

# SLOVENSKI STANDARD oSIST prEN IEC 62541-18:2024

01-marec-2024

Enotna arhitektura OPC - 18. del: Varnost na podlagi vlog

OPC unified architecture - Part 18: Role-based security

Ta slovenski standard je istoveten z: prEN IEC 62541-18:2024

ICS:

Merjenje in krmiljenje 0.4746-cc Industrial process 18233c3/osist-pren-iec-62541-18-2024 https://st25.040.40

industrijskih postopkov measurement and control

35.240.50 Uporabniške rešitve IT v IT applications in industry

industriji

oSIST prEN IEC 62541-18:2024 en,fr,de oSIST prEN IEC 62541-18:2024

oSIST prEN IEC 62541-18:2024

PROJECT NUMBER: IEC 62541-18 ED1

DATE OF CIRCULATION:



# 65E/1043/CDV

### COMMITTEE DRAFT FOR VOTE (CDV)

CLOSING DATE FOR VOTING:

	2024-01-26		2024-04-19
	SUPERSEDES DOCUM	ENTS:	
	65E/953/NP, 65E/	1013/RVN	
IEC SC 65E : DEVICES AND INTEGRATION I	N ENTERPRISE SYSTEM	S	
SECRETARIAT:		SECRETARY:	
United States of America		Mr Donald (Bob) L	attimer
OF INTEREST TO THE FOLLOWING COMMITTE	EES:	PROPOSED HORIZON	FAL STANDARD:
		Other TC/SCs are re in this CDV to the se	equested to indicate their interest, if any, ecretary.
FUNCTIONS CONCERNED:			
☐ EMC ☐ ENVIR	TNAMNC	Quality assuran	ICE SAFETY
SUBMITTED FOR CENELEC PARALLEL V		_	OR CENELEC PARALLEL VOTING
Attention IEC-CENELEC parallel voting	g i'leh Sta	andards	
The attention of IEC National Comm CENELEC, is drawn to the fact that this Vote (CDV) is submitted for parallel votir	Committee Draft for	dards.ite	eh.ai)
The CENELEC members are invited to vote through the CENELEC online voting system.		t Previe	W
oSIST prEN IEC 62541-18:2024			
This document is still under study and subject to change. It should not be used for reference purposespren-lec-6254			
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.			n of any relevant patent rights of which
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 fo submitting ISC clauses. (SEE <u>AC/22/2007</u> OR <u>NEW GUIDANCE DOC</u> ).			
TITLE:			
OPC Unified Architecture – Part 18	3: Role-Based Sec	urity	
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.			preparing National Committee positions.

CONTENTS

2		

3	1	Scop	De	1
4	2	Norn	native references	1
5	3	Tern	ns, definitions, abbreviated terms and conventions	1
6		3.1	Terms and definitions	1
7	4	Role	Model	2
8		4.1	General	2
9		4.2	RoleSetType	3
10		4.2.1	RoleSetType definition	3
11		4.2.2	AddRole Method	3
12		4.2.3	RemoveRole Method	4
13		4.3	RoleSet	4
14		4.4	RoleType	8
15		4.4.1	RoleType definition	8
16		4.4.2	2 EndpointType1	0
17		4.4.3	B IdentityMappingRuleType1	0
18		4.4.4	ldentityCriteriaType1	2
19		4.4.5	5 AddIdentity Method 1	2
20		4.4.6	Removeldentity Method1	2
21		4.4.7	7 AddApplication Method1	3
22		4.4.8		
23		4.4.9	'	
24		4.4.1	(https://standards.itah.ai)	
25		4.5	RoleMappingRuleChangedAuditEventType1	
26	5	User	Management Model 1	
27		5.1	General 1	6
28		5.2	UserManagementType1	
29		5.2.1		
30		5.2.2	PasswordOptionsMask 3eb0d7d6-ce1f-4f78-8bf1-77934d8233e3/osist-pren-1	7
31		5.2.3	3 UserConfigurationMask1	8
32		5.2.4	UserManagementDataType1	8
33		5.2.5		
34		5.2.6	•	
35		5.2.7		
36		5.2.8	· ·	
37		5.3	UserManagement	21
38				
39 40			FIGURES	
41	Fig	gure 1	– Role management overview	2
42	Fig	gure 2	User management overview1	6
43	•	=	-	
44 45			TABLES	
46	Ta	ble 1 –	RoleSetType definition	3

IEC	CDV	62541	12 €	IEC	2023
ILC	$\cup$	0/04/	- IO (C	, , , , , ,	/U/3

67

ı	ı	

47	Table 2 – RoleSet definition	4
48	Table 3 – RoleSet Additional Conformance Units	5
49	Table 4 – RoleType definition	8
50	Table 5 – EndpointType Structure	10
51	Table 6 – EndpointType definition	10
52	Table 7 – IdentityMappingRuleType	10
53	Table 8 – Order for subject name criteria	11
54	Table 9 – IdentityMappingRuleType definition	11
55	Table 10 – IdentityCriteriaType Values	12
56	Table 11 – IdentityCriteriaType Definition	12
57	Table 12 – RoleMappingRuleChangedAuditEventType definition	15
58	Table 13 – UserManagementType definition	16
59	Table 14 – PasswordOptionsMask values	17
60	Table 15 – PasswordOptionsMask definition	17
61	Table 16 – UserConfigurationMask values	18
62	Table 17 – UserConfigurationMask definition	18
63	Table 18 – UserManagementDataType structure	18
64	Table 19 – DataSetMetaDataType definition	18
65	Table 20 – UserManagement definition	21
66		

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

oSIST prEN IEC 62541-18:2024

https://standards.iteh.gi/catalog/standards/sist/3eh0d7d6-cc1f\_4f78\_8hf1\_77934d8233c3/osist\_pren\_iec\_62541\_18\_202

### INTERNATIONAL ELECTROTECHNICAL COMMISSION

**OPC UNIFIED ARCHITECTURE -**

Part 18: Role-Based Security

**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

of opinion on the relevant subjects since each technical committee has representation from all interested IEC National

that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC

2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus

3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in

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

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

7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of

8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable

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 62541-18 has been prepared by subcommittee 65E: Devices and integration

in enterprise systems, of IEC technical committee 65: Industrial-process measurement, control and

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

Report on voting

65E/XX/RVC

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,

Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights.

cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.

the corresponding national or regional publication shall be clearly indicated in the latter.

6) All users should ensure that they have the latest edition of this publication.

use of, or reliance upon, this IEC Publication or any other IEC Publications.

IEC shall not be held responsible for identifying any or all such patent rights.

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

CDV

65E/XX/CDV

68

# 69

70

## 71

# 73

## 74

## 75

### 76 78 79

#### 80 81 82 83

## 84 85

the two organizations.

independent certification bodies.

for the correct application of this publication.

on voting indicated in the above table.

Committees.

### 86 87

#### 88 89 90

### 91 92

- 93
- 94 95
- 96
- 97
- 98
- 99 100 101
- 102 103
- 104 105
- 106 107 108
- 109 110

111

112

automation.

113

- 114 115
- 116 This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.
- 117
- Throughout this document and the other Parts of the series, certain document conventions are used:

IEC CDV 62541-18 © IEC 2023

iv

118 *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.

- 120 *Italics* are also used to denote the name of a service input or output parameter or the name of a structure 121 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
- 132 reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- 135 amended.

136

138

139 140

141 142

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.

Document Preview

oSIST prEN IEC 625/1-18:202/

https://standards.iteh.ai/catalog/standards/sist/3eb0d7d6-cc1f-4f78-8bf1-77934d8233c3/osist-pren-iec-62541-18-202

IEC CDV 62541-18 © IEC 2023

143	OPC Unified Architecture Specification
144	
145	Part 18: Role-Based Security
146	
147	
148	
149	1 Scope
150	This part of the OPC Unified Architecture defines an Information Model. The Information Model
151	describes the basic infrastructure to model role-based security.
152	Note: In the previous version, Role-Based Security was in IEC 62541-5, Annex F
153	2 Normative references
154	The following documents, in whole or in part, are normatively referenced in this document and
155	are indispensable for its application. For dated references, only the edition cited applies. For
156	undated references, the latest edition of the referenced document (including any amendments
157	and errata) applies.
158	IEC 62541-1, OPC Unified Architecture – Part 1: Overview and Concepts
159	IEC 62541-3, OPC Unified Architecture – Part 3: Address Space Model
160	IEC 62541-4, OPC Unified Architecture – Part 4: Services
161	IEC 62541-5, OPC Unified Architecture – Part 5: Information Model
162	IEC 62541-6, OPC Unified Architecture – Part 6: Mappings
163	IEC 62541-7, OPC Unified Architecture – Part 7: Profiles
164	IEC 62541-8, OPC Unified Architecture – Part 8: Data Access
165	IEC 62541-12, OPC Unified Architecture – Part 12: Discovery and Global Services
os://si 166	tandards.iteh.ai/catalog/standards/sist/3eb0d7d6-cc1f-4f78-8bf1-77934d8233c3/osist-pren-iec-62:
167	3 Terms, definitions, abbreviated terms and conventions
.01	
168	3.1 Terms and definitions
169	For the purposes of this document, the terms and definitions given in IEC 62541-1, IEC 62541-
170	3 and IEC 62541-5 apply.

2

#### 4 Role Model

#### 4.1 General

172

173

178

179

180

181

182

187

OPC UA defines a standard approach for implementing role-based security. Servers may choose to implement part or all of the mechanisms defined here. The OPC UA approach assigns *Permissions* to *Roles* for each *Node* in the *AddressSpace*. Clients are then granted *Roles* when they create a *Session* based on the information provided by the *Client*.

Roles are used to separate authentication (determining who a Client is with a user token and Client application identity) from authorization (Permissions determining what the Client is allowed to do). By separating these tasks Servers can allow centralized services to manage user identities and credentials while the Server only manages the Permissions on its Nodes assigned to Roles.

183 IEC 62541-3 defines the possible *Permissions* and the representation as *Node Attributes*.

Figure 1 depicts the *ObjectTypes*, *Objects* and their components used to represent the *Role* management.

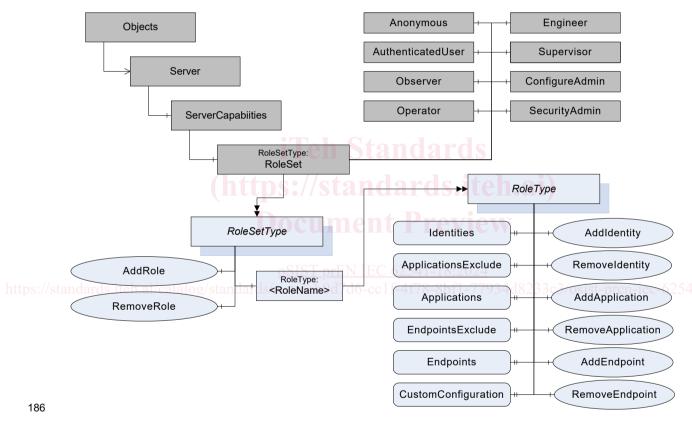


Figure 1 - Role management overview

### 4.2 RoleSetType

188

189

192

193

195

196

205

206

207

208

209

#### 4.2.1 RoleSetType definition

The RoleSet Object defined in IEC 62541-5 is a RoleSetType which is formally defined in Table 1.

#### Table 1 - RoleSetType definition

Attribute	Value				
BrowseName	RoleSetType				
IsAbstract	False				
References	Node Class	BrowseName	DataType	TypeDefinition	Modelling Rule
Subtype of BaseC	<i>bjectType</i> define	ed in IEC 62541-5			
HasComponent	Object	<rolename></rolename>		RoleType	OptionalPlaceholder
HasComponent	Method	AddRole	Defined in 4.2.2		Mandatory
HasComponent	Method	RemoveRole	Defined in 4.2.3.		Mandatory
Conformance Units					
Base Info ServerT	уре				

The AddRole Method allows configuration Clients to add a new Role to the Server.

The RemoveRole Method allows configuration Clients to remove a Role from the Server.

#### 4.2.2 AddRole Method

197 This Method is used to add a Role to the RoleSet Object.

The combination of the NamespaceUri and *RoleName* parameters are used to construct the BrowseName for the new *Node*. The BrowseName shall be unique within the *RoleSet Object*.

If the optional *Properties EndpointsExclude* and *ApplicationsExclude* are available on the *Role*Object created with this *Method*, the initial values of the *EndpointsExclude* and
ApplicationsExclude Properties shall be TRUE.

The *Client* shall use an encrypted channel and shall provide user credentials with administrator rights like *SecurityAdmin Role* when invoking this *Method* on the *Server*.

IEC 62541-3 defines well-known *Roles*. If this *Method* is used to add a well-known *Role*, the name of the *Role* from IEC 62541-3 is used together with the OPC UA namespace URI. The *Server* shall use the *Nodelds* for the well-known *Roles* in this case. The *Nodelds* for the well-known *Roles* are defined in IEC 62541-6.

### **Signature**

210	AddRole (	
211	[in] String	RoleName,
212	[in] String	NamespaceUri,
213	[out] NodeId	RoleNodeId
214	) ;	

Argument	Description
RoleName	The name of the <i>Role</i> .
NamespaceUri	The NamespaceUri qualifies the RoleName. If this value is null or empty then the resulting BrowseName will be qualified by the Server's NamespaceUri.
RoleNodeld	The Nodeld assigned by the Server to the new Node.

216

215