SLOVENSKI STANDARD
oSIST prEN IEC 62541-2:2024

01-marec-2024

Enotna arhitektura OPC - 2. del: Varnostni model

OPC unified architecture - Part 2: Security model

Ta slovenski standard je istoveten z: **prEN IEC 62541-2:2024**

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 62541-2:2024 **en,fr,de**

65E/1040/CDV

COMMITTEE DRAFT FOR VOTE (CDV)

PROJECT NUMBER: **IEC 62541-2 ED1**	
DATE OF CIRCULATION: **2024-01-26**	CLOSING DATE FOR VOTING: **2024-04-19**
SUPERSEDES DOCUMENTS: **65E/950/NP, 65E/1010/RVN**	

IEC SC 65E : DEVICES AND INTEGRATION IN ENTERPRISE SYSTEMS

SECRETARIAT: United States of America	SECRETARY: Mr Donald (Bob) Lattimer
OF INTEREST TO THE FOLLOWING COMMITTEES:	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 2: Security Model

PROPOSED STABILITY DATE: 2026

NOTE FROM TC/SC OFFICERS:

CONTENTS

Figures

Tables

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

The main task of IEC technical committees is to prepare International Standards. However, a technical committee may propose the publication of a technical report when it has collected data of a different kind from that which is normally published as an International Standard, for example "state of the art".

International Standard 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.

The text of this international standard is based on the following documents:

CDV	Report on voting
65E/XX/CDV	65E/XX/RVC

Full information on the voting for the approval of this international standard can be found in the report on voting indicated in the above table.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

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 definition” 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 of the IEC 62541 series is included in IEC 62541-1 clause 4 Structure of the OPC UA series and published under the general title OPC Unified Architecture, can be found on the IEC website.

The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the IEC web site under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

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.

OPC Unified Architecture Specification

Part 2: Security Model

1 Scope

This document 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 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.

Note that there are many different aspects of security that have to be 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.

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, in whole or in part, are normatively referenced in this document and are indispensable for its application. 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*

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 62541-12, *OPC Unified Architecture – Part 12: Discovery and Global Services*

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

IEC 62541-18, *OPC Unified Architecture – Part 18: Role-Based Security*

TLS: RFC 2246: The TLS Protocol Version 1.0
https://www.ietf.org/rfc/rfc2246.txt

X509: X.509 Public Key Certificate Infrastructure
https://www.itu.int/rec/T-REC-X.509-200003-I/e

HTTP: RFC 2616: Hypertext Transfer Protocol - HTTP/1.1
https://www.ietf.org/rfc/rfc2616.txt

HTTPS: RFC 2818: HTTP Over TLS
https://www.ietf.org/rfc/rfc2818.txt

IS Glossary: Internet Security Glossary
https://www.ietf.org/rfc/rfc2828.txt

NIST 800-12: Introduction to Computer Security
https://csrc.nist.gov/publications/nistpubs/800-12/

NIST 800-57: Part 3: Application-Specific Key Management Guidance
https://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_PART3_key-management_Dec2009.pdf

NERC CIP: CIP 002-1 through CIP 009-1, by North-American Electric Reliability Council
https://www.nerc.com/page.php?cid=2|20

SPP-ICS: Guide to Industrial Control Systems (ICS) Security
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

SHA-1: Secure Hash Algorithm RFC
https://tools.ietf.org/html/rfc3174

PKI: Public Key Infrastructure article in Wikipedia
https://en.wikipedia.org/wiki/Public_key_infrastructure

X509 PKI: Internet X.509 Public Key Infrastructure
https://www.ietf.org/rfc/rfc3280.txt

RFC 5958: Asymmetric Key Packages
https://tools.ietf.org/search/rfc5208

PKCS #10: Certification Request Syntax Specification
https://tools.ietf.org/html/rfc2986

OAuth2: The OAuth 2.0 Authorization Framework
https://tools.ietf.org/html/rfc6749

JWT: JSON Web Token (JWT)
https://tools.ietf.org/html/rfc7519

OpenID: OpenID Connect Discovery 1.0
https://openid.net/specs/openid-connect-discovery-1_0.html

3 Terms, definitions, and abbreviations

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC 62541-1 as well as the following apply.

3.1.1 AccessRestriction

A 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**

A 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**

the 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**

the 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**

the 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 **AuthenticatedEncryption**

an encryption scheme which simultaneously assures the data confidentiality and authenticity

Note 1 to entry: AuthenticatedEncryption algorithms may allow for associated data to be signed but not encrypted.

3.1.11 **Authentication**

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

3.1.12 **Authorization**

the 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.