BS EN IEC 62541-15:2025

BSI Standards Publication

OPC Unified Architecture

Part 15: Safety

Documents
Document Sharing Hub

Full document details: BS EN IEC 62541-15:2025

National foreword

This British Standard is the UK implementation of EN IEC 62541-15:2025. It is identical to IEC 62541-15:2025.

The UK participation in its preparation was entrusted to Technical Committee GEL/65/3, Industrial communications: process measurement and control, including fieldbus.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

© The British Standards Institution 2025
Published by BSI Standards Limited 2025

ISBN 978 0 539 28589 5

ICS 25.040.40; 35.100.05

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 April 2025.

Amendments/corrigenda issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: BS EN IEC 62541-15:2025

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN IEC 62541-15

April 2025

ICS 25.040.40

English Version

OPC Unified Architecture - Part 15: Safety (IEC 62541-15:2025)

Architecture unifiée OPC - Partie 15: Sécurité
(IEC 62541-15:2025)

OPC Unified Architecture - Teil 15: Sicherheit
(IEC 62541-15:2025)

This European Standard was approved by CENELEC on 2025-04-03. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and the United Kingdom.

European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

© 2025 CENELEC All rights of exploitation in any form and by any means reserved worldwide for CENELEC Members.

Ref. No. EN IEC 62541-15:2025 E

Documents
Document Sharing Hub

Full document details: BS EN IEC 62541-15:2025

European foreword

The text of document 65C/1334/FDIS, future edition 1 of IEC 62541-15, prepared by SC 65C "Industrial networks" of IEC/TC 65 "Industrial-process measurement, control and automation" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN IEC 62541-15:2025.

The following dates are fixed:

- latest date by which the document has to be implemented at national level by publication of an identical national standard or by endorsement (dop) 2026-04-30
- latest date by which the national standards conflicting with the document have to be withdrawn (dow) 2028-04-30

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CENELEC shall not be held responsible for identifying any or all such patent rights.

Any feedback and questions on this document should be directed to the users' national committee. A complete listing of these bodies can be found on the CENELEC website.

Endorsement notice

The text of the International Standard IEC 62541-15:2025 was approved by CENELEC as a European Standard without any modification.

In the official version, for Bibliography, the following notes have to be added for the standard indicated:

IEC 61000-6-7	NOTE	Approved as EN 61000-6-7
IEC 61511 series	NOTE	Approved as EN 61511 series
IEC 62061	NOTE	Approved as EN IEC 62061
ISO 13849 series	NOTE	Approved as EN ISO 13849 series
ISO 13849-1	NOTE	Approved as EN ISO 13849-1
ISO 13849-2	NOTE	Approved as EN ISO 13849-2
IEC 62541-7	NOTE	Approved as EN IEC 62541-7
IEC 62541-8	NOTE	Approved as EN IEC 62541-8

AVA Documents
Document Sharing Hub

Full document details: BS EN IEC 62541-15:2025

Annex ZA
(normative)

Normative references to international publications with their corresponding European publications

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.

NOTE 1 Where an International Publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

NOTE 2 Up-to-date information on the latest versions of the European Standards listed in this annex is available here: www.cencenelec.eu.

Publication	Year	Title	EN/HD	Year
IEC 61508	series	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1: General requirements (see Functional Safety and IEC 61508)	EN 61508	series
IEC 61784-3	2021	Industrial communication networks - Profiles - Part 3: Functional safety fieldbuses - General rules and profile definitions	EN IEC 61784-3	2021
IEC 62443	series	Security for industrial automation and control systems	EN IEC 62443	series
IEC/TR 62541-1	2020	OPC Unified Architecture - Part 1: Overview and concepts	CLC IEC/TR 62541-1	2021
IEC 62541-3	2020	OPC Unified Architecture - Part 3: Address Space Model	EN IEC 62541-3	2020
IEC 62541-4	2020	OPC Unified Architecture - Part 4: Services	EN IEC 62541-4	2020
IEC 62541-5	2020	OPC Unified Architecture - Part 5: Information Model	EN IEC 62541-5	2020
IEC 62541-6	2020	OPC Unified Architecture - Part 6: Mappings	EN IEC 62541-6	2020
IEC 62541-14	-	OPC unified architecture - Part 14: PubSub	EN IEC 62541-14	-
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	-	-

AVA Documents
Document Sharing Hub

Full document details: BS EN IEC 62541-15:2025

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

AVA Documents Document Sharing Hub

Full document details: BS EN IEC 62541-15:2025

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

AVA Documents
Document Sharing Hub

Full document details: BS EN IEC 62541-15:2025

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

AVA Documents
Document Sharing Hub

Full document details: BS EN IEC 62541-15:2025

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

Documents
Document Sharing Hub
Full document details: BS EN IEC 62541-15:2025

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.

Documents
Document Sharing Hub

Full document details: BS EN IEC 62541-15:2025

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.

Documents
Document Sharing Hub

Full document details: BS EN IEC 62541-15:2025

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.

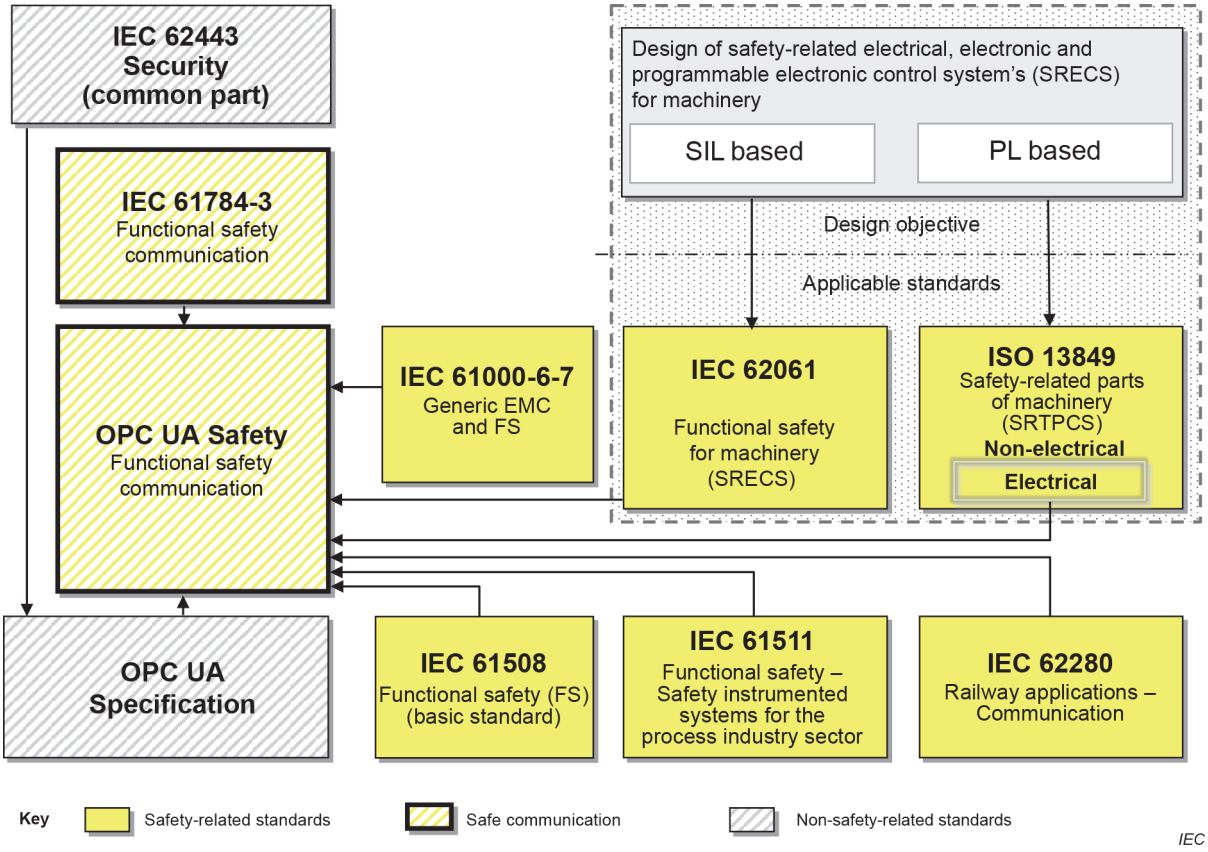

Figure 1 – Relationships of OPC UA safety with other standards

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.

Documents
Document Sharing Hub
Full document details: BS EN IEC 62541-15:2025

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*

AVA Documents Document Sharing Hub

Full document details: BS EN IEC 62541-15:2025

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*

3 Terms, definitions, symbols, abbreviated terms and conventions

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC 62541-1:2020, IEC 62541-3:2020, IEC 62541-4:2020, IEC 62541-6:2020 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 IEC 62541 information modeling to describe the concepts in this document.

3.1.1 Common terms and definitions

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, 3.10]

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 60050-192:2024, 192-03-02, modified – notes added]

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 can 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, new note to entry added]

Documents
Document Sharing Hub
Full document details: BS EN IEC 62541-15:2025

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: IEV 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]

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

[SOURCE: ISO/IEC 2382:2015, 2123031, modified – insertion of "(usually octets)", deletion of notes and source]

3.1.1.5
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 13849-1:2023, 3.1.5]

3.1.1.6
residual error probability
probability of an error undetected by the *SCL* safety measures

[SOURCE: IEC 61784-3:2021, 3.1.35]

3.1.1.7
residual error rate
statistical rate at which the *SCL* safety measures fail to detect errors

[SOURCE: IEC 61784-3:2021, 3.1.36]

3.1.1.8
safety communication layer
SCL
communication layer above the IEC 62541 communication stack that includes all necessary additional measures to ensure safe transmission of data in accordance with the requirements of IEC 61508

Note 1 to entry: The *SCL* provides several services, the most important ones being the *SafetyProvider* and the *SafetyConsumer*.

[SOURCE: IEC 61784-3:2021, 3.1.39, modified – "FAL" replaced by "IEC 62541 communication stack", note to entry added]

3.1.1.9
safety function response time
worst case elapsed time following an actuation of a safety sensor connected to a fieldbus, until the corresponding safe state of its safety actuator(s) is achieved in the presence of errors or failures in the safety function

Note 1 to entry: This concept is introduced in IEC 61784-3:2021, 5.2.4 and is addressed by the functional safety communication profiles defined in the IEC 61784-3 series of documents.

[SOURCE: IEC 61784-3:2021, 3.1.44]

Documents
Document Sharing Hub
Full document details: BS EN IEC 62541-15:2025

3.1.1.10
safety integrity level
SIL
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

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 Table 2 and Table 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]

3.1.1.11
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 61784-3:2021, 5.3 and 5.4.

[SOURCE: IEC 61784-3:2021, 3.1.46]

3.1.1.12
safety PDU
SPDU
PDU transferred through the *safety communication channel*

Note 1 to entry: The SPDU may include more than one copy of the *SafetyData* 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 IEC 62541 frame.

[SOURCE: IEC 61784-3:2021, 3.1.47]

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

Documents
Document Sharing Hub
Full document details: BS EN IEC 62541-15:2025

3.1.2.4
globally unique identifier
GUID
128-bit number used to identify information in computer systems

Note 1 to entry: The term universally unique identifier (UUID) is also used.

Note 2 to entry: In this document, UUID version 4 is used.

3.1.2.5
MonitoringNumber
MNR
means used to ensure the correct order among transmitted safety PDUs and to monitor the communication delay

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

Note 2 to entry: 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 3 to entry: The transmitted *MNR* is protected by the transmitted *CRC* signature of the ResponseSPDU.

3.1.2.6
non-safety-
predicate meaning that the respective object is a "standard" object and has not been designed and implemented to fulfil 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

Note 1 to entry: Depending on which services of IEC 62541 are being used (e.g. *Client/Server* or *PubSub*), different mappers can be specified.

3.1.2.8
process values
PV
input and output data (in a safety PDU) that are required to control an automated process

3.1.2.9
qualifier
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
SafetyAutomationComponent
SafetyAC
communication partner in a unidirectional safety link

Note 1 to entry: A *SafetyAutomationComponent* can be a *SafetyProvider* (data source), a *SafetyConsumer* (data sink), or both.

3.1.2.11
SafetyConsumer
entity (usually software) that implements the data sink of a unidirectional safety link

Documents
Document Sharing Hub
Full document details: BS EN IEC 62541-15:2025

3.1.2.12
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.

3.1.2.13
SafetyProvider
entity (usually software) that implements the data source of a unidirectional safety link

3.1.2.14
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 an instance of connection authentication as described in IEC 61784-3.

3.1.2.15
SafetyProviderID
user-assigned, locally unique identifier which is used to safely authenticate *SafetyProviders* within a certain area

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

Note 2 to entry: All *SafetyProviders* within an area such defined may share an identical *SafetyBaseID*.

3.1.2.16
standard transmission system
part of the transmission system (implemented in hardware and software) that is not implemented according to any safety standards

Note 1 to entry: This document is using the services of the *standard transmission system* to transmit prebuilt safety packets.

3.2 Symbols and abbreviated terms

For the purposes of this document, the following symbols and abbreviated terms apply.

3.2.1 Abbreviated terms from IEC 61784-3

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	

Documents
Document Sharing Hub
Full document details: BS EN IEC 62541-15:2025

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
TRA	threat and risk analysis

3.2.2.2 Symbols

p	bit error probability
$P_{re,cond}$	conditional residual error probability

3.3 Conventions

3.3.1 General conventions

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 bits ("res") are set to "0" and ignored by the receiver to avoid 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.

AVA Documents Document Sharing Hub

Full document details: BS EN IEC 62541-15:2025

For an informative index of all the requirements in this document, see 10.3.

3.3.3 Conventions in state machines

See Table 1 for the conventions used 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 IEC 61508 series and IEC 61784-3. This document uses a *MonitoringNumber*, a timeout, a set of IDs and a *cyclic redundancy check* (*CRC*) for the detection of all possible communication errors which can happen in the underlying IEC 62541 *standard transmission system.* These *safety 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 *SIL*4.

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 equipment, 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 the IEC 61508 series and shall meet the target *SIL*.

Documents
Document Sharing Hub
Full document details: BS EN IEC 62541-15:2025

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 necessary (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 *SafetyData* 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 can change during runtime,
  - either an increase or decrease, or both, in the number of safety communication partners can occur.
- Well-defined text-strings are used for diagnostic purposes.
- Safety communication and standard communication are independent. However, standard devices and safety devices can use the same *standard transmission system* at the same time.
- Functional safety can be achieved without using structurally redundant *standard transmission system*s i.e. a single channel approach can be used. Redundancy can 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 octet to 1 500 octets, structures of basic *DataTypes*, see 6.2.5.

4.4 Security policy

In the final application, an appropriate security environment is necessary to protect both the operational environment and the safety-related systems.

This document does not cover security aspects, nor does it provide any requirements for security.

A threat and risk analysis (TRA) according to the IEC 62443 series shall be carried out on a final application system level.

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.

Documents
Document Sharing Hub
Full document details: BS EN IEC 62541-15:2025

5 General

5.1 External documents providing specifications for the profile

No other external documents are providing specifications in addition to the Normative references given in Clause 2.

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 *SIL*4 (see the IEC 61508 series) and PL e (see ISO 13849-1).

b) Combination of *SIL* 1 to 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 *safety 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 61784-3:2021, 5.5, see Table 2.

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

Table 2 – Deployed safety 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.

Documents
Document Sharing Hub
Full document details: BS EN IEC 62541-15:2025

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

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

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

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

5.4 Safety communication layer structure

This document is based on:

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

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

- Random errors, for example due to electromagnetic interference on the transmission channel;
- Failures or faults of the standard hardware;
- Systematic malfunctions of components within the standard hardware and software.

This principle delimits the assessment effort to the "safe transmission functions". The *standard transmission system* does not require any additional functional safety assessment.

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

Documents
Document Sharing Hub
Full document details: BS EN IEC 62541-15:2025

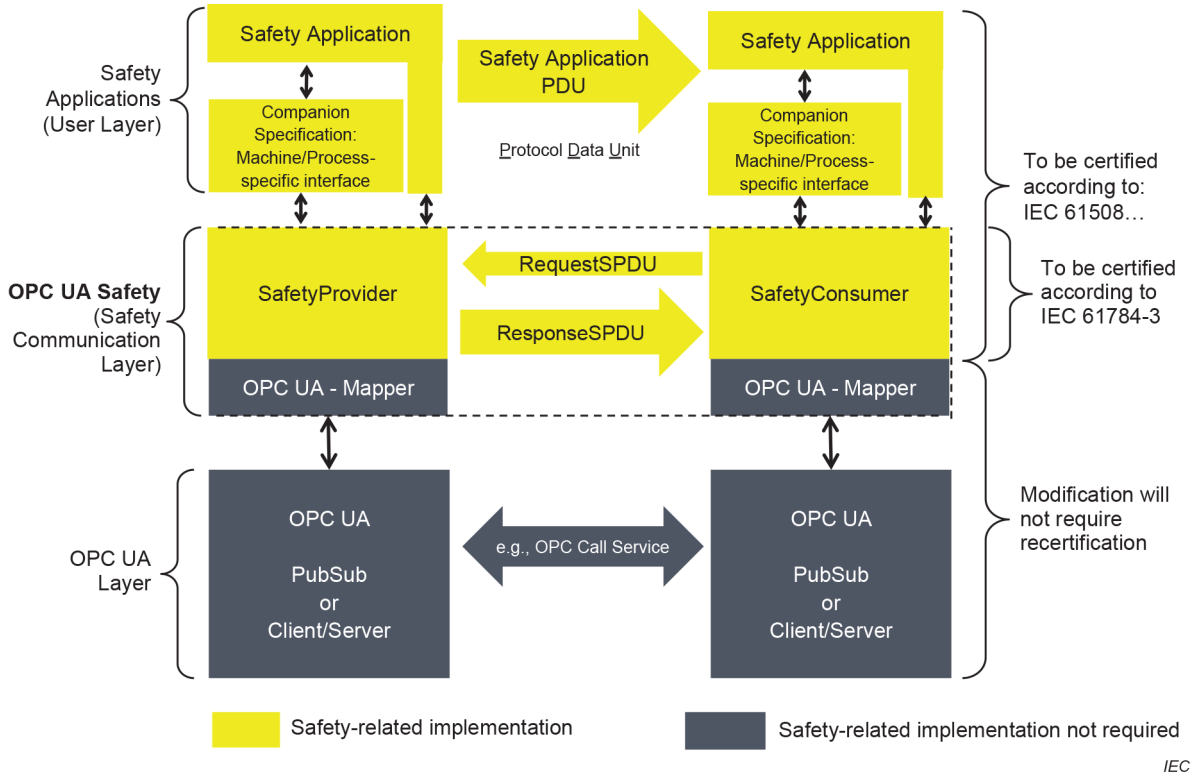

Figure 2 – Safety layer architecture

Summary of the architecture:

Part: User layer

The safety applications in the User Layer are either directly connected to the *SafetyProvider* or *SafetyConsumer*, or they are connected via a machine-specific or process-specific interface, which is described in companion specifications (e.g. sectoral).

The safety applications are expected to be designed and implemented according to the IEC 61508 series.

The Safety applications in the User Layer are not within the scope of this document.

Part: OPC UA Safety (Safety Communication Layer)

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 the IEC 61508 series.

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

When *SafetyConsumers* connect to *SafetyProviders*, they have prior expectations 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, it is not necessary for a *SafetyProvider* to know the *SafetyConsumerID* of the *SafetyConsumer* and will provide its *process values* to any *SafetyConsumer* requesting it.

AVA Documents Document Sharing Hub

Full document details: BS EN IEC 62541-15:2025

SafetyProviders can not detect communication errors. All required error detection is performed by the *SafetyConsumer*.

If it is necessary for a pair of safety applications to exchange SafetyData in both directions, two pairs of *SafetyProviders* and *SafetyConsumers* shall be established, one pair for each direction.

Refer to B.2 in Annex B for use cases how *SafetyProviders* and *SafetyConsumers* can be connected.

The OPC UA mapper implements the parts of the *safety communication 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 communication layer* can be implemented independent of the IEC 62541 *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.

Documents
Document Sharing Hub
Full document details: BS EN IEC 62541-15:2025

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. It is assumed that errors can occur during the transfer of the *Information Model* from one engineering system to another in the context of offline engineering. Therefore, the programmer of the safety application is responsible for the verification and validation of the safety application.

Consequently, all type values described in 6.2 are defined as read-only, i.e. they cannot 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 *SafetyConsumers*. *SafetyACSet* is intended for safety-related purposes only. It should not reference *non-safety*-related items.

See Table 3 for the definition of the *SafetyACSet*.

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 *DataType SafetyProviderType* for each *SafetyProvider* it implements, and one IEC 62541 *Object* derived from *DataType 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.

Documents
Document Sharing Hub
Full document details: BS EN IEC 62541-15:2025

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 62541 *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 62541 *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 behaviour on the layer of this document. Within the *PubSub* context, both requests and responses are realized by repeatedly publishing and subscribing *Messages*, see Figure 14.

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

Documents
Document Sharing Hub
Full document details: BS EN IEC 62541-15:2025

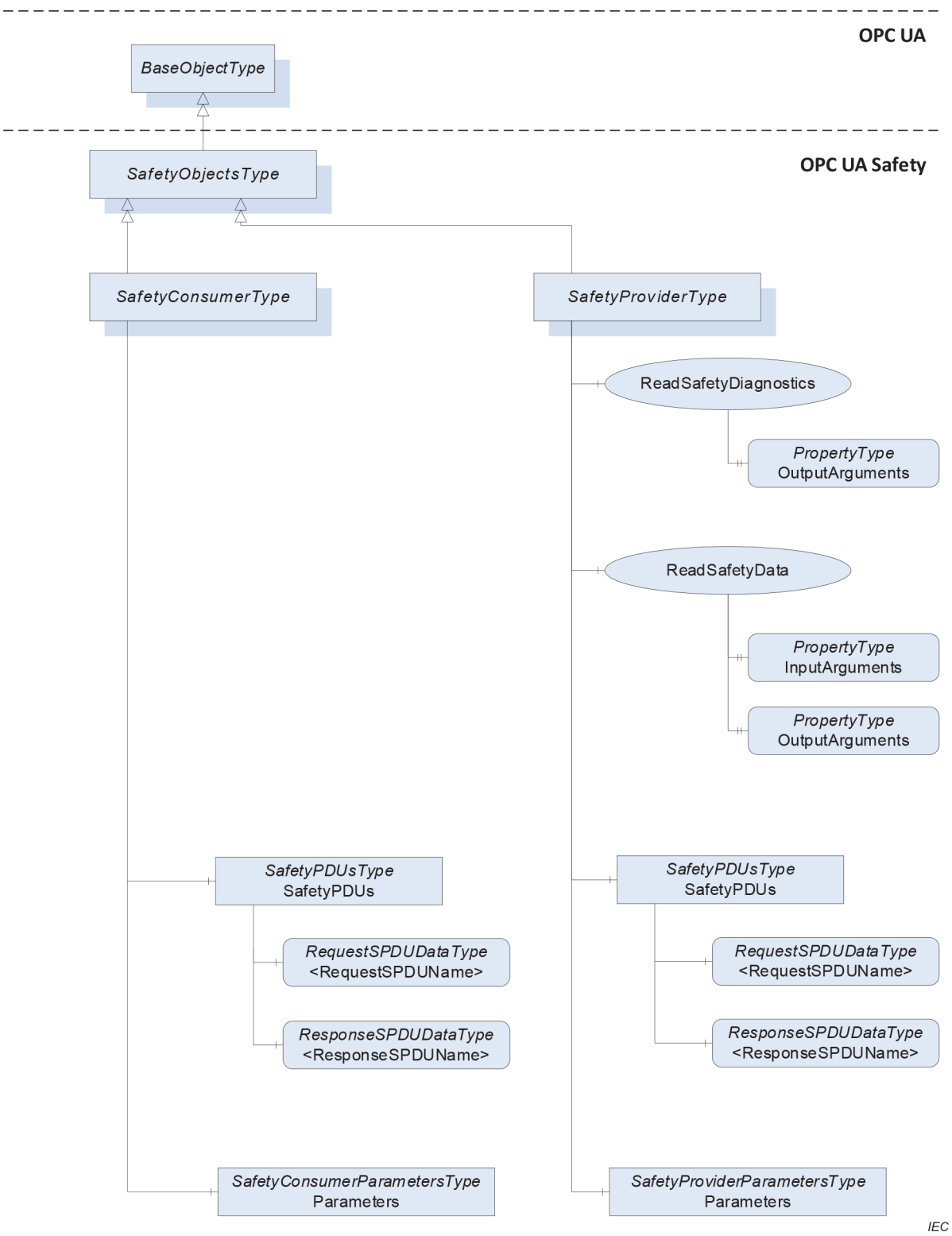

Figure 3 – Server Objects for OPC UA Safety

NOTE 3 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 *DataType Structure*. Each instance of a *SafetyProvider* requires its own copy of the *Methods* which contain the concrete *DataTypes* for *OutSafetyData* and *OutNonSafetyData*.

AVA Documents Document Sharing Hub

Full document details: BS EN IEC 62541-15:2025

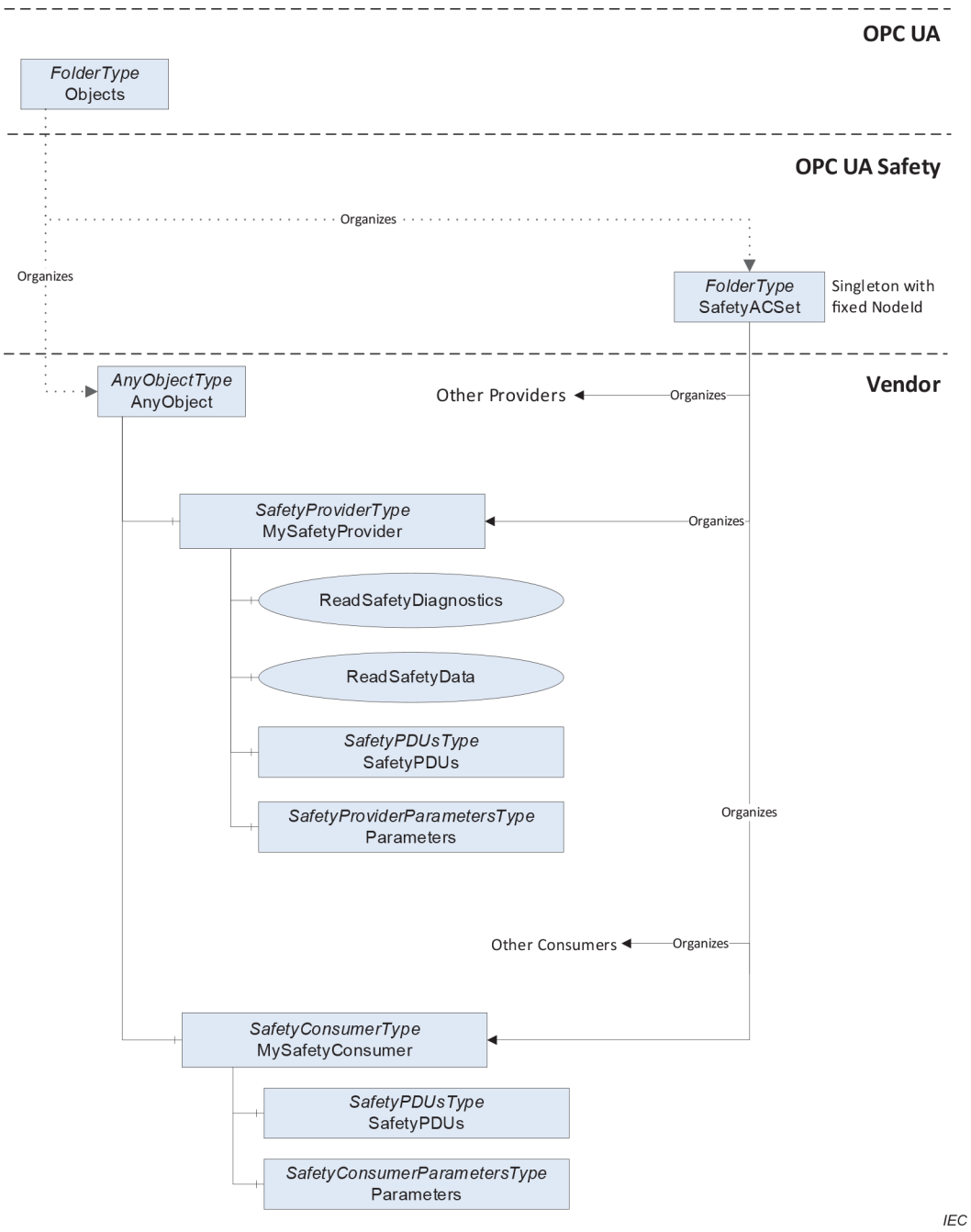

Figure 4 – Instances of Server Objects for this document

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 *DataTypes* derived from *SafetyProviderType* or *SafetyConsumerType*):

1) The references shown in Figure 4 originating at *SafetyProviderType* or *SafetyConsumerType* and below shall be of *ReferenceType HasComponent* (and shall not be derived from *ReferenceType HasComponent*) for *Object References* or *ReferenceType HasProperty* (and shall not be derived from *ReferenceType 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.

Documents
Document Sharing Hub
Full document details: BS EN IEC 62541-15:2025

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 order of *Method* arguments is relevant.

See Table 4 for the definition of the *SafetyObjectsType*.

Table 4 – SafetyObjectsType definition

Attribute	Value				
BrowseName	SafetyObjectsType				
IsAbstract	True				
References	**Node class**	**BrowseName**	**DataType**	**TypeDefinition**	**Modelling rule**
Subtype of BaseObjectType					
Conformance units					
SafetySupport					

See Table 5 for the definition of the *SafetyProviderType*.

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*.

See Table 6 for the definition of the *SafetyConsumerType*.

Documents
Document Sharing Hub
Full document details: BS EN IEC 62541-15:2025

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		SafetyConsumerParameters Type	Mandatory
Conformance units					
SafetyConsumerParameters					

6.2.2.3 Method ReadSafetyData

This *Method* is mandatory for the *Facet SafetyProviderServerMapper*. 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* can receive invalid responses resulting in a safe reaction which can lead to either spurious trips or system unavailability, or both.

See Table 7 for *Method ReadSafetyData*'s arguments and Table 8 for its *AdressSpace* definition.

The *Method* argument *OutSafetyData* has an application-specific *DataType* derived from *Structure*. This *DateType* (including the *DataTypeID*) 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 substitute values* instead (see state S16 in Table 34 as well as 7.2.3.2 and 7.2.3.5). The *Method* argument *OutNonSafetyData* has an application-specific *DataType* derived from *Structure*.

Documents
Document Sharing Hub
Full document details: BS EN IEC 62541-15:2025

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	"*MonitoringNumber* of the *RequestSPDU*", see 7.2.1.3 and *MonitoringNumber* in Table 23.
InFlags	"Octet with *non-safety*-related *flags* from *SafetyConsumer*", see 6.2.3.1.
OutSafetyData	"*SafetyData*", see 7.2.1.5.
OutFlags	"Octet 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	*MonitoringNumber* of the *ResponseSPDU*, see 7.2.1.9, 7.2.3.1, and Figure 11.
OutCRC	*CRC* over the *ResponseSPDU*, see 7.2.3.6.
OutNonSafetyData	"Non-safe data" see 7.2.1.11.

Documents
Document Sharing Hub
Full document details: BS EN IEC 62541-15:2025

Table 8 – ReadSafetyData Method AddressSpace definition

Attribute	Value				
BrowseName	ReadSafetyData				
References	**NodeClass**	**BrowseName**	**DataType**	**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 *Facet SafetyProviderServerMapper* and optional for the *Facet SafetyProviderPubSubMapper*. It is provided for each *SafetyProvider* serving as a *Diagnostic Interface*, see 6.4.3.

See Table 9 for the arguments of *Method ReadSafetyDiagnostics* and Table 10 for its *AddressSpace* definition.

The *Method* arguments *OutSafetyData* and *OutNonSafetyData* are application-specific types derived from *Structure*.

Documents
Document Sharing Hub
Full document details: BS EN IEC 62541-15:2025