



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: <input type="checkbox"/> Other TC/SCs are requested to indicate their interest, if any, in this CDV to the secretary.
FUNCTIONS CONCERNED: <input type="checkbox"/> EMC <input type="checkbox"/> ENVIRONMENT <input type="checkbox"/> QUALITY ASSURANCE <input type="checkbox"/> SAFETY	
<input checked="" type="checkbox"/> 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.	<input type="checkbox"/> NOT SUBMITTED FOR CENELEC PARALLEL VOTING

oSIST prEN IEC 62541-2:2024

<https://standards.iteh.ai/document/iec-62541-2-2024> 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:

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

CONTENTS

		Page
1		
2		
3		
4	1 Scope	1
5	2 Normative References	1
6	3 Terms, definitions, and abbreviations	2
7	3.1 Terms and definitions	2
8	3.2 Abbreviations	7
9	3.3 Conventions for security model figures	7
10	4 OPC UA security architecture	7
11	4.1 OPC UA security environment	7
12	4.2 Security objectives	8
13	4.2.1 Overview	8
14	4.2.2 Authentication	8
15	4.2.3 Authorization	9
16	4.2.4 Confidentiality	9
17	4.2.5 Integrity	9
18	4.2.6 Non- Repudiation	9
19	4.2.7 Auditability	9
20	4.2.8 Availability	9
21	4.3 Security threats to OPC UA systems	9
22	4.3.1 Overview	9
23	4.3.2 Denial of Service	9
24	4.3.3 Eavesdropping	10
25	4.3.4 Message spoofing	11
26	4.3.5 Message alteration	11
27	4.3.6 Message replay	11
28	4.3.7 Malformed Messages	11
29	4.3.8 Server profiling	11
30	4.3.9 Session hijacking	12
31	4.3.10 Rogue Server	12
32	4.3.11 Rogue Publisher	12
33	4.3.12 Compromising user credentials	12
34	4.3.13 Repudiation	12
35	4.4 OPC UA relationship to site security	12
36	4.5 OPC UA security architecture	13
37	4.5.1 Overview	13
38	4.5.2 Client / Server	14
39	4.5.3 Publish-Subscribe	15
40	4.6 SecurityPolicies	16
41	4.7 Security Profiles	16
42	4.8 Security Mode Settings	17
43	4.9 User Authentication	17
44	4.10 Application Authentication	17
45	4.11 User Authorization	17
46	4.12 Roles	18
47	4.13 OPC UA security related Services	18
48	4.14 Auditing	19
49	4.14.1 General	19
50	4.14.2 Single Client and Server	20

51	4.14.3	Aggregating Server	20
52	4.14.4	Aggregation through a non-auditing Server	21
53	4.14.5	Aggregating Server with service distribution	22
54	5	Security reconciliation	23
55	5.1	Reconciliation of threats with OPC UA security mechanisms	23
56	5.1.1	Overview	23
57	5.1.2	Denial of Service	23
58	5.1.3	Eavesdropping	24
59	5.1.4	Message spoofing	24
60	5.1.5	Message alteration	25
61	5.1.6	Message replay	25
62	5.1.7	Malformed Messages	25
63	5.1.8	Server profiling	25
64	5.1.9	Session hijacking	25
65	5.1.10	Rogue Server or Publisher	25
66	5.1.11	Compromising user credentials	26
67	5.1.12	Repudiation	26
68	5.2	Reconciliation of objectives with OPC UA security mechanisms	26
69	5.2.1	Overview	26
70	5.2.2	Application Authentication	26
71	5.2.3	User Authentication	26
72	5.2.4	Authorization	26
73	5.2.5	Confidentiality	27
74	5.2.6	Integrity	27
75	5.2.7	Auditability	27
76	5.2.8	Availability	27
77	6	Implementation and deployment considerations	28
78	6.1	Overview	28
79	6.2	Appropriate timeouts:	28
80	6.3	Strict Message processing	28
81	6.4	Random number generation	28
82	6.5	Special and reserved packets	29
83	6.6	Rate limiting and flow control	29
84	6.7	Administrative access	29
85	6.8	Cryptographic Keys	29
86	6.9	Alarm related guidance	29
87	6.10	Program access	30
88	6.11	Audit event management	30
89	6.12	OAuth2, JWT and User roles	30
90	6.13	HTTPs, TLS & Websockets	30
91	6.14	Reverse Connect	31
92	6.15	Passwords	31
93	6.16	Additional Security considerations	31
94	7	Unsecured Services	31
95	7.1	Overview	31
96	7.2	Multi Cast Discovery	31
97	7.3	Global Discovery Server Security	32
98	7.3.1	Overview	32
99	7.3.2	Rogue GDS	32

100	7.3.3	Threats against a GDS.....	32
101	7.3.4	Certificate management threats.....	33
102	8	Certificate management	33
103	8.1	Overview.....	33
104	8.2	Self signed certificate management	33
105	8.3	CA Signed Certificate management.....	34
106	8.4	GDS Certificate Management.....	35
107	8.4.1	Overview.....	35
108	8.4.2	Developers Certificate management.....	35
109			

iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

[oSIST prEN IEC 62541-2:2024](https://standards.iteh.ai/catalog/standards/sist/132c5e72-1e64-4a93-a774-4e9070db4cd7/osist-pren-iec-62541-2-2024)

<https://standards.iteh.ai/catalog/standards/sist/132c5e72-1e64-4a93-a774-4e9070db4cd7/osist-pren-iec-62541-2-2024>

110		
	Figures	
111	Figure 1 – OPC UA network example	8
112	Figure 2 – OPC UA security architecture – Client / Server	13
113	Figure 3 – OPC UA security architecture- Publisher - Subscriber.....	14
114	Figure 4 – Role overview	18
115	Figure 5 – Simple Servers	20
116	Figure 6 – Aggregating Servers	20
117	Figure 7 – Aggregation with a non-auditing Server	21
118	Figure 8 – Aggregate Server with service distribution	22
119	Figure 9 – Manual Certificate handling	34
120	Figure 10 – CA Certificate handling	35
121	Figure 11 – Certificate handling.....	36
122		
	Tables	
123		
124	Table 1 – Security Reconciliation Threats Summary	23
125		
126		

iTeh Standards
 (<https://standards.iteh.ai>)
 Document Preview

[oSIST prEN IEC 62541-2:2024](https://standards.iteh.ai/catalog/standards/sist/132c5e72-1e64-4a93-a774-4e9070db4cd7/osist-pren-iec-62541-2-2024)

<https://standards.iteh.ai/catalog/standards/sist/132c5e72-1e64-4a93-a774-4e9070db4cd7/osist-pren-iec-62541-2-2024>

127

INTERNATIONAL ELECTROTECHNICAL COMMISSION

128

129

130

131

132

133

134

OPC UNIFIED ARCHITECTURE –**Part 2: Security Model****FOREWORD**

135

136

137

138

139

140

141

142

143

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.

144

145

146

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.

147

148

149

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.

150

151

152

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.

153

154

155

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.

156

157

158

159

160

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.

161

162

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.

163

164

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.

165

166

167

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".

168

169

170

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.

171

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

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

172

173

174

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.

175

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

176

Throughout this document and the other Parts of the series, certain document conventions are used:

177 *Italics* are used to denote a defined term or definition that appears in the “Terms and definition” clause
178 in one of the parts of the series.

179 *Italics* are also used to denote the name of a service input or output parameter or the name of a structure
180 or element of a structure that are usually defined in tables.

181 The *italicized terms* and *names* are also often written in camel-case (the practice of writing compound
182 words or phrases in which the elements are joined without spaces, with each element's initial letter
183 capitalized within the compound). For example, the defined term is *AddressSpace* instead of Address
184 Space. This makes it easier to understand that there is a single definition for *AddressSpace*, not
185 separate definitions for Address and Space.

186 A list of all parts of the IEC 62541 series is included in IEC 62541-1 clause 4 Structure of the OPC UA
187 series and published under the general title OPC Unified Architecture, can be found on the IEC website.

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

- 191 • reconfirmed,
- 192 • withdrawn,
- 193 • replaced by a revised edition, or
- 194 • amended.

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

196

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.

197

198

199

200

(<https://standards.iteh.ai>)
Document Preview

[oSIST prEN IEC 62541-2:2024](https://standards.iteh.ai/catalog/standards/sist/132c5e72-1e64-4a93-a774-4e9070db4cd7/osist-pren-iec-62541-2-2024)

<https://standards.iteh.ai/catalog/standards/sist/132c5e72-1e64-4a93-a774-4e9070db4cd7/osist-pren-iec-62541-2-2024>

OPC Unified Architecture Specification

Part 2: Security Model

201
202
203
204

205 1 Scope

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

215 Note that there are many different aspects of security that have to be addressed when developing
216 applications. However, since OPC UA specifies a communication protocol, the focus is on securing
217 the data exchanged between applications. This does not mean that an application developer can
218 ignore the other aspects of security like protecting persistent data against tampering. It is important
219 that the developers look into all aspects of security and decide how they can be addressed in the
220 application.

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

226 2 Normative References

227 The following documents, in whole or in part, are normatively referenced in this document and are
228 indispensable for its application. For dated references, only the edition cited applies. For undated
229 references, the latest edition of the referenced document (including any amendments) applies.

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

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

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

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

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

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

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

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

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

239

240 TLS: RFC 2246: The TLS Protocol Version 1.0

241 <https://www.ietf.org/rfc/rfc2246.txt>

242 X509: X.509 Public Key Certificate Infrastructure

243 <https://www.itu.int/rec/T-REC-X.509-200003-I/e>

- 244 HTTP: RFC 2616: Hypertext Transfer Protocol - HTTP/1.1
245 <https://www.ietf.org/rfc/rfc2616.txt>
- 246 HTTPS: RFC 2818: HTTP Over TLS
247 <https://www.ietf.org/rfc/rfc2818.txt>
- 248 IS Glossary: Internet Security Glossary
249 <https://www.ietf.org/rfc/rfc2828.txt>
- 250 NIST 800-12: Introduction to Computer Security
251 <https://csrc.nist.gov/publications/nistpubs/800-12/>
- 252 NIST 800-57: Part 3: Application-Specific Key Management Guidance
253 [https://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_PART3_key-](https://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_PART3_key-management_Dec2009.pdf)
254 [management_Dec2009.pdf](https://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_PART3_key-management_Dec2009.pdf)
- 255 NERC CIP: CIP 002-1 through CIP 009-1, by North-American Electric Reliability Council
256 <https://www.nerc.com/page.php?cid=2|20>
- 257 SPP-ICS: Guide to Industrial Control Systems (ICS) Security
258 <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf>
- 259 SHA-1: Secure Hash Algorithm RFC
260 <https://tools.ietf.org/html/rfc3174>
- 261 PKI: Public Key Infrastructure article in Wikipedia
262 https://en.wikipedia.org/wiki/Public_key_infrastructure
- 263 X509 PKI: Internet X.509 Public Key Infrastructure
264 <https://www.ietf.org/rfc/rfc3280.txt>
- 265 RFC 5958: Asymmetric Key Packages
266 <https://tools.ietf.org/search/rfc5208>
- 267 PKCS #10: Certification Request Syntax Specification
268 <https://tools.ietf.org/html/rfc2986>
- 269 OAuth2: The OAuth 2.0 Authorization Framework
270 <https://tools.ietf.org/html/rfc6749>
- 271 JWT: JSON Web Token (JWT)
272 <https://tools.ietf.org/html/rfc7519>
- 273 OpenID: OpenID Connect Discovery 1.0
274 https://openid.net/specs/openid-connect-discovery-1_0.html
275
- 276 **3 Terms, definitions, and abbreviations**
- 277 **3.1 Terms and definitions**
- 278 For the purposes of this document, the terms and definitions given in IEC 62541-1 as well as the
279 following apply.
- 280 **3.1.1 AccessRestriction**
- 281 A limit on the circumstances under which an operation, such as a read, write or a call, can be
282 performed on a *Node*.

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

285 3.1.2 **AccessToken**

286 A digitally signed document that asserts that the subject is entitled to access a *Resource*.

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

288 3.1.3 **ApplicationInstance**

289 individual installation of a program running on one computer.

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

292 3.1.4 **ApplicationInstanceCertificate**

293 *Certificate* of an individual *ApplicationInstance* that has been installed in an individual host.

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

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

298 3.1.5 **Asymmetric Cryptography**

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

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

309 3.1.6 **Asymmetric Encryption**

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

312 3.1.7 **Asymmetric Signature**

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

315 3.1.8 **Auditability**

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

317 3.1.9 **Auditing**

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

320 3.1.10

321 **AuthenticatedEncryption**

322 an encryption scheme which simultaneously assures the data confidentiality and authenticity

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

324 3.1.11 **Authentication**

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

327 3.1.12 **Authorization**

328 the ability to grant access to a system resource

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