SLOVENSKI STANDARD
oSIST prEN IEC 62541-21:2024

01-marec-2024

Enotna arhitektura OPC - 21. del: Vključevanje naprav

OPC unified architecture - Part 21: Device onboarding

Ta slovenski standard je istoveten z: **prEN IEC 62541-21:2024**

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 62541-21:2024 **en,fr,de**

65E/1046/CDV

COMMITTEE DRAFT FOR VOTE (CDV)

PROJECT NUMBER: **IEC 62541-21 ED1**	
DATE OF CIRCULATION: **2024-01-26**	CLOSING DATE FOR VOTING: **2024-04-19**
SUPERSEDES DOCUMENTS: **65E/956/NP, 65E/1016/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 21: Device Onboarding

PROPOSED STABILITY DATE: 2026

NOTE FROM TC/SC OFFICERS:

CONTENTS

Page

82 **FIGURES**

94

95

96 # TABLES

135

136

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

OPC UNIFIED ARCHITECTURE –

Part 21: Device Onboarding

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 62541-21 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:

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

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

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

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

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

201 • reconfirmed,
202 • withdrawn,
203 • replaced by a revised edition, or
204 • amended.

205

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

207

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.

208

209

210

211

OPC UNIFIED ARCHITECTURE

Part 21: Device Onboarding

1 Scope

This part defines the life cycle of *Devices* and *Composites* and mechanisms to verify their authenticity, set up their security and maintain their configuration.

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 and errata) applies.

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 62541-9, *OPC Unified Architecture – Part 9: Alarms and Conditions*

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

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

IEC 62541-22, *OPC Unified Architecture – Part 22: Base Network Model*

IEC 62541-100, *OPC Unified Architecture – Part 100: Device Model*

ISO/IEC 11889, Information technology — Trusted platform module library
https://www.iso.org/standard/66510.html

802.1AR, Secure Device Identity
https://1.ieee802.org/security/802-1ar/

RFC 3161, Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)
https://tools.ietf.org/html/rfc3161

RFC 5280, Internet X.509 Public Key Infrastructure Certificate
https://tools.ietf.org/html/rfc5280

RFC 7515, JSON Web Signature (JWS)
https://tools.ietf.org/html/rfc7515

RFC 7518, JSON Web Algorithms (JWA)

https://tools.ietf.org/html/rfc7518

RFC 2045, Multipurpose Internet Mail Extensions (MIME) Part One

https://tools.ietf.org/html/rfc2045

RFC 4648, The Base16, Base32, and Base64 Data Encodings

https://tools.ietf.org/html/rfc4648

DIN 91406, Automatic identification of physical objects and information on physical objects in IT systems

https://www.en-standard.eu/din-spec-91406-automatische-identifikation-von-physischen-objekten-und-informationen-zum-physischen-objekt-in-it-systemen-insbesondere-iot-systemen-text-deutsch-und-englisch/

3 Terms, definitions, and conventions

3.1 Terms and definitions

For the purposes of this document the following terms and definitions as well as the terms and definitions given in IEC 62541-1, IEC 62541-2, IEC 62541-3, IEC 62541-4, IEC 62541-6, IEC 62541-9 and IEC 62541-100 apply.

3.1.1
Application
a program that runs on a *Device* and communicates with other *Applications* on the network.

Note 1 to entry: Each *Application* has an identifier that is unique within the network.

Note 2 to entry: An *OPC UA Application* is an *Application* that supports OPC UA.

3.1.2
ApplicationUri
a globally unique identifier for an *OPC UA Application* running on a particular *Device*.

Note 3 to entry: The *Application Instance Certificate* has the *ApplicationUri* in the *subjectAltName* field.

3.1.3
Composite
a collection of *Devices* or *Composites* assembled into a single unit.

Note 1 to entry: Each *Composite* has a globally unique identifier.

Note 2 to entry: A *Composite* may act as a single *Device* when connected to a network.

Note 3 to entry: A *Composite* may appear as multiple *Devices* when connected to a network.

3.1.4
CompositeBuilder
an organization that creates *Composites.*

3.1.5
CompositeInstanceUri
a globally unique resource identifier assigned by a builder to a *Composite*..

3.1.6
DCA Client
a DCA which is a *Client* and supports *PullManagement*.

3.1.7
DCA Server
a DCA which is a *Server* and supports *PushManagement*.

294 **3.1.8**
295 **Device**
296 As defined in IEC 62541-100.

297 Note 1 to entry: For this document a *Device* also executes one or more *OPC UA Applications.*

298 Note 2 to entry: a generic computer or mobile device may be a *Device* if it has a *DeviceIdentity Certificate*
299

300 **3.1.9**
301 **Device Configuration Application (DCA)**
302 a *Client* or *Server* installed on a *Device* used to configure other applications installed on the
303 same *Device*.

304 Note 1 to entry: a DCA which is a *Client* uses *PullManagement* (see 7.2) to interact with the *Registrar.*

305 Note 2 to entry: the *Registrar* uses *PushManagement* (see 7.3) to interact with a DCA which is a *Server.*

306 **3.1.10**
307 **DeviceIdentity Certificate**
308 a *Certificate* issued to a *Device* that identifies the *Device*.

309 Note 1 to entry: All *DeviceIdentity Certificates* have the *ProductInstanceUri* as a *subjectAltName*.

310 Note 2 to entry: All *DeviceIdentity Certificates* are IDevID or LDevID Certificates as defined by 802.1AR.

311 Note 3 to entry: The *ProductInstanceUri* is the *ApplicationUri* when the *DeviceIdentity Certificate* is used to create a
312 *SecureChannel*.

313 **3.1.11**
314 **Distributor**
315 an organization that re-sells *Devices* and/or Composites.

316 Note 1 to entry: A *Distributor* may enhance *Devices* and *Composites* by adding customized products or services.

317 **3.1.12**
318 **Manufacturer**
319 an organization that creates *Devices.*

320 **3.1.13**
321 **OwnerOperator**
322 an organization deploying and operating a system that comprises of *Devices*, *Composites* or
323 other computers connected via a network.

324 **3.1.14**
325 **Privilege**
326 a named set of permissions or access rights which are needed to perform a task.

327 **3.1.15**
328 **ProductInstanceUri**
329 a globally unique resource identifier assigned by the manufacturer to a *Device*.

330 **3.1.16**
331 **Registrar**

332 an *OPC UA Application* that registers and authenticates *Devices* added to the network.

333 **3.1.17**
334 **SystemIntegrator**

335 an organization that installs and configures a system for an *OwnerOperator* that comprises of
336 *Devices*, *Composites* or other computers connected via a network.

337 **3.1.18**
338 **SecureElement**

339 a hardware component that protects *Private Keys* from unauthorized access and disclosure.

340 **3.1.19**
341 **Ticket**

342 a document that identifies a *Device* or *Composite* and has a *DigitalSignature*.

3.2 Abbreviations and symbols

API	Application Programming Interface
ASN.1	Abstract Syntax Notation #1
CA	Certificate Authority
CRL	Certificate Revocation List
DCA	Device Configuration Application
DER	ASN.1 Distinguished Encoding Rules
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
ERP	Enterprise Resource Planning
GDS	Global Discovery Server
IDevID	Initial Device Identifier
LDevID	Locally Significant Device Identifier
LDS	Local Discovery Server
mDNS	Multicast Domain Name System
NAT	Network Address Translation
PKCS	Public Key Cryptography Standards
TLS	Transport Layer Security
TPM	Trusted Platform Module
UA	Unified Architecture
URI	Uniform Resource Identifier
URN	Uniform Resource Name

4 Onboarding Model

4.1 Device Lifecycle

The Onboarding model is designed to allow the configuration of a *Device* to be managed over the complete lifecycle of the *Device* from manufacture to decommissioning. The entire lifecycle approach is needed because *Devices*, unlike PC-class computers, are often shipped with automation software pre-installed and are connected directly to sensitive networks. This requires a process to authenticate *Devices* before they are given access to a sensitive network.

The complete life cycle of a *Device* is shown in Figure 1.

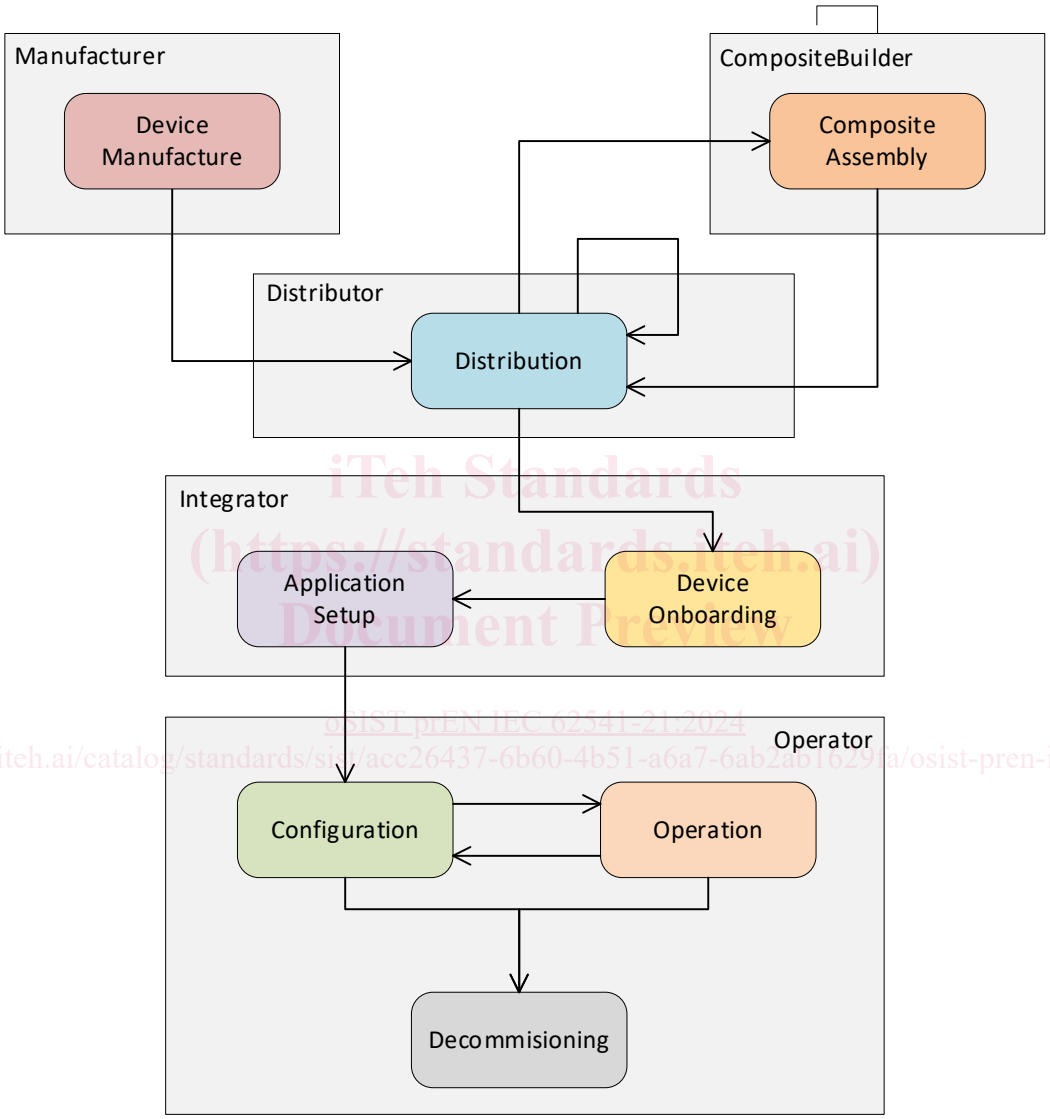

Figure 1 – The Lifecycle of a Device

The actors in the *Device* lifecycle are described in Table 1.

Table 1 – The Actors in the Device Lifecycle

Actor	Description
Device	A computer that is able to communicate via a network. A *Device* has a unique identifier and may have one or more *Applications* (see 3.1.4)