



DPC: 23 / 30479757 DC

BSI Group Headquarters

389 Chiswick High Road London W4 4AL

Tel: +44 (0)20 8996 9000

Fax: +44 (0)20 8996 7400

www.bsigroup.com

Date: 13 September 2023

Origin: International

Latest date for receipt of comments: 25 October 2023

Project No. 2023/02098

Responsible committee: GEL/65/3 Industrial Networks

Interested committees:

Title: BS EN IEC 62541-15 OPC Unified Architecture

Part 15: Safety

Please notify the secretary if you are aware of any keywords that might assist in classifying or identifying the standard or if the content of this standard

- i) has any issues related to 3rd party IPR, patent or copyright
- ii) affects other national standard(s)
- iii) requires additional national guidance or information

**WARNING: THIS IS A DRAFT AND MUST NOT BE REGARDED OR USED AS A BRITISH STANDARD.
THIS DRAFT IS NOT CURRENT BEYOND 25 October 2023**

This draft is issued to allow comments from interested parties; all comments will be given consideration prior to publication. No acknowledgement will normally be sent. **See overleaf for information on the submission of comments.**

No copying is allowed, in any form, without prior written permission from BSI except as permitted under the Copyright, Designs and Patent Act 1988 or for circulation within a nominating organization for briefing purposes. Electronic circulation is limited to dissemination by e-mail within such an organization by committee members.

Further copies of this draft may be purchased from BSI Shop <http://shop.bsigroup.com> or from BSI Customer Services, Tel: +44(0) 20 8996 9001 or email cservices@bsigroup.com. British, International and foreign standards are also available from BSI Customer Services.

Information on the co-operating organizations represented on the committees referenced above may be obtained from <http://standardsdevelopment.bsigroup.com>

Responsible Committee Secretary: Ms Charmaine Mukherjee (BSI)

Direct tel:

E-mail: charmaine.mukherjee@bsigroup.com

Introduction

This draft standard is based on national and international discussions. Your comments on this draft are invited and will assist in the preparation of the consequent standard.

For international standards, comments will be reviewed by the relevant UK national committee before sending the consensus UK vote and comments to the international committee, which will then decide appropriate action. If the international standard is approved, it is usual for the text to be published as a British Standard.

For national standards, comments will be reviewed by the relevant UK national committee and the resulting standards published as a British Standard.

UK Vote

Please indicate whether you consider the UK should submit a negative (with supporting technical reasons) or positive vote on this draft. Please indicate if you are aware of any reason why this draft standard should not be published as a British Standard.

Submission of Comments

- **Annotated drafts are not acceptable and will be rejected.**
- All comments should be submitted online at <https://standardsdevelopment.bsigroup.com/>. You will need to register in order to comment.

Template for comments and secretariat observations

Date: xx/xx/20xx	Document: ISO/DIS xxxx
------------------	------------------------

1	2	(3)	4	5	(6)	7
MB	Clause No./ Subclause No./Annex (e.g. 3.1)	Paragraph/Figure/ Table/Note	Type of comment	Commend (justification for change) by the MB	Proposed change by the MB	Secretariat observations on each comment submitted
	3.1	Definition 1	ed	Definition is ambiguous and needs clarifying.	Amend to read '...so that the mains connector to which no connection...'	
	6.4	Paragraph 2	te	The use of the UV photometer as an alternative cannot be supported as serious problems have been encountered in its use in the UK.	Delete reference to UV photometer.	

PROJECT NUMBER:
IEC 62541-15 ED1

DATE OF CIRCULATION:
2023-09-01

CLOSING DATE FOR COMMENTS:
2023-11-24

SUPERSEDES DOCUMENTS:
65C/1253/NP, 65C/1266/RVN

IEC SC 65C : INDUSTRIAL NETWORKS

SECRETARIAT:
France

SECRETARY:
Ms Valérie DEMASSIEUX

OF INTEREST TO THE FOLLOWING COMMITTEES:
SC 65E

PROPOSED HORIZONTAL STANDARD:
☐

Other TC/SCs are requested to indicate their interest, if any, in this CD to the secretary.

FUNCTIONS CONCERNED:

☐ EMC

☐ ENVIRONMENT

☐ QUALITY ASSURANCE

☐ SAFETY

This document is still under study and subject to change. It should not be used for reference purposes.

Recipients of this document are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Recipients of this document are invited to submit, with their comments, notification of any local regulations or technical reasons that may exist and should be considered should this proposal proceed, recognizing that failure to address such requirements could result in the need for new or existing "In Some Countries" clauses. (SEE [AC/22/2007](#) OR [NEW GUIDANCE DOC](#)).

TITLE:

OPC Unified Architecture - Part 15: Safety

NOTE FROM TC/SC OFFICERS:

NC comments on this CD will be addressed during the dedicated SC65C/WG12 virtual meeting on January 9th-11th, 2024. Meeting details will be sent at a later date by the convenor.

Copyright © 2023 International Electrotechnical Commission, IEC. All rights reserved. It is permitted to download this electronic file, to make a copy and to print out the content for the sole purpose of preparing National Committee positions. You may not copy or "mirror" the file or printed version of the document, or any part of it, for any other purpose without permission in writing from IEC.

CONTENTS

1		
2		
3	FOREWORD.....	7
4	INTRODUCTION.....	9
5	1 Scope.....	10
6	2 Normative references	10
7	3 Terms, definitions and conventions.....	11
8	3.1 Terms and definitions.....	11
9	3.1.1 Terms and definitions from IEC 61784-3.....	11
10	3.1.2 Additional terms and definitions	13
11	3.2 Symbols and abbreviated terms	15
12	3.2.1 Abbreviated terms from IEC 61784-3	15
13	3.2.2 Additional symbols and abbreviated terms	15
14	3.3 Conventions.....	15
15	3.3.1 General Conventions	15
16	3.3.2 Conventions for Requirements Numbering	16
17	3.3.3 Conventions in state machines	16
18	4 Overview of OPC UA Safety	16
19	4.1 General.....	16
20	4.2 Implementation aspects	17
21	4.3 Features	17
22	4.4 Security policy	17
23	5 General	18
24	5.1 External documents providing specifications for the profile	18
25	5.2 Safety functional requirements.....	18
26	5.3 Safety measures.....	18
27	5.4 Safety communication layer structure.....	19
28	5.5 Requirements for CRC calculation	21
29	6 Safety communication layer services	21
30	6.1 General.....	21
31	6.2 Information Models	21
32	6.2.1 General	21
33	6.2.2 Object and ObjectType Definitions	22
34	6.2.3 Datatype Definition	31
35	6.2.4 SafetyProvider Version	34
36	6.2.5 DataTypes and length of SafetyData.....	34
37	6.2.6 Connection establishment.....	34
38	6.3 Service interfaces	35
39	6.3.1 Overview	35
40	6.3.2 OPC UA Platform interface (OPC UA PI)	35
41	6.3.3 SafetyProvider interfaces.....	36
42	6.3.4 SafetyConsumer interfaces.....	40
43	6.3.5 Cyclic and acyclic safety communication	45
44	6.3.6 Principle for “Application variables with qualifier”	46
45	6.4 Diagnostics	46
46	6.4.1 General	46
47	6.4.2 Diagnostics messages of the SafetyConsumer	46

48	6.4.3	Method ReadSafetyDiagnostics of the SafetyProvider	48
49	7	Safety communication layer protocol	49
50	7.1	General.....	49
51	7.2	SafetyProvider and SafetyConsumer.....	49
52	7.2.1	SPDU formats.....	49
53	7.2.2	Behavior	51
54	7.2.3	Subroutines	65
55	8	Safety communication layer management.....	71
56	8.1	General.....	71
57	8.2	Safety function response time part of communication.....	71
58	9	System requirements (SafetyProvider & SafetyConsumer).....	73
59	9.1	Constraints on the SPDU-Parameters	73
60	9.1.1	SafetyBaseID and SafetyProviderID	73
61	9.1.2	SafetyConsumerID	75
62	9.2	Initialization of the MNR in the SafetyConsumer	75
63	9.3	Constraints on the calculation of system characteristics.....	75
64	9.3.1	Probabilistic considerations (informative).....	75
65	9.3.2	Safety related assumptions (informative)	77
66	9.4	PFH/PFD-values of a logical safety communication link	77
67	9.5	Safety manual	78
68	9.6	Indicators and displays	79
69	10	Assessment.....	79
70	10.1	Safety policy	79
71	10.2	Obligations	80
72	10.3	Automated layer test for this document (informative).....	80
73	10.3.1	General	80
74	10.3.2	OPC UA Safety Compliance Test Tool (UASCTT).....	80
75	10.3.3	Testing principle	80
76	10.3.4	Test configuration.....	81
77	10.4	Index of Requirements (informative)	83
78	11	Profiles and Conformance Units	85
79	11.1	General.....	85
80	11.2	Conformance units.....	86
81	11.3	Profiles	86
82	11.3.1	Profile list	86
83	11.3.2	Facets and Profiles.....	87
84	12	Namespaces.....	88
85	12.1	Namespace Metadata	88
86	12.2	Handling of IEC 62541 Namespaces.....	88
87	Annex A (normative)	Safety Namespace and mappings	90
88	Annex B (informative)	Additional information.....	91
89	B.1	CRC-calculation using tables, for the polynomial 0xF4ACFB13.....	91
90	B.2	Use cases.....	93
91	B.2.1	Unidirectional communication	93
92	B.2.2	Bidirectional communication	93
93	B.2.3	Safety Multicast.....	93
94	B.3	Use cases for Operator Acknowledgment.....	94
95	B.3.1	Explanation	94

96	B.3.2	Use case 1: unidirectional comm. and OA on the SafetyConsumer side	94
97	B.3.3	Use case 2: bidirectional comm. and dual OA	95
98	B.3.4	Use case 3: bidirectional comm. and single, one-sided OA	96
99	B.3.5	Use case 4: bidirectional comm. and single, two-sided OA	96
100	Bibliography		97
101			
102	Figure 1 – Relationships of OPC UA Safety with other standards (informative		
103	information)		9
104	Figure 2 – Safety layer architecture		20
105	Figure 3 – Server Objects for OPC UA Safety		23
106	Figure 4 – Instances of server objects for this document.....		24
107	Figure 5 – Safety Multicast with three recipients using IEC 62541 PubSub		28
108	Figure 6 – Safety Parameters for the SafetyProvider and the SafetyConsumer.		29
109	Figure 7 – Safety communication layer overview.....		35
110	Figure 8 – SafetyProvider interfaces		36
111	Figure 9 – Example combinations of SIL capabilities.....		40
112	Figure 10 – SafetyConsumer interfaces		41
113	Figure 11 – RequestSPDU		49
114	Figure 12 – ResponseSPDU		49
115	Figure 13 (informative) – Sequence diagram for requests and responses		
116	(Client/Server)		51
117	Figure 14 (informative) – Sequence diagram for requests and responses (PubSub).....		52
118	Figure 15 – Simplified representation of the state diagram for the SafetyProvider		53
119	Figure 16 – Principle state diagram for SafetyConsumer		56
120	Figure 17 – Sequence diagram for OA		65
121	Figure 18 – Overview of task for SafetyProvider		66
122	Figure 19 – Calculation of the SPDU_ID		66
123	Figure 20 – Calculation of the CRC (on little-endian machines, CRC32_Backward)		70
124	Figure 21 – Calculation of the CRC (on big-endian machines, CRC32_Forward).....		71
125	Figure 22 – Overview of delay times and watchdogs		72
126	Figure 23 – Conditional residual error probability of the CRC-check.....		76
127	Figure 24 – Counter example: data lengths not supported by OPC Safety.....		77
128	Figure 25 – Automated SafetyProvider / SafetyConsumer test		81
129	Figure 26 – “Upper Tester” within the SafetyProvider		82
130	Figure 27 – “Upper Tester” within the SafetyConsumer		82
131	Figure 28 (informative) – Facets and Conformance Units.....		85
132	Figure 29 – Unidirectional Communication		93
133	Figure 30 – Bidirectional Communication		93
134	Figure 31 – Safety Multicast		93
135	Figure B.1 – OA in unidirectional safety communication		94
136	Figure B.2 – Two-sided OA in bidirectional safety communication		95
137	Figure B.3 – One sided OA in bidirectional safety communication		96
138	Figure B.4 – One sided OA on each side is possible		96

140	Table 1 – Conventions used in state machines	16
141	Table 2 – Deployed measures to detect communication errors	19
142	Table 3 – SafetyACSet definition	22
143	Table 4 – SafetyObjectsType Definition	25
144	Table 5 – SafetyProviderType Definition	25
145	Table 6 – SafetyConsumerType Definition	25
146	Table 7 – ReadSafetyData Method Arguments	26
147	Table 8 – ReadSafetyData Method AddressSpace definition	26
148	Table 9 – ReadSafetyDiagnostics Method Arguments	27
149	Table 10 – ReadSafetyDiagnostics Method AddressSpace definition	27
150	Table 11 – SafetyPDUsType Definition	28
151	Table 12 – SafetyProviderParametersType Definition	30
152	Table 13 – SafetyConsumerParametersType Definition	31
153	Table 14 – InFlagsType Values	31
154	Table 15 – InFlagsType Definition	32
155	Table 16 – OutFlagsType Values	32
156	Table 17 – OutFlagsType Definition	32
157	Table 18 – RequestSPDUDataType Structure	33
158	Table 19 – RequestSPDUDataType definition	33
159	Table 20 – ResponseSPDUDataType Structure	33
160	Table 21 – ResponseSPDUDataType definition	34
161	Table 22 – NonSafetyDataPlaceholderDataType Structure	34
162	Table 23 – SAPI of the SafetyProvider	36
163	Table 24 – SPI of the SafetyProvider	38
164	Table 25 – SAPI of the SafetyConsumer	41
165	Table 26 – SPI of the SafetyConsumer	43
166	Table 27 – Example “Application Variables with qualifier”	46
167	Table 28 – Safety layer diagnostic messages	46
168	Table 29 – Symbols used for state machines	53
169	Table 30 – SafetyProvider instance internal items	53
170	Table 31 – States of SafetyProvider instance	55
171	Table 32 – SafetyProvider transitions	55
172	Table 33 – SafetyConsumer internal items	56
173	Table 34 – SafetyConsumer states	60
174	Table 35 – SafetyConsumer transitions	61
175	Table 36 – Presentation of the SPDU_ID	67
176	Table 37 – Coding for the SafetyProviderLevel_ID	67
177	Table 38 – Examples for cryptographically strong random number generators	74
178	Table 39 – The total residual error rate for the safety communication channel	78
179	Table 40 – Information to be included in the safety manual	78
180	Table 41 – Index of Requirements (informative)	83
181	Table 42 – Conformance Units for Safety	86
182	Table 43 – Profile URIs for Safety	87

183	Table 44 – SafetyProviderServerMapper Facet	87
184	Table 45 – SafetyProviderPubSubMapper Facet	87
185	Table 46 – SafetyProvider Facet	87
186	Table 47 – SafetyConsumerPubSubMapper Facet	88
187	Table 48 – SafetyConsumer Facet	88
188	Table 49 – SafetyAutomationComponent Facet	88
189	Table 50 – NamespaceMetadata Object for this document	88
190	Table 51 – Namespaces used in a Safety Server	89
191	Table B.1 – The CRC32 lookup table for 32-bit CRC signature calculations	92
192		

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/XX/FDIS	65C/XX/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 series, certain document conventions are used:

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.

A bilingual version of this publication may be issued at a later date.

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

OPC UA Safety extends OPC UA to fulfill the requirements of functional safety as defined in the IEC 61508 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/required for a given product.

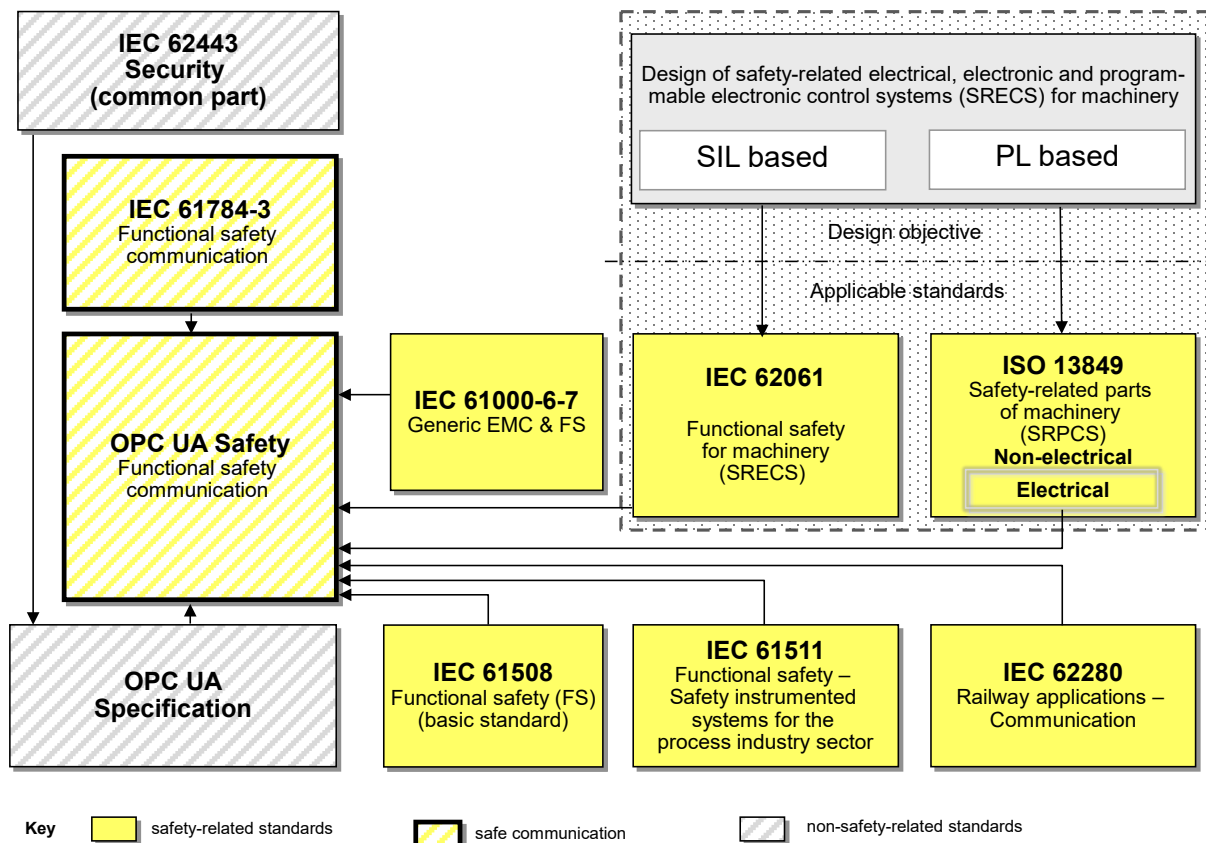


Figure 1 – Relationships of OPC UA Safety with other standards (informative information)

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 application layer which can then act in an appropriate way, e.g. by switching to a safe state.

The document describes the behavior 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 safety data 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 IEC 61508 series and IEC 61784-3 for functional safety. These mechanisms may 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 61000-6-7, *Electromagnetic compatibility (EMC) – Part 6-7: Generic standards – Immunity requirements for equipment intended to perform functions in a safety related system (functional safety) in industrial locations*

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

IEC 61511 (all parts), *Functional safety – Safety instrumented systems for the process industry sector*

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

IEC 62061, *Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems*

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

IEC 62541-2, *OPC Unified Architecture – Part 2: Security*

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

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

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

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

IEC 62541-7, *OPC Unified Architecture – Part 7: Profiles*

IEC 62541-8, *OPC Unified Architecture – Part 8: Data Access*

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

ISO/IEC 9834-8, *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*

ISO 13849-1, *Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design*

ISO 13849-2, *Safety of machinery – Safety-related parts of control systems – Part 2: Validation*

3 Terms, definitions and conventions

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC 62541-1, IEC 62541-3, IEC 62541-6, IEC 61784-3 and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

- IEC Electropedia: available at <https://www.electropedia.org/>
- ISO Online browsing platform: available at <https://www.iso.org/obp>

NOTE This document uses concepts of OPC UA information modeling to describe OPC UA Safety.

3.1.1 Terms and definitions from IEC 61784-3

3.1.1.1

cyclic redundancy check (CRC)

<value> redundant data derived from, and stored or transmitted together with, a block of data in order to detect data corruption

<method> procedure used to calculate the redundant data

Note 1 to entry: Terms “CRC code” and “CRC signature”, and labels such as CRC1, CRC2, may also be used in this document to refer to the redundant data.

[SOURCE: IEC 61784-3:2021, 3.1]

3.1.1.2

error

discrepancy between a computed, observed or measured value or condition and the true, specified or theoretically correct value or condition

Note 1 to entry: Errors may be due to design mistakes within hardware/software and/or corrupted information due to electromagnetic interference and/or other effects.

Note 2 to entry: Errors do not necessarily result in a failure or a fault.

[SOURCE: IEC 61508-4:2010, 3.6.11]

3.1.1.3

failure

termination of the ability of a functional unit to perform a required function or operation of a functional unit in any way other than as required

Note 1 to entry: Failure may be due to an error (for example, problem with hardware/software design or message disruption).

[SOURCE: IEC 61508-4:2010, 3.6.4, modified – notes and figures deleted]

3.1.1.4

fault

abnormal condition that may cause a reduction in, or loss of, the capability of a functional unit to perform a required function

Note 1 to entry: IEC 191-05-01 defines "fault" as a state characterized by the inability to perform a required function, excluding the inability during preventive maintenance or other planned actions, or due to lack of external resources.

[SOURCE: IEC 61508-4:2010, 3.6.1, modified – figure reference deleted]

3.1.1.5

message

<information theory and communication theory> ordered sequence of characters (usually octets) intended to convey information

[SOURCE: ISO/IEC 2382:2015, 2123205, modified – insertion of "(usually octets)", deletion of notes and source]

3.1.1.6

performance level (PL)

discrete level used to specify the ability of safety-related parts of control systems to perform a safety function under foreseeable conditions

[SOURCE: ISO 13849-1:2015, 3.1.23]

3.1.1.7

residual error probability

probability of an error undetected by the SCL safety measures

[SOURCE: IEC 61784-3:2021 3.1]

3.1.1.8

residual error rate

statistical rate at which the SCL safety measures fail to detect errors

[SOURCE: IEC 61784-3:2021, 3.1]

3.1.1.9

safety communication layer (SCL)

communication layer above the OPC UA communication stack that includes all necessary additional measures to ensure safe transmission of data in accordance with the requirements of IEC 61508.

The SCL provides several services, the most important ones being the SafetyProvider and the SafetyConsumer.

[SOURCE: IEC 61784-3:2021, 3.1 modified]

3.1.1.10

safety function response time

worst-case elapsed time of a safety function, following an actuation of a safety sensor connected to a fieldbus, until the corresponding safe state of the safety function's actuator(s) is achieved, in the presence of errors or failures.

Note 1 to entry: This concept is introduced in IEC 61784-3, 5.2.4 and is addressed by the functional safety communication profiles defined in that specification.

[SOURCE: IEC 61784-3:2021, 3.1 modified]

3.1.1.11**safety integrity level**

discrete level (one out of a possible four), corresponding to a range of safety integrity values, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest level of safety integrity

Note 1 to entry: The target failure measures (see IEC 61508-4:2010, 3.5.17) for the four safety integrity levels are specified in Tables 2 and 3 of IEC 61508-1:2010.

Note 2 to entry: Safety integrity levels are used for specifying the safety integrity requirements of the safety functions to be allocated to the E/E/PE safety-related systems.

Note 3 to entry: A safety integrity level (SIL) is not a property of a system, subsystem, element or component. The correct interpretation of the phrase “SIL_n safety-related system” (where *n* is 1, 2, 3 or 4) is that the system is potentially capable of supporting safety functions with a safety integrity level up to *n*.

[SOURCE: IEC 61508-4:2010, 3.5.8]

3.1.1.12**safety measure**

measure to control possible communication errors that is designed and implemented in compliance with the requirements of IEC 61508

Note 1 to entry: In practice, several safety measures are combined to achieve the required safety integrity level.

Note 2 to entry: Communication errors and related safety measures are detailed in IEC 61784-3, 5.3 and 5.4.

[SOURCE: IEC 61784-3:2021, 3.1]

3.1.1.13**safety PDU (SPDU)**

PDU transferred through the safety communication channel

Note 1 to entry: The SPDU may include more than one copy of the safety data using differing coding structures and hash functions together with explicit parts of additional protections such as a key, a sequence count, or a time stamp mechanism.

Note 2 to entry: Redundant SCLs may provide two different versions of the SPDU for insertion into separate fields of the OPC UA frame.

[SOURCE: IEC 61784-3:2021, 3.1]

3.1.2 Additional terms and definitions**3.1.2.1****fail-safe**

ability of a system that, by adequate technical or organizational measures, prevents from hazards either deterministically or by reducing the risk to a tolerable measure

Note 1 to entry: Equivalent to functional safety

3.1.2.2**fail-safe substitute values (FSV)**

values which are issued or delivered instead of process values when the safety function is set to a fail-safe state

Note 1 to entry: In this document, the fail-safe substitute values (FSV) are always set to binary “0”.

3.1.2.3**flag**

a one-bit value used to indicate a certain status or control information.

3.1.2.4**Globally Unique Identifier**

a globally unique identifier (GUID) is a 128-bit number used to identify information in computer systems. The term universally unique identifier (UUID) is also used. In this document, UUID version 4 is used.

3.1.2.5

MonitoringNumber (MNR)

a means used to ensure the correct order among transmitted safety PDUs and to monitor the communication delay. The MNR starts at a random value and is incremented with each request. It rolls over to a minimum threshold value that is not zero.

Note 1 to entry: Instance of sequence number as described in IEC 61784-3.

Note 2 to entry: The transmitted MNR is protected by the transmitted CRC signature of the ResponseSPDU.

3.1.2.6

Non-safety-

a predicate meaning that the respective object is a “standard” object and has not been designed and implemented to fulfill any requirements with respect to functional safety.

3.1.2.7

OPC UA Mapper

non-safety-related part of the implementation of this document which maps the SPDU to the actual IEC 62541 services. Depending on which services are used (e.g. Client/Server or PubSub), different mappers can be specified.

3.1.2.8

process values

input and output data (in a safety PDU) that are required to control an automated process

3.1.2.9

qualifier

Qualifier is an attribute (bit or Boolean), indicating whether the corresponding value is valid or not (e.g. being a fail-safe substitute value).

3.1.2.10

SafetyConsumer

Entity (usually software) that implements the data sink of a unidirectional safety link.

3.1.2.11

SafetyData

application data transmitted across a safety network using a safety protocol

Note 1 to entry: The safety communication layer does not ensure the safety of the data itself, but only that the data is transmitted safely.

3.1.2.12

SafetyProvider

Entity (usually software) that implements the data source of a unidirectional safety link.

3.1.2.13

SafetyBaseID

Randomly generated authenticity ID which is used to safely authenticate SafetyProviders having the same SafetyProviderID.

Note 1 to entry: Together with the SafetyProviderID, it is the instance of connection authentication as described in IEC 61784-3.

3.1.2.14

SafetyProviderID

User-assigned, locally unique ID which is used to safely authenticate SafetyProviders within a certain area. All SafetyProviders within this area may share the identical SafetyBaseID.

Note 1 to entry: Together with the SafetyBaseID, it is the instance of connection authentication as described in IEC 61784-3.

3.1.2.15

standard transmission system

the part of the transmission system (implemented in hardware and software) that is not implemented according to any safety standards. This document is using the services of the standard transmission system to transmit prebuilt safety packets.

3.2 Symbols and abbreviated terms

3.2.1 Abbreviated terms from IEC 61784-3

BSC	Binary Symmetric Channel	
CRC	Cyclic Redundancy Check	
PDU	Protocol Data Unit	[ISO/IEC 7498-1]
PL	Performance Level	[ISO 13849-1]
PLC	Programmable Logic Controller	
SCL	Safety Communication Layer	
SIL	Safety Integrity Level	[IEC 61508-4]
SPDU	Safety PDU, Safety Protocol Data Unit	

3.2.2 Additional symbols and abbreviated terms

3.2.2.1 Abbreviated terms

FSV	Fail-safe substitute Values
HMI	Human-machine interface
ID	Identifier
LSB	Least significant bit
MNR	MonitoringNumber
MSB	Most significant bit
OA	Operator Acknowledgment
OPC UA PI	OPC UA Platform Interface
PI	Platform Interface
PV	Process Values
SAPI	Safety Application Program Interface
SFRT	Safety Function Response Time
SPI	Safety Parameter Interface
STrailer	Safety Trailer
UASCTT	OPC UA Safety Compliance Test Tool

3.2.2.2 Symbols

p	Bit error probability
$P_{re,cond}$	Conditional residual error probability

3.3 Conventions

3.3.1 General Conventions

Italics are used to denote a defined term or definition that appears in Subclause 3.1.

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 often 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. Terms or names where two capital letters of abbreviations are in sequence or for separation to a suffix are written with underscores in between.

The abbreviation “F” is an indication for safety related items, technologies, systems, and units (fail-safe, functional safe).

The default data that are used in case of unit failures or errors, are called fail-safe substitute Values (FSV) and are set to binary “0”.

Reserved bit (“res”) are set to “0” and ignored by the receiver for avoiding problems with future versions of this document.

The notation 0x... represents a hexadecimal value.

3.3.2 Conventions for Requirements Numbering

Requirements in this document are designated as [RQx.yz], where x denotes the chapter number, y is a counter and z is an optional character to link closely related requirements. The following are examples of valid requirements designations: [RQ8.15] (requirement 15 in chapter 8); [RQ47.11a], [RQ47.11b] (requirements 11a and 11b in chapter 47, which are closely related).

The initial numbering of requirements was chosen such that counters within each chapter are in ascending order. However, the addition of further requirements leads to deviations from this rule since existing requirements shall keep their initial designation.

For an informative index of all the requirements in this document, see 10.4.

3.3.3 Conventions in state machines

Table 1 – Conventions used in state machines

Convention	Meaning
:=	Assignment: value of an item on the left is replaced by value of the item on the right.
<	Less than: a logical condition yielding TRUE if and only if an item on the left is less than the item on the right.
<=	Less or equal than: a logical condition yielding TRUE if and only if an item on the left is less or equal than the item on the right.
>	Greater than: a logical condition yielding TRUE if and only if the item on the left is greater than the item on the right.
>=	Greater or equal than: a logical condition yielding TRUE if and only if the item on the left is greater or equal than the item on the right.
==	Equality: a logical condition yielding TRUE if and only if the item on the left is equal to an item on the right.
<>	Inequality: a logical condition yielding TRUE if and only if the item on the left is not equal to an item on the right.
&&	Logical “AND” (Operation on binary values or results)
	Logical “OR” (Operation on binary values or results)
⊕	Logical “XOR” (Operation on binary values or digital values)
[..]	UML Guard condition, if and only if the guard is TRUE the respective transition is enabled

4 Overview of OPC UA Safety

4.1 General

This document specifies a safety communication layer (SCL) allowing safety-related devices to use the services of IEC 62541 for the safe exchange of safety-related data. A safety device that implements OPC UA Safety correctly will be able to exchange safety-related data and hereby fulfill the requirements of the international specifications IEC 61508 and IEC 61784-3. This document uses a monitoring number, a timeout, a set of IDs and a cyclic redundancy code for the detection of all possible communication errors which may happen in the underlying IEC 62541 communication channel. These measures have been quantitatively evaluated and offer a probability of dangerous failure per hour (PFH) and a probability of dangerous failure on demand (PFD) sufficing to build safety related applications with a safety integrity level of up to SIL4.

OPC UA Safety itself is an application-independent, general solution. The length and structure of the data sent is defined by the safety application. However, application-dependent companion specifications (addressing for example electro-sensitive protective

electric drives with safety functions, forming presses, robot safety, and automated guided vehicles) are expected to be defined by application-experts in appropriate OPC UA companion specifications.

4.2 Implementation aspects

[RQ4.1] All technical measures for error detection described in this document shall be implemented within the SCL in devices designed in accordance with IEC 61508 and shall meet the target SIL.

4.3 Features

- Runs on top of:
 - IEC 62541 Client/Server with the Method Service Set.
 - IEC 62541 PubSub.
- From an architectural point of view: easy extensibility for other ways of communication.
- goal: no modification of existing OPC UA framework.
- The state machines of this document are independent from the OPC UA Mapper, allowing for a simplified exchange of the mapper.
- Ready for wireless transmission channels.
- Modest requirements on safety network nodes:
 - No clock synchronization is needed (no requirements regarding the accuracy between clocks at different nodes).
 - Within the SafetyConsumer, a safety-related, local timer is required for implementing the SafetyConsumerTimeout. The accuracy of this timer depends on the timing requirements of the safety application.
- End-to-End Safety: Functional safety data is transported between two safety endpoint devices across a standard network that is not functionally safety compliant. This includes the lower transport layers such as the IEC 62541 stack, underlying physical media, and non-safety network elements (e.g. routers and switches).
- “Dynamic” systems:
 - Safety communication partners may change during runtime,
 - and/or increase/decrease in number.
- Well-defined text-strings are used for diagnostic purposes.
- Safety communication and standard communication are independent. However, standard devices and safety devices may use the same communication channel at the same time.
- Functional safety can be achieved without using structurally redundant communication channels i.e. a single channel approach can be used. Redundancy may be used optionally for increased availability.
- For diagnostic purposes, the last SPDU sent and received is accessible in the information model of the SafetyProvider.
- Length of user data: 1-1500 bytes, structures of basic data types, see 6.2.5.

4.4 Security policy

In the final application, an appropriate security environment is needed to be in place for protecting both the operational environment and the safety-related systems.

For this purpose, a threat and risk analysis (TRA) according to IEC 62443 is needed to be carried out on a final application system level.

An adequate reduction of risk against malevolent attacks is necessary for a meaningful application of this document. This document does not describe any measures which will lower the risk of malevolent attacks, but addresses the topic “functional safety”, only

During compliance tests for this document, security aspects are not part of the scope, as it is assumed that the underlying base mechanisms (i.e. methods) already provide adequate security.

5 General

5.1 External documents providing specifications for the profile

In addition to the normative references given in Clause 2, the OPC Test Lab Specification [6] provides information on the testing principles used for Conformance Units referenced in 10.4.

5.2 Safety functional requirements

The following requirements apply for the development of this document:

- a) Safety communication suitable for Safety Integrity Level up to SIL4 (see IEC 61508) and PL e (see ISO 13849-1).
- b) Combination of SIL 1 – 4 devices according to this document as well as non-safety devices on one communication network.
- c) Implementation of the safety transmission protocol is restricted to the safety layer.
- d) The safety-relevant time-out monitoring is implemented in the safety layer.
- e) Safety communication meet the requirements of IEC 61784-3.
- f) [RQ5.1] This document is intended for implementation in safety devices exclusively. Exceptions (e.g. for debugging, simulation, testing, and commissioning) shall be discussed with a notified body.

5.3 Safety measures

[RQ5.2] For an implementation of this document, the following measures shall be implemented: MonitoringNumber; timeout with receipt in the SafetyConsumer; set of IDs for the SafetyProvider; Data Integrity check.

Together, these safety measures address all possible transmission errors as listed in IEC 61784-3, 5.5, see Table 2.

[RQ5.3] The safety measures shall be processed and monitored within the SCL.

643

Table 2 – Deployed measures to detect communication errors

Communication error	Safety measures			
	MonitoringNumber ^a	Timeout with receipt ^b	Set of IDs for SafetyProvider ^c	Data integrity check ^d
Corruption	–	–	–	X
Unintended repetition	X	X	–	–
Incorrect sequence	X	–	–	–
Loss	X	X	–	–
Unacceptable delay	–	X	–	–
Insertion	X	–	–	–
Masquerade	X	–	X	X
Addressing	–	–	X	–
^a Instance of “sequence number” of IEC 61784-3. ^b Instance of “time expectation” (Timeout) and “feedback message” (Receipt) of IEC 61784-3. ^c Instance of “connection authentication” of IEC 61784-3. ^d Instance of “data integrity assurance” of IEC 61784-3, based on CRC signature.				

644 The SafetyConsumer is specified in such a way that for any communication error according to
645 Table 2, a defined fault reaction will occur.

646 In all cases, the faulty SPDU will be discarded, and not forwarded to the safety application.

647 Moreover, if the error rate is too high, the SafetyConsumer is defined in such a way that it will
648 cease to deliver actual process values to the safety application but will deliver fail-safe
649 substitute values instead. In addition, an indication at the Safety Application Program Interface
650 is set which can be queried by the safety application.

651 In case the error rate is still considered acceptable, the state machine repeats the request, see
652 9.4.

653 5.4 Safety communication layer structure

654 This document is based on:

- 655 • the standard transmission system according to IEC 62541
- 656 • an additional safety transmission protocol on top of this standard transmission system

657 Safety applications and standard applications are sharing the same standard IEC 62541
658 communication systems at the same time. The safe transmission function incorporates
659 measures to detect faults or hazards that originate in the standard transmission system which
660 have a potential to compromise the safety subsystems. This includes faults such as:

- 661 • Random errors, for example due to electromagnetic interference on the transmission
662 channel;
- 663 • Failures / faults of the standard hardware;
- 664 • Systematic malfunctions of components within the standard hardware and software.

665 This principle delimits the assessment effort to the “safe transmission functions”. The “standard
666 transmission system” does not need any additional functional safety assessment.

667 The basic communication layers of this document are shown in Figure 2.

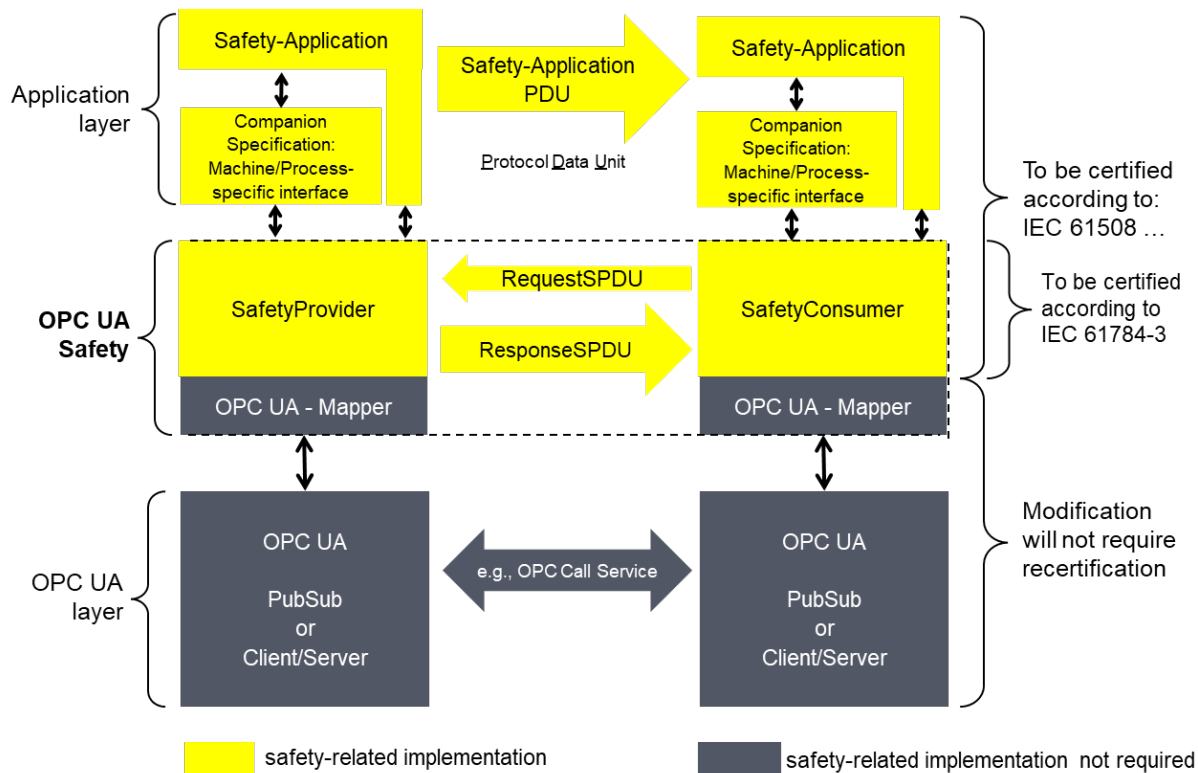


Figure 2 – Safety layer architecture

Summary of the Safety layer architecture:

Part: Application layer

The safety application is either directly connected to the SafetyProvider / SafetyConsumer, or it is connected via a machine-specific or process-specific interface, which is described in companion specifications (e.g. sectoral).

The Safety application layer is expected to be designed and implemented according IEC 61508.

The Safety application layer is not within the scope of this document.

Part: OPC UA Safety

This layer is within the scope of this document. It defines the two services SafetyProvider and SafetyConsumer as basic building blocks. Together, they form the safety communication layer (SCL), implemented in a safety-related way according to IEC 61508.

Safety data is transmitted using point-to-point communication (unidirectional). Each unidirectional data flow internally communicates in both directions, using a request/response pattern. This allows for checking the timeliness of messages using a single clock in the SafetyConsumer, thus eliminating the need for synchronized clocks.

When SafetyConsumers connect to SafetyProviders, they have prior expectation regarding the pair of SafetyProviderID and SafetyBaseID (e.g. by configuration). If this expectation is not fulfilled by the SafetyProvider, fail-safe substitute values are delivered to the safety application instead of the received process values. In contrast, a SafetyProvider does not need to know the ID of the SafetyConsumer and will provide its process value to any SafetyConsumer requesting it.

SafetyProviders are not capable of detecting communication errors. All required error detection is performed by the SafetyConsumer.

If a pair of safety applications needs to exchange safety data in both directions, two pairs of SafetyProvider and SafetyConsumer must be established, one pair for each direction.

The OPC UA Mapper implements the parts of the safety layer which are specific for the IEC 62541 communication service in use, i.e. “PubSub” or “Client/Server”. Therefore, the remaining parts of the safety layer can be implemented independent of the OPC UA service being used.

Part: OPC UA layer

Client/Server:

- The SafetyProvider is implemented using an IEC 62541 server providing a method.
- The SafetyConsumer is implemented using an IEC 62541 client calling the method provided by the SafetyProvider.

PubSub:

- The SafetyProvider publishes the ResponseSPDU and subscribes to the RequestSPDU.
- The SafetyConsumer publishes the RequestSPDU and subscribes to the ResponseSPDU.

5.5 Requirements for CRC calculation

[RQ5.4] Any CRC signature calculation shall start with a preset value of “1”.

[RQ5.5] Any CRC signature calculation resulting in a “0” value, shall use the value “1” instead.

[RQ5.6] SPDUs with all values (incl. CRC signature) being zero shall be ignored by the receiver (SafetyConsumer and SafetyProvider).

6 Safety communication layer services

6.1 General

Clause 6 describes the integration of this document into the IEC 62541 information models in 6.2 and the resulting service interfaces in 6.3. Diagnostic services are described in 6.4.

6.2 Information Models

6.2.1 General

Subclause 6.2 describes the identifiers, types and structure of the objects and methods that are used to implement the OPC UA mappers defined in this document. This implementation serves three purposes:

- support of the safe exchange of SPDUs at runtime
- online browsing, to identify SafetyConsumers and SafetyProviders, and to check their parameters for diagnostic purposes
- offline engineering: the information model of one controller can be exported in a standardized file on its engineering system, be imported in another engineering system, and finally deployed on another controller. This allows for a vendor-independent exchange of the communication interfaces of safety applications, e.g., for establishing connections between devices.

NOTE Neither online browsing nor offline engineering currently supports any features to detect errors. Hence, no guarantees with respect to functional safety are made. This means that online browsing can only be used for diagnostic purposes, and not for exchanging safety-relevant data. In the context of offline engineering, the programmer of the safety application is responsible for the verification and validation of the safety application. It must be assumed that errors may occur during the transfer of the information model from one engineering system to another.

As a consequence, all type values described in 6.2 are defined as read-only, i.e., they can not be written by general IEC 62541 write commands.

6.2.2 Object and ObjectType Definitions

6.2.2.1 SafetyACSet Object

[RQ6.1] Each server shall have a singleton folder called SafetyACSet with a fixed NodeId in the namespace of this document. Because all SafetyProviders and SafetyConsumers on this server contain a hierarchical reference from this object to themselves, it can be used to directly access all SafetyProviders and/or SafetyConsumers. SafetyACSet is intended for safety-related purposes only. It should not reference to non-safety-related items.

Table 3 – SafetyACSet definition

Attribute	Value		
BrowseName	SafetyACSet		
References	NodeClass	BrowseName	Comment
OrganizedBy by the Objects Folder defined in IEC 62541-5.			
HasTypeDefinition	ObjectType	FolderType	Entry point for all SafetyProviders and SafetyConsumers
Conformance Units			
SafetyACSet			

[RQ6.2] In addition, a server shall comprise one IEC 62541 object derived from type SafetyProviderType for each SafetyProvider it implements, and one IEC 62541 object derived from type SafetyConsumerType for each SafetyConsumer it implements. The corresponding information models shown in Figure 3 and Figure 4 shall be used.

A description of the graphical notation for the different types of nodes and references (shown in Figure 3, Figure 4, and Figure 6) can be found in IEC 62541-3.

Figure 3 describes the SafetyProvider and the SafetyConsumer.

NOTE 1 This document assumes (atomic) consistent data exchange between OPC mappers of the two endpoints.

[RQ6.3a] For implementations supporting IEC 62431 Client/Server, the Call Service of the Method Service Set (see IEC 62541-4) shall be used. The Method “ReadSafetyData” has a set of input arguments that make up the RequestSPDU and a set of output arguments that make up the ResponseSPDU. The SafetyConsumer uses the IEC 62541 Client with the IEC 62541 Service Call.

[RQ6.3b] For implementations supporting IEC 62431 PubSub, the IEC 62541 object SafetyPDUs with its properties RequestSPDU and ResponseSPDU shall be used. RequestSPDU is published by the SafetyConsumer and subscribed by the SafetyProvider. ResponseSPDU is published by the SafetyProvider and subscribed by the SafetyConsumer.

NOTE 2 The terms “request” and “response” refer to the behavior on the layer of this document. Within the PubSub context, both requests and responses are realized by repeatedly publishing and subscribing datagrams, see Figure 14.

[RQ6.4] For diagnostic purposes, the SPDUs received and sent shall be accessible by calling the method ReadSafetyDiagnostics.

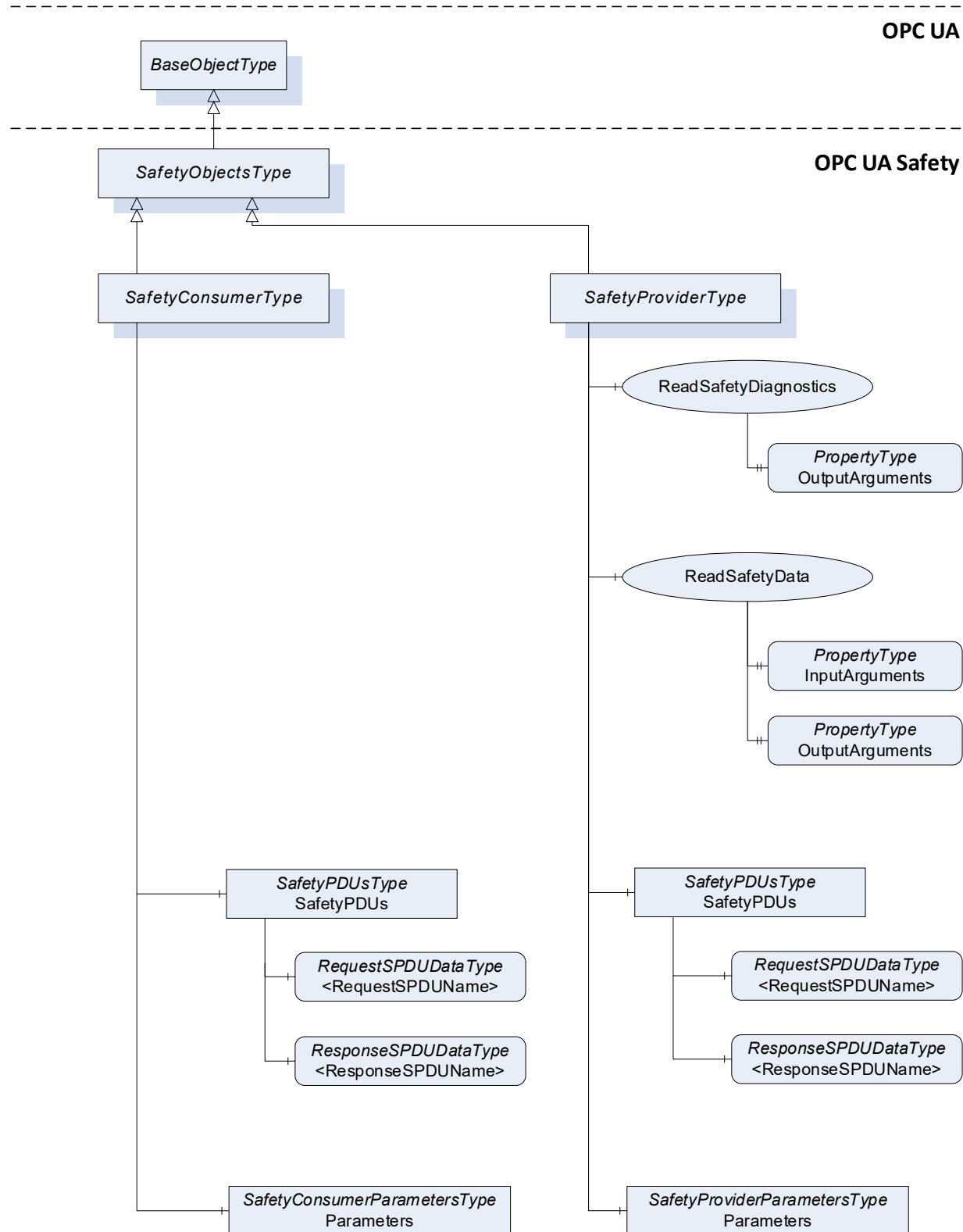
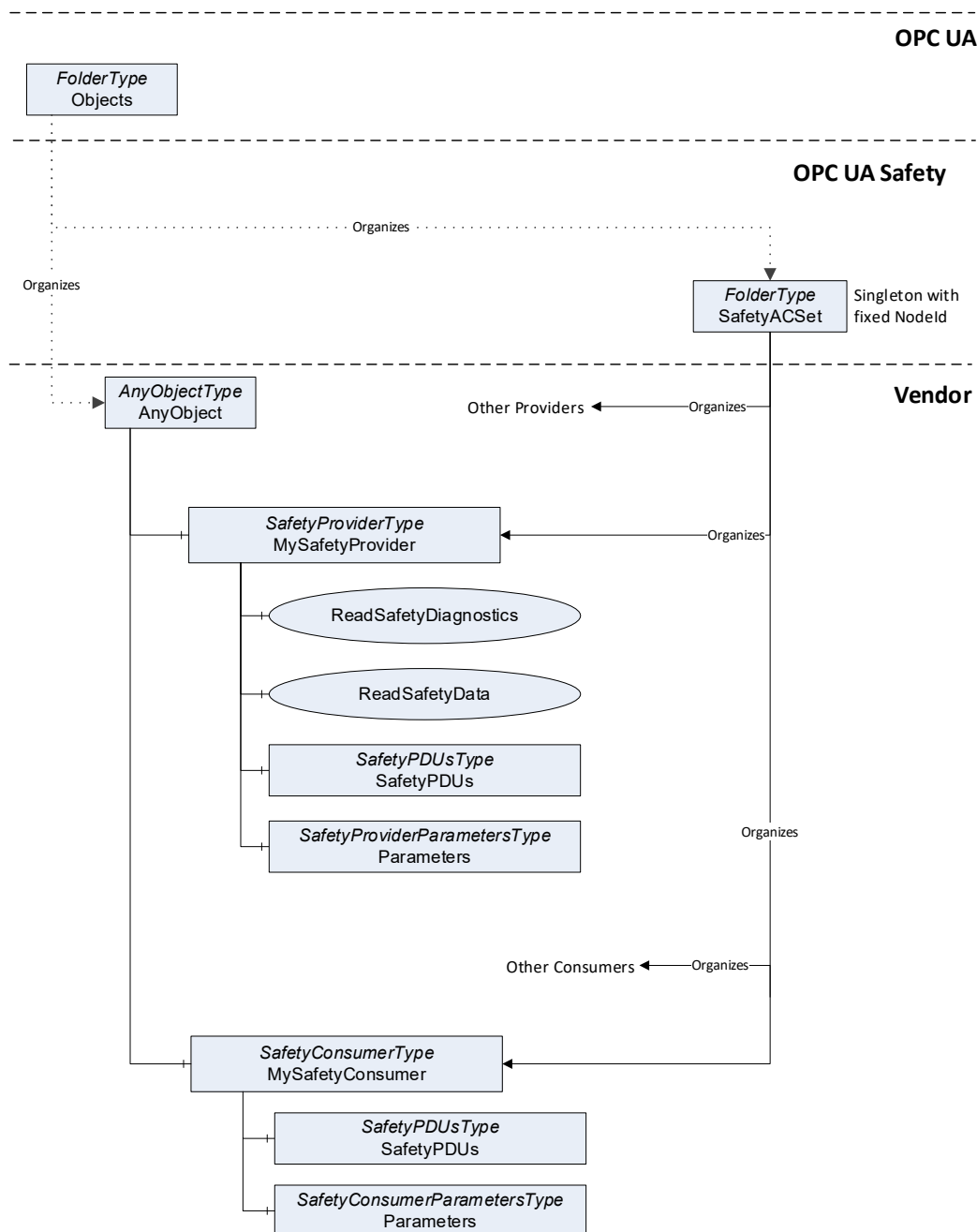


Figure 3 – Server Objects for OPC UA Safety

NOTE For the input/output arguments of the methods ReadSafetyData and ReadSafetyDiagnostics, see 6.2.2.3 and 6.2.2.4. For the parameters of the SafetyProvider and SafetyConsumer, see Figure 6, Table 12, and Table 13. For RequestSPDU and ResponseSPDU, see Table 7, Table 18, Table 20, and 7.2.1.

Figure 4 shows the instances of server objects for this document. The ObjectType for the SafetyProviderType contains methods having outputs of the abstract data type "Structure". Each instance of a SafetyProvider needs its own copy of the methods which contain the concrete DataTypes for "OutSafetyData" and "OutNonSafetyData".

778



779

780

Figure 4 – Instances of server objects for this document

781

6.2.2.2 Safety ObjectType definitions

[RQ6.5] To reduce the number of variations and to alleviate validation testing, the following restrictions apply to instances of SafetyProviderType and SafetyConsumerType (or instances of types derived from SafetyProviderType or SafetyConsumerType):

- 1) The references shown in Figure 4 originating at SafetyProviderType or SafetyConsumerType and below shall be of type HasComponent (and shall not be derived from HasComponent) for object references or HasProperty (and shall not be derived from HasProperty) for property references.
- 2) As BrowseNames (i.e. name and namespace) are used to find methods, the names of objects and properties shall be locally unique.

790

791

3) The DataType of both Properties and MethodArguments shall be used as specified, and no derived DataTypes shall be used (exception: OutSafetyData and OutNonSafetyData).

4) In IEC 62541, the sequence of MethodArguments is relevant.

Table 4 – SafetyObjectsType Definition

Attribute	Value				
BrowseName	SafetyObjectsType				
IsAbstract	True				
References	Node Class	BrowseName	DataType	TypeDefinition	Modelling Rule
Subtype of BaseObjectType					
Conformance Units					
SafetySupport					

Table 5 – SafetyProviderType Definition

Attribute	Value				
BrowseName	SafetyProviderType				
IsAbstract	False				
References	Node Class	BrowseName	DataType	TypeDefinition	Modelling Rule
Subtype of SafetyObjectsType					
HasComponent	Method	ReadSafetyData			Optional
HasComponent	Method	ReadSafetyDiagnostics			Optional
HasComponent	Object	SafetyPDUs		SafetyPDUsType	Optional
HasComponent	Object	Parameters		SafetyProviderParametersType	Mandatory
Conformance Units					
SafetyProviderParameters					

[RQ6.6] Instances of SafetyProviderType shall use non-abstract DataTypes for the arguments OutSafetyData and OutNonSafetyData.

Table 6 – SafetyConsumerType Definition

Attribute	Value				
BrowseName	SafetyConsumerType				
IsAbstract	False				
References	Node Class	BrowseName	DataType	TypeDefinition	Modelling Rule
Subtype of SafetyObjectsType					
HasComponent	Object	SafetyPDUs		SafetyPDUsType	Optional
HasComponent	Object	Parameters		SafetyConsumerParametersType	Mandatory
Conformance Units					
SafetyConsumerParameters					

6.2.2.3 Method ReadSafetyData

This method is mandatory for the profile SafetyProviderServerMapper (see 11.3.2.1). It is used to read SafetyData from the SafetyProvider. It is in the responsibility of the safety application, that this method is not concurrently called by multiple SafetyConsumers. Otherwise, the SafetyConsumer may receive invalid responses resulting in a safe reaction which may lead to spurious trips and/or system unavailability.

The method argument OutSafetyData has an application-specific type derived from Structure. This type (including the type identifier) is expected to be the same in both the SafetyProvider and the SafetyConsumer. Otherwise, the SafetyConsumer will not accept the transferred data

and switch to fail-safe values instead (see state S16 in Table 34 – SafetyConsumer states as well as 7.2.3.2 and 7.2.3.4).

Signature

ReadSafetyData (

```
[in]    UInt32                InSafetyConsumerID,
[in]    UInt32                InMonitoringNumber,
[in]    InFlagsType           InFlags,
[out]   Structure            OutSafetyData,
[out]   OutFlagsType          OutFlags,
[out]   UInt32                OutSPDU_ID_1,
[out]   UInt32                OutSPDU_ID_2,
[out]   UInt32                OutSPDU_ID_3,
[out]   UInt32                OutSafetyConsumerID,
[out]   UInt32                OutMonitoringNumber,
[out]   UInt32                OutCRC,
[out]   Structure            OutNonSafetyData)
```

;

Table 7 – ReadSafetyData Method Arguments

Argument	Description
InSafetyConsumerID	“Safety Consumer Identifier”, see SafetyConsumerID in Table 23.
InMonitoringNumber	“Monitoring Number of the RequestSPDU”, see 7.2.1.3 and MonitoringNumber in Table 23.
InFlags	“Byte with non-safety-related flags from SafetyConsumer”, see 6.2.3.1.
OutSafetyData	“Safety Data”, see 7.2.1.5.
OutFlags	“Byte with safety-related flags from SafetyProvider”, see 6.2.3.2.
OutSPDU_ID_1	“Safety PDU Identifier Part1”, see 7.2.3.2.
OutSPDU_ID_2	“Safety PDU Identifier Part2”, see 7.2.3.2.
OutSPDU_ID_3	“Safety PDU Identifier Part3”, see 7.2.3.2.
OutSafetyConsumerID	“Safety Consumer Identifier”, see SafetyConsumerID in Table 23 and Table 26.
OutMonitoringNumber	Monitoring Number of the ResponseSPDU, see 7.2.1.9, 7.2.3.1, and Figure 11.
OutCRC	CRC-checksum over the ResponseSPDU, see 7.2.3.5.
OutNonSafetyData	“Non-safe data” see 7.2.1.11.

Table 8 – ReadSafetyData Method AddressSpace definition

Attribute	Value				
BrowseName	ReadSafetyData				
References	NodeClass	BrowseName	Data Type	TypeDefinition	ModellingRule
HasProperty	Variable	InputArguments	Argument[]	PropertyType	Mandatory
HasProperty	Variable	OutputArguments	Argument[]	PropertyType	Mandatory
Conformance Units					
ReadSafetyData					

6.2.2.4 Method ReadSafetyDiagnostics

This method is mandatory for the profile SafetyProviderServerMapper and optional for the profile SafetyProviderPubSubMapper (see 11.3.2.1). It is provided for each SafetyProvider serving as a diagnostic interface, see 6.4.3.

Signature

```

ReadSafetyDiagnostics (
    [out] UInt32                InSafetyConsumerID,
    [out] UInt32                InMonitoringNumber,
    [out] InFlagsType           InFlags,
    [out] Structure           OutSafetyData,
    [out] OutFlagsType          OutFlags,
    [out] UInt32                OutSPDU_ID_1,
    [out] UInt32                OutSPDU_ID_2,
    [out] UInt32                OutSPDU_ID_3,
    [out] UInt32                OutSafetyConsumerID,
    [out] UInt32                OutMonitoringNumber,
    [out] UInt32                OutCRC,
    [out] Structure           OutNonSafetyData)
;

```

Table 9 – ReadSafetyDiagnostics Method Arguments

Argument	Description
InSafetyConsumerID	see Table 7
InMonitoringNumber	see Table 7
InFlags	see Table 7
OutSafetyData	see Table 7
OutFlags	see Table 7
OutSPDU_ID_1	see Table 7
OutSPDU_ID_2	see Table 7
OutSPDU_ID_3	see Table 7
OutSafetyConsumerID	see Table 7
OutMonitoringNumber	see Table 7
OutCRC	see Table 7
OutNonSafetyData	see Table 7

Table 10 – ReadSafetyDiagnostics Method AddressSpace definition

Attribute	Value				
BrowseName	ReadSafetyDiagnostics				
References	NodeClass	BrowseName	DataType	TypeDefinition	ModellingRule
HasProperty	Variable	OutputArguments	Argument[]	PropertyType	Mandatory
Conformance Units					
ReadSafetyDiagnostics					