

PUBLICLY AVAILABLE SPECIFICATION

**Communication networks and systems for power utility automation -
Part 90-19: Use of Role-Based Access Control (RBAC) with IEC 61850**

Sample Document

get full document from standards.iteh.ai



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2026 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

IEC Secretariat
3, rue de Varembe
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigendum or an amendment might have been published.

IEC publications search -

webstore.iec.ch/advsearchform

The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee, ...). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

IEC Customer Service Centre - webstore.iec.ch/csc

If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: sales@iec.ch.

IEC Products & Services Portal - products.iec.ch

Discover our powerful search engine and read freely all the publications previews, graphical symbols and the glossary. With a subscription you will always have access to up to date content tailored to your needs.

Electropedia - www.electropedia.org

The world's leading online dictionary on electrotechnology, containing more than 22 500 terminological entries in English and French, with equivalent terms in 25 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

Warning! Make sure that you obtained this publication from an authorized distributor.

CONTENTS

FOREWORD.....	5
1 Scope.....	7
1.1 General	7
1.2 Published versions of the standard and related namespace names	7
1.3 Identification of the Code Components.....	7
1.3.1 IEC 61850-90-19 XML namespace for O2OS	7
1.3.2 IEC 61850-90-19 XML namespace for SCLSig	8
1.4 Code Component distribution	8
2 Normative references	9
3 Terms, definitions and abbreviated terms	9
3.1 Terms and definitions	10
3.2 Abbreviated terms.....	12
4 Use cases for RBAC	13
4.1 General	13
4.2 Use cases and actors.....	13
4.3 Factory Configuration.....	14
4.3.1 General.....	14
4.3.2 Product Onboarding into the system	15
4.3.3 Operational system configuration.....	15
4.3.4 Operation.....	15
5 RBAC engineering for IEC 61850	16
5.1 General	16
5.2 Roles and associated permissions for IEC 61850	17
5.3 Permission to data object binding using operationSets	20
5.4 Definition of user defined permissions and restrictions.....	22
5.4.1 General.....	22
5.4.2 Illustrative Example.....	22
5.5 IEC 61850 RBAC Implementation	24
5.5.1 General.....	24
5.5.2 Definition of mandatory permissions other than security permissions.....	24
5.5.3 Logging.....	25
5.5.4 Configuration of devices	25
5.6 Engineering process	25
6 Impact on IEC 61850-7-4.....	27
7 Impact on IEC 61850-8-1/8-2	27
8 Default Right to IEC 61850 ACSI Service Mapping	28
8.1 General	28
8.2 VIEW.....	28
8.3 READVALUES	28
8.4 DATASET	29
8.5 REPORTING	29
8.6 FILEREAD	29
8.7 FILEWRITE.....	29
8.8 CONTROL	29
8.9 CONFIG	29
8.10 SETTINGGROUP	29

8.11	FILEMNGT.....	30
8.12	SECURITY.....	30
9	Security of RBAC Configuration	30
9.1	General	30
9.2	Protection of contents	30
9.2.1	General.....	30
9.2.2	IEC 62351-11 Profile	30
9.3	Exchange of Configuration.....	33
9.4	At Rest Security	33
10	Serialization Mappings	34
10.1	Serialization to XACML	34
10.1.1	General Structure	34
10.1.2	Uniform Resource Names for additional XACML attributes	34
10.1.3	Uniform Resource Names for PolicySets, Policies and Rules.....	34
10.1.4	RootPolicySet.....	35
10.1.5	IEC62351-8RoleInfo	35
10.1.6	Policy	36
10.1.7	Rules.....	36
10.1.8	Target.....	36
10.1.9	ORProcess.....	36
10.1.10	AndProcess.....	36
10.1.11	Match	36
10.1.12	MatchKind	37
10.1.13	OperationalState.....	37
10.1.14	Area of responsibility.....	38
10.1.15	Obligations.....	40
10.1.16	Short term access	41
10.2	OperationSet XACML files	42
10.2.1	General structure	42
10.2.2	Root PolicySet.....	42
10.2.3	OperationSet PolicySet.....	42
10.2.4	Role-to-Permission Mapping for an OperationSet	42
10.2.5	Standard- and Custom Permissions	43
10.2.6	Including Operational States	43
10.2.7	XACML Attributes	43
10.2.8	Remarks and Policy Evaluation	44
11	O2OS XML file definition	45
11.1	File version management.....	45
11.1.1	General.....	45
11.1.2	Header	45
11.1.3	History	46
11.1.4	SCLFile.....	46
11.1.5	XACMLFile.....	46
11.2	Mapping between ObjectForOperationSet and SCL elements	47
11.2.1	General.....	47
11.2.2	ObjectForOperationSet	47
11.2.3	IED.....	47
11.2.4	ApplicableAccessPoint	48
11.2.5	LDevice	48

11.2.6	LNode.....	48
11.2.7	DataObject.....	49
11.2.8	DataAttribute	49
11.2.9	ControlBlock.....	50
11.2.10	Files	50
12	Engineering use cases	50
12.1	General	50
12.2	Engineering with device template phase.....	51
12.3	Engineering with specification phase	52
12.4	Specifying device specific OperationSet assignment	53
12.5	Engineering with O2OS for a set of device instances following a device template	55
12.6	Engineering with AccessPoint specific OperationSet	55
Annex A	(informative) Examples	57
Annex B	(normative) Signing of IEC 61850-6 SCL File	64
B.1	General	64
B.2	Explanation of XML Elements and Attributes	66
B.2.1	XML Namespace.....	66
B.2.2	SignatureEntries	66
B.2.3	SignatureInfo.....	67
B.3	Tooling Requirements	68
B.4	Generation of Signature	68
B.5	Validation of Signature.....	69
Bibliography		70
Figure 1	– High level RBAC use cases.....	13
Figure 2	– Scope of operationSet files.....	21
Figure 3	– Assignment of restricted operationSets to example objects	21
Figure 4	– Example objects provided in SCL	22
Figure 5	– Assignment of existing (manufacturer defined) operationSets to example objects	22
Figure 6	– Assignment of restricted operationSets to example objects.....	23
Figure 7	– Commissioning of an IED.....	25
Figure 8	– Handling of Permission to Object assignment using SCL, XACML, an O2P Files.....	26
Figure 9	– General IEC 62351-11 XSD layout.....	31
Figure 10	– XSD ComplexType definition of HeaderType.....	31
Figure 11	– XSD ComplexType definition of information	32
Figure 12	– SignedInfotype XML structure.....	32
Figure 13	– SignatureMethodType structure	33
Figure 14	– Transforming a received request into a XACML request context.....	34
Figure 15	– Definition of OperationSets using XACML	42
Figure 16	– O2OS Header UML definition	45
Figure 17	– Object to OperationSet class diagram	47
Figure 18	– O2OS engineering with ICD file and superseding O2OS assignment	51
Figure 19	– O2OS engineering with ICD files.....	52

Figure 20 – O2OS engineering with ISD files	53
Figure 21 – O2OS engineering with IID files	54
Figure 22 – O2OS engineering with ICD file and superseding O2OS assignment	55
Figure 23 – AccessPoint specific OperationSet.....	56
Figure B.1 – Position of Signing Information in SCL	65
Figure B.2 – Signing of IEC 61850 SCL files	66
Table 1 – Published versions and related namespace names	7
Table 2 – Attributes of the O2OS XML namespace.....	7
Table 3 – Attributes of the IEC 61850-6 Signature XML namespace.....	8
Table 4 – Actors and actor definitions	14
Table 5 – Pre-defined roles (as of IEC 62351-8)	17
Table 6 – List of pre-defined role-to-permission assignments for IEC 61850	18
Table 7 – List of mandatory pre-defined permissions.....	19
Table 8 – User-Defined Permission	23
Table 9 – LISTOBJECTS permission and associated ACSI services	24
Table 10 – Attributes of the Header element.....	45
Table 11 – Attributes of the Hitem element.....	46
Table 12 – Attributes of the SCLFile element.....	46
Table 13 – Attributes of the XACMLFile element.....	46
Table 14 – Attributes of the ObjectForOperationSet element.....	47
Table 15 – Attributes of the IED element.....	48
Table 16 – Attributes of the ApplicableAccessPoint element	48
Table 17 – Attributes of the LDevice element.....	48
Table 18 – Attributes of the LNode element.....	49
Table 19 – Attributes of the DataObject element	49
Table 20 – Attributes of the DataAttribute element	49
Table 21 – Attributes of the ControlBlock element.....	50
Table 22 – Attributes of the Files element	50
Table A.1 – DER Capabilities vs Roles for the Normal OperationalState.....	58
Table A.2 – DER Capabilities vs Roles for the Lockout OperationalState.....	60
Table A.3 – DER Capabilities vs Roles for the Test/Maintenance OperationalState	62
Table B.1 – Allowed algorithm identifiers	67

INTERNATIONAL ELECTROTECHNICAL COMMISSION

Communication networks and systems for power utility automation - Part 90-19: Use of Role Based Access Control (RBAC) with IEC 61850

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) IEC [draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). IEC takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, IEC had not received notice of (a) patent(s), which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at <https://patents.iec.ch> [and/or] www.iso.org/patents. IEC shall not be held responsible for identifying any or all such patent rights.

IEC 61850-90-19 has been prepared by IEC Technical Committee 57: Power system control and associated communications. It is a Publicly Available Specification.

The text of this Publicly Available Specification is based on the following documents:

Draft	Report on voting
57/2888/DPAS	57/2946/RVDPAS

Full information on the voting for its approval can be found in the report on voting indicated in the above table.

The language used for the development of this Publicly Available Specification is English.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement, available at www.iec.ch/members_experts/refdocs. The main document types developed by IEC are described in greater detail at www.iec.ch/publications.

NOTE The following print types are used:

- Definitions from Clause 3: in *Courrier New* type.

This document includes Code Components i.e. components that are intended to be directly processed by a computer.

Such content is any text found between the markers <CODE BEGINS> and <CODE ENDS>, or otherwise is clearly labelled in this document as a Code Component.

The purchase of this document carries a copyright license for the purchaser to sell software containing Code Components from this standard to end users either directly or via distributors, subject to IEC software licensing conditions, which can be found at: www.iec.ch/CCv1.

A list of all parts of the IEC 61850 series, under the general title: *Communication networks and systems for power utility automation*, can be found on the IEC website.

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under webstore.iec.ch in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn, or
- revised.

NOTE In accordance with ISO/IEC Directives, Part 1, IEC PASs are automatically withdrawn after 4 years.

1 Scope

1.1 General

The general requirements for Role-Based Access Control (RBAC) are defined in IEC 62351-8. This part of IEC 61850, which is a Publicly Available Specification, applies those requirements to the IEC 61850 environment, including the RBAC modelling considerations, the impacts on IEC 61850 models and protocols, and the resulting engineering process requirements.

This document takes over the IEC 61850 data model specific definitions such as the definition of permissions and their assignment to roles from IEC 62351-8.

Additionally, the binding of permissions to objects is defined to allow an interoperable implementation regarding the semantic of roles. This is achieved by an assignment to unique data objects based on the SCL description. Note that for this, [IEC 61850-6:2009+AMD1:2018+AMD2:2024](#) is a prerequisite as it defined a unique identification of objects in SCL.

1.2 Published versions of the standard and related namespace names

Table 1 provides a reference between all published editions, amendments or corrigenda of this document and the full name of the namespace.

Table 1 – Published versions and related namespace names

Edition	Publication date	Webstore	Namespace
Edition 1.0	2026-07	IEC 61850-90-19:2026	IEC 61850-90-19-O2OS:2024A4
Edition 1.0	2026-07	IEC 61850-90-19:2026	IEC 61850-90-19-SCLSig:2024A2

1.3 Identification of the Code Components

1.3.1 IEC 61850-90-19 XML namespace for O2OS

The namespace associated with this document for O2OS structure is an XML schema (XSD). The parameters which identify the namespace are provided in Table 2:

Table 2 – Attributes of the O2OS XML namespace

Attribute	Content
Namespace nameplate	
Namespace Identifier (xmlns)	http://www.iec.ch/61850/2024/O2OS/90-19
Version	2024
Revision	A
Release	4
XSD version header attribute	2024A4
Mandatory reference name	eIEC61850-90-19
Code Component Name	IEC_61850-90-19.O2OS.2024A4.DPAS
Namespace dependencies	
includes	

1.3.2 IEC 61850-90-19 XML namespace for SCLSig

The namespace associated with this document for signing SCL files is an XML schema (XSD). The parameters which identify the namespace are provided in Table 2:

Table 3 – Attributes of the IEC 61850-6 Signature XML namespace

Attribute	Content
Namespace nameplate	
Namespace Identifier (xmlns)	http://www.iec.ch/61850/2024/SCLSig/90-19
Version	2024
Revision	A
Release	2
XSD version header attribute	2024A2
Mandatory reference name	eIEC61850-90-19-SCLSig
Code Component Name	IEC_61850-90-19.SCLSig.2024A2.DPAS
Namespace dependencies	
includes	

1.4 Code Component distribution

Each Code Component is a ZIP package containing the electronic representation of the Code Component itself, with a file describing the content of the package (IECManifest.xml).

The life cycle of a code component is not restricted to the life cycle of the related publication. The publication life cycle goes through two stages, Version (corresponding to an edition) and Revision (corresponding to an amendment). A third publication stage (Release) allows publication of Code Component in case of urgent fixes of InterOp Tissues, thus without need to publish an amendment.

Consequently, new releases of the Code Component may be released, which supersedes the previous release, and will be distributed through the IEC TC57 web site at:

<https://www.iec.ch/tc57/supportdocuments>

The latest version/release of the code component will be found by selecting the file for the code component with the highest value for VersionStateInfo, e.g. IEC_61850-90-19.XSD.{VersionStateInfo}.full.zip.

The code component associated to this PAS is an XML schema file (XSD). It is available as a full version only. It is freely accessible on the IEC website for download at <https://www.iec.ch/tc57/supportdocuments>, but the usage remains under the licensing conditions.

In case of any differences between the downloadable code component and the IEC pdf published content, the downloadable code component is the valid one; it may be subject to updates. See included history files.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 61850-6:2009, *Communication networks and systems for power utility automation - Part 6: Configuration description language for communication in electrical substations related to IEDs*
IEC 61850-6:2009/AMD2:2024

IEC 61850-7-2, *Communication networks and systems for power utility automation - Part 7-2: Basic information and communication structure - Abstract communication service interface (ACSI)*

IEC TR 61850-90-30, *Communication networks and systems for power utility automation – Part 90-30: IEC 61850 Function Modelling in SCL*

IEC TS 62351-1, *Power systems management and associated information exchange - Data and communications security - Part 1: Communication network and system security - Introduction to security issues*

IEC 62351-6, *Power systems management and associated information exchange - Data and communications security - Part 6: Security for IEC 61850*

IEC 62351-8, *Power systems management and associated information exchange - Data and communications security - Part 8: Role-based access control for power system management*

IEC 62351-11, *Power systems management and associated information exchange - Data and communications security - Part 11: Security for XML documents*

IEC 62351-14, *Power systems management and associated information exchange - Data and communications security - Part 14: Cyber security event logging¹*

RFC 6960, *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP*

XACML, *eXtensible Access Control Markup Language (XACML) Version 3.0 [OASIS]*

W3C Canonical XML Version 2.0
<https://www.w3.org/TR/xml-c14n2/>

3 Terms, definitions and abbreviated terms

For the purposes of this document, the terms and definitions given in IEC 62351-2 and the following definitions, which are taken from IEC 62351-8:2025 and enhanced with further information, apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

- IEC Electropedia: available at <https://www.electropedia.org/>
- ISO Online browsing platform: available at <https://www.iso.org/obp>

¹ Under preparation. Stage at the time of publication: IEC/ACDV 62351-14:2025.

3.1 Terms and definitions

3.1.1

area of responsibility

range of authority

Note 1 to entry: Some examples: geographical area; based on network segregation; control center; or software applications.

3.1.2

access token

evidence or testimonials concerning one's right to credit, confidence, or authority

3.1.3

holder

entity that possesses or owns an access token

3.1.4

issuer

entity that issues an access token

3.1.5

object

any system resource subject to access control such as a file, printer, terminal, database record, etc.

3.1.6

operation

executable image of a program which upon invocation executes some function/activity for the subject

3.1.7

OperationSet

tuple(s) of a role and a permission, which can be assigned to dedicated objects = object instances (e.g. FW)

3.1.8

permission

right to execute an action on a system object (e.g., permission = FILEWRITE: action = write; system object = FILE)

Note 1 to entry: Normative reference can be found in IEC 62351-8.

3.1.9

privilege

attribute or property assigned to a subject by an authority

Note 1 to entry: Normative reference can be found in IEC 62351-8.

3.1.10

right

atomic set of independent actions (e.g., read, write)

Note 1 to entry: Normative reference can be found in IEC 62351-8.

3.1.11

role

job function within the context of an organization with some semantics associated regarding the authority and responsibility conferred on the user assigned to the role

Note 1 to entry: A Role subsumes a set of rights.

Pre-defined role: a role that is defined in this document.

Default role: a role that is defined by the vendor of the protection equipment (not by its specification) and that is valid generally for all objects of that vendor.

Specific role: a role that is defined by the utility operator for its particular needs.

3.1.12

security

cyber-security

3.1.13

service

right/privilege/permission granted to an entity to use the abstract service

Note 1 to entry: IEC 61850 defines abstract services in IEC 61850-7-2. The Service construct in this document correlates to an IEC 62351-8 action.

3.1.14

session

encounter between a user and an application or with the computer in general

Note 1 to entry: One user session is the time between starting the communication channel (either local or remote) and terminating (either by the user or the system).

3.1.15

static separation of duty

SSD

enforcement constraints on the assignment of users to roles

Note 1 to entry: Membership in one role may prevent the User from being a member of one or more other roles, depending on the SSD rules enforced.

3.1.16

out-of-band

communications which occur outside of a previously established communication method or channel

3.1.17

subject

user or automated agent

Note 1 to entry: A subject is a right holder. It shall have a name attribute whose value is mandatory. It is this name that shall be used to enroll a subject in a particular role.

3.1.18

token

physical instance of an access token

3.1.19

user

human being

3.2 Abbreviated terms

For the purposes of this document, the terms and definitions of IEC TS 62351-1 apply, as well as the following.

Acronym	Meaning
AC	Attribute certificate
ACL	Access control list
ACRL	Attribute certificate revocation list
ACSI	Abstract communication system interface
AMI	Advanced metering infrastructure
AoR	Area of responsibility
Categories	Collection of rights to ease administration of custom defined roles
CIM	Common Information model
CRL	Certificate revocation list
DCB	Device configuration bundle
DER	Distributed energy resource
HMAC	Keyed-hash message authentication code
HMI	Human machine interface
IED	Intelligent electronic device; stands for a field device, a gateway or a PC in the net control centre
ID	Identity
IS	International standard
ISA	Instrument system and automation society
LDAP	Lightweight directory access protocol
LD	Logical device (IEC 61850)
LN	Logical node (IEC 61850)
MRID	Master Resource Identifier
O2OS	Object-to-OperationSet (configuration file)
OCSP	Online certificate status protocol
OID	Object identifier
OSI	Open systems interconnection
PKI	Public key infrastructure; the complete set of processes required to provide encryption and digital signature services
PDP	Policy decision point
PEP	Policy Enforcement Point
PMI	Privilege management infrastructure; the complete set of processes required to provide an authorization service
RBAC	Role-based access control
SCL	System configuration language (IEC 61850)
SSL	Secure socket layer
SW	Software
TCP	Transport control protocol
TLS	Transport layer security
UID	Universal identifier
XACML	eXtended Access Control Markup Language

4 Use cases for RBAC

4.1 General

This clause describes the use cases and involved actors motivating the support of role-based access control. It outlines specifics for which in the following clauses technical approaches and solutions are specified, which map role based access control as outlined in IEC 62351-8 to the IEC 61850 data model.

4.2 Use cases and actors

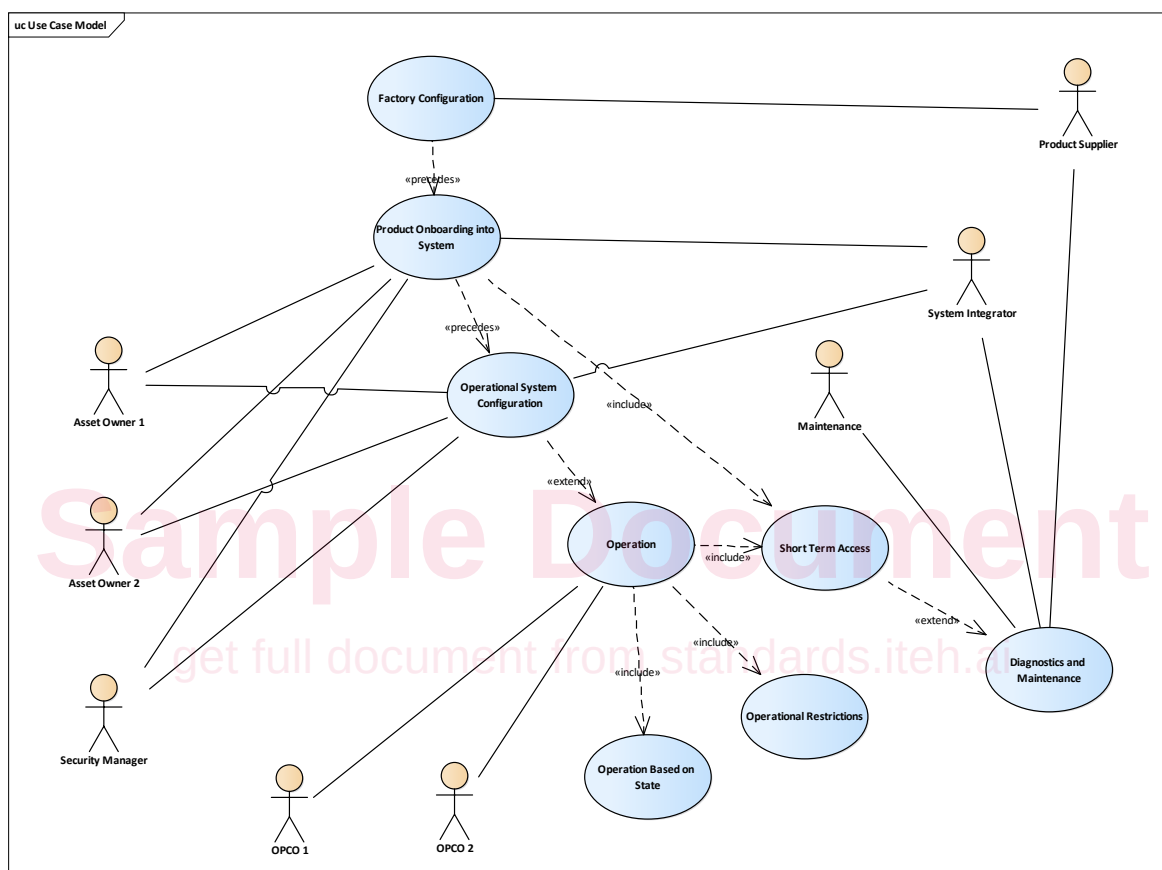


Figure 1 – High level RBAC use cases

Figure 1 shows the high-level use cases that are used to derive the requirements for this standard. The figure defines both actors and use cases.