IEC 62541-15

Edition 1.0 2025-02

INTERNATIONAL STANDARD

NORME INTERNATIONALE

OPC Unified Architecture – Part 15: Safety

Architecture unifiée OPC – Partie 15: Sécurité

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

ICS 25.040.40

ISBN 978-2-8327-0212-3

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.

® Registered trademark of the International Electrotechnical Commission
Marque déposée de la Commission Electrotechnique Internationale

CONTENTS

FOREWORD....6
INTRODUCTION....8
1 Scope....9
2 Normative references....9
3 Terms, definitions, symbols, abbreviated terms and conventions....10
3.1 Terms and definitions....10
3.1.1 Common terms and definitions....10
3.1.2 Additional terms and definitions....12
3.2 Symbols and abbreviated terms....14
3.2.1 Abbreviated terms from IEC 61784-3....14
3.2.2 Additional symbols and abbreviated terms....15
3.3 Conventions....15
3.3.1 General conventions....15
3.3.2 Conventions for requirements numbering....15
3.3.3 Conventions in state machines....16
4 Overview of OPC UA Safety....16
4.1 General....16
4.2 Implementation aspects....16
4.3 Features....17
4.4 Security policy....17
5 General....18
5.1 External documents providing specifications for the profile....18
5.2 Safety functional requirements....18
5.3 Safety measures....18
5.4 Safety communication layer structure....19
5.5 Requirements for CRC calculation....21
6 Safety communication layer services....21
6.1 General....21
6.2 Information models....22
6.2.1 General....22
6.2.2 Object and ObjectType Definitions....22
6.2.3 DataType definition....34
6.2.4 SafetyProvider version....38
6.2.5 DataTypes and length of SafetyData....38
6.2.6 Connection establishment....38
6.3 Service interfaces....38
6.3.1 Overview....38
6.3.2 OPC UA Platform interface (OPC UA PI)....39
6.3.3 SafetyProvider interfaces....39
6.3.4 SafetyConsumer interfaces....46
6.3.5 Cyclic and acyclic safety communication....53
6.3.6 Principle for "application variables with qualifier"....53
6.4 Diagnostics....53
6.4.1 General....53
6.4.2 Diagnostics messages of the SafetyConsumer....54
6.4.3 Method ReadSafetyDiagnostics of the SafetyProvider....56

7 Safety communication layer protocol 56
7.1 General 56
7.2 SafetyProvider and SafetyConsumer 56
7.2.1 SPDU formats 56
7.2.2 Behaviour 58
7.2.3 Subroutines 76
8 Safety communication layer management 82
8.1 General 82
8.2 Safety function response time part of communication 82
9 System requirements (SafetyProvider and SafetyConsumer) 84
9.1 Constraints on the SPDU parameters 84
9.1.1 SafetyBaseID and SafetyProviderID 84
9.1.2 SafetyConsumerID 85
9.2 Initialization of the MNR in the SafetyConsumer 86
9.3 Constraints on the calculation of system characteristics 86
9.3.1 Probabilistic considerations (informative) 86
9.3.2 Safety related assumptions (informative) 88
9.4 PFH and PFD values of a logical safety communication link 88
9.5 Safety manual 89
9.6 Indicators and displays 90
10 Assessment 90
10.1 Safety policy 90
10.2 Obligations 91
10.3 Index of requirements (informative) 91
11 Profiles and conformance units 94
12 Namespaces 94
12.1 Namespace metadata 94
12.2 Handling of IEC 62541 namespaces 95
Annex A (normative) Safety namespace and mappings 96
Annex B (informative) Additional information 97
B.1 CRC calculation using tables, for the polynomial 0xF4ACFB13 97
B.2 Use cases 98
B.2.1 Unidirectional communication 98
B.2.2 Bidirectional communication 99
B.2.3 Safety multicast 99
B.3 Use cases for operator acknowledgment 100
B.3.1 Explanation 100
B.3.2 Use case 1: unidirectional communication and OA on the SafetyConsumer side 100
B.3.3 Use case 2: bidirectional communication and dual OA 101
B.3.4 Use case 3: bidirectional communication and single, one-sided OA 101
B.3.5 Use case 4: bidirectional communication and single, two-sided OA 102
Annex C (informative) Information for assessment 103
Bibliography 104

Figure 1 – Relationships of OPC UA safety with other standards 8
Figure 2 – Safety layer architecture 20

Figure 3 – Server Objects for OPC UA Safety 24
Figure 4 – Instances of Server Objects for this document 25
Figure 5 – Safety multicast with three recipients using IEC 62541 PubSub 31
Figure 6 – Safety parameters for the SafetyProvider and the SafetyConsumer 32
Figure 7 – Safety communication layer overview 39
Figure 8 – SafetyProvider interfaces 40
Figure 9 – Example combinations of SIL capabilities 46
Figure 10 – SafetyConsumer interfaces 47
Figure 11 – RequestSPDU 56
Figure 12 – ResponseSPDU 57
Figure 13 – Sequence diagram for requests and responses (Client/Server) 59
Figure 14 – Sequence diagram for requests and responses (PubSub) 60
Figure 15 – Duration of demand example for missed demand value in case of currently available SafetyData not being provided until second change of MNR 61
Figure 16 – Duration of demand example for received demand value in case of currently available SafetyData being provided 62
Figure 17 – Simplified representation of the state diagram for the SafetyProvider 62
Figure 18 – Principle state diagram for SafetyConsumer 65
Figure 19 – Sequence diagram for OA 75
Figure 20 – Overview of task for SafetyProvider 76
Figure 21 – Calculation of the SPDU_ID 77
Figure 22 – Example for the calculation of SPDU_ID_1, SPDU_ID_2 and SPDU_ID_3 78
Figure 23 – Calculation of the CRC (on little-endian machines, CRC32_Backward) 81
Figure 24 – Calculation of the CRC (on big-endian machines, CRC32_Forward) 82
Figure 25 – Overview of delay times and watchdogs 83
Figure 26 – Conditional residual error probability of the CRC check 87
Figure 27 – Counter example: data lengths not supported by OPC Safety 88
Figure 28 – Facets and ConformanceUnits 94
Figure B.1 – Unidirectional communication 99
Figure B.2 – Bidirectional communication 99
Figure B.3 – Safety multicast 99
Figure B.4 – OA in unidirectional safety communication 100
Figure B.5 – Two-sided OA in bidirectional safety communication 101
Figure B.6 – One sided OA in bidirectional safety communication 101
Figure B.7 – One sided OA on each side is possible 102

Table 1 – Conventions used in state machines 16
Table 2 – Deployed safety measures to detect communication errors 18
Table 3 – SafetyACSet definition 22
Table 4 – SafetyObjectsType definition 26
Table 5 – SafetyProviderType definition 26
Table 6 – SafetyConsumerType definition 27
Table 7 – ReadSafetyData Method arguments 28
Table 8 – ReadSafetyData Method AddressSpace definition 29

Table 9 – ReadSafetyDiagnostics Method arguments 30
Table 10 – ReadSafetyDiagnostics Method AddressSpace definition 30
Table 11 – SafetyPDUsType definition 31
Table 12 – SafetyProviderParametersType definition 33
Table 13 – SafetyConsumerParametersType definition 34
Table 14 – InFlagsType values 35
Table 15 – InFlagsType definition 35
Table 16 – OutFlagsType values 35
Table 17 – OutFlagsType definition 36
Table 18 – RequestSPDUDataType structure 36
Table 19 – RequestSPDUDataType definition 36
Table 20 – ResponseSPDUDataType structure 37
Table 21 – ResponseSPDUDataType definition 37
Table 22 – NonSafetyDataPlaceholderDataType structure 37
Table 23 – SAPI of the SafetyProvider 41
Table 24 – SPI of the SafetyProvider 42
Table 25 – SAPI of the SafetyConsumer 47
Table 26 – SPI of the SafetyConsumer 50
Table 27 – Example "application variables with qualifier" 53
Table 28 – Safety layer diagnostic messages 54
Table 29 – Symbols used for state machines 62
Table 30 – SafetyProvider instance internal items 63
Table 31 – States of SafetyProvider instance 64
Table 32 – SafetyProvider transitions 64
Table 33 – SafetyConsumer internal items 66
Table 34 – SafetyConsumer states 70
Table 35 – SafetyConsumer transitions 71
Table 36 – Presentation of the SPDU_ID 77
Table 37 – Coding for the SafetyProviderLevel_ID 78
Table 38 – Examples for cryptographically strong random number generators 85
Table 39 – The total residual error rate for the safety communication channel 89
Table 40 – Information to be included in the safety manual 89
Table 41 – Index of requirements (informative) 92
Table 42 – NamespaceMetadata Object for this document 95
Table 43 – Namespaces used in a safety Server 95
Table B.1 – The CRC32 lookup table for 32-bit CRC signature calculations 98

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

OPC UNIFIED ARCHITECTURE –

Part 15: Safety

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 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.

IEC 62541-15 has been prepared by subcommittee 65C: Industrial networks, of IEC technical committee 65: Industrial-process measurement, control and automation. It is an International Standard.

The text of this International Standard is based on the following documents:

Draft	Report on voting
65C/1334/FDIS	65C/1339/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 International Standard 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.

Throughout this document and the referenced other parts of the IEC 62541 series, certain document conventions are used:

Italics are used to denote a defined term or definition that appears in Clause 3 in one of the parts of the series.

Italics are also used to denote the name of a service input or output parameter or the name of a structure or element of a structure that are usually defined in tables.

The *italicized terms* and *names* are also, with a few exceptions, written in camel-case (the practice of writing compound words or phrases in which the elements are joined without spaces, with each element's initial letter capitalized within the compound). For example, the defined term is *AddressSpace* instead of Address Space. This makes it easier to understand that there is a single definition for *AddressSpace*, not separate definitions for Address and Space.

A list of all parts of the IEC 62541 series, published under the general title *OPC Unified Architecture*, 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

OPC UA safety extends OPC UA to fulfill the requirements of functional safety as defined in the IEC 61508 series and IEC 61784-3 series of standards.

Figure 1 shows the relationship between this document and the relevant safety and OPC UA standards in an industrial environment. An arrow from Document A to Document B means "Document A is referenced in Document B". This reference can be either normative or informative. Not all of these standards are applicable or required for a given product.

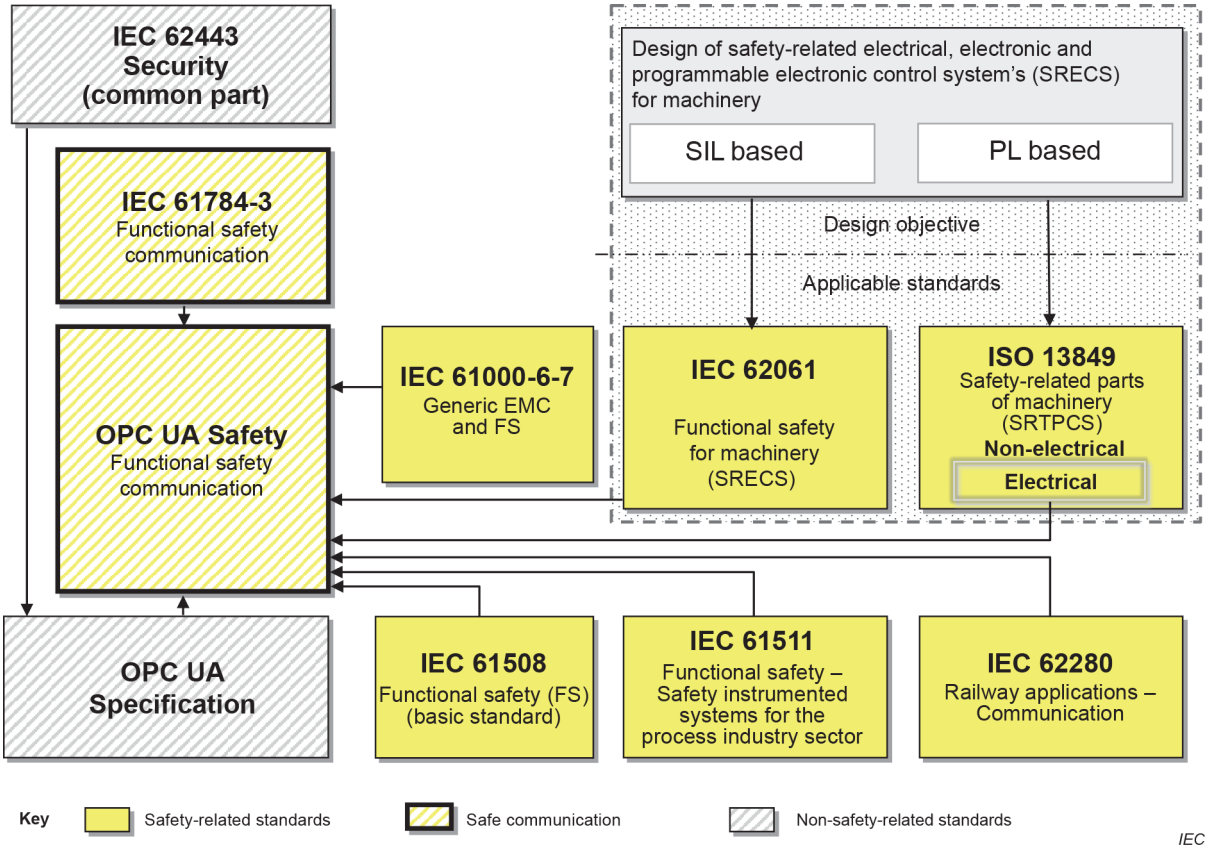


Figure 1 – Relationships of OPC UA safety with other standards

Implementing this document allows for detecting all types of communication errors encountered in the lower network layers. In case an error is detected, this information is shared with the safety applications in the user layer which can then act in an appropriate way, e.g. by switching to a safe state.

The document describes the behaviour of the individual endpoints for safe communication, as well as the OPC UA *Information Model* which is used to access these endpoints.

This document is application-independent and does not pose requirements on the structure and length of the application data. Application-specific requirements are expected to be described in appropriate companion specifications.

This document can be used for applications requiring functional safety up to the *safety integrity level* (*SIL*) 4.

OPC UNIFIED ARCHITECTURE –

Part 15: Safety

1 Scope

This document describes a *safety communication layer* (services and a protocol) for the exchange of *SafetyData* using IEC 62541 mechanisms. It identifies the principles for functional safety communications defined in IEC 61784-3 that are relevant for this *safety communication layer*. This *safety communication layer* is intended for implementation in *safety* devices only.

NOTE 1 This document targets controller-to-controller communication. However, easy expandability to other use-cases (e.g. OPC UA field level communication) has already been considered in the design of this document.

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

This document defines mechanisms for the transmission of safety-relevant messages among participants within a network using OPC UA technology in accordance with the requirements of the IEC 61508 series and IEC 61784-3 for functional safety. These mechanisms can be used in various industrial applications such as process control, manufacturing, automation, and machinery.

This document provides guidelines for both developers and assessors of compliant devices and systems.

NOTE 3 The resulting *SIL* claim of a system depends on the implementation of this document within the system – implementation of this document in a standard device is not sufficient to qualify it as a safety device.

2 Normative references

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

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

IEC 61784-3:2021, *Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions*

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

IEC 62541-1:2020, *OPC Unified Architecture – Part 1: Overview and Concepts*

IEC 62541-3:2020, *OPC Unified Architecture – Part 3: Address Space Model*

IEC 62541-4:2020, *OPC Unified Architecture – Part 4: Services*

IEC 62541-5:2020, *OPC Unified Architecture – Part 5: Information Model*

IEC 62541-6:2020, *OPC Unified Architecture – Part 6: Mappings*

IEC 62541-14, *OPC Unified Architecture – Part 14: PubSub*

ISO/IEC 9834-8:2014, *Information technology – Procedures for the operation of object identifier registration authorities – Part 8: Generation of universally unique identifiers (UUIDs) and their use in object identifiers*

SOMMAIRE

AVANT-PROPOS 110
INTRODUCTION 112
1 Domaine d'application 113
2 Références normatives 113
3 Termes, définitions, symboles, abréviations et conventions 114
3.1 Termes et définitions 114
3.1.1 Termes et définitions communs 114
3.1.2 Termes et définitions supplémentaires 117
3.2 Symboles et abréviations 119
3.2.1 Abréviations de l'IEC 61784-3 119
3.2.2 Symboles et abréviations supplémentaires 119
3.3 Conventions 120
3.3.1 Conventions générales 120
3.3.2 Conventions pour la numérotation des exigences 120
3.3.3 Conventions dans les diagrammes d'états 121
4 Vue d'ensemble de la sécurité OPC UA 121
4.1 Généralités 121
4.2 Aspects relatifs à la mise en œuvre 121
4.3 Caractéristiques 122
4.4 Politique de sûreté 122
5 Généralités 123
5.1 Documents externes de spécifications applicables au profil 123
5.2 Exigences fonctionnelles de sécurité 123
5.3 Mesures de sécurité 123
5.4 Structure de la couche de communication de sécurité 124
5.5 Exigences relatives au calcul du CRC 126
6 Services de la couche de communication de sécurité 126
6.1 Généralités 126
6.2 Modèles d'information 127
6.2.1 Généralités 127
6.2.2 Définition des objets et des ObjectTypes 127
6.2.3 Définition de DataType 139
6.2.4 Version de SafetyProvider 143
6.2.5 DataTypes et longueur de SafetyData 143
6.2.6 Établissement de la connexion 143
6.3 Interfaces de services 143
6.3.1 Vue d'ensemble 143
6.3.2 Interface de plateforme OPC UA (OPC UA PI) 144
6.3.3 Interfaces du SafetyProvider 144
6.3.4 Interfaces du SafetyConsumer 149
6.3.5 Communication de sécurité cyclique et acyclique 155
6.3.6 Principe applicable aux "variables d'application avec qualificatif" 155
6.4 Diagnostics 156
6.4.1 Généralités 156
6.4.2 Messages de diagnostic du SafetyConsumer 156
6.4.3 Méthode ReadSafetyDiagnostics du SafetyProvider 158

7 Protocole de couche de communication de sécurité 158
7.1 Généralités 158
7.2 SafetyProvider et SafetyConsumer 158
7.2.1 Format des SPDU 158
7.2.2 Comportement 160
7.2.3 Sous-routines 178
8 Gestion de la couche de communication de sécurité 184
8.1 Généralités 184
8.2 Partie temps de réponse de la fonction de sécurité de la communication 184
9 Exigences système (SafetyProvider et SafetyConsumer) 186
9.1 Contraintes sur les paramètres de la SPDU 186
9.1.1 SafetyBaseID et SafetyProviderID 186
9.1.2 SafetyConsumerID 188
9.2 Initialisation du MNR dans le SafetyConsumer 188
9.3 Contraintes liées au calcul des caractéristiques du système 188
9.3.1 Considérations probabilistes (informatif) 188
9.3.2 Hypothèses relatives à la sécurité (informatif) 190
9.4 Valeurs PFH et PFD d'une liaison de communication de sécurité logique 190
9.5 Manuel de sécurité 191
9.6 Indicateurs et affichages 192
10 Évaluation 192
10.1 Politique de sécurité 192
10.2 Obligations 193
10.3 Index des exigences (informatif) 193
11 Profils et unités de conformité 196
12 Espaces de noms 196
12.1 Métadonnées de l'espace de noms 196
12.2 Gestion des espaces de noms IEC 62541 197
Annexe A (normative) Espace de noms et mappings de sécurité 198
Annexe B (informative) Information supplémentaires 199
B.1 Calcul du CRC à l'aide de tables de conversion pour le polynôme 0xF4ACFB13 199
B.2 Cas d'utilisation 200
B.2.1 Communication unidirectionnelle 200
B.2.2 Communication bidirectionnelle 201
B.2.3 Multidiffusion de sécurité 201
B.3 Cas d'utilisation pour l'acquittement de l'opérateur 202
B.3.1 Explication 202
B.3.2 Cas d'utilisation 1: communication unidirectionnelle et OA côté SafetyConsumer 202
B.3.3 Cas d'utilisation 2: communication bidirectionnelle et double OA 203
B.3.4 Cas d'utilisation 3: communication bidirectionnelle et simple OA unilatéral 203
B.3.5 Cas d'utilisation 4: communication bidirectionnelle et simple OA bilatéral 204
Annexe C (informative) Informations pour l'évaluation 205
Bibliographie 206

Figure 1 – Relations entre la sécurité OPC UA et d'autres normes 112
Figure 2 – Architecture de la couche de sécurité 125

Figure 3 – Objets Serveur pour la sécurité OPC UA 129
Figure 4 – Instances d'objets de serveur pour le présent document 130
Figure 5 – Multidiffusion de sécurité avec trois destinataires utilisant le PubSub IEC 62541 136
Figure 6 – Paramètres de sécurité du SafetyProvider et du SafetyConsumer 137
Figure 7 – Vue d'ensemble de la couche de communication de sécurité 144
Figure 8 – Interfaces du SafetyProvider 145
Figure 9 – Exemples de combinaisons de capacités SIL 149
Figure 10 – Interfaces du SafetyConsumer 150
Figure 11 – RequestSPDU 158
Figure 12 – ResponseSPDU 159
Figure 13 – Diagramme de séquence des demandes et réponses (Client/Serveur) 161
Figure 14 – Diagramme de séquence des demandes et réponses (PubSub) 162
Figure 15 – Exemple de durée de sollicitation pour une valeur sollicitée ignorée lorsque les SafetyData actuellement disponibles ne sont pas fournies tant qu'une deuxième modification du MNR n'a pas lieu 163
Figure 16 – Exemple de durée de sollicitation pour une valeur sollicitée reçue lorsque les SafetyData actuellement disponibles sont fournies 164
Figure 17 – Représentation simplifiée du diagramme d'états du SafetyProvider 164
Figure 18 – Diagramme d'états de principe du SafetyConsumer 167
Figure 19 – Diagramme de séquence pour l'OA 177
Figure 20 – Vue d'ensemble de la tâche pour le SafetyProvider 178
Figure 21 – Calcul du SPDU_ID 179
Figure 22 – Exemple de calcul de SPDU_ID_1, SPDU_ID_2 et SPDU_ID_3 180
Figure 23 – Calcul du CRC (sur les machines petit-boutistes, CRC32_Backward) 183
Figure 24 – Calcul du CRC (sur les machines gros-boutistes, CRC32_Forward) 184
Figure 25 – Vue d'ensemble des délais et des chiens de garde 185
Figure 26 – Probabilité d'erreurs résiduelles conditionnelles de la vérification du CRC 189
Figure 27 – Exemple de compteur: longueurs de données non prises en charge par la sécurité OPC 190
Figure 28 – Facettes et ConformanceUnits 196
Figure B.1 – Communication unidirectionnelle 201
Figure B.2 – Communication bidirectionnelle 201
Figure B.3 – Multidiffusion de sécurité 201
Figure B.4 – OA dans une communication de sécurité unidirectionnelle 202
Figure B.5 – OA bilatéral dans une communication de sécurité bidirectionnelle 203
Figure B.6 – OA unilatéral dans une communication de sécurité bidirectionnelle 203
Figure B.7 – Un OA unilatéral est possible de chaque côté 204

Tableau 1 – Conventions utilisées dans les diagrammes d'états 121
Tableau 2 – Mesures de sécurité déployées pour détecter les erreurs de communication 123
Tableau 3 – Définition de SafetyACSet 127
Tableau 4 – Définition de SafetyObjectsType 131
Tableau 5 – Définition de SafetyProviderType 131

Tableau 6 – Définition de SafetyConsumerType 132
Tableau 7 – Arguments de la méthode ReadSafetyData 133
Tableau 8 – Définition de l'AddressSpace pour la méthode ReadSafetyData 134
Tableau 9 – Arguments de la méthode ReadSafetyDiagnostics 135
Tableau 10 – Définition de l'AddressSpace pour la méthode ReadSafetyDiagnostics 135
Tableau 11 – Définition de SafetyPDUsType 136
Tableau 12 – Définition de SafetyProviderParametersType 138
Tableau 13 – Définition de SafetyConsumerParametersType 139
Tableau 14 – Valeurs d'InFlagsType 140
Tableau 15 – Définition d'InFlagsType 140
Tableau 16 – Valeurs d'OutFlagsType 140
Tableau 17 – Définition d'OutFlagsType 141
Tableau 18 – Structure de RequestSPDUDataType 141
Tableau 19 – Définition de RequestSPDUDataType 141
Tableau 20 – Structure de ResponseSPDUDataType 142
Tableau 21 – Définition de ResponseSPDUDataType 142
Tableau 22 – Structure de NonSafetyDataPlaceholderDataType 142
Tableau 23 – SAPI du SafetyProvider 146
Tableau 24 – SPI du SafetyProvider 147
Tableau 25 – SAPI du SafetyConsumer 150
Tableau 26 – SPI du SafetyConsumer 153
Tableau 27 – Exemples de "variables d'application avec qualificatif" 155
Tableau 28 – Messages de diagnostic de la couche de sécurité 156
Tableau 29 – Symboles utilisés pour les diagrammes d'états 164
Tableau 30 – Éléments internes d'une instance de SafetyProvider 165
Tableau 31 – États d'une instance de SafetyProvider 166
Tableau 32 – Transitions du SafetyProvider 166
Tableau 33 – Éléments internes du SafetyConsumer 168
Tableau 34 – États du SafetyConsumer 172
Tableau 35 – Transitions du SafetyConsumer 173
Tableau 36 – Présentation du SPDU_ID 179
Tableau 37 – Codage pour le SafetyProvideLevel_ID 180
Tableau 38 – Exemples de générateurs de nombres aléatoires forts sur le plan cryptographique 187
Tableau 39 – Taux total d'erreurs résiduelles pour le canal de communication de sécurité 191
Tableau 40 – Informations à inclure dans le manuel de sécurité 191
Tableau 41 – Index des exigences (informatif) 194
Tableau 42 – Objet NamespaceMetadata pour le présent document 197
Tableau 43 – Espaces de noms utilisés dans un Serveur de sécurité 197
Tableau B.1 – Table de conversion CRC32 pour les calculs de signature CRC à 32 bits 200

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

ARCHITECTURE UNIFIÉE OPC –

Partie 15: Sécurité

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 avait 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 ne pas avoir identifié tout ou partie de tels droits de brevet.

L'IEC 62541-15 a été établie par le sous-comité 65C: Réseaux industriels, du comité d'études 65 de l'IEC: Mesure, commande et automation dans les processus industriels. Il s'agit d'une Norme internationale.

Le texte de cette Norme internationale est issu des documents suivants:

Projet	Rapport de vote
65C/1334/FDIS	65C/1339/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 cette Norme internationale 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.

Tout au long du présent document et des autres parties référencées de la série IEC 62541, certaines conventions documentaires sont utilisées:

Le format *italique* est utilisé pour mettre en évidence un terme défini ou une définition qui apparaît à l'Article 3 dans l'une des parties de la série.

Le format *italique* est également utilisé pour mettre en évidence le nom d'un paramètre d'entrée ou de sortie de service, ou le nom d'une structure ou d'un élément de structure habituellement défini dans les tableaux.

Par ailleurs, les *termes* et *noms en italique* sont, à quelques exceptions près, écrits en camel-case (pratique qui consiste à joindre, sans espace, les éléments des mots ou expressions composés, la première lettre de chaque élément étant en majuscule). Par exemple, le terme défini est *AddressSpace* et non Espace d'Adressage. Cela permet de mieux comprendre qu'il existe une définition unique pour *AddressSpace*, et non deux définitions distinctes pour Espace et pour Adressage.

Une liste de toutes les parties de la série IEC 62541, publiées sous le titre général *Architecture unifiée OPC*, 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

La sécurité OPC UA étend l'OPC UA pour satisfaire aux exigences de sécurité fonctionnelle définies dans les séries de normes IEC 61508 et IEC 61784-3.

La Figure 1 représente la relation entre le présent document et les normes de sécurité et OPC UA pertinentes dans un environnement industriel. Une flèche du Document A au Document B signifie que le Document A est référencé dans le Document B. Cette référence peut être normative ou informative. Toutes ces normes ne sont pas applicables ou exigées pour un produit donné.

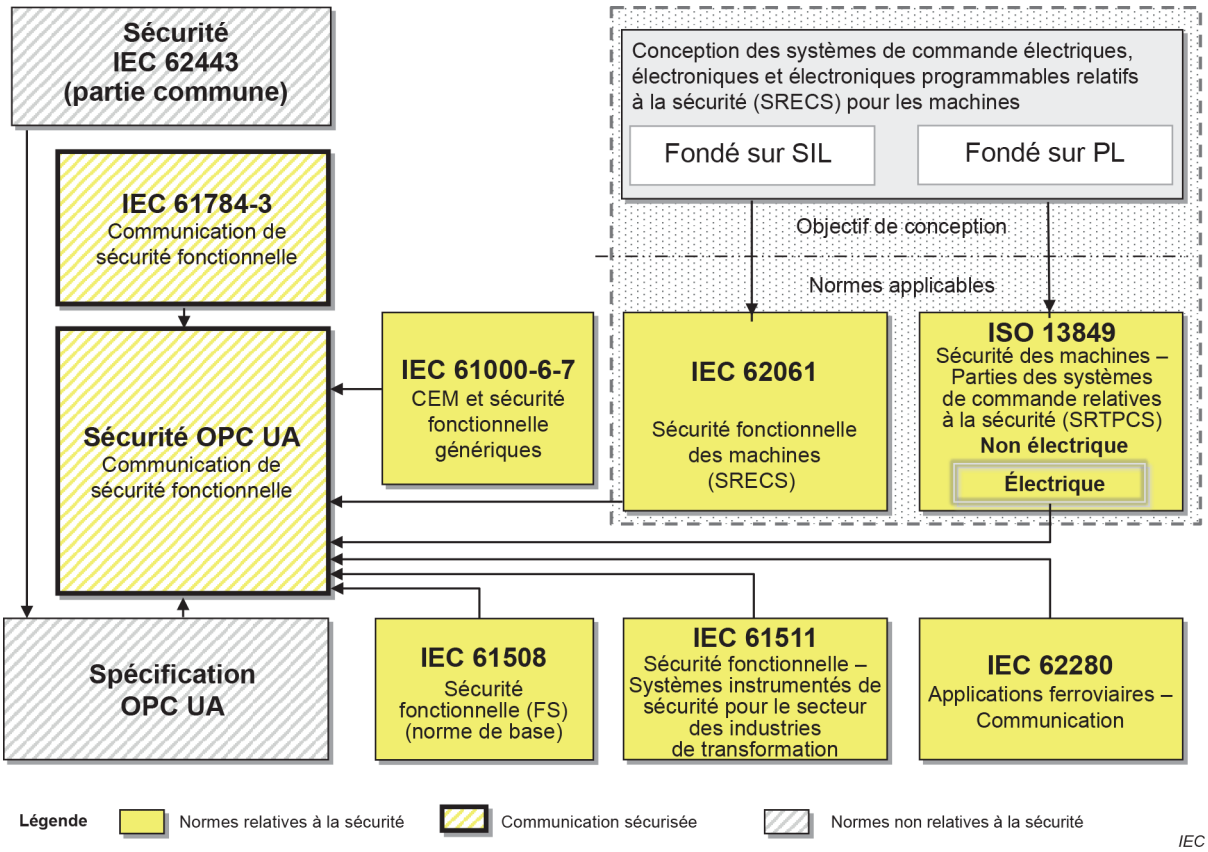


Figure 1 – Relations entre la sécurité OPC UA et d'autres normes

La mise en œuvre du présent document permet de détecter tous les types d'erreurs de communication rencontrés dans les couches réseau inférieures. Si une erreur est détectée, ces informations sont partagées avec les applications de sécurité de la couche utilisateur, qui peuvent alors agir de manière appropriée, par exemple en basculant dans un état de sécurité.

Le document décrit le comportement des points d'extrémité individuels pour une communication sûre, ainsi que le *Modèle d'information* OPC UA qui est utilisé pour accéder à ces points d'extrémité.

Le présent document est indépendant de l'application et n'impose aucune exigence quant à la structure et à la longueur des données d'application. Il est attendu que les exigences spécifiques à l'application soient décrites dans les spécifications associées appropriées.

Le présent document peut être utilisé pour des applications qui exigent une sécurité fonctionnelle jusqu'au *niveau d'intégrité de sécurité* (*SIL*) 4.

ARCHITECTURE UNIFIÉE OPC –

Partie 15: Sécurité

1 Domaine d'application

Le présent document décrit une *couche de communication de sécurité* (services et protocole) pour l'échange de *SafetyData* à l'aide des mécanismes de l'IEC 62541. Il identifie les principes qui s'appliquent aux communications de sécurité fonctionnelle définies dans l'IEC 61784-3, associés à cette *couche de communication de sécurité*. Cette *couche de communication de sécurité* est destinée à être mise en œuvre sur les appareils de *sécurité* uniquement.

NOTE 1 Le présent document cible la communication de contrôleur à contrôleur. Cependant, la facilité d'extension à d'autres cas d'utilisation (par exemple, communication au niveau du terrain OPC UA) a déjà été prise en compte dans la conception du présent document.

NOTE 2 Le présent document ne traite pas des aspects relatifs à la sécurité électrique et à la sécurité intrinsèque. La sécurité électrique concerne les dangers comme les chocs électriques. La sécurité intrinsèque concerne les dangers associés aux atmosphères explosibles.

Le présent document définit les mécanismes de transmission des messages relatifs à la sécurité entre les participants d'un réseau, en utilisant la technologie OPC UA conformément aux exigences de la série IEC 61508 et de l'IEC 61784-3 concernant la sécurité fonctionnelle. Ces mécanismes peuvent être utilisés dans différentes applications industrielles, par exemple la commande de processus, la fabrication, l'automatisation et les machines.

Le présent document fournit des lignes directrices aux développeurs, ainsi qu'aux évaluateurs d'appareils et de systèmes conformes.

NOTE 3 Le *SIL* ainsi revendiqué pour un système dépend de la mise en œuvre du présent document au sein du système (la mise en œuvre du présent document dans un appareil normal ne suffit pas à le qualifier d'appareil de sécurité).

2 Références normatives

Les documents suivants sont cités dans le texte de sorte qu'ils constituent, pour tout ou partie de leur contenu, des exigences du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

IEC 61508 (toutes les parties), *Sécurité fonctionnelle des systèmes électriques/électroniques/ électroniques programmables relatifs à la sécurité.*

IEC 61784-3:2021, *Réseaux de communication industriels – Profils – Partie 3: Bus de terrain de sécurité fonctionnelle – Règles générales et définitions de profils.*

IEC 62443 (toutes les parties), *Sécurité des systèmes d'automatisation et de commande industrielles.*

IEC 62541-1:2020, *Architecture unifiée OPC – Partie 1: Vue d'ensemble et concepts.*

IEC 62541-3:2020, *Architecture unifiée OPC – Partie 3: Modèle d'espace d'adressage.*

IEC 62541-4:2020, *Architecture unifiée OPC – Partie 4: Services.*

IEC 62541-5:2020, *Architecture unifiée OPC – Partie 5: Modèle d'information.*

IEC 62541-6:2020, *Architecture unifiée OPC – Partie 6: Mappings.*

IEC 62541-14, *Architecture unifiée OPC – Partie 14: PubSub.*

ISO/IEC 9834-8:2014, *Technologies de l'information – Procédures opérationnelles pour les organismes d'enregistrement d'identificateur d'objet – Partie 8: Génération des identificateurs uniques universels (UUID) et utilisation de ces identificateurs dans les composants d'identificateurs d'objets.*