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 It also gives information on projects, replaced and withdrawn publications.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.

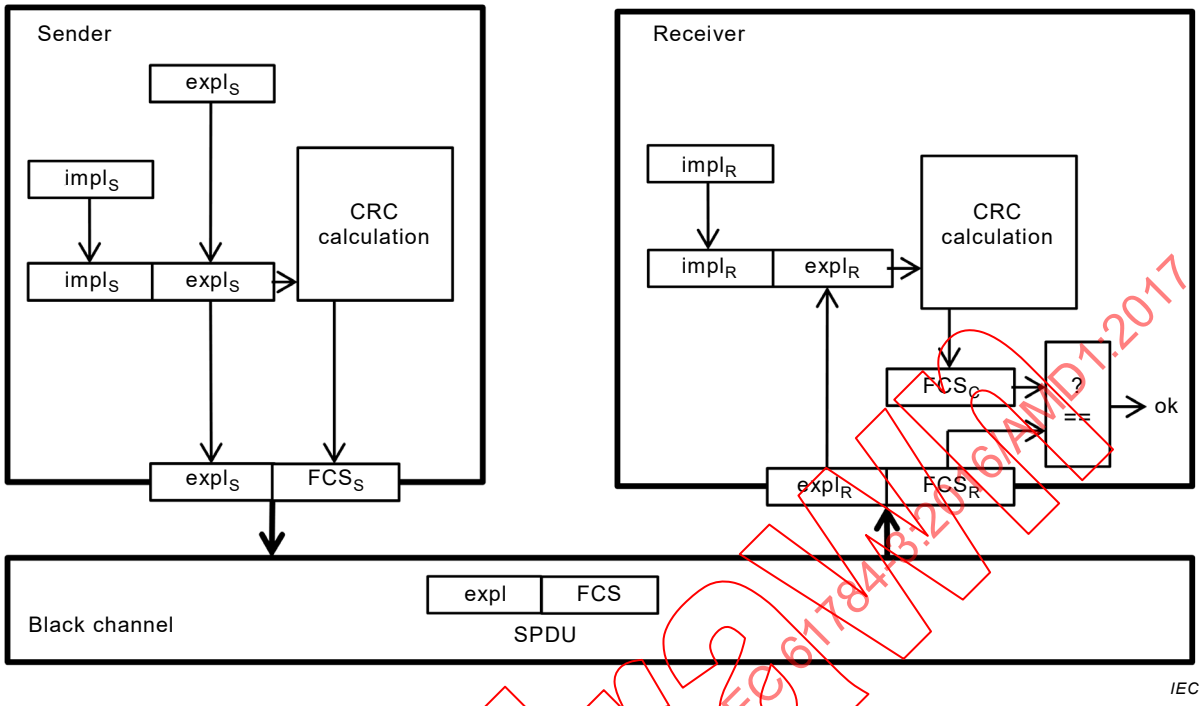
G.2 Basic principles

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.

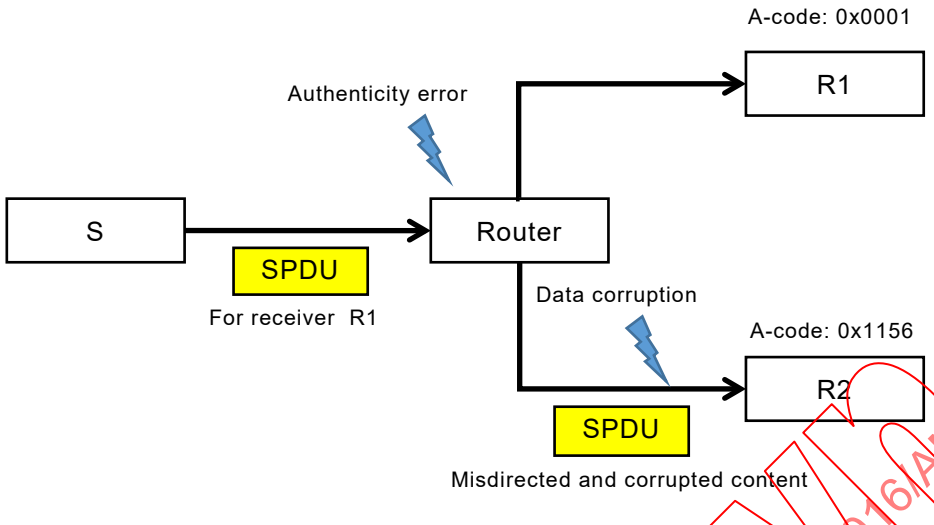


Figure G.2 – Example of an incorrect transmission with multiple error causes

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.

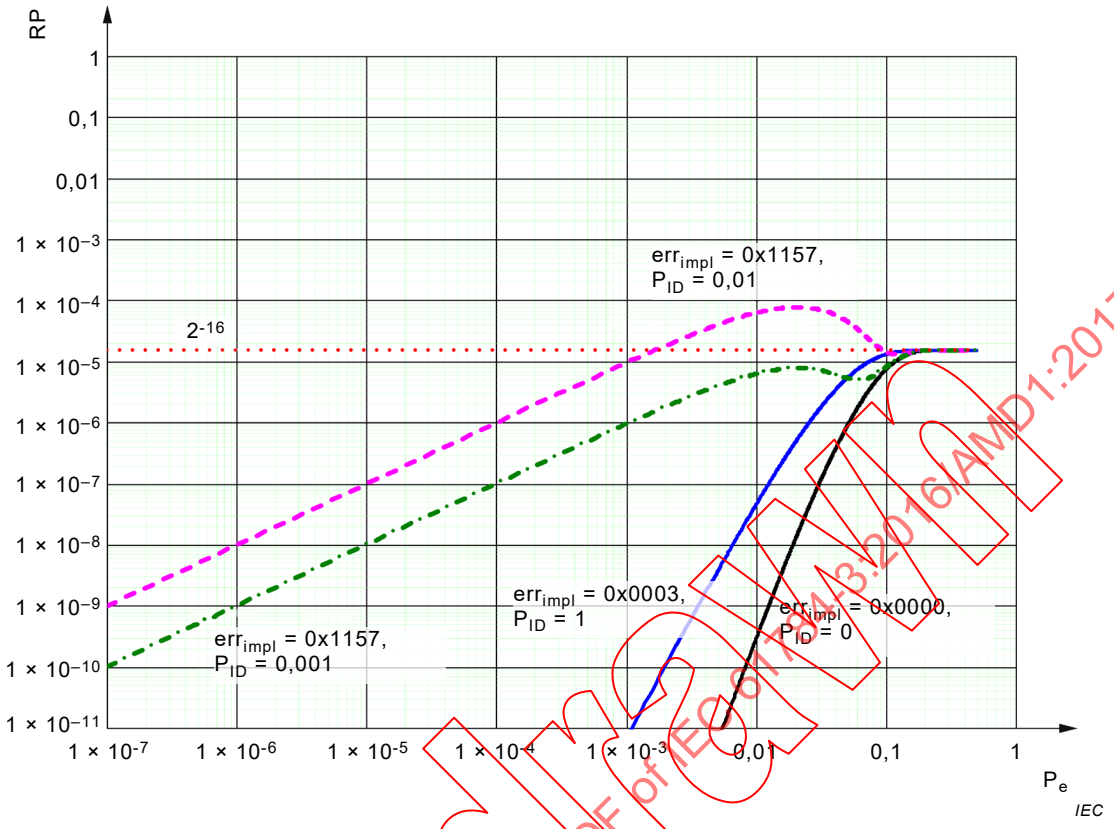


Figure G.3 – Impact of errors in implicit data on the residual error probability

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").

This leads to the formulae for cases 2, 3 and 4 detailed in the following paragraphs.

Case 2 (IC)

$RP_2 = P_{ID} \times (1 - P_{IED}) \times P_{IC}$
$= P_{ID} \times (1 - P_{IED}) \times 2^{-r}$

Explanations on P_{IC}:

- If i > r, this probability is 2^{-r}, because
  - by assumption, the bitwise disjunction of $impl_S$ and $impl_R$ is uniformly distributed in the interval $[0;2^i-1]$;
  - therefore, the bitwise disjunction of $FCS_S = FCS_R$ and FCS_C is uniformly distributed in the interval $[0;2^r-1]$;
  - therefore, the probability that the bitwise disjunction of FCS_R and FCS_C equals zero is 2^{-r};
  - therefore, the probability that FCS_R is equal to FCS_C is 2^{-r}.
- If i = r, this probability is 2^{-r}, because
  - FCS_R is equal to FCS_C, if and only if $err_{impl} = 0$, because the length of err_{impl} does not exceed the degree of the CRC polynomial. CRC-codes detect all burst errors of length less than or equal to r;
  - the probability that $err_{impl} = 0$ is 2^{-r} because of the uniform distribution in the interval $[0;2^r-1]$.

Case 3 (CI)

$RP_3 = (1-P_{ID}) \times P_{IED} \times P_{CI}$
$= (1-P_{ID}) \times RP_I$
$\leq (1-P_{ID}) \times 2^{-r}$ for proper polynomials.

Case 4 (II)

$RP_4 = P_{ID} \times P_{IED} \times P_{II}$
$= P_{ID} \times P_{IED} \times 2^{-r}$

Explanations:

- Due to the assumptions, err_{impl} takes all values from $[0;2^i-1]$ with equal probability.
- Hence, each bit of err_{impl} takes the value 0 or 1 with equal probability 0,5.
- Because CRC-codes are linear codes, and because $|err_{impl}| \geq r$, each bit of err_{impl} determines the result of one bit in the bitwise exclusive disjunction of FCS_R and FCS_C.
- Hence, the bits in the bitwise exclusive disjunction of FCS_R and FCS_C can be treated as independent random variables, each taking the values 0 and 1 with equal probability 0,5.
- The bitwise exclusive disjunction of FCS_R and FCS_c is a uniformly distributed random variable, taking all values from $[0;2^r-1]$ with equal probability.
- The probability that the bitwise exclusive disjunction of FCS_R and FCS_C equals zero is 2^{-r}.
- The probability that FCS_C is identical to FCS_R is 2^{-r}.

In summary, the residual error probability of an FSCP using implicit mechanisms for the detection of timeliness and authenticity error (guaranteeing that the error in the implicit data is uniformly distributed in the interval $[0;2^i-1]$ can be calculated using the following formula:

RP_{TOTAL} = RP2 + RP3 + RP4
= $(P_{ID} \times (1 - P_{IED}) \times 2^{-r}) + ((1-P_{ID}) \times P_{IED} \times P_{CI}) + (P_{ID} \times P_{IED} \times 2^{-r})$
= $(P_{ID} \times 2^{-r}) + ((1-P_{ID}) \times P_{IED} \times P_{CI})$
= $(P_{ID} \times 2^{-r}) + ((1-P_{ID}) \times RP_I)$

Explanation:

- Cases 2 to 4 are disjoint events.

In case of a proper polynomial, the following applies:

RP_{TOTAL} = RP2 + RP3 + RP4
= $(P_{ID} \times (1 - P_{IED}) \times 2^{-r}) + ((1-P_{ID}) \times P_{IED} \times P_{CI}) + (P_{ID} \times P_{IED} \times 2^{-r})$
≤ $(P_{ID} \times (1 - P_{IED}) \times 2^{-r}) + ((1-P_{ID}) \times 2^{-r}) + (P_{ID} \times P_{IED} \times 2^{-r})$
≤ 2^{-r}

Explanations:

- Cases 2 to 4 are disjoint events.
- This upper bound of RP_{TOTAL} is independent of the values of P_{IED} and P_{ID}.

G.4.3 Uniform distribution in the interval [1;2^r-1], i = r

For this variant, it is assumed i = r, i.e. the length of the implicit data is exactly the degree of the CRC polynomial, and that err_{impl} is uniformly distributed within the interval [1;2^r-1]. In contrast to the variant shown in G.4.2, err_{impl} is always unequal to 0 in case of an incorrect delivery.

The following cases of error combinations 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 Due to the uniform distribution within [1;2^r-1], $err_{impl} \neq 0$ is guaranteed. Hence, the event "incorrect delivery" is equivalent to the event "incorrect implicit data" in this case.

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;

$P_{EIC}(i)$ is the probability that the error pattern in the explicit data err_{expl} complements the error pattern in the implicit data err_{impl} making the error undetectable, under the condition that "err_{impl} = i";

r is the length of the implicit data and the length of the FCS (degree of the CRC polynomial);

n is the number of bits in 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").

This leads to the formulae for cases 2, 3 and 4 detailed in the following paragraphs.

Case 2 (IC)

$$RP_2 = P_{ID} \times (1 - P_{IED}) \times P_{IC}$$
$$= 0$$

Explanation:

- Errors of type 2 are always detected, because the length of err_{impl} does not exceed r. CRC-codes detect all burst errors of length less than or equal to r. Hence P_{IC} is equal to 0 in this case.

Case 3 (CI)

$$RP_3 = (1-P_{ID}) \times P_{IED} \times P_{CI}$$
$$= (1-P_{ID}) \times RP_I$$
$$\leq (1-P_{ID}) \times 2^{-r} \text{ for proper polynomials.}$$

Case 4 (II)

$$RP_4 = P_{ID} \times P_{IED} \times P_{II}$$
$$\approx P_{ID} \times P_{IED} \times 2^{-r}$$

Explanations:

- $$P_{II} = \sum_{i=1}^{2^r-1} P\{err_{impl} = i\} \times P_{EIC}(i)$$
$$= \sum_{i=1}^{2^r-1} \frac{1}{2^r-1} \times P_{EIC}(i)$$
$$= \frac{1}{2^r-1} \times \sum_{i=1}^{2^r-1} P_{EIC}(i)$$
$$= \frac{1}{2^r-1} \text{ (because for all possible } err_{expl} \text{ there is exactly one matching } err_{impl})$$
$$\approx 2^{-r}$$

In summary, the residual error probability of an FSCP using implicit mechanisms for the detection of timeliness and authenticity error guaranteeing that the error in the implicit data is uniformly distributed in the interval $[1;2^r-1]$, can be calculated using the following formula:

$$RP_{TOTAL} = RP2 + RP3 + RP4$$
$$= (P_{ID} \times (1 - P_{IED}) \times 2^{-r}) + ((1-P_{ID}) \times P_{IED} \times P_{CI}) + (P_{ID} \times P_{IED} \times 2^{-r})$$
$$= (P_{ID} \times 2^{-r}) + ((1-P_{ID}) \times P_{IED} \times P_{CI})$$

$= (P_{ID} \times 2^{-r}) + ((1-P_{ID}) \times RP_I)$

Explanation:

- Cases 2 to 4 are disjoint events.

G.5 General case

The calculations presented in G.4.2 and G.4.3 are only valid under the assumption of a uniform distribution of err_{impl} and with certain restrictions on the length of the implicit data field. In the general case, RP_{TOTAL} can be calculated as follows, if the conditional weight distribution of the code is known for each possible value of err_{impl}.

$$RP_{TOTAL} = P_{ID} \times \sum_{j=0}^{2^i-1} P\{ err_{impl} = j\} \times P\{ FCS_C = FCS_R \mid err_{impl} = j\} + (1-P_{ID}) \times P_{re}^{CRC,BSC}$$

where

$P\{ err_{impl} = j\}$ is the probability that the error pattern in implicit data has the value j (under the condition that there is a misdirected SPDU);

$P\{ FCS_C = FCS_R \mid err_{impl} = j\}$ is the probability that no error is indicated for the given CRC-polynomial and code length under the condition that the error pattern in implicit data has the value j;

$P_{re}^{CRC,BSC}$ is the residual error probability for the given CRC-polynomial and code length without implicit data.

$P_{re}^{CRC,BSC}$ and $P\{ FCS_C = FCS_R \mid err_{impl} = j\}$ are given by:

$$P_{re}^{CRC,BSC} = \sum_{k=1}^{n} A_k(err_{impl} = 0) \times P_e^k \times (1-P_e)^{n-k}$$

$$P\{ FCS_C = FCS_R \mid err_{impl} = j\} = \sum_{k=0}^{n} A_k(err_{impl} = j) \times P_e^k \times (1-P_e)^{n-k}$$

where

$A_k(err_{impl} = j)$ is the weight distribution of the code under the condition that the error pattern in the implicit data takes the value j.

Explanations:

- $P\{ FCS_C = FCS_R \mid err_{impl} = 0\} = P_{re}^{CRC,BSC} + (1-P_e)^n$.

G.6 Calculation of P_{ID}

If both the T-code and the A- code are implicit, P_{ID} can be calculated as follows:

$$P_{ID} = \min\left(\frac{R_T + R_A}{\nu}, 1\right)$$

where

P_{ID} is the probability that due to for example an authenticity or timeliness error an SPDU is erroneously delivered to the FSCP;

R_T is the rate of occurrence for incorrect sequence safety PDUs (see F.5.2.4);

R_A is the rate of occurrence for misdirected safety PDUs (see F.5.2.3);

v is the maximum number of SPDU samples by the SCL ("sample rate") per hour (see F.5.2.2).

Explanation:

- Due to approximation, $R_T + R_A$ may become greater than one. In this case, the value 1 shall be used for P_{ID}.

If only the T-code is implicit, P_{ID} can be calculated as follows:

$$P_{ID} = \frac{R_T}{v}$$

If only the A-code is implicit, P_{ID} can be calculated as follows:

$$P_{ID} = \frac{R_A}{v}$$

Calculation of the total residual error rate

According to F.10.1, the total residual error rate is calculated by (see Equation (F.6)):

$$\lambda_{SC} = RR_T + RR_A + RR_I + RR_M$$

Alternatively, the following formula can be used:

$$\lambda_{SC} = v \times RP_{TOTAL}$$

Bibliography

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

[35] D. KNUTH, *The Art of Computer Programming, Volume 2: Seminumerical Algorithms*, 3rd Edition, Addison-Wesley, 1997

AVANT-PROPOS

Le présent amendement 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:

FDIS	Rapport de vote
65C/879/FDIS	65C/886/RVD

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

Le comité a décidé que le contenu de cet amendement et de la publication de base ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous "http://webstore.iec.ch" dans les données relatives à la publication recherchée. A cette date, la publication sera

- reconduite,
- supprimée,
- remplacée par une édition révisée, ou
- amendée.

IMPORTANT – Le logo *"colour inside"* qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.

INTRODUCTION

Le présent Amendement 1 traite des concepts de mécanismes de sécurité reposant sur des données implicites destinés à être utilisés dans les protocoles de communication de sécurité fonctionnelle (FSCP, *functional safety communications protocols*) spécifiés dans l'IEC 61784-3:2016.

3 Termes, définitions, symboles, abréviations et conventions

3.1 Termes et définitions

Ajouter les nouveaux termes et définitions 3.1.56 et 3.1.57 suivants:

3.1.56
données explicites
données qui sont transmises

3.1.57
données implicites
données additionnelles qui ne sont pas transmises, mais sont connues de l'émetteur et du récepteur

[SOURCE: IEC 62280:2014, 3.1.25]

3.2 Symboles et abréviations

Ajouter deux nouveaux Paragraphes 3.2.1 et 3.2.2, comme spécifié ci-dessous.

3.2.1 Abréviations

Déplacer la liste existante des symboles et abréviations dans ce nouveau Paragraphe 3.2.1.

Supprimer “Pe” *et* “RP” *de la liste existante des abréviations. Ajouter, dans l'ordre alphabétique, les nouvelles abréviations suivantes à la liste des abréviations:*

Code A	Code d'authenticité
Code T	Code d'opportunité

3.2.2 Symboles

Ajouter, dans ce nouveau Paragraphe 3.2.2, la liste des symboles suivants:

A_k	Répartition du poids du code: nombre de mots de code valides à k bits définis sur "un"
e	Longueur binaire des données explicites
err_{impl}	Disjonction bit à bit de $impl_S$ et $impl_R$
expl	Données explicites
$expl_R$	Données explicites côté récepteur
$expl_S$	Données explicites côté émetteur
FCS_C	Séquence de contrôle de trame calculée au niveau du récepteur
FCS_R	Séquence de contrôle de trame reçue
FCS_S	Séquence de contrôle de trame émise
i	Longueur binaire des données implicites

ID	Remise incorrecte (*Incorrect Delivery*)
$impl_R$	Données implicites côté récepteur
$impl_S$	Données implicites côté émetteur
n	Longueur binaire du SPDU
P_e	Probabilité d'erreurs sur les éléments binaires
P_{ID}	Probabilité de remise incorrecte
r	Longueur binaire de la FCS (degré de polynôme générateur)
RP	Probabilité d'erreurs résiduelles

Ajouter, à la suite de l'Annexe F, la nouvelle Annexe informative G suivante:

Annexe G
(informative)

Mécanismes de sécurité reposant sur des données implicites pour les profils de communication de sécurité fonctionnelle (FSCP) définis dans l'IEC 61784-3

G.1 Vue d'ensemble

L'Annexe G traite des concepts de mécanismes de sécurité reposant sur des données implicites destinés à être utilisés dans les protocoles de communication de sécurité fonctionnelle (FSCP) spécifiés dans la présente norme. Les données implicites sont les données qui ne sont pas explicitement transmises dans un PDU. Au lieu de cela, les valeurs des données implicites sont connues à la fois de l'émetteur (source) et du récepteur (collecteur). Les valeurs des données implicites sont validées par la valeur d'une ou plusieurs séquences de contrôle de trame (FCS, *Frame Check Sequence*) calculées à l'aide d'une chaîne de données globale constituée de la chaîne de données implicites à laquelle est accolée la chaîne de données explicites. Les données implicites n'étant pas transmises, la charge sur le support de transmission s'en trouve réduite.

Aujourd'hui, les FSCP qui utilisent des mécanismes reposant sur des données implicites s'en servent pour communiquer des codes d'opportunité (codes T) complets ou partiels et/ou des codes d'authenticité (codes A), voir l'Annexe E. Ces FSCP utilisent également des algorithmes de contrôle de redondance cyclique (CRC) exclusivement pour la séquence de contrôle de trame (FSC). Par conséquent, l'Annexe G est limitée à l'analyse des codes A et des codes T transmis implicitement à l'aide d'algorithmes de CRC.

Conformément à l'Article E.8, concernant les données implicites, "En raison de la diversité des méthodes possibles, aucune formule générique ne peut être fournie. Il incombe au FSCP individuel de démontrer des probabilités d'erreurs résiduelles suffisantes." Dans la perspective de faire évoluer l'IEC 61784-3 pour la prochaine édition et les suivantes, cette nouvelle Annexe G a pour objet d'approfondir la compréhension des modèles de formulation pour les probabilités d'erreurs des FSCP utilisant des algorithmes de CRC afin d'assurer la transmission implicite de codes T et de codes A lorsqu'un code FCS unique est utilisé par le protocole.

L'Annexe G propose deux exemples de formules applicables pour deux cas spécifiques, qui permettent de mieux comprendre les modèles de formulation afin de développer de nouvelles formules (spécifiques et générales).

Elle propose également une méthode d'addition généralement applicable lorsque les répartitions du poids conditionnel pour les configurations d'erreurs dans les données implicites sont connues et peuvent être quantifiées de manière à obtenir une solution en forme fermée, ou bien de manière adaptée à une addition itérative avec un temps d'exécution aux limites raisonnables.

G.2 Principes de base

Les calculs donnés dans l'Annexe G utilisent également le modèle de canal symétrique binaire (BSC, *binary symmetric channel*) spécifié dans l'Annexe B.

NOTE 1 Bien qu'il ne tienne pas compte des erreurs en rafale, le modèle BSC avec une probabilité d'erreurs sur les éléments binaires estimée suffisante est le moyen le plus pratique actuellement connu pour réaliser les calculs de probabilités nécessaires à déterminer le taux d'erreurs résiduelles du FSCP.

La Figure G.1 représente le principe de base d'un FSCP utilisant des mécanismes de protection FCS simples impliquant des données implicites. Côté émetteur, une somme de

contrôle CRC sur les données implicites $impl_S$ concaténées avec les données explicites $expl_S$ est générée, formant ainsi une séquence de contrôle de trame FCS_S. Lorsque plusieurs codes FCS sont utilisés dans un format FSCP, le calcul doit être réalisé pour chaque code FCS. Lorsque $expl_S$ et FCS_S sont transmis explicitement par le canal noir, $impl_S$ n'est pas transmise, mais influe sur la valeur de FCS_S. Par conséquent, elle ne peut contenir que des données dont la valeur est déjà connue du récepteur. Des données implicites sont utilisées pour détecter, par exemple, des SPDU mal acheminés dans l'espace ("erreur d'authentification") ou le temps ("erreur d'opportunité"). Cette opération est accomplie par dérivation des données implicites à partir du code A (par exemple, un identifiant de connexion) et/ou le code T (par exemple, un numéro de séquence) d'un SPDU.

NOTE 2 Les détails d'initialisation font l'objet du F.12.1.

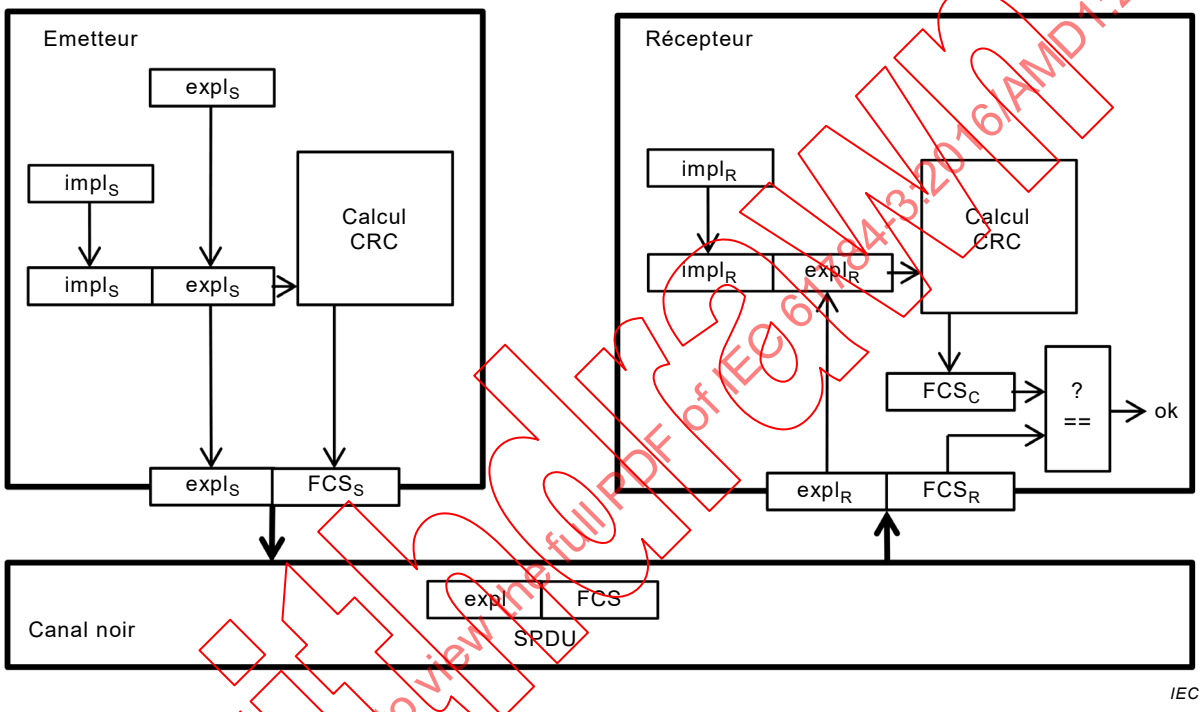


Figure G.1 – FSCP à transmission implicite de codes d'authenticité et/ou d'opportunité

Lorsque le SPDU comprenant expl et FCS est transmis à la couche FSCP dans le récepteur, elle peut contenir des erreurs de transmission, c'est-à-dire que la valeur d'arrivée peut différer de la valeur envoyée. A des fins de distinction, les symboles $expl_R$ et FCS_R sont utilisés dans le récepteur.

La valeur attendue des données implicites est appelée $impl_R$. En cas d'absence d'erreur, cette valeur est identique à $impl_S$. En cas, par exemple, d'erreur d'acheminement d'un SPDU, $impl_R$ et $impl_S$ peuvent différer.

Le récepteur génère une ou plusieurs séquences de contrôle de trame FCS_C en créant une somme de contrôle CRC pour la concaténation de $impl_R$ et $expl_R$. Lorsque chaque FCS_C est identique à la valeur FCS_R correspondante, l'hypothèse selon laquelle aucune erreur ne s'est produite est retenue. Autrement, une erreur a été détectée.

Les longueurs des chaînes de bits pour un FCS unique sont définies comme suit:

r longueur de la FCS (degré de polynôme générateur);

i longueur des données implicites (l'hypothèse retenue est: $i \geq r$);

e longueur des données explicites;

n longueur du SPDU, avec n = e + r.

G.3 Enoncé du problème: valeurs constantes pour les données implicites

Dans les FSCP utilisant des données implicites, le contrôle CRC côté récepteur est utilisé pour la détection d'erreurs concernant l'intégrité des données, l'acheminement ou encore l'opportunité des SPDU. Par conséquent, il peut arriver que le mécanisme de CRC soit "surchargé" par de multiples erreurs simultanées, ce qui conduit à une augmentation de la probabilité globale d'erreurs résiduelles. Un exemple de ce cas est représenté dans le scénario suivant, à la Figure G.2.

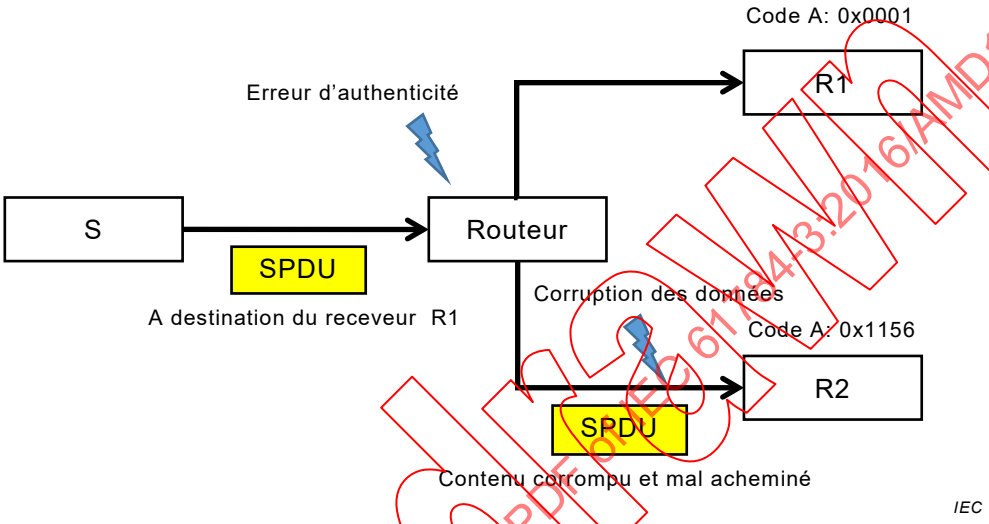


Figure G.2 – Exemple de transmission incorrecte due à des causes d'erreur multiples

Le scénario prend l'hypothèse d'un émetteur S envoyant des SPDU à un récepteur R1 et à un récepteur R2 via un canal noir contenant un routeur. Les données implicites utilisées comportent un champ unique contenant un code d'authenticité (code A) de 16 bits, identifiant le récepteur (voir Figure E.4). Pour chaque SPDU transmis de S à R1, le code A de R1 est utilisé comme donnée implicite, de la même manière que le code A de R2 pour les SPDU transmis de S à R2. De plus, il est pris pour hypothèse que les erreurs suivantes peuvent se produire lors de la transmission d'un SPDU.

a) Erreur d'authenticité: En raison d'une anomalie dans le routeur, le SPDU est transmis au mauvais récepteur (soit le récepteur R2 au lieu du récepteur R1, ou inversement). Ainsi, le code d'authenticité implicite $impl_S$ utilisé pour calculer le FCS_S côté émetteur n'est pas égal au code d'authenticité attendu $impl_R$ côté récepteur.

b) Corruption des données: En raison, par exemple, d'interférences ou de bruits sur le support de transmission, le contenu du SPDU est corrompu (expl et/ou FCS).

De plus, il est pris pour hypothèse que le canal noir lui-même ne détecte aucune de ces erreurs. Par conséquent, les erreurs, et potentiellement une combinaison d'erreurs, doivent être détectées par la vérification réalisée dans la couche de sécurité du récepteur. La configuration d'erreur err_{impl} provoquée par l'erreur d'authenticité est définie par la disjonction exclusive (XOR) bit à bit des codes A utilisés. Dans le cas représenté, à deux récepteurs seulement, cette configuration d'erreur est constante. La configuration d'erreur err_{expl} est définie comme la disjonction exclusive (XOR) bit à bit de $expl_S$ et $expl_R$. Elle est modélisée par un BSC (voir l'Annexe B).

La Figure G.3 représente les probabilités d'erreurs résiduelles pour différents paramètres lors de l'utilisation du polynôme générateur exact $x^{16}+x^{14}+x^{11}+x^{10}+x^9+x^7+x^5+x^3+x+1$ (0x14EAB) de degré 16.

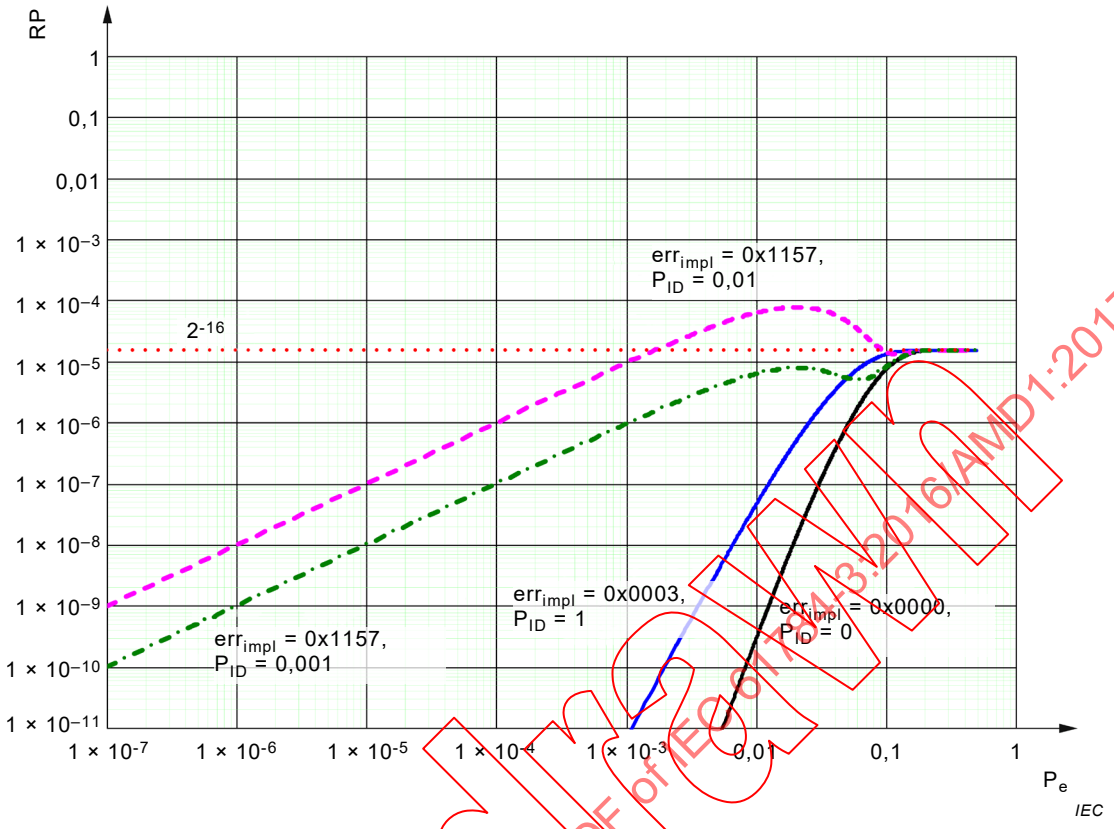


Figure G.3 – Influence des erreurs dans les données implicites sur la probabilité d'erreurs résiduelles

La Figure G.3 s'appuie sur des données générées par un algorithme exhaustif de vérification de toutes les configurations d'erreur possible. En plus du polynôme générateur, les données d'entrée suivantes ont été utilisées dans l'algorithme:

P_{ID} probabilité de remise incorrecte (ici: erreur d'adressage);

err_{impl} configuration d'erreur constante provoquée par une erreur d'adressage (disjonction bit à bit des codes A).

Il est important de noter que la probabilité d'erreurs résiduelles ne dépend pas seulement de p et de P_{ID}, mais également de la constance de la variable err_{impl}, et donc des valeurs des codes A choisies pendant la mise en service.

La courbe correspondant à P_{ID} = 0 (noir continu) démontre l'exactitude du polynôme générateur. Dans ce cas où aucune erreur n'est détectée dans les données implicites, la probabilité d'erreurs résiduelles est toujours inférieure à la limite de 2^{-16} et la courbe augmente de façon monotone.

La courbe en tirets violets et la courbe en pointillés verts représentent les caractéristiques associées à une utilisation de codes A résultant en une variable err_{impl} de 0x1157 (par exemple, les codes A 0x0001 et 0x1156). La probabilité d'erreurs résiduelles n'augmente plus de manière monotone mais présente une valeur maximale supérieure à 2^{-16}. Pour $P_{ID}=10^{-3}$, la courbe (pointillés verts) ne dépasse pas la limite de 2^{-16}. Cependant, si P_{ID} est défini sur 10^{-2} (tirets violets), la valeur maximale est supérieure à la limite 2^{-16} (soit un cas défavorable). Par conséquent, la limite 2^{-r} ne peut pas être utilisée comme approximation même si l'exactitude du polynôme générateur a été démontrée pour le cas P_{ID} = 0.

Les courbes verte et violette sont observées seulement pour certaines valeurs rares de err_{impl}. Pour la plupart des autres valeurs de err_{impl}, les courbes se situent en dessous de la limite, même pour une probabilité d'occurrence P_{ID} = 1. Par exemple, la courbe correspondant

à err_{impl} = 0x0003 (par exemple, codes A égaux à 0x0001 et 0x0002) représente ces caractéristiques (bleu continu).

Conclusion: Lorsque des mécanismes de transmission implicites sont utilisés, la probabilité d'erreurs résiduelles n'est pas nécessairement limitée par 2^{-r}. Cette limite est valide seulement si le FSCP fournit des mécanismes supplémentaires tels que ceux indiqués dans les articles suivants.

NOTE La limitation incorrecte d'un FCS n'entraînerait pas nécessairement une erreur résiduelle insuffisante lorsque d'autres mesures de protocole spécifiques au FSCP sont associées dans le schéma de détection d'erreurs.

G.4 RP pour les FSCP avec une variable err_{impl} aléatoire et uniformément répartie

G.4.1 Généralités

L'Article G.4 examine le cas d'une variable err_{impl} aléatoire en accordant une probabilité égale à chaque valeur possible ("répartition uniforme"). Comme indiqué dans l'Article G.3, où err_{impl} est constante, cette hypothèse n'est pas toujours justifiée et doit être garantie de manière démontrable par la conception du FSCP correspondant.

Comme défini ci-dessus, err_{impl} est la disjonction exclusive (XOR) bit à bit entre les données implicites $impl_S$ utilisées côté émetteur du paquet erroné et la valeur attendue pour les données implicites $impl_R$ côté récepteur. Clairement, si $impl_S$ et $impl_R$ sont uniformément distribuées, des variables aléatoires indépendantes, soit err_{impl}, sont uniformément réparties, c'est-à-dire qu'elles adoptent chaque valeur possible selon une possibilité égale. Cependant, dans la mesure où l'hypothèse selon laquelle les erreurs se produisent à des points "aléatoires" dans le temps peut être retenue, il est également possible d'assurer la répartition uniforme de err_{impl} si $impl_S$ et $impl_R$ sont des variables non aléatoires. Afin de confirmer si err_{impl} adopte une répartition uniforme, des vérifications statistiques telles que le test du khi carré ou le test de Kolmogoroff-Smirnoff peuvent être utilisées (voir par exemple [35]).

NOTE 1 La variable err_{impl} étant répartie de manière uniforme, elle ne requiert pas que toutes ses valeurs possibles soient observées à fréquence égale pendant un intervalle de temps fini. Par conséquent, il n'est pas toujours possible d'évaluer un générateur de nombres aléatoires par simple décompte du nombre d'occurrences dans un intervalle de temps limité.

En fonction de la conception du FSCP, il existe deux variantes raisonnables de l'hypothèse "err_{impl} est uniformément répartie":

a) err_{impl} adopte chaque valeur hors de l'intervalle $[0;2^i-1]$ selon une probabilité de 2^{-i};

b) err_{impl} adopte chaque valeur hors de l'intervalle $[1;2^i-1]$ selon une probabilité de $1/(2^i-1)$.

NOTE 2 Il existe une légère différence entre les deux variantes: dans la seconde variante, la valeur err_{impl} = 0 indique que le SPDU a été transmis correctement, car une erreur de remise de SPDU se traduit systématiquement par une valeur $err_{impl} \neq 0$. Dans la première variante, la valeur err_{impl} = 0 n'implique pas nécessairement une remise correcte.

Dans le second cas, des mesures doivent être mises en œuvre pour garantir qu'une valeur unique pour les données implicites soit attribuée à chaque SPDU. Par conséquent, la configuration d'erreur en cas de SPDU mal acheminé ne peut jamais être égale à zéro. Dans le premier cas, aucune mesure de ce type n'est mise en œuvre, la configuration d'erreur "zéro" peut donc se produire. Clairement, une telle erreur ne peut pas être détectée côté récepteur à moins qu'il n'existe des erreurs d'intégrité de données détectables supplémentaires ou d'autres vérifications spécifiques aux FSCP.

Les deux variantes sont représentées séparément ci-après.

Les autres modèles, potentiellement plus détaillés, se situent hors du domaine d'application du présent document. Par exemple, il est possible d'éliminer des configurations d'erreur dans les données avec une certitude de détection démontrée à l'aide du polynôme de CRC.

EXEMPLE Les distances de Hamming inférieures aux distances de Hamming minimales pour le polynôme de CRC sur la longueur du bloc de données, les erreurs en rafale de longueur r, un nombre impair d'erreurs dans les bits, etc., sont des exemples de ces configurations d'erreur dans les données.

Le Paragraphe G.4.2 donne un exemple dans lequel le champ des données implicites est au moins aussi long que le FCS et les valeurs des données implicites sont générées aléatoirement de telle sorte que l'unicité des codes A n'est pas garantie pour chaque point d'extrémité, que l'unicité des codes T n'est pas garantie pour chaque temps de SPDU, et que l'unicité des combinaisons de codes A et de codes T n'est pas garantie.

Le Paragraphe G.4.3 donne un exemple dans lequel le champ des données implicites est exactement aussi long que la FCS et l'unicité des codes A et des codes T est garantie pour chaque point d'extrémité et chaque temps de SPDU. En application réelle, des termes supplémentaires peuvent être nécessaires pour tenir compte des exceptions, par exemple un bouclage de code T.

L'Article G.5 donne une méthode d'addition généralement applicable lorsque les répartitions du poids conditionnel pour les configurations d'erreurs dans les données implicites sont connues et peuvent être quantifiées.

G.4.2 Répartition uniforme dans l'intervalle $[0;2^i-1]$, $i \geq r$

Ce cas s'applique en particulier aux FSCP qui utilisent des générateurs de nombres aléatoires pour dériver des valeurs de données implicites.

A un niveau de granularité grossière, deux types principaux d'erreurs peuvent être distingués:

- contenu incorrect d'un SPDU, c'est-à-dire erreurs d'intégrité des données;
- remise incorrecte d'un SPDU, c'est-à-dire que le SPDU est transmis au mauvais récepteur ou à la mauvaise instance temporelle.

En combinant ces deux types, les cas distincts suivants peuvent être distingués:

- Cas 1. CC: Aucune erreur (remise correcte, et données explicites correctes);
- Cas 2. IC: Remise incorrecte, et données explicites correctes;
- Cas 3. CI: Remise correcte, et données explicites incorrectes;
- Cas 4. II: Remise incorrecte, et données explicites incorrectes.

Les probabilités d'erreurs résiduelles RP_2, RP_3, et RP_4, pour chacun des cas 2, 3 et 4, sont calculées à partir des paramètres suivants:

P_{ID} est la "probabilité de remise incorrecte", c'est-à-dire la probabilité qu'un SPDU soit transmis de manière erronée au FSCP en raison, par exemple, d'une erreur d'authenticité ou d'opportunité;

NOTE 1 L'évènement de "remise incorrecte" peut se traduire par $err_{impl} \neq 0$. Cependant, en raison de la répartition uniforme dans l'intervalle $[0;2^r-1]$, le cas où $err_{impl} = 0$ peut également se produire.

P_{IED} est la probabilité de données explicites incorrectes, c'est-à-dire la probabilité qu'une corruption des données se produise;

P_{IC} est la probabilité qu'une erreur ne soit pas détectée au niveau du récepteur à condition que le cas 2 se produise;

P_{CI} est la probabilité qu'une erreur ne soit pas détectée au niveau du récepteur à condition que le cas 3 se produise;

P_{II} est la probabilité qu'une erreur ne soit pas détectée au niveau du récepteur à condition que le cas 4 se produise;

RP_I est la probabilité d'erreur résiduelle pour la corruption des données telle que définie à l'Annexe F.

R_{CRC} est la probabilité d'erreur résiduelle pour les polynômes CRC tels que définis dans l'Equation B.3.

NOTE 2 $RP_I \leq R_{CRC}$ car d'autres mesures de sécurité que le CRC peuvent réduire davantage la valeur de RP_I.

r est la longueur de la FCS, identique au degré du polynôme de CRC;

i est la longueur des données implicites, avec i ≥ r;

n est le nombre de bits du SPDU.

Les évènements IC, CI et II étant distincts, la probabilité globale d'erreurs résiduelles peut être calculée en faisant la somme de leurs valeurs RP_x respectives.

En général, RP_x est calculée comme suit:

RP_x = P("l'erreur x a lieu") × P("l'erreur x n'est pas détectable").

Ce calcul donne les formules pour les cas 2, 3 et 4 décrits dans les alinéas suivants.

Cas 2 (IC)

$$RP_2 = P_{ID} \times (1 - P_{IED}) \times P_{IC}$$
$$= P_{ID} \times (1 - P_{IED}) \times 2^{-r}$$

Explication de P_{IC}:

- Si i > r, la probabilité de ce cas est de 2^{-r}, car
  - par hypothèse, la disjonction bit à bit de $impl_S$ et $impl_R$ est uniformément répartie dans l'intervalle $[0;2^i-1]$;
  - par conséquent, la disjonction bit à bit de $FCS_S = FCS_R$ et FCS_C est uniformément répartie dans l'intervalle $[0;2^r-1]$;
  - par conséquent, la probabilité que la disjonction bit à bit de FCS_R et FCS_C soit égale à zéro est de 2^{-r};
  - par conséquent, la probabilité que FCS_R soit égal à FCS_C est de 2^{-r}.
- Si i = r, la probabilité de ce cas est de 2^{-r}, car
  - FCS_R est égal à FCS_C, si et seulement si $err_{impl} = 0$, car la longueur de err_{impl} ne dépasse pas le degré du polynôme de CRC. Les codes CRC détectent toutes les erreurs en rafale de longueur inférieure ou égale à r;
  - La probabilité que $err_{impl} = 0$ est de 2^{-r} en raison de la répartition uniforme dans l'intervalle $[0;2^r-1]$.

Cas 3 (CI)

$$RP_3 = (1-P_{ID}) \times P_{IED} \times P_{CI}$$
$$= (1-P_{ID}) \times RP_I$$
$$\leq (1-P_{ID}) \times 2^{-r} \text{ pour les polynômes exacts.}$$

Cas 4 (II)

$$RP_4 = P_{ID} \times P_{IED} \times P_{II}$$
$$= P_{ID} \times P_{IED} \times 2^{-r}$$

Explication:

- Par hypothèse, err_{impl} adopte toutes les valeurs de l'intervalle $[0;2^i-1]$ selon une égale probabilité.