5 Relations types entre les erreurs et les mesures de sécurité

Remplacer, au début du deuxième alinéa, "La protection réelle d'une mesure contre les erreurs" par "L'efficacité d'une mesure contre les erreurs".

Tableau 1 – Présentation générale de l'efficacité des différentes mesures sur les erreurs possibles

Remplacer le Tableau 1 (titre et contenu) par le nouveau titre et le nouveau tableau suivants:

Tableau 1 – Relations types entre les erreurs et les mesures de sécurité

Erreurs de communication	Mesures de sécurité						
	Numéro de séquence (voir le 5.4.2)	Horodatage (voir le 5.4.3)	Délai (voir le 5.4.4)	Authentification de connexion (voir le 5.4.5)	Message en retour (voir le 5.4.6)	Assurance d'intégrité des données (voir le 5.4.7)	Redondance avec contre-vérification (voir le 5.4.8)
Corruption (voir le 5.3.2)					X ^d	X	X
Répétition non prévue (voir le 5.3.3)	X	X					
Séquence incorrecte (voir le 5.3.4)	X	X					
Perte (voir le 5.3.5)	X				X		
Retard inacceptable (voir le 5.3.6)		X	X ^b				
Insertion (voir le 5.3.7)	X ^e	X ^e		X ^a	X		
Déguisement (voir le 5.3.8)	X	X		X	X ^d	X	X
Adressage (voir le 5.3.9)				X			
NOTE Tableau adapté selon le Tableau 1 de l'IEC 62280:2014.							
^a Uniquement pour l'identification de l'émetteur. Ne détecte que l'insertion d'une source non valide. ^b Exigé dans tous les cas. ^c Vide ^d Efficace uniquement si le message en retour contient les données d'origine ou des informations sur ces dernières et si le récepteur agit uniquement sur les données après acquittement du message en retour. ^e Efficace uniquement si les numéros de séquence ou les horodatages des entités sources sont différents.							

5.8.5.2.5 Contribution des erreurs de déguisement (RR_M)

Ajouter la nouvelle phrase suivante à la fin du premier alinéa:

Cette Équation (3) repose sur l'hypothèse que la structure SPDU diffère de celle des PDU non relatifs à la sécurité en ce qui concerne l'emplacement des champs d'unicité.

5.8.6.3 Probabilité d'erreurs résiduelles pour l'intégrité des données RP_i

Ajouter, à la fin du paragraphe, la nouvelle note suivante:

NOTE L'Annexe I complète l'Annexe B en fournissant un modèle d'intégrité de données complet qui utilise le contrôle d'erreurs CRC.

5.8.12.1 Généralités

Remplacer, dans la Note 1 et la Note 3, "l'IEC 62061:2005, 6.11.2.3" par "l'IEC 62061:2021, 6.7.3 et l'IEC 62061:2021, 6.7.4".

5.12 Manuel de sécurité

Ajouter, à la fin du paragraphe, le nouveau texte et le nouveau tableau suivants:

Le Tableau 5 contient le résumé des sujets à ajouter dans le manuel de sécurité des produits portant application de l'IEC 61784-3-x, le cas échéant.

Tableau 5 – Sujets destinés au manuel de sécurité des produits portant application de l'IEC 61784-3-x

#	Élément	Référence	Notes
1	Décomposition d'une fonction de sécurité PFH, PFDavg	5.1 et 5.8.10	Les recommandations relatives aux calculs de la PFH ou de la PFDavg pour une fonction de sécurité doivent être fournies.
2	Aspects relatifs à l'installation du FSCP	5.7 5.8.4	Si le comportement de sécurité d'un FSCP ou ses valeurs fournies PFH et PFDavg dépendent de conditions préalables établies pour le canal de communication sous-jacent, il convient de mentionner ces conditions préalables dans le manuel. Les conditions préalables potentielles sont entre autres les suivantes: • nombre maximal de points d'extrémité du réseau de sécurité; • nombre maximal de points d'extrémité du réseau non liés à la sécurité; • nombre maximal d'appareils du réseau (routeurs, commutateurs); • taux maximal ou minimal de PDU de sécurité et de PDU non relatif à la sécurité; • temps de fonctionnement du chien de garde. Le cas échéant, il convient d'expliquer dans le manuel de quelle manière l'utilisateur final peut vérifier si les conditions préalables sont remplies ou non.
3	Guide d'installation	5.11	Les exigences d'installation des matériels qui utilisent les technologies de communication spécifiées dans l'IEC 61784-3 sont spécifiées dans l'IEC 61918 et l'IEC 61784-5-x.
4	Authenticité	5.8.7.1	Conformément au 5.8.7.1, les exigences d'authenticité doivent être respectées pendant toutes les phases de communication indiquées au 5.6 pour lesquelles l'authentification de connexion est pertinente. Si les contrôles automatiques d'authenticité ne sont pas possibles pour certaines phases (par exemple, lors de l'établissement de la première connexion), cela doit être consigné par écrit.
5	Configuration et paramétrage	5.8.12.1	Les erreurs systématiques de configuration et de paramétrage ne peuvent être évitées en toute sécurité que par la vérification et la validation. Les manuels de sécurité doivent donner les instructions nécessaires. (Voir les informations connexes dans l'IEC 62061:2021, 6.7.3, 6.7.4 et l'ISO 13849-1:2015, 4.6.4)
6	Sécurité électrique	5.10.1	Le manuel de sécurité doit spécifier les contraintes exigées des appareils reliés à un système de communication de sécurité fonctionnelle, qu'il s'agisse d'appareils relatifs à la sécurité ou d'appareils non relatifs à la sécurité, dont les éléments de réseau actifs.

#	Élément	Référence	Notes
7	Sûreté	5.9	La sûreté doit être prise en compte pour les applications relatives à la sécurité qui incluent des systèmes de communication de sécurité fonctionnelle. La sûreté des systèmes d'automatisation industrielle et de commande (IACS) est traitée dans l'IEC 62443 (toutes les parties).
8	Temps de réponse de la fonction de sécurité (SFRT, <i>Safety function response time</i>)	D.4.6	Le temps de réponse maximal de la fonction de sécurité spécifié par le fabricant et le temps exigé pour produire une réaction relative à la sécurité ne doivent pas être dépassés, même en présence d'erreurs et de défaillances.

15 Famille de profils de communication 18 (Fieldbus SafetyNET p™) – Profils de sécurité fonctionnelle

Supprimer cet article et la note de bas de page 14.

Ajouter, après l'Annexe H, la nouvelle Annexe I informative suivante:

Annexe I (informative)

Modèle complet d'intégrité des données du canal de communication de sécurité qui utilise le contrôle d'erreurs CRC

I.1 Vue d'ensemble

L'Annexe I comporte un modèle de canal noir pour les calculs d'intégrité des données qui reposent sur un canal symétrique binaire en plus des anomalies de corruption des données affectant plusieurs bits contigus.

Pour les calculs d'intégrité des données des canaux de communication de sécurité, l'application du modèle de canal symétrique binaire (BSC) permet à elle seule d'évaluer les comparaisons de l'efficacité du contrôle d'erreurs CRC. Toutefois, il n'est pas suffisant pour modéliser plusieurs types d'erreurs de corruption de données.

L'Annexe B recommande l'utilisation du modèle BSC, à moins qu'un modèle différent ne s'avère plus approprié pour un protocole de communications de sécurité fonctionnelle (FSCP). L'historique de cette recommandation repose sur la reconnaissance du fait que les modèles alternatifs étaient généralement complexes et difficiles à calculer, et que l'utilisation d'une limite supérieure suffisamment prudente pour la probabilité d'erreurs sur les éléments binaires P_e donne des valeurs suffisamment prudentes pour la probabilité d'erreurs résiduelles RP_1 qui peut être utilisée pour évaluer l'efficacité relative des mises en œuvre du contrôle d'erreurs CRC.

La présente Annexe I décrit un modèle complet de corruption des données qui est plus applicable que le BSC seul pour évaluer l'intégrité des données des FSCP. Outre la probabilité d'erreur sur un élément binaire unique (BSC), ce modèle complet prend en compte les défauts qui affectent plusieurs bits de données lors d'une même occurrence de défaut. Ces anomalies de données de plusieurs bits sont un type courant d'anomalies de corruption de données affectant les canaux noirs.