SLOVENSKI STANDARD
SIST EN IEC 62541-2:2026

01-junij-2026

Enotna arhitektura OPC - 2. del: Varnostni model (IEC 62541-2:2026)

OPC unified architecture - Part 2: Security Model (IEC 62541-2:2026)

OPC Unified Architecture – Teil 2: Modell für die IT-Sicherheit (IEC 62541-2:2026)

Architecture unifiée OPC - Partie 2: Modèle de sécurité (IEC 62541-2:2026)

Ta slovenski standard je istoveten z: **EN IEC 62541-2:2026**

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

SIST EN IEC 62541-2:2026 **en,fr,de**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN IEC 62541-2

March 2026

ICS 25.040

Supersedes CLC IEC/TR 62541-2:2021

English Version

OPC unified architecture - Part 2: Security Model (IEC 62541-2:2026)

Architecture unifiée OPC - Partie 2: Modèle de sécurité (IEC 62541-2:2026)

OPC Unified Architecture - Teil 2: Modell für die IT-Sicherheit (IEC 62541-2:2026)

This European Standard was approved by CENELEC on 2026-03-19. 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

Ref. No. EN IEC 62541-2:2026 E

European foreword

The text of document 65E/1201/FDIS, future edition 1 of IEC 62541-2, prepared by SC 65E "Devices and integration in enterprise systems" 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 62541-2:2026.

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) 2027-03-31
- latest date by which the national standards conflicting with the document have to be withdrawn (dow) 2029-03-31

This document supersedes CLC IEC/TR 62541-2:2021 and all of its amendments and corrigenda (if any).

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 62541-2:2026 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 62541-3	NOTE	Approved as EN IEC 62541-3
IEC 62541-4	NOTE	Approved as EN IEC 62541-4
IEC 62541-5	NOTE	Approved as EN IEC 62541-5
IEC 62541-6	NOTE	Approved as EN IEC 62541-6
IEC 62541-7	NOTE	Approved as EN IEC 62541-7
IEC 62541-12	NOTE	Approved as EN IEC 62541-12
IEC 62541-14	NOTE	Approved as EN IEC 62541-14
IEC 62541-18	NOTE	Approved as EN IEC 62541-18
IEC 62541-21	NOTE	Approved as EN IEC 62541-21
IEC 62443-4-2	NOTE	Approved as EN IEC 62443-4-2

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 62541-1	-	OPC Unified Architecture - Part 1: Overview and concepts	EN IEC 62541-1	-

IEC 62541-2

Edition 1.0 2026-02

INTERNATIONAL STANDARD

OPC unified architecture –
Part 2: Security Model

ICS 25.040

ISBN 978-2-8327-1035-7

IEC 62541-2:2026-02(en)

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

OPC unified architecture - Part 2: Security Model

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 not 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 62541-2 has been prepared by subcommittee 65E: Devices and integration in enterprise systems, of IEC technical committee 65: Industrial-process measurement, control, and automation. It is an International Standard.

This edition cancels and replaces the third edition of IEC TR 62541-2, published in 2020.This edition constitutes a technical revision.

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

Draft	Report on voting
65E/1201/FDIS	65E/1206/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 other Parts of the series, certain document conventions are used:

Italics are used to denote a defined term or definition that appears in the "Terms and definitions" clause 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 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.

A list of all parts in 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.

1 Scope

This part of IEC 62541 describes the OPC Unified Architecture (OPC UA) security model. It describes the security threats of the physical, hardware, and software environments in which OPC UA is expected to run. It describes how OPC UA relies upon other standards for security. It provides definition of common security terms that are used in this and other parts of the IEC 62541 series. It gives an overview and concept of the security features that are specified in other parts of the series. It references services, mappings, and *Profile*s that are specified normatively in other parts of the 62541 series. It provides suggestions or best practice guidelines on implementing security. Any seeming ambiguity between this document and one of the other normative parts does not remove or reduce the requirement specified in the other normative part.

There are many different aspects of security that are addressed when developing applications. However, since OPC UA specifies a communication protocol, the focus is on securing the data exchanged between applications. This does not mean that an application developer can ignore the other aspects of security like protecting persistent data against tampering. It is important that the developers look into all aspects of security and decide how they can be addressed in the application. Common security features for industrial Controls are defined in IEC 62443-4-2 and OPC UA defined a relationship to them in Annex A.

This document is directed to readers who will develop OPC UA applications. It is also for end Users that wish to understand the various security features and functionality provided by OPC UA. It also offers some recommendations that can be applied when deploying systems. These recommendations are generic in nature since the details would depend on the actual implementation of the *OPC UA* applications and the choices made for the site security.

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

3 Terms, definitions, abbreviated terms and conventions

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC 62541-1 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

3.1.1
AccessRestriction
limit on the circumstances under which an operation, such as a read, write or a call, can be performed on a *Node*

Note 1 to entry: Operations can only be performed on a *Node* if the *Client* has the necessary *Permissions* and has satisfied all of the *AccessRestrictions*.

3.1.2
AccessToken
digitally signed document that asserts that the subject is entitled to access a *Resource*

Note 1 to entry: The document includes the name of the subject and the *Resource* being accessed.

3.1.3
ApplicationInstance
individual installation of a program running on one computer

Note 1 to entry: There can be several *ApplicationInstances* of the same application running at the same time on several computers or possibly the same computer.

3.1.4
ApplicationInstanceCertificate
Certificate of an individual *ApplicationInstance* that has been installed in an individual host

Note 1 to entry: Different installations of one software product would have different *ApplicationInstanceCertificates*. The use of an *ApplicationInstanceCertificate* for uses outside of what is described in the specification could greatly reduce the security provided by the *ApplicationInstanceCertificate* and should be discouraged.

Note 2 to entry: also written as *ApplicationInstance Certificate*

3.1.5
Asymmetric Cryptography
Cryptography method that uses a pair of keys, one that is designated the *Private Key* and kept secret, the other called the *Public Key* that is generally made available

Note 1 to entry: 'Asymmetric Cryptography, also known as "public-key cryptography". In an Asymmetric Encryption algorithm when an entity "A" requires *Confidentiality* for data sent to entity "B", then entity "A" encrypts the data with a Public Key provided by entity "B". Only entity "B" has the matching Private Key that is needed to decrypt the data. In an asymmetric Digital Signature algorithm when an entity "A" requires message Integrity or to provide *Authentication* for data sent to entity "B", entity A uses its Private Key to sign the data. To verify the signature, entity B uses the matching Public Key that entity A has provided. In an asymmetric key agreement algorithm, entity A and entity B each send their own Public Key to the other entity. Then each uses their own Private Key and the other's Public Key to compute the new key value.' according to IS Glossary.

3.1.6
Asymmetric Encryption
mechanism used by *Asymmetric Cryptography* for encrypting data with the *Public Key* of an entity and for decrypting data with the associated *Private Key*

3.1.7
Asymmetric Signature
mechanism used by *Asymmetric Cryptography* for signing data with the *Private Key* of an entity and for verifying the data's signature with the associated *Public Key*

3.1.8
Auditability
security objective that assures that any actions or activities in a system can be recorded

3.1.9
Auditing
tracking of actions and activities in the system, including security related activities where *Audit* records can be used to review and verify system operations

3.1.10
Authentication
process that assures that the identity of an entity such as a *Client*, *Server*, *Publisher* or user can be verified

3.1.11
Authorization
ability to grant access to a system resource

Note 1 to entry: *Authorization* of access to resources should be based on the need-to-know principle. It is important that access is restricted in a system.

3.1.12
AuthorizationService
Server which validates a request to access a *Resource* returns an *AccessToken* that grants access to the *Resource*

Note 1 to entry: The *AuthorizationService* is also called STS (Security Token Service) in other standards.

3.1.13
Availability
security objective that assures that the system is running normally. That is, no services have been compromised in such a way to become unavailable or severely degraded

3.1.14
Certificate Authority
entity that can issue *Certificate*s, also known as a CA

Note 1 to entry: The *Certificate* certifies the ownership of a *Public Key* by the named subject of the *Certificate*. This allows others (relying parties) to rely upon signatures or assertions made by the *Private Key* that corresponds to the *Public Key* that is certified. In this model of trust relationships, a CA is a trusted party that is trusted by both the subject (owner) of the *Certificate* and the party relying upon the *Certificate*. CA s are characteristic of many *Public Key infrastructure* (PKI) schemes

Note 2 to entry: A private CA system (or a private sub-CA) could be used as long as all parties trust it.

3.1.15
CertificateStore
persistent location where *Certificate*s and *Certificate* revocation lists (CRLs) are stored

Note 1 to entry: It can be a disk resident file structure or on Windows platforms it can be a Windows registry location.

3.1.16
Claim
statement in an *AccessToken* that asserts information about the subject which the *Authorization Service* knows to be true

Note 1 to entry: *Claims* can include username, email, and *Roles* granted to the subject.

3.1.17
Confidentiality
security objective that assures the protection of data from being read by unintended parties

3.1.18
Cryptography
algorithm to transform clear, meaningful information into an enciphered, unintelligible form using an algorithm and a key

3.1.19
Cyber Security Management System
program designed by an organization to maintain the security of the entire organization's assets to an established level of *Confidentiality*, *Integrity*, and *Availability*, whether they are on the business side or the industrial automation and control systems side of the organization