IEC 61784-3

Edition 3.0 2017-08

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

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 61784-3:2016-05/AMD1:2017-08(en-fr)

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

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

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

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

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

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 It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and also once a month by email.

Electropedia - www.electropedia.org
The world's leading online dictionary of electronic and electrical terms, containing 20 000 terms and definitions in English and French, with equivalent terms in 16 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

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

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

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

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

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

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

IEC Just Published - webstore.iec.ch/justpublished
Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et aussi une fois par mois par email.

Electropedia - www.electropedia.org
Le premier dictionnaire en ligne de termes électroniques et électriques. Il contient 20 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans 16 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

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

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

IEC 61784-3

Edition 3.0 2017-08

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

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

ISBN 978-2-8322-4585-9

FOREWORD

This amendment 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:

FDIS	Report on voting
65C/879/FDIS	65C/886/RVD

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

The committee has decided that the contents of this amendment and the base publication will remain unchanged until the stability date indicated on the IEC website under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

This Amendment 1 discusses the concepts of implicit data safety mechanisms for use in functional safety communications protocols (FSCPs) as specified in IEC 61784-3:2016.

3 Terms, definitions, symbols, abbreviated terms and conventions

3.1 Terms and definitions

Add the following new terms and definitions 3.1.56 and 3.1.57:

3.1.56
explicit data
data that is transmitted

3.1.57
implicit data
additional data that is not transmitted but is known to the sender and receiver

[SOURCE: IEC 62280:2014, 3.1.25]

3.2 Symbols and abbreviated terms

Add two new Subclauses 3.2.1 and 3.2.2, as specified below:

3.2.1 Abbreviated terms

Move the existing list of symbols and abbreviated terms to this new Subclause 3.2.1.

Delete "Pe" and "RP" from the existing list of abbreviated terms. Add, in alphabetical order, in the list of abbreviated terms the following new abbreviated terms:

A-code	Authenticity code
T-code	Timeliness code

3.2.2 Symbols

Add, in this new Subclause 3.2.2 the following list of 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

Add, after Annex F, the following new informative Annex G:

Annex G
(informative)

Implicit data safety mechanisms for IEC 61784-3 functional safety communication profiles (FSCPs)

G.1 Overview

Annex G discusses the concepts of implicit data safety mechanisms for use in functional safety communications protocols (FSCPs) as specified in this standard. Implicit data is that which is not explicitly transmitted in a PDU. Instead, the implicit data values are known by both the sender (source) and the receiver (sink). Implicit data values are validated by the value of one or more transmitted frame check sequence(s) (FCS) which are calculated using an overall data string comprised of the implicit data string appended with the explicit data string. Because the implicit data is not transmitted, the load on the transmission media is reduced.

Today, the FSCPs that use implicit data mechanisms do so in order to communicate complete or partial timeliness codes (T-codes) and/or authenticity codes (A-codes), see Annex E. These FSCPs also use cyclic redundancy check (CRC) algorithms for the frame check sequence (FCS) exclusively. Therefore, Annex G is limited to the analysis of implicitly transmitted T-codes and A-codes using CRC-algorithms.

According to Clause E.8, with regard to implicit data, "Due to the various possible approaches generic formulae cannot be provided. It is up to the individual FSCP to prove sufficient residual error probabilities." In the hope of advancing IEC 61784-3 for the next edition and beyond, the subject of this new Annex G is to improve the understanding of formulating models for the residual error probabilities of FSCPs using CRC-algorithms to implicitly transmit T-codes and A-codes when a single FCS code is used by the protocol.

Presented in Annex G are two formulae examples, applicable for two special cases, and from which a better understanding is promoted for the development of additional (specific and general) formulae.

Also presented is a summation method generally applicable when conditional weight distributions for implicit data error patterns are known and can be quantified in a way either leading to a closed-form solution, or suitable for iterative summation with a reasonably bounded execution time.

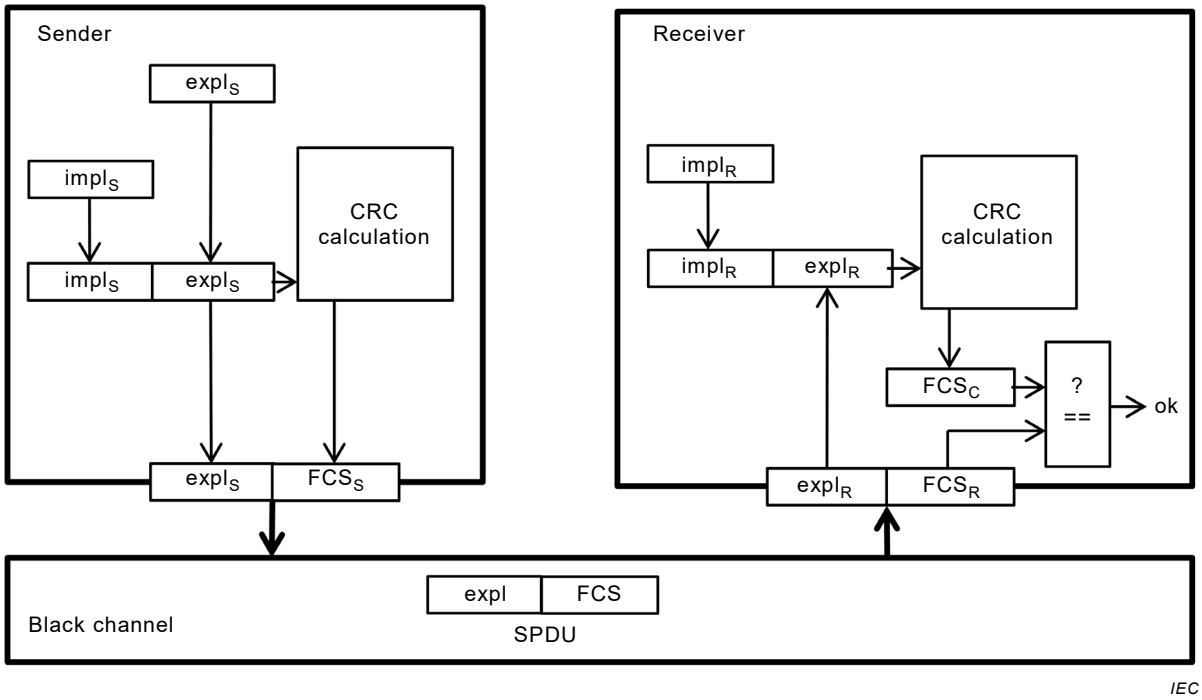
G.2 Basic principles

Calculations in Annex G also use the binary symmetric channel (BSC) model as specified in Annex B.

NOTE 1 Although it does not take into account burst errors, the BSC model with a sufficiently conservative bit error probability is so far the most practical known for use in probability calculations needed for the determination of the FSCP residual error rate.

Figure G.1 shows the basic principle of an FSCP using single FCS protection mechanisms involving implicit data. In the sender, a CRC-checksum over the implicit data $impl_S$ concatenated with the explicit data $expl_S$ is generated, resulting in a frame check sequence FCS_S. When multiple FCS codes are used in an FCSP format, the calculation shall be done for each FCS code. While $expl_S$ and FCS_S are explicitly transmitted over the black channel, $impl_S$ is not transmitted, but impacts the value of the FCS_S. Therefore, it can only contain data whose value is already known to the receiver. Implicit data is used to detect e.g. SPDUs which were misdirected in either space (“authentication error”) or time (“timeliness error”). This is accomplished by deriving the implicit data from the A-code (e.g. connection identifier) and/or the T-code (e.g. sequence number) of an SPDU.

NOTE 2 Initialization details are addressed in F.12.1.



Key Symbols are specified in 3.2.2

Figure G.1 – FSCP with implicit transmission of authenticity and/or timeliness codes

When the SPDU comprising expl and FCS is delivered to the FSCP-layer in the receiver, it may contain transmission errors, i.e. the value delivered may differ from the value sent. For discrimination, the symbols expl$_R$ and FCS$_R$ are used in the receiver.

The expected value of the implicit data is called impl$_R$. In the error free case, this expectation is identical to impl$_S$. In case of, for example, a misdirected SPDU, impl$_R$ and impl$_S$ may differ.

The receiver generates one or more frame check sequence(s) FCS$_C$ by building a CRC-checksum over the concatenation of impl$_R$ and expl$_R$. When each FCS$_C$ is identical to its corresponding FCS$_R$, it is assumed that no error occurred. Otherwise an error has been detected.

The lengths of the bitstrings for a single FCS are defined as follows:

r length of FCS (degree of generator-polynomial);

i length of implicit data (it is assumed that i ≥ r);

e length of explicit data;

n length of SPDU, with n = e + r.

G.3 Problem statement: constant values for implicit data

In FSCPs using implicit data, the CRC-check in the receiver is used for both the detection of data integrity errors as well as the detection of mis-directed or mis-timed SPDUs. Therefore, it may happen that the CRC-mechanism becomes “overburdened” by multiple simultaneous errors, resulting in an increase of the overall residual error probability. This is exemplified in the following scenario in Figure G.2.

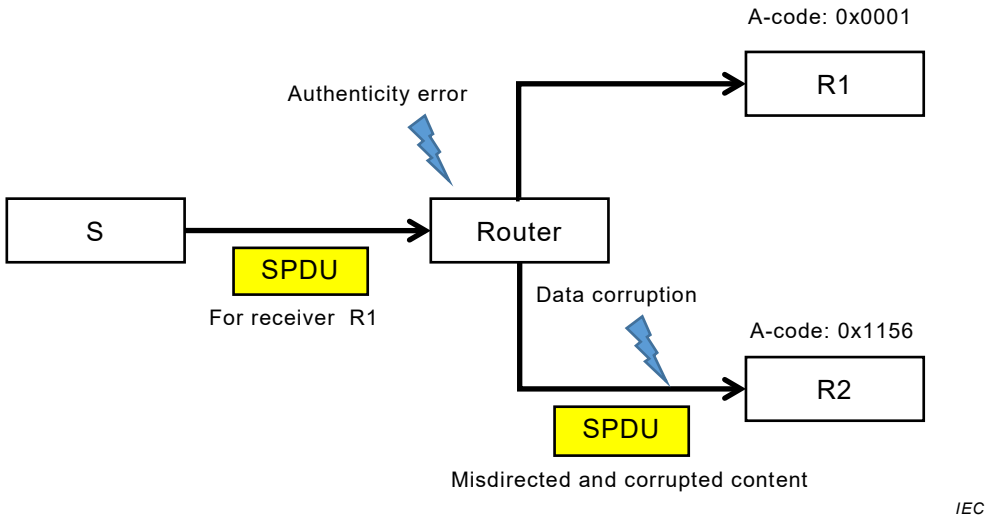


Figure G.2 – Example of an incorrect transmission with multiple error causes

The scenario assumes a sender S sending SPDUs to receiver R1 and receiver R2, using a black channel containing a router. The implicit data used comprises a single field containing an authenticity-code (A-code) of length 16 bits, identifying the receiver (see Figure E.4). For each SPDU sent from S to R1, the A-code of R1 is used as implicit data, and similarly the A-code of R2 for SPDUs sent from S to R2. It is further assumed that the following errors can occur during the transmission of an SPDU.

a) Authenticity error: Due to a fault within the router, the SPDU is delivered to the incorrect receiver (receiver R2 instead of receiver R1 or vice versa). Thus, the implicit authenticity code $impl_S$ used to calculate the FCS_S in the sender is unequal to the expected authenticity code $impl_R$ in the receiver.

b) Data corruption: Due to for example interference or noise on the transmission media, the content of the SPDU is corrupted (expl and/or FCS).

It is further assumed that the black channel itself does not detect any of these errors. Therefore, the errors, and possibly a combination of errors shall be detected by the check within the safety layer of the receiver. The error pattern err_{impl} caused by the authenticity error is defined by the bit-wise exclusive disjunction (XOR) of the A-codes in use. In this case with only two receivers, this error pattern is constant. The error pattern err_{expl} is defined as the bit-wise exclusive disjunction (XOR) of $expl_S$ and $expl_R$. It is modelled by a BSC (see Annex B).

Figure G.3 shows the residual error probabilities for different parameters when using the proper generator polynomial $x^{16}+x^{14}+x^{11}+x^{10}+x^9+x^7+x^5+x^3+x+1$ (0x14EAB) of degree 16.

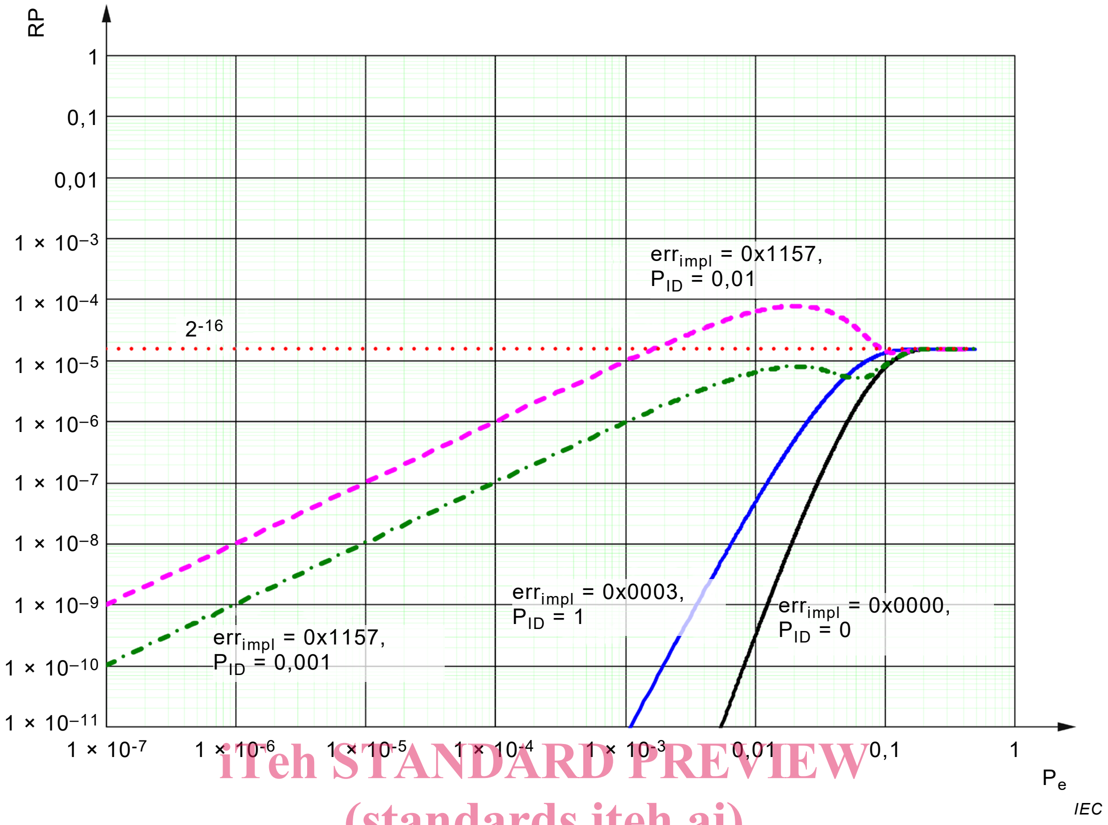


Figure G.3 – Impact of errors in implicit data on the residual error probability

Figure G.3 is based on data which was generated by a brute force algorithm checking all possible error patterns. In addition to the generator polynomial, the following input data was used in the algorithm:

P_{ID} probability of incorrect delivery (here: addressing error);

err_{impl} constant error pattern caused by an addressing error (bitwise disjunction of the A-codes).

It is important to note that the residual error probability does not only depend on p and P_{ID}, but also on the constant err_{impl} and hence on the values of the A-codes chosen during commissioning.

The curve for P_{ID} = 0 (solid black) proves the properness of the generator polynomial. In this case of no errors in implicit data, the residual error probability is always below the limit 2^{-16} and the curve is monotonically increasing.

The dashed purple curve and the dotted-dashed green curve show the characteristics when using A-codes resulting in an err_{impl} of 0x1157 (for example the A-codes 0x0001 and 0x1156). The residual error probability is no longer monotonically increasing but has a maximum greater than 2^{-16}. For $P_{ID} = 10^{-3}$, the corresponding curve (dotted-dashed green) does not pass the limit of 2^{-16}. However, if P_{ID} is set to 10^{-2} (dashed purple), the maximum is greater (worse) than the limit 2^{-16}. As a consequence the limit 2^{-r} cannot be used as an approximation even if the generator polynomial has proven properness for the case P_{ID} = 0.

The green and purple curve is only observed for certain rare values of err_{impl}. For most other values of err_{impl}, the curves are below the limit even for a probability of occurrence P_{ID} = 1. As an example, the curve for err_{impl} = 0x0003 (e.g. A-codes equal to 0x0001 and 0x0002) shows this characteristics (solid blue).

Conclusion: When using implicit transmission mechanisms, the residual error probability is not necessarily bounded by 2^{-r}. This bound is only valid if the FSCP provides additional mechanisms such as the ones shown in the following clauses.

NOTE Improper bounding of an FCS would not necessarily lead to insufficient residual error when other FSCP specific protocol measures are combined in the error detection scheme.

G.4 RP for FSCPs with random, uniformly distributed err_{impl}

G.4.1 General

Clause G.4 investigates the case of a random err_{impl} taking each possible value with equal probability ("uniform distribution"). As seen in Clause G.3 where err_{impl} is constant, this assumption is not always justified and shall be provably guaranteed by the design of the respective FSCP.

As already defined earlier, err_{impl} is the bitwise exclusive disjunction (XOR) between the implicit data $impl_S$ used in the sender of the erroneous packet, and the expected value for the implicit data $impl_R$ in the receiver. Clearly, if $impl_S$ and $impl_R$ are uniformly distributed, independent random variables, also err_{impl} is uniformly distributed, i.e. takes each possible value with equal possibility. However, because errors can be assumed to happen at 'random' points of time, it is also possible to achieve a uniformly distributed err_{impl} if $impl_S$ and $impl_R$ are non-random variables. In order to validate whether err_{impl} follows a uniform distribution, statistical checks such as the Chi-Square-Test or the Kolmogoroff-Smirnoff-Test can be used, (see for example [35]).

NOTE 1 err_{impl} being a uniformly distributed random variable, it does not require that all possible values are observed with equal frequency during a finite interval of time. It is therefore not always possible to evaluate a random number generator by simply counting the number of occurrences within a limited time interval.

Depending on the design of the FSCP, there are two reasonable variants of the assumption "err_{impl} is uniformly distributed":

a) err_{impl} takes each value out of $[0;2^i-1]$ with probability 2^{-i};

b) err_{impl} takes each value out of $[1;2^i-1]$ with probability $1/(2^i-1)$.

NOTE 2 There is a slight difference in the two variants: in the second variant, a value of $err_{impl} = 0$ means that the SPDU was delivered correctly, as an incorrectly delivered SPDU will always result in a value $err_{impl} \neq 0$. In the first variant, a value of $err_{impl} = 0$ does not necessarily imply a correct delivery.

In the second case, measures shall be implemented to ensure that each SPDU is assigned a unique value for implicit data. Hence, the error pattern in case of a misdirected SPDU can never become zero. In the first case, no such measures are implemented and hence the error pattern 'zero' may occur. Clearly, such an error cannot be detected in the receiver unless there are additional detectable data integrity errors or other FSCP specific checks.

In the following, the two variants are shown separately.

Other and perhaps more detailed models are beyond the scope of this document. For example, it is possible to eliminate data error patterns with demonstrated certainty of detection by the CRC polynomial.

EXAMPLE Examples of these data error patterns include: Hamming distances less than the minimum Hamming distance for the CRC polynomial over the data block length; burst errors of length r; odd number of bit errors; and others.

Subclause G.4.2 shows an example where the implicit data field is at least as long as the FCS and the implicit data values are randomly generated in such a way that A-codes are not guaranteed unique for each endpoint, T-codes are not guaranteed unique for each SPDU time, and the combinations of A-code and T-code are not guaranteed unique.

Subclause G.4.3 shows an example where the implicit data field is exactly as long as the FCS and A-codes and T-codes are guaranteed unique for each endpoint and SPDU time. In actual application, additional terms may be necessary to account for exceptions such as T-code wrap around.

Clause G.5 shows a summation method for general applicability when conditional weight distributions for implicit data error patterns are known and can be quantified.

G.4.2 Uniform distribution within the interval [0;2^i-1], i ≥ r

This case applies in particular to FSCPs that use random number generators to derive implicit data values.

At a coarse-grained level, two main types of errors can be discriminated:

- Incorrect content of an SPDU, i. e. data integrity errors;
- Incorrect delivery of an SPDU, i.e. the SPDU is delivered to the wrong receiver or at the wrong instance of time.

In combination, the following disjoint cases can be discriminated:

- Case 1. CC: No error (correct delivery, and correct explicit data);
- Case 2. IC: Incorrect delivery, and correct explicit data;
- Case 3. CI: Correct delivery, and incorrect explicit data;
- Case 4. II: Incorrect delivery, and incorrect data.

The residual error probabilities RP_2, RP_3, and RP_4 for each of the cases 2, 3, and 4 are calculated from the following parameters:

P_{ID} is the "probability of incorrect delivery", i.e. the probability that due to for example an authenticity or timeliness error an SPDU is erroneously delivered to the FSCP;

NOTE 1 The event "incorrect delivery" can result in an $err_{impl} \neq 0$. However, due to the uniform distribution within [0;2^r-1] the case $err_{impl} = 0$ can also occur.

P_{IED} is the probability of incorrect explicit data, i.e. the probability that data corruption occurs;

P_{IC} is the probability that an error is not detected in the receiver under the condition that case 2 occurs;

P_{CI} is the probability that an error is not detected in the receiver under the condition that case 3 occurs;

P_{II} is the probability that an error is not detected in the receiver under the condition that case 4 occurs;

RP_I is the residual error probability for data corruption as defined in Annex F.

R_{CRC} is the residual error probability for CRC polynomials as defined in Equation B.3.

NOTE 2 $RP_I \leq R_{CRC}$ because other safety measures than CRC can further reduce the value of RP_I.

r is the length of the FCS, identical to the degree of the CRC polynomial;

i is the length of the implicit data, with i ≥ r;

n is the number of bits of the SPDU.

Because the events IC, CI, and II are disjoint, the overall residual error probability can be obtained by building the sum of the respective RP_x values.

In general, RP_x is calculated by:

RP_x = P("error case x takes place") × P("error case x is not detectable").