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:

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 62541-18:2024 **en,fr,de**

65E/1043/CDV

COMMITTEE DRAFT FOR VOTE (CDV)

PROJECT NUMBER: **IEC 62541-18 ED1**	
DATE OF CIRCULATION: **2024-01-26**	CLOSING DATE FOR VOTING: **2024-04-19**
SUPERSEDES DOCUMENTS: **65E/953/NP, 65E/1013/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 **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.		□ NOT SUBMITTED FOR CENELEC PARALLEL VOTING	

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 18: Role-Based Security

PROPOSED STABILITY DATE: 2026

NOTE FROM TC/SC OFFICERS:

CONTENTS

FIGURES

TABLES

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 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 62541-18 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 18: Role-Based Security

1 Scope

This part of the OPC Unified Architecture defines an Information Model. The Information Model describes the basic infrastructure to model role-based security.

Note: In the previous version, Role-Based Security was in IEC 62541-5, Annex F

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 62541-3, *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 62541-8, *OPC Unified Architecture – Part 8: Data Access*

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

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, IEC 62541-3 and IEC 62541-5 apply.

4 Role Model

4.1 General

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*.

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.

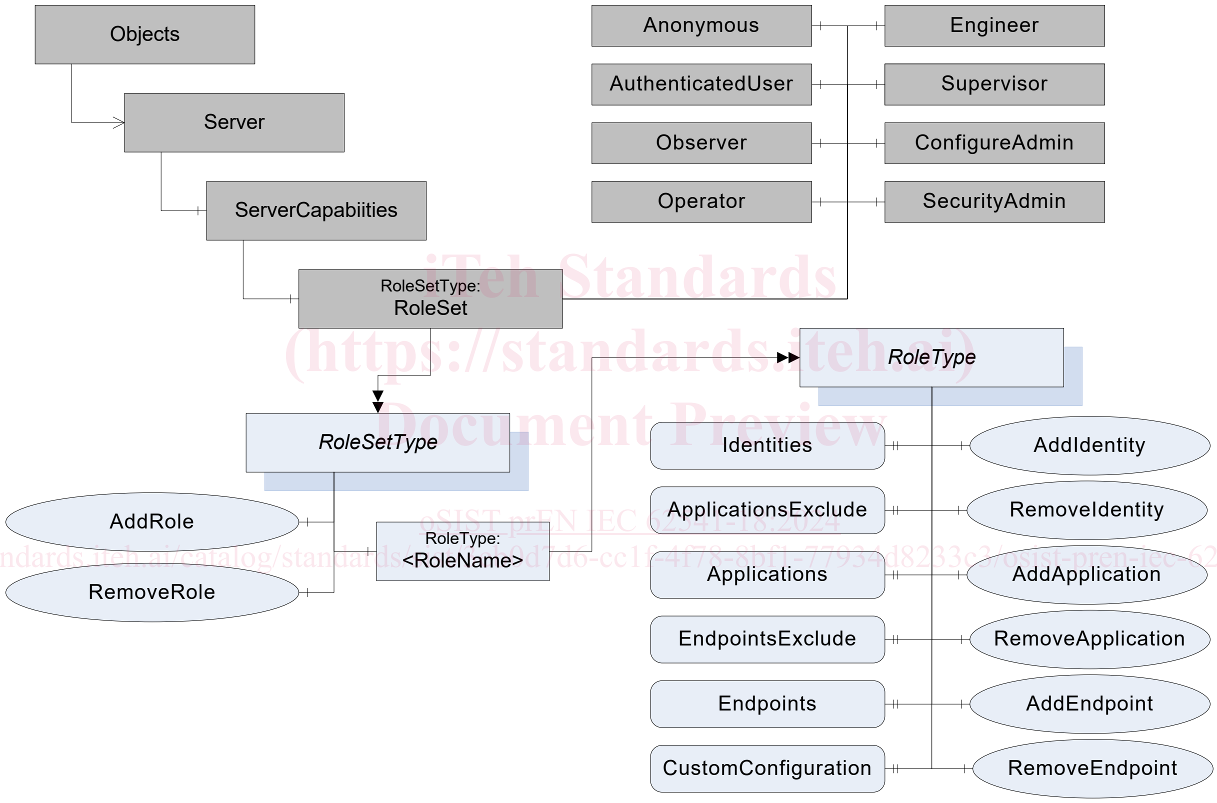

Figure 1 – Role management overview

4.2 RoleSetType

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 *BaseObjectType* defined in IEC 62541-5					
HasComponent	Object	<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 ServerType					

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

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 *NodeIds* for the well-known *Roles* in this case. The *NodeIds* for the well-known *Roles* are defined in IEC 62541-6.

Signature

```
AddRole (
   [in]  String          RoleName,
   [in]  String          NamespaceUri,
   [out] NodeId          RoleNodeId
   );
```

Argument	**Description**
RoleName	The name of the *Role*.
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*.
RoleNodeId	The *NodeId* assigned by the *Server* to the new *Node*.