SLOVENSKI STANDARD

oSIST prEN IEC 62541-15:2024

01-junij-2024

Enotna arhitektura OPC - 15. del: Varnost

OPC Unified Architecture - Part 15: Safety

Architecture unifiée OPC - Partie 15: Sécurité fonctionnelle

Ta slovenski standard je istoveten z: **prEN IEC 62541-15:2024**

ICS:

25.040.40	Merjenje in krmiljenje industrijskih postopkov	Industrial process measurement and control
35.240.50	Uporabniške rešitve IT v industriji	IT applications in industry

oSIST prEN IEC 62541-15:2024 **en,fr,de**

65C/1292/CDV

COMMITTEE DRAFT FOR VOTE (CDV)

PROJECT NUMBER: **IEC 62541-15 ED1**	
DATE OF CIRCULATION: **2024-03-22**	CLOSING DATE FOR VOTING: **2024-06-14**
SUPERSEDES DOCUMENTS: **65C/1269/CD, 65C/1285A/CC**	

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 CDV to the secretary.

FUNCTIONS CONCERNED:

☐ EMC ☐ ENVIRONMENT ☐ QUALITY ASSURANCE ☐ SAFETY

☒ SUBMITTED FOR CENELEC PARALLEL VOTING	☐ NOT SUBMITTED FOR CENELEC PARALLEL VOTING

Attention IEC-CENELEC parallel voting

The attention of IEC National Committees, members of CENELEC, is drawn to the fact that this Committee Draft for Vote (CDV) is submitted for parallel voting.

The CENELEC members are invited to vote through the CENELEC online voting system.

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 relevant "In Some Countries" clauses to be included should this proposal proceed. Recipients are reminded that the CDV stage is the final stage for submitting ISC clauses. (SEE AC/22/2007 OR NEW GUIDANCE DOC).

TITLE:

OPC Unified Architecture - Part 15: Safety

PROPOSED STABILITY DATE: 2028

NOTE FROM TC/SC OFFICERS:

NC comments on this CDV will be addressed during the SC65C/WG12 virtual meeting on July 1st-4th, 2024 (four Zoom sessions from 13:00 to 16:00 Geneva time, 11:00 to 14:00 UTC). Meeting details will be sent at a later date by the convenor.

CONTENTS

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.

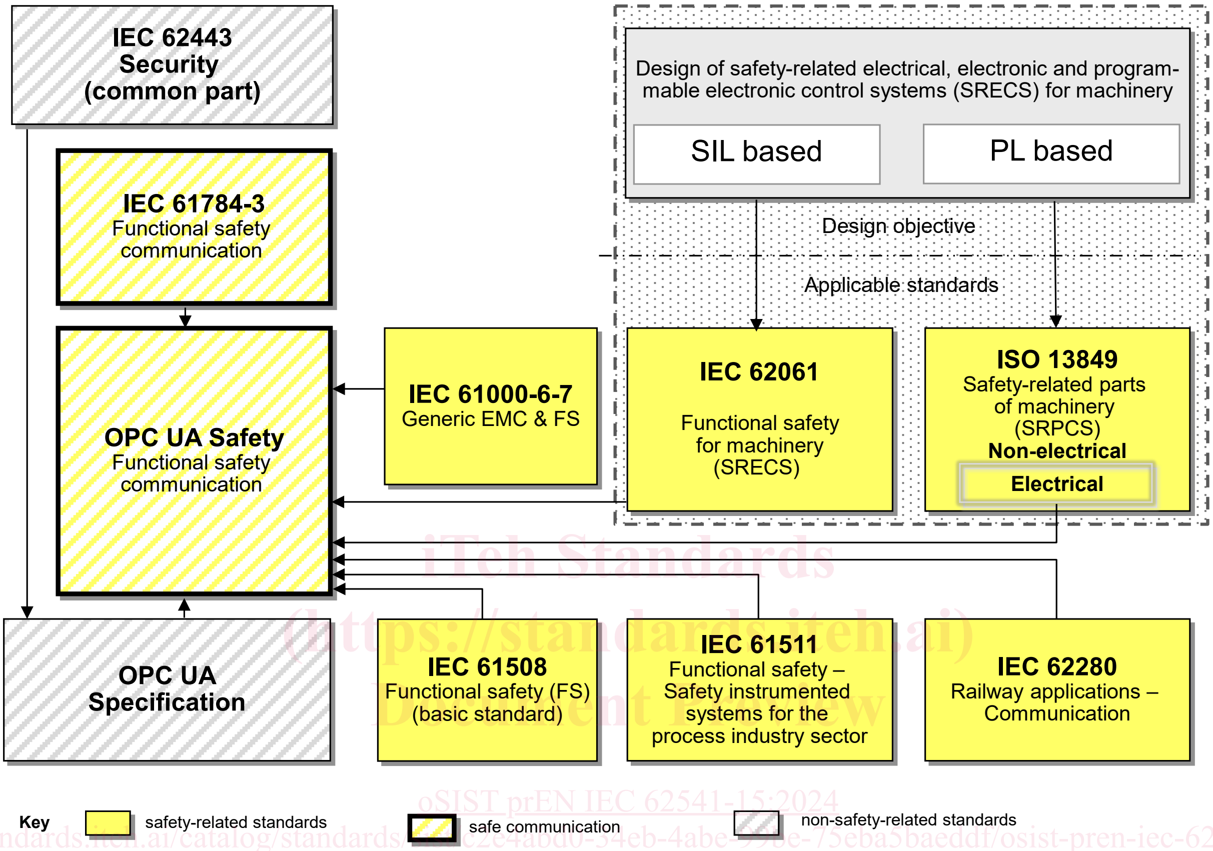
IEC 62443
Security
(common part)
IEC 61784-3
Functional safety communication
OPC UA Safety
Functional safety communication
OPC UA Specification
IEC 61000-6-7
Generic EMC & FS
Design of safety-related electrical, electronic and programmable electronic control systems (SRECS) for machinery
SIL based
PL based
Design objective
Applicable standards
IEC 62061
Functional safety for machinery (SRECS)
ISO 13849
Safety-related parts of machinery (SRPCS)
Non-electrical
Electrical
IEC 61508
Functional safety (FS) (basic standard)
IEC 61511
Functional safety – Safety instrumented systems for the process industry sector
IEC 62280
Railway applications – Communication
Key
safety-related standards
safe communication
non-safety-related standards

Figure 1 (informative) – 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 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 IEC 62541 information modeling to describe the concepts in this document.

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: 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]

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 13849-1:2023, 3.1.5]

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 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 modified – “FAL” replaced by “IEC 62541 communication stack”]

3.1.1.10
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, 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]

3.1.1.11
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 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 “SILn 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 IEC62541 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
one-bit value used to indicate a certain status or control information.

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.