Access to Additional Content

For: IEC TR 62351-90-1, Dated: 01/2018

(Click **here** to view the publication)

This Page is not part of the original publication

This page has been added by IHS Markit as a convenience to the user in order to provide access to additional content as authorized by the Copyright holder of this document

Click the link(s) below to access the content and use normal procedures for downloading or opening the files.

- Files associated with IEC TR 62351-90-1

If you have any questions, or need technical assistance please contact IHS Markit Support.

IHS Markit Additional Content Page

IEC TR 62351-90-1

Edition 1.0 2018-01

TECHNICAL REPORT

colour inside

Power systems management and associated information exchange – Data and communications security –
Part 90-1: Guidelines for handling role-based access control in power systems

IEC TR 62351-90-1:2018-01(en)

IEC Central Office
3, rue de Varembé
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 corrigenda or an amendment might have been published.

IEC Catalogue - webstore.iec.ch/catalogue
The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

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 It also gives information on projects, replaced and withdrawn publications.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 also once a month by email.

Electropedia - www.electropedia.org
The world's leading online dictionary of electronic and electrical terms containing 21 000 terms and definitions in English and French, with equivalent terms in 16 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary
67 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

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 TR 62351-90-1

Edition 1.0 2018-01

TECHNICAL REPORT

colour inside

Power systems management and associated information exchange – Data and communications security – Part 90-1: Guidelines for handling role-based access control in power systems

INTERNATIONAL ELECTROTECHNICAL COMMISSION

ICS 33.200

ISBN 978-2-8322-5233-8

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

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

POWER SYSTEMS MANAGEMENT AND ASSOCIATED INFORMATION EXCHANGE – DATA AND COMMUNICATIONS SECURITY –

Part 90-1: Guidelines for handling role-based access control in power systems

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".

IEC TR 62351-90-1, which is a technical report, has been prepared by IEC technical committee 57: Power systems management and associated information exchange.

This publication contains attached files in the form of electronic machine readable files. These files are intended to be used as a complement and do not form an integral part of the publication.

The text of this technical report is based on the following documents:

Enquiry draft	Report on voting
57/1905/DTR	57/1942/RVDTR

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

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

A list of all the parts in the IEC 62351 series, published under the general title *Power systems management and associated information exchange – Data and communications security,* can be found on the IEC website.

This IEC Technical Report 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 labeled in this standard as a Code Component.

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

The Code Components included in this IEC standard are also available as electronic machine readable files at: http: //www.iec.ch/public/TC57/IEC_62351-90-1.XACML-Examples.full.TR.zip.

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

INTRODUCTION

The power system sector is adopting security measures to ensure the reliable delivery of energy. One of these measures comprises Role-based Access Control (RBAC), allowing utility operators, energy brokers and end-users to utilize roles to restrict the access to equipment and energy automation functionalities on a need-to-handle basis. The specific measures to realize this functionality have been defined in the context of IEC TS 62351-8. It defines three profiles for the transmission of RBAC related information. This information includes, but not limited to, being contained in public key certificates, attribute certificates, or software tokens. Moreover, especially for IEC 61850, it defines a set of mandatory roles and associated rights. IEC 61850 also allows the definition of custom roles and associated rights, but this is not specified in a way to ensure interoperability.

Implementations of RBAC have shown that utilities are likely to have their own set of roles and associated rights that need to be supported. Therefore, this technical report enhances the solution for role based access control in power systems defined in IEC TS 62351-8. It provides best practice guidelines for the distribution of role-to-right information targeting the definition of custom roles besides the mandatory roles defined in IEC TS 62351-8. As defined in IEC TS 62351-8, roles of a user are transported in a container called an access token. Access tokens are assumed to be created and administered by an identity management tool. IEC TS 62351-8 currently defines three different formats for such access tokens.

This technical report targets the provisioning of guidance for the implementation of RBAC. More specifically it focuses on means to describe custom roles, as well as the management of these new roles and associated rights, which are typically administered in a management tool and enforced in the endpoints. By defining categories, the workflow is simplified for defining new roles and associated rights besides the predefined roles in IEC TS 62351-8 as well as the assignment to subjects. Consequently the information exchange necessary to distribute the RBAC information is also a target of this technical report to ensure interoperability between different vendor’s products. This is achieved by utilizing the existing standard XACML. In addition to IEC TS 62351-8 further constraints of role execution are considered. These constraints are bound to the execution environment rather than the access token carrying the role information itself.

POWER SYSTEMS MANAGEMENT AND ASSOCIATED INFORMATION EXCHANGE – DATA AND COMMUNICATIONS SECURITY –

Part 90-1: Guidelines for handling role-based access control in power systems

1 Scope

This part of IEC 62351, which is a technical report, addresses the handling of access control of users and automated agents to data objects in power systems by means of role-based access control (RBAC) as defined in IEC TS 62351-8. IEC TS 62351-8 defines three different profiles to distribute role information and also defines a set of mandatory roles to be supported. Adoption of RBAC has shown that the defined mandatory roles are not always sufficient and it is recommended that the method for defining custom roles be standardized to ensure interoperability. Hence, the main focus of this document lies in developing a standardized method for defining and engineering custom roles, their role-to-right mappings and the corresponding infrastructure support needed to utilize these custom roles in power systems. This is achieved by defining categories and sub level categories, which provide a distinction of actions, connected with dedicated rights as well as a proposal for a format to distribute the custom role-to-right mappings. Moreover, a format is being proposed to distribute the information on custom defined roles and associated rights by utilizing XACML as an established standard for access control.

Besides the discussion of handling custom roles, this document also addresses the following issues:

– Providing recommendations and/or examples for role-right-operation and (object) association to ensure interoperability from operational and developers point of view.

– Providing mechanisms and rules to avoid overloading of existing roles by allowing for an aligned way to define new (custom) roles.

– Easing the administration of roles in IEDs from a device management point of view:

  - Allowing for centralized assignment of roles, by maintaining the same associations on device/application level.
  - Avoiding the definition of role-right-operation on command level to cope with diverse application environment of IEC TS 62351-8 (e.g. IED, substation level, control centre, SCADA).

– Enhancing available constraints for acting in a specific role considering the local environment with respect to operational constraints.

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, *Communication networks and systems for power utility automation – Part 6: Configuration description language for communication in electrical substations related to IEDs*

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 62351-3, *Power systems management and associated information exchange – Data and communications security – Part 3: Communication network and system security – Profiles including TCP/IP*

IEC TS 62351-4, *Power systems management and associated information exchange – Data and communications security – Part 4: Profiles including MMS*

IEC TS 62351-5, *Power systems management and associated information exchange – Data and communications security – Part 5: Security for IEC 60870-5 and derivatives*

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

IEC 62351-7, *Power systems management and associated information exchange – Data and communications security – Part 7: Network and System Management (NSM) data object models*

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

IEC 62351-9, *Power systems management and associated information exchange – Data and communications security – Part 9: Cyber security key management for power system equipment*

IEC 62443-3-3, *Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels*

ISO 9594-8/ITU-T Recommendation X.509:2005, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*

OASIS XACML eXtensible Access Control Markup Language, Version 3

3 Terms, definitions and abbreviated terms

For the purposes of this document, the terms and definitions given in IEC TS 62351-1 and IEC TS 62351-8 and the following apply.

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

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

3.1 Terms and definitions

3.1.1
categories
collection of rights to ease administration of custom defined roles

3.2 Abbreviated terms

AC attribute certificate

ANSI american national standards institute

AMI advanced metering infrastructure

AoR area of responsibility

BDEW	Bundesverband der Energie- und Wasserwirtschaft (Germany)
BSI	Bundesamt für Sicherheit in der Informationstechnik (Germany)
CIM	common Information model
CIP	critical infrastructure protection
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
ISMS	Information security management system
LDAP	lightweight directory access protocol
LD	logical device (IEC 61850)
LED	light emitting dode
LN	logical node (IEC 61850)
MMS	manufacturing message specification
NERC	North American electric reliability cooperation
OASIS	organization for the advancement of structured information standards
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
RBAC	role-based access control
SCADA	system control and data acquisition
SCD	substation configuration description
SCL	system configuration description language (IEC 61850-6)
SOA	service oriented architecture
SW	software
TLS	transport layer security
UID	universal identifier
XACML	eXtended Access Control Markup Language
XML	eXtended Markup Language

4 Overview

4.1 General

This document provides guidance for the application of RBAC within multi-vendor power systems utilizing IEC TS 62351-8. IEC TS 62351-8 defines three different profiles to distribute role information and also defines a set of mandatory roles to be supported. It has been acknowledged that in several use cases the defined (mandatory to support) roles are not sufficient. Therefore, the definition of custom roles in an interoperable way is seen as the consequent next step.

As stated in the scope, the main focus of this document lies in the definition of a standardized method for defining and engineering custom roles, role-to-right mappings and the corresponding infrastructure support to utilize these custom roles in power systems. This document addresses this by discussing the workflow to create custom roles as well as the means to distribute the information of custom defined roles and associated rights. More specifically, the workflow includes the defining categories and sub categories, which provide a distinction of actions, connected with dedicated rights. This categorization simplifies the administrative effort when managing (creating) roles. Regarding the distribution of role-to-right information, this document relies on the existing standard XACML for the file format and infrastructure, and defines the structure for the information transfer.

Further guidance for the application of RBAC in this report relates to operational handling, including:

– Providing an example for role definition based on the categorization of actions
– Handling of synchronous vs. asynchronous RBAC enforcement
– Role changes during a session
– Application of RBAC under specific circumstances
– Handling of roles changes

4.2 Current definitions from IEC TS 62351-8

IEC TS 62351-8 specifies the integration of role-based access control in the context of power system communication to ease the burden of access management. IEC TS 62351-8 defines seven mandatory roles to be supported, and a set of predefined rights for each role. The focus for the definition has been placed on logical device access control for power automation using IEC 61850. The definition of mandatory roles for other domains (e.g., AMI, DER, CIM) was left open at the time of issuing IEC TS 62351-8.

Figure 1 provides an overview of the scope of definitions of IEC TS 62351-8.

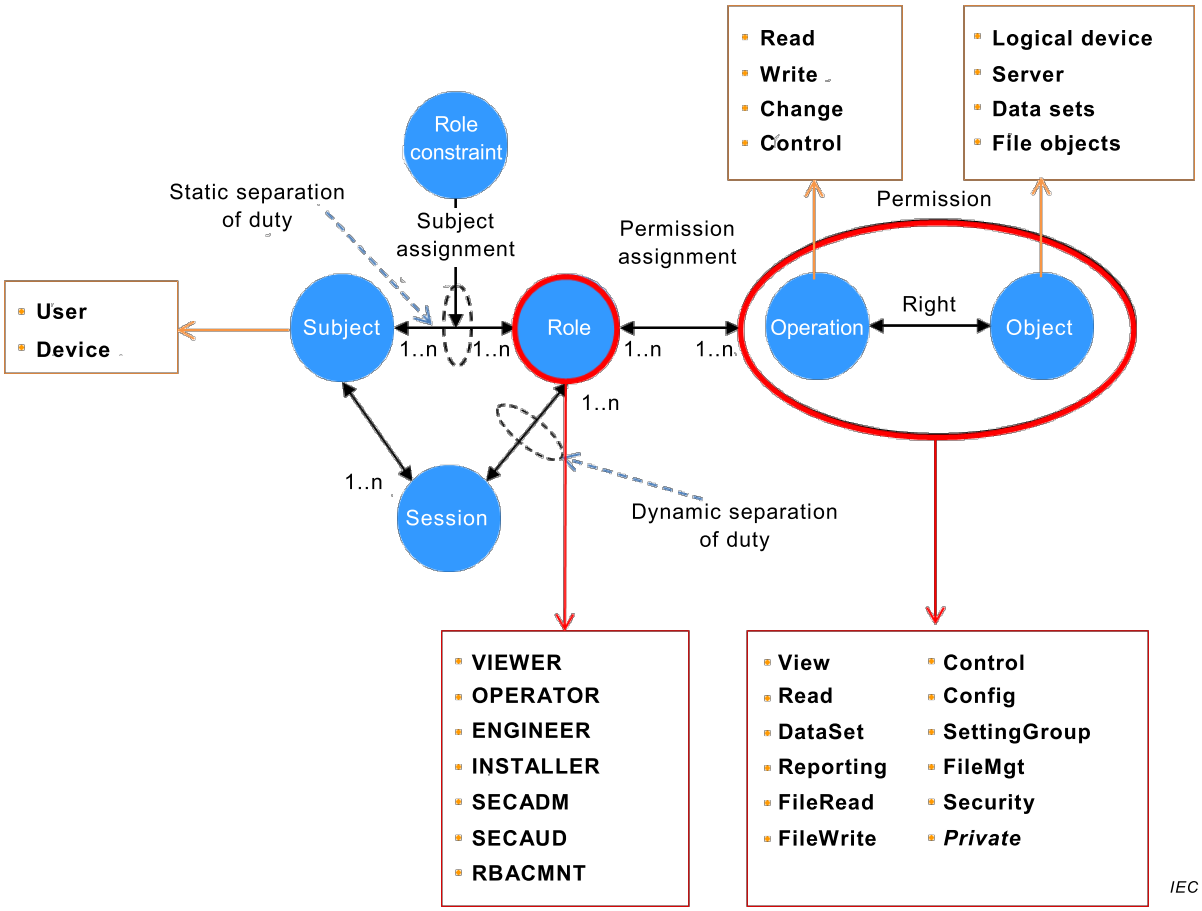

Figure 1 – Scope of RBAC as defined in IEC TS 62351-8

The mandatory roles for IEC 61850, stated in Figure 1, are characterized by the definition of associated rights as depicted in Table 1.

Table 1 – Pre-defined roles in IEC TS 62351-8

VIEWER	OPERATOR	ENGINEER	INSTALLER	SECADM	SECAUD	RBACMNT
• can view what objects are present within a Logical-Device by presenting the type ID of those objects.	• can view what objects and values are present within a Logical-Device by presenting the type ID of those objects • perform control actions.	• can view what objects and values are present within a Logical-Device by presenting the type ID of those objects. • has full access to DateSets and Files • can configure the server locally or remotely.	• can view what objects and values are present within a Logical-Device by presenting the type ID of those objects • can write files and can configure the server locally or remotely.	• can change subject-to-role assignments (outside the device) and role-to-right assignment (inside the device) and validity periods • change security setting such as certificates for subject authentication and access token verification.	• Security auditor can view audit logs.	• RBAC management can change role-to-right assignment.

IEC TS 62351-8 also defines three profiles to bind and transmit the role information as:

– Profile A: X.509v3 public key certificate with included role information as certificate extension

– Profile B: X.509v3 Attribute certificate bound to a public key certificate, which uses the same certificate extension

– Profile C: Software token (HMAC-protected structure, Kerberos like), which encapsulates the same information contained in the certificate extension

Besides the definition of the three profiles, also the delivery of the RBAC credential has been defined in terms of support for a PULL and PUSH model to retrieve the role information. PULL and PUSH are defined in the context of IEC TS 62351-8 and basically describe if the user accessing an IED is providing his role information (PUSH) or if the IED is retrieving this information (PULL) from a repository. Here, especially LDAP was addressed to fetch security credentials. IEC TS 62351-8 is currently also referenced from IEC TS 62351-5 for application within IEEE 1815 and IEC 60870-5-104. Specifically for IEC 60870-5-104 the application of the security according to IEC TS 62351-5 is described in IEC TS 60870-5-7.

4.3 Example standards and guidelines requiring RBAC

4.3.1 General

Subclauses 4.3.2 to 4.3.8 provide an overview of connected specifications in the area of power systems showing their scope of roles for RBAC. Also covered are documents which require role-based access control without defining specific roles as well as documents describing specific solutions for RBAC. This subsection is intended to motivate the described option to define custom roles, which go beyond the mandatory defined roles in IEC TS 62351-8.

Note that the described roles typically provide a minimum set of roles to address the required functionality on one hand and interoperability between different vendor's products on the other. The definition of custom roles in the context of operation will most likely result in additional roles and right definitions, which may better align with an operator's environment.

4.3.2 BDEW Whitepaper

The BDEW Whitepaper describes essential security measures for control and telecommunication systems and has been developed for power industry organizations. It targets to sufficiently protect the operation of these systems against security threats. The security measures described in the whitepaper are recommended for all newly procured control and telecommunication systems. Note that the BDEW Whitepaper refers to ISO 27001/2 for the definition of security controls according to an ISMS.

Regarding RBAC, the BDEW Whitepaper explicitly defines:

– Administrator: A user, who installs, maintains and administrates the system. Therefore the administrator role has the authorization and the according privileges to change the system and security configuration and settings.
– Auditor: User role, which solely has the permission to inspect and archive the audit logs and (if applicable) the exclusive right to delete them.
– Operator: User who performs regular system operations. This may include the right to change operational parameters (e.g. changing thresholds) or the right to execute security relevant actions (e.g. switch operation, removal of interlocks).
– Data-Display: User, who is allowed to view the status of the system and to read defined datasets but is not allowed to make any changes to the system or to execute commands.
– If applicable, a "Backup Operator" role is defined, which is allowed to backup relevant system and application data.

4.3.3 IEEE 1686

IEEE 1686 defines the functions and features to be provided in intelligent electronic devices (IEDs) to accommodate critical infrastructure protection (CIP) programs. IEEE 1686 addresses security regarding the access, operation, configuration, firmware revision and data retrieval from an IED. Encryption of communications to and from the IED is also addressed.

According to IEEE 1686, roles shall have the capability of supporting:

– View data: refers to the ability to view operational data (voltage, current, power, energy, status, alarms, et al) of the IED which are not intended to be available as general information display.
– View configuration settings: refers to the ability to view configuration settings of the IED such as scaling, communications addressing, programmable logic routines and the firmware version numbers.
– Force values: refers to the ability to manually override real data with manually inputted data and/or the ability to cause a control output operation to occur.
– Configuration change: refers to the ability to download and upload configuration files to the unit and/or effect changes to the existing configuration.
– Firmware change: refers to the ability to load new firmware which does not require a corresponding hardware change.
– ID/Password or RBAC management: refers to the ability to create, delete or modify user IDs, passwords, roles and/or password and role authorization levels.
– Audit trail: refers to the ability to view and download the audit trail.

4.3.4 ISO/IEC 27019

ISO/IEC 27019 provides guiding principles based on ISO/IEC 27002 “Code of practice for information security management” for information security management applied to process control systems as used in the energy utility industry. Therefore it extends the ISO/IEC 27000 series to the domain of process control systems and automation technology, allowing the energy utility industry to implement a standardized information security management system (ISMS) in accordance with ISO/IEC 27001 that extends from the business to the process control level. While ISO 27019 does not mandate specific roles, the base document ISO/IEC 27002 defines areas for which individuals are responsible should be stated. In particular the following should take place:

– the assets and security processes associated with each particular system should be identified and defined;
– the entity responsible for each asset or security process should be assigned and the details of this responsibility should be documented;
– authorization levels should be defined and documented;
– to be able to fulfil responsibilities in the information security area, the appointed individuals should be competent in the area and be given opportunities to keep up with developments;
– coordination and oversight of security aspects of supplier relationships should be identified and documented.

4.3.5 IEC 62443

IEC 62443 is a standard series addressing security in automation systems by defining policies and procedures, as well as technical requirements to systems and components. Specifically IEC 62443-3-3 defines foundational security requirements to be addressed by systems and solutions. Moreover, four security levels are defined to have a distinction of the applied means to address a dedicated requirement, based on the strength of a potential adversary. Here, role based access control is required to be supported to address security level 2 for the two foundational requirements:

– FR1: Identification and Authentication, specifically for the requirements related to the identification of human users, software processes and devices as well as account and identifier management.
– FR2: Use Control, specifically to support authorization enforcements by mapping permissions to roles.

4.3.6 NERC CIP

The North American Electric Reliability Corporation (NERC) maintains comprehensive reliability standards that define requirements for planning and operating the collective bulk power system. Among these are the Critical Infrastructure Protection (CIP) Cyber Security Standards, which are intended to ensure the protection of the Critical Cyber Assets that control or effect the reliability of North America's bulk electric systems.

This set of documents does not define specific roles, but CIP-004-5 explicitly relates in requirement 4, "Access Management", to the implementation of role-based access. This involves determining the specific roles on the system (e.g. system operator, technician, report viewer, administrator, etc.) then grouping access privileges to the role and assigning users to the role.

4.3.7 BSI TR 03109

The German BSI released the technical guideline TR 03109 to describe requirements for the secure operation of intelligent metering systems. The underlying architecture uses a smart meter gateway, to be placed between the actual smart meter at a premises and the meter data management, controlled by a smart meter gateway administrator. This guideline defines authorized roles to operate a smart meter gateway as:

– Consumer: juridical person withdrawing energy, gas, water or producing energy using a DER.
– Authorized External Entity: Every external except the smart meter gateway administrator.
– Smart Meter Gateway Administrator: responsible for configuration, monitoring and control of the smart meter gateway.
– Service Technician: can utilize the local diagnosis interface of the smart meter gateway.

4.3.8 Further requirements

Following requirements originate from discussions with utilities and are related to the general RBAC handling:

– In addition to user related roles, system related roles should be supported to ensure that there is the option to associate different rights to dedicated work environments (maintenance, back office, etc.). System related rights should be stronger than user related rights.
– There should be an option to have time restrictions for acting in specific roles.
– There should be an option to consider the operational constraints for the execution when operating in a specific role. Example situations include emergency situations and contractual changes to authorizations.

5 Categorization of actions to ease the definition of custom roles

5.1 General

To ease the workflow of defining custom roles, a categorization of actions is proposed. This categorization has two main goals. First, it is used to provide means for an operator, e.g. a utility, to easily define its own custom roles, which can be used and applied in an interoperable way in a multivendor environment. In this case, the categorization provides a grouping of atomic actions or rights to facilitate an association with a role to be defined. Second, the categorization supports interoperability between different vendor's products by defining a set of permissions/rights to be supported. A right or permission supported at the interface level of a device or application should be treated in a similar way by different vendors products but may be implemented in a vendor-specific way.

For the definition of custom roles, certain rights of a particular category of actions or subcategories of actions or specific actions may be grouped to define a new role. Hence, the

goal of this document is not the definition of new roles or custom roles, but to propose how those can be defined.

Categorization of actions is intended to improve usability, based on:

– Finite/limited set of generic action categories on abstract level
– Subcategories to improve granularity and understanding on generic operations within each category
– Multi-level of subcategories (or deeper branches) are abstractions of sets of atomic rights and may be associated with potential operations (e.g. IEC 61850) or commands (e.g. for device management) or engineering
– Mapping of roles and rights to categories or subcategories or even on specific action/operations level to define custom roles and associated rights

Besides the pure association of actions on resources described by the role definition, additional restrictions may be defined. This is already provided through the parameter “area of responsibility” (AoR) in the IEC TS 62351-8 access token definition, which can be used to define a geographical area or organizational unit, in which the specific role is entitled to act. This association in general is independent of the role definition. In addition to the AoR it is also possible to provide further restrictions like a specific validity time period of the access token.

The definition of custom roles using categorization is intended to be done on an abstract level, i.e. the described categories or subcategories describe a target functionality to be allowed or not, but do not imply any specific implementation. This leaves the option for vendor specific implementations of this functionality in a device as needed locally in an interoperable way.

In Subclauses 5.2 to 5.6, the first two levels are enumerated and explained.

NOTE The categorization can also be presented using a table as depicted in Figure 3 to ease visibility and editing of new subcategories down to atomic actions/rights. The following subsections explain the content of the actions category table.

5.2 Main category overview

The main categories constitute the entry point for the definition of custom roles.

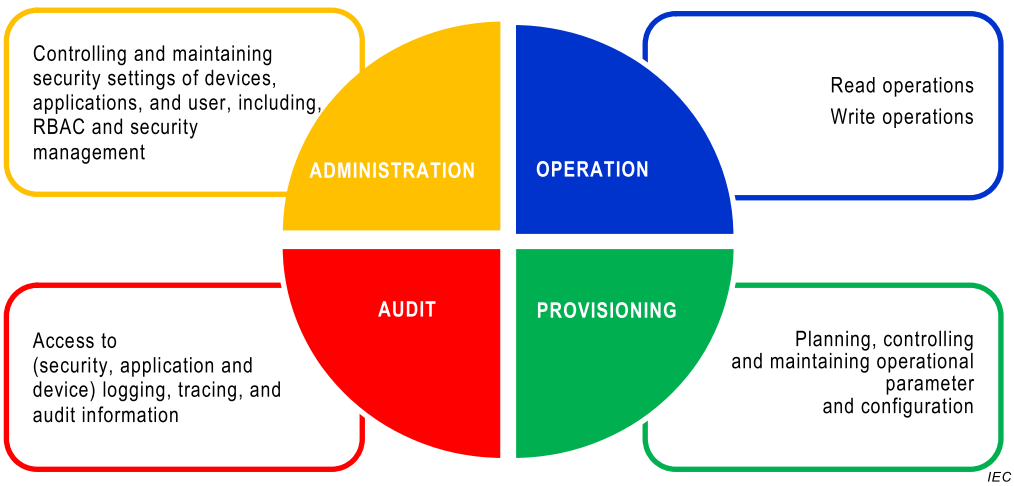

Figure 2 – Main categories

Figure 2 shows a limited set of rather generic categories on abstract level. For these categories further subcategories with different levels have been defined to better distinguish

specific topics within a category. Subcategories may be associated with potential operations (e.g. IEC 61850) or commands (e.g. for device management) or engineering.

Figure 3 shows an example of existing subcategories of level 1 and level 2 to the main category “Administration”

Categories	Subcategories Level 1	Subcategories Level 2
Administration		
	UserManagement	
		ViewUserAccounts
		EditUsersAccountData
		AddUserAccounts
		DeletaUserAccounts
		AccountsEnablingDisabling

IEC

Figure 3 – Level structure of categories (example)

Subclauses 5.3 to 5.6 describe the different levels of subcategories for each of the main categories stated above.

5.3 Category: Administration

Administration is for personnel with the highest administrative rights in the facility. These are typically the administrators. Table 2 lists subcategories for administration.

Table 2 – Subcategories for administration

Level 1 Subcategories	Level 2 Subcategories of actions – Permissions to be defined
User Management	View user accounts; Add new users; Edit existing users’ data; Deletion of user accounts; Enabling and disabling user accounts (e.g. vacation days).
Password Management	Manage (set/reset) users’ passwords; Edit password policies of the facility or entity.
Roles Assignment	Assign roles to users and applications (can have one or more roles).
AoR Assignment	Assign AoRs to users (Roles can be bound to an Area of Responsibility. Users may have one or more AoRs assigned to them).
Role Management	Create new roles; Manage custom roles permissions; Delete custom roles (besides the pre-defined roles in IEC TS 62351-8, custom roles can be defined, based on an own combination of rights).
AoR Management	Create new AoRs; Rename AoRs; Delete AoRs; Manage AoR valid times.
Certificate Management	Certificate management is part of a PKI infrastructure: Manage trusted certificates; Manage certificate white lists; Manage device certificates; Issue Certificates; Revoke Certificates.

5.4 Category: Provisioning

Provisioning is primary for the system integrator, knowledgeable users and device manufacturing personnel that have a good understanding of the installed equipment at the facility.

Provisioning may involve the operator in order to authorize certain actions. Table 3 lists subcategories for provisioning.

Table 3 – Subcategories for provisioning

Level 1 Subcategories	Level 2 Subcategories of actions – Permissions to be defined
Maintenance mode	View diagnostic data; Delete diagnostic data View disturbance data; Delete disturbance data; View application logs; Delete application logs.
Test / Simulate	Enabling & disabling: Test mode; Simulation mode; Emulation mode; Diagnostic mode Perform tests.
HMI Settings	Influence HMI settings of the device: LED reset; Change Menus & Toolbars; Change Synoptics.
Entity Management	Settings Management; Configuration Management; Firmware/Software Management.
Parameterization	Management of: General parameters; Automation parameters; Communication parameters; Control parameters; Cyber Security parameters; Maintenance parameters; Pricing parameters; Protection parameters; Service parameters; Other parameters.

5.5 Category: Operation

Operation covers daily business actions at an installation. Table 4 lists subcategories for operation.

Table 4 – Subcategories for operation

Level 1 Subcategories	Level 2 Subcategories of actions – Permissions to be defined
Operations View	Granular permissions to view: Aggregated data; Billing data; Control data; Diagnostic data; Maintenance data; Monitoring data; Process data; Service data; Settlement data. An operator with the Operation Viewing (read) permissions has not only read access to the corresponding data. Subcategories and atomic operations may further restrict the information to be accessed. An operator with the role as Viewer, can read information with the services defined in IEC 61850-7-2.[a] Rights can be defined down to an Object level[b]
Operations Write	Granular permissions to act on: Billing operations; Control operations[c]; Diagnostic operations; Maintenance operations; Protection operations; Service operations; Alarms acknowledgement
Standard operations	Logon and logout to entity

[a] **(Read)** GetServerDirectory, GetLogicalDeviceDirectory, GetLogicalNodeDirectory, GetAllDataValues, GetDataDefinition, GetDataDirectory, GetDataSetDirectory, GetBRCBValues, GetURCBValues, GetLCBValues, QueryLogByTime, QueryLogAfter, GetLogStatusValues

[b] **(Object definition)** Logical Device, Logical Node, DataSet, File

[c] **(Write)** SetDataValue, SetDataSetValues, CreateDataSet, DeleteDataSet, Operate, TimeActivatedOperate, SetBRCBValues, SetURCBValues, SetLCBValues

5.6 Category: Audit

The audit category encloses audit actions that should be performed by specially trained personnel. Table 5 lists subcategories for audit.

Table 5 – Subcategories for audit

Level 1 Subcategories	Description
Certificate logs	The entity must always have a read-only 'certificate log' with documentation of all the certificate handling since last audit. Certificate logs should record certificate actions, such as when new certificates are created, when certificates are revoked and installed or uninstalled.
Security logs	The entity must always have a read-only 'security log' reports of all the security relevant actions since last audit. Security relevant actions includes: password handling, role/right assignments, firmware updates, user activities and more.
Generation of User Activities reports	Organizations must produce regularly reports of user activities to make available for regular audits.
Change Management logs	The entity must always have a read-onlx log of entity management actions with documentation handling since last audit.
Roles/Right Permissions	The entity must always have a configuration file for the current role/right assignments, which can be read as part of the audit process.

6 RBAC Operation

6.1 General

Clause 6 describes cross relations to consider when integrating RBAC into power systems. These points have been identified during the integration of RBAC into the devices and processes, and there exists a need for clarification and guidance.

6.2 Synchronous versus asynchronous RBAC operation

This subclause discusses differences between actions carried out in the context of an explicit role depending on the online/offline state of the entity verifying the RBAC credential. In IEC 62351 the target is typically the provisioning of end-to-end security. This explicitly applies to the authentication of communicating peers and also to the authorization to act in a specific role.

There are two distinct properties of the communication with an IED (synchronous and asynchronous), in which the enforcement of RBAC differs. For this discussion it is assumed that both sides use X.509 certificates for authentication, which also carry the role information as extension. In both cases, RBAC must be enforced through the IED.

– Synchronous (online) (see Figure 4): A session, e.g., for engineering, is established between two entities, in which one entity is performing dedicated actions on resources of the other. At the beginning of the session, the IED (server) authenticates the client (user/device) and verifies the role information of the client and allows actions to be performed according to the entitled role and according to the defined role-to-right mapping available on that entity. It is assumed that there may be multiple sessions associated to different role information used to do a complete engineering. The managed entity is expected to perform the actions in a synchronous fashion.

RBAC bound to a communication session may be done using a TLS connection used to protect the engineering operation as base. It may also be related to an MMS session (assumed the currently defined enhancements for the A-Profiles in IEC TS 62351-4 are used).

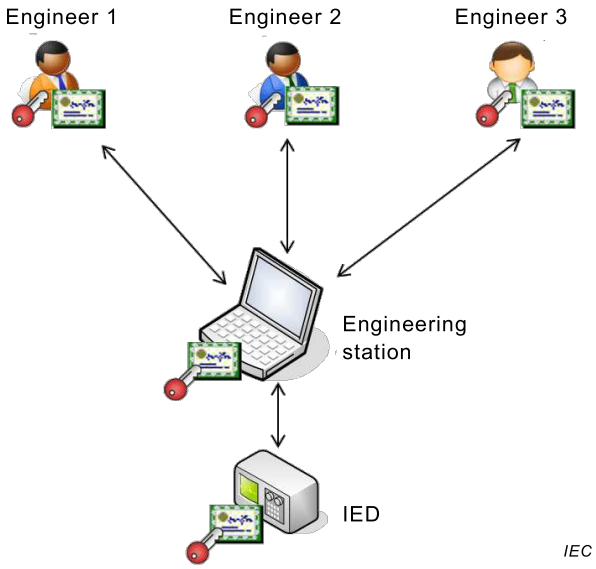

Figure 4 – Online engineering session (synchronous)

If there are roles with overlapping rights and there are sequential or parallel sessions with the IED to be administered, it is a security policy decision how to handle a change or action made by concurrent roles. A simple approach is based on timeliness, leading to the acceptance of the setting of a dedicated value from the last authorized role.

– Asynchronous (offline): Certain information may also be prepared upfront, before actually submitting it to the IED. This information may be an engineered SCL file containing the base settings for the IED. The SCD itself contains different values, which need to be provided by the appropriate role. The process of compiling the SCL file needs to take the role of the information provider into account.

  As with the synchronous case, it is a security policy decision on how to handle concurrent changes of the same value by different roles in offline engineering. A simple approach is based on timeliness, leading to the acceptance of the setting of a dedicated value from the last authorized role. The installer at the end has the right to change the configuration and thus is able to submit the offline engineered data to the IED.

Both cases require that the appropriate RBAC credentials are provided to the IED. Additionally the policy engine for matching the provided role information to the allowed actions on the resources needs to available on the IED directly or can be accessed remotely.

6.3 Role changes during a communication session

Roles (as currently defined in IEC TS 62351-8) are intended to be used on a per session base. A session may be constituted by a TLS connection or by a MMS connection. This is defined in

– IEC 62351-3/4/5/6/7/9 for the application of TLS
– IEC TS 62351-4 for MMS, which additionally provides an A-Profile for authenticating a dedicated user/entity at the beginning of the MMS session.

In all cases, if the X.509 certificate used to establish the session carries the RBAC extension as defined in IEC TS 62351-8 profile A or B, the role is bound to the session. Consequently, if the role changes, a new session is created requiring the use of the certificate associated with the new (alternative) role to be used.

6.4 Application of RBAC under specific circumstances

In certain situations, e.g. emergency access, specific roles and associated rights are necessary. An example is given through the traffic light concept (green – normal, yellow – alert, and red – emergency situations), reflecting specific conditions of the electricity networks

and thus requiring a prioritization of actions performed by specific roles. It is proposed to issue specific roles to be used in these situations. This approach aligns with the option to define custom roles defined in this document. Moreover, the signalling or detection of a specific situation is outside the scope of this document.

Using specific roles may be accomplished by the RBAC token issuing process. The process may already consider the operational environment of a component to be managed and therefore define situations specific roles. Alternatively the situation may be detected by the IED or signalled to the IED.

The concept is that different IED users can be defined. During normal operation conditions these IED users use their associated RBAC credential implying their normal role. When the electrical system is in an “exceptional state”, for instance according to traffic light condition notification, then the role to right association may change (for instance a user should be able to operate within a different AoR, in order to allow the operator takeover during an emergency case, or remote users may be prevented from certain actions that must be performed by local users only).

According to IEC TS 62351-8, the user role information can be delivered to the IED using different options. For each option the role and the role related authorization must be delivered to the device in advance, during a configuration phase taking place in normal operational conditions.

The user’s identity, role association and authorization are intended to be managed using a centralized management system. Users and role administrators must be entitled to define, change and remove users and roles in normal condition and in special traffic light conditions as well.

There are two basic possible scenarios in traffic light status notification handling:

1) Notify to all IEDs the status change, and starting from that moment the devices will associate to the user’s role a different set of authorizations. The user will not change its own role.
2) Notify the traffic light conditions change to the centralized management system, allowing the association of the traffic light special roles to the needed user set. The association of the users to special roles can be required to be carried out under the authorization of multiple user administrators in order to avoid the abuse of special role assignment. No changes are required on IEDs because the new role is already deployed.

The first scenario requires the notification of the special traffic light condition to a large number of IED in order to make each device aware of the change. This status change information is also sensitive from security perspective.

The second scenario requires the temporary issue of special user authorization token within the central user management side. According to IEC TS 62351-8, this temporary authorization can be assigned using any of the supported profiles. Profile B (X.509 attribute certificates) can be a better option against Profile A (X.509 ID certificate with extension) choice because can be more flexible and attribute certificate are well suited for short term life authorization.

A potential advantage of second scenario over the first is that when the exceptional condition takes place then the specific access to the device can be obtained with a centralized action that will not involve a massive notification to a large number of IEDs.

A specific realization option of RBAC in an emergency case is known as “Break-the-Glass” policy. This approach refers to means to gain controlled access to an application or system in specific situation even though the appropriate access privileges are not available in normal situations.

Break-the-Glass is based upon pre-defined access policies and may be directly connected with “emergency” accounts, managed in a way to make them available with reasonable administrative overhead. A “Break-the-Glass” policy can be implemented in different ways, depending on the target systems and applications like:

– As special condition for existing RBAC credentials requiring the system/application to be aware of the specific situation in which these associated access rights can be granted.
– Separate individual accounts with associated extended rights, to be used in emergencies only.
– Generic credentials (username/password, magnetic card, smart card, etc.) to be protected in a way that access is only granted in emergency situations

A “Break-the-Glass” policy needs to determine the credential management from distribution, activation, monitoring, application, until deactivation to be able to have an audit trail for these credentials. This requires technical means as well as integration into the business process.

To introduce the specific circumstances into the RBAC model utilized in IEC TS 62351-8, a new constraint is introduced, which is not directly bound to the role itself, but to the execution environment. This is illustrated in Figure 5 as the circle “Operational constraint, e.g. State”.

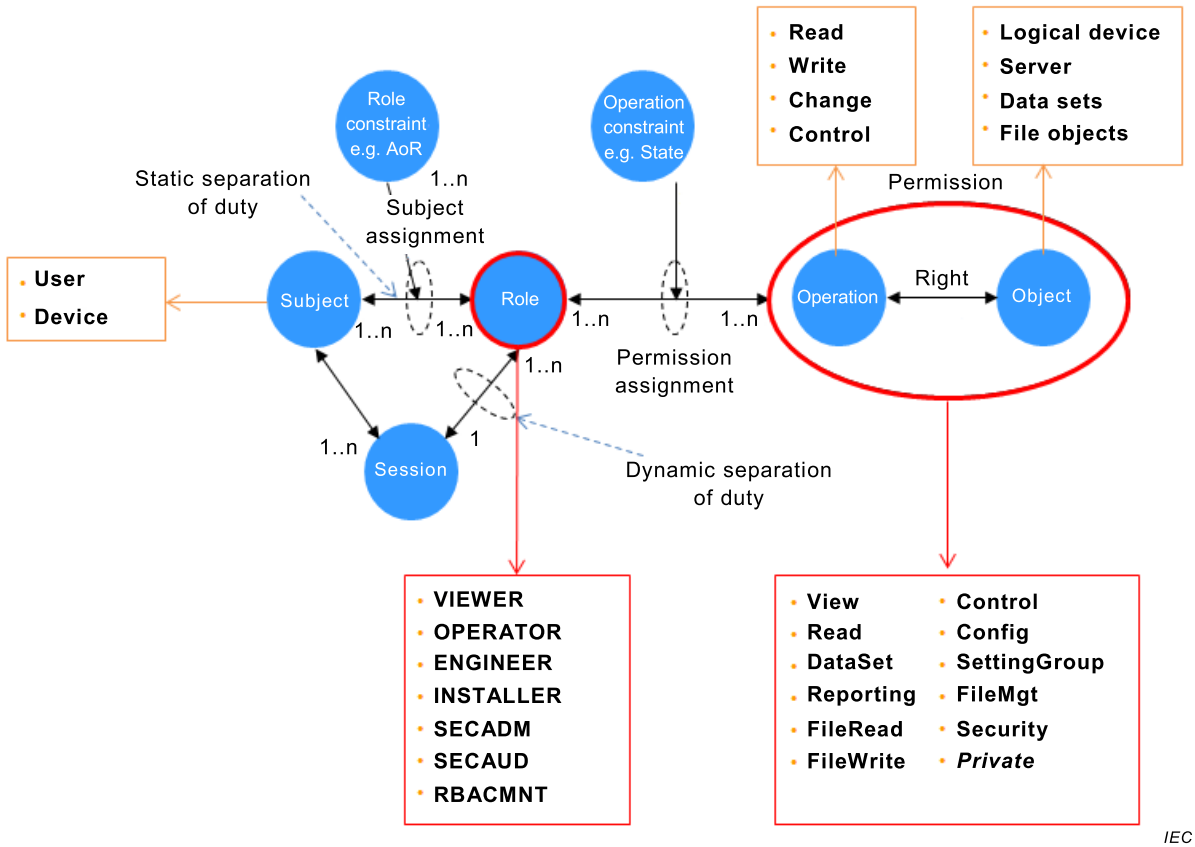

Figure 5 – Enhancement of the RBAC approach with operational constraints

'Not bound to the role' essentially means that this constraint is not visible in the access token associated to a user but is known to the device that is operating on the role information. This requires the distribution of potential restrictions of a role due to specific circumstances as described above in the emergency case.

7 Information exchange of defined custom roles and associated rights

7.1 General

Clause 7 contains the encoding and distribution of role definitions.

7.2 Encoding and exchange of custom Role Definitions

There are several possible ways to exchange RBAC and custom roles configuration, and one of them is the XACML standard. XACML stands for eXtensible Access Control Markup Language and defines both:

– a declarative access control policy language implemented in XML

– a processing model describing how to evaluate access requests according to the rules defined in policies.

In the XACML specification, the language core is separated from the application environment by the XACML context. The XACML context is defined in XML schema, describing a canonical representation for the inputs and outputs of the Policy Decision Point (PDP).

One of the reasons for using XACML is that it is capable of formalizing several Access control models, including the RBAC model defined in IEC TS 62351-8.

Figure 6 represents the decision processing environment in XACML.

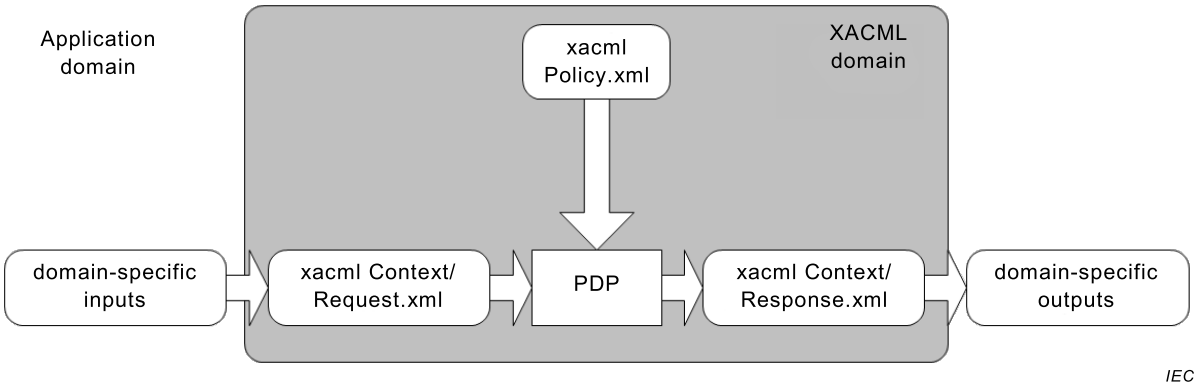

Figure 6 – XACML Overview

The decision is taken by an agent known as Policy Decision Point, from a context request and is based on a XACML policy. The result is given in the form of a context request.

Taken as a whole, XACML is a very heavy mechanism that fits well in SOA architectures, but not at all in the embedded software world. The interest here is not the full exchange of XACML requests / responses, but rather the formalisation of the IEC TS 62351-8 model as an XACML policy. Such formalisation of an RBAC model as a policy is even given as an example in the XACML standard.

Utilizing XACML is typically done during engineering for the configuration of the role to right assignment. This enables two different options for the utilization of XACML in terms of the involved components. Depending on the device capabilities, XACML may be directly processed within the IED as outlined in Figure 7. This moves the policy administration point directly into the IED. It also enables a direct interaction with potentially existing XACML components (not necessary for the outlined concept). This existing XACML data may comprise for instance pre-defined roles, like the roles defined in IEC TS 62351-8. As shown in Figure 7 the IED incorporates the Policy Decision Point and the Policy Enforcement Point. The configuration of the IED with the appropriate information enables the performance of

these tasks. This may be done by a security administrator (SECADM) defining roles (and their associated rights) based on the capabilities of the IEDs (e.g. by utilizing the SCL description of the IED).

During operations, when the IED is presented with one of the RBAC access tokens defined in IEC TS 62351-8, the Policy Enforcement Point can perform role based access control based on the presented token and the configured role information.

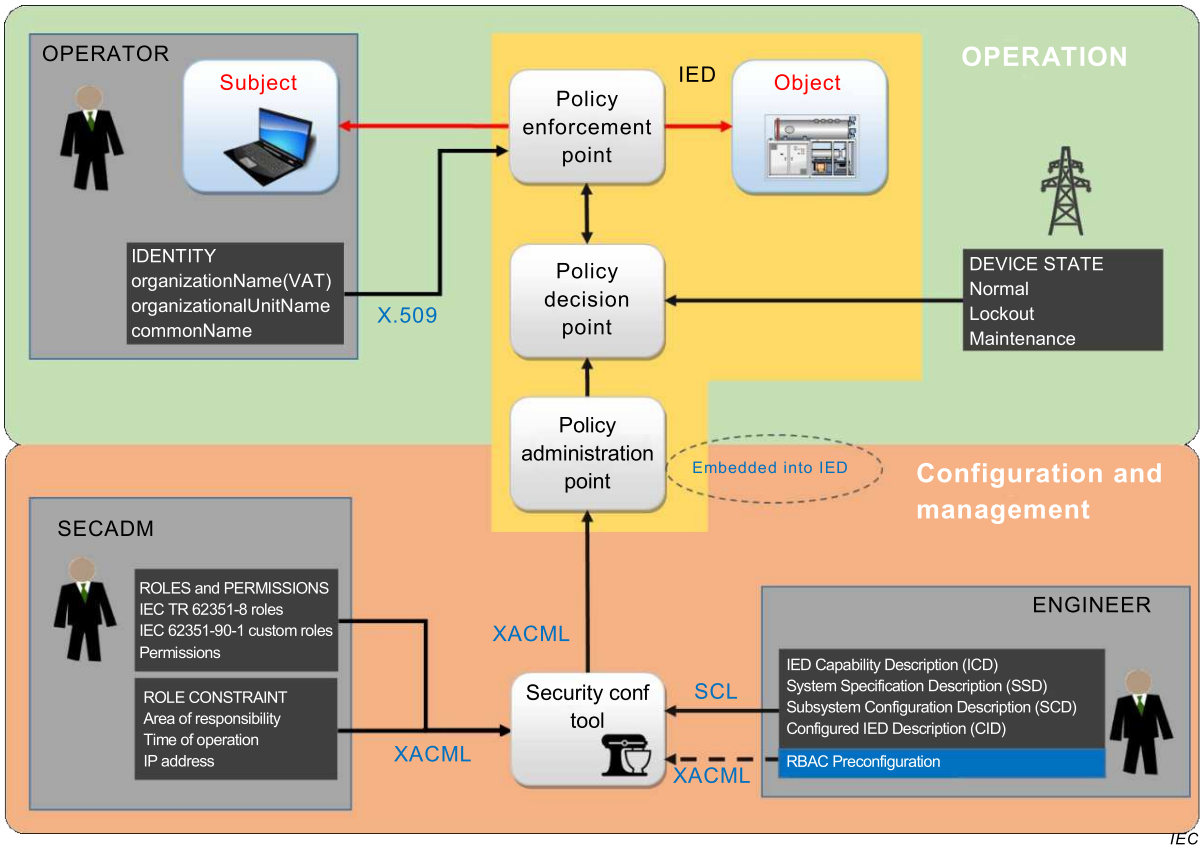

Figure 7 – Terminating XACML at the IED directly

Alternatively, as shown in Figure 8, XACML may be terminated in the IED configuration tool. This leaves the option to map the RBAC configuration data to already existing engineering interfaces to the IEDs. The operational part stays the same.

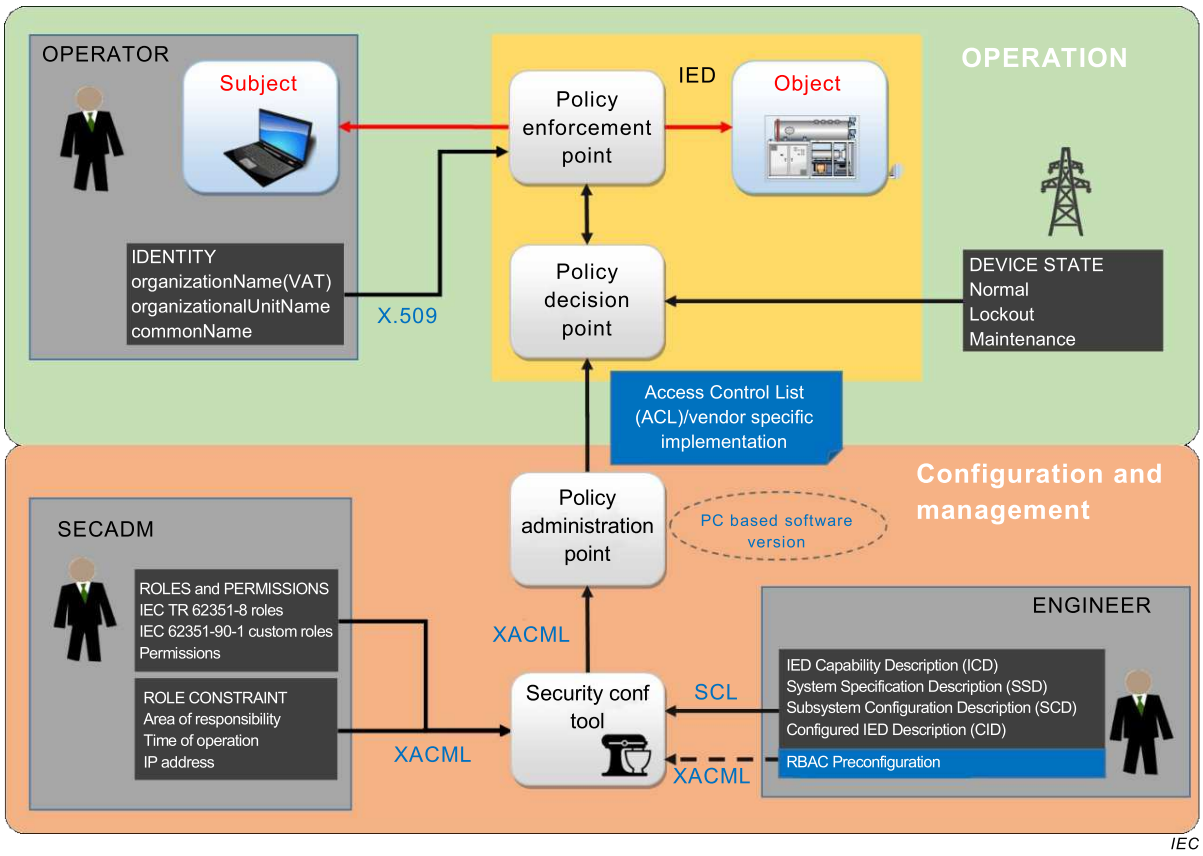

Figure 8 – Terminating XACML at the security engineering tool

Based on the features and functionalities provided by XACML, it may be used for modelling even very complex situations and systems from a single device and associated objects / actions couples to potentially a whole substation.

Note that for the configuration and definition of roles, separation of duty as described in IEC TS 62351-8 between the definition of roles and the association of roles to users' should be obeyed.

The Organization for the Advancement of Structured Information Standards – OASIS – specified the usage of XACML to also be applicable to describe RBAC. As described in the OASIS example application for RBAC [20][1], the XACML policy will be separated into two files as shown in Figure 9.

1 Numbers in square brackets refer to the bibliography.

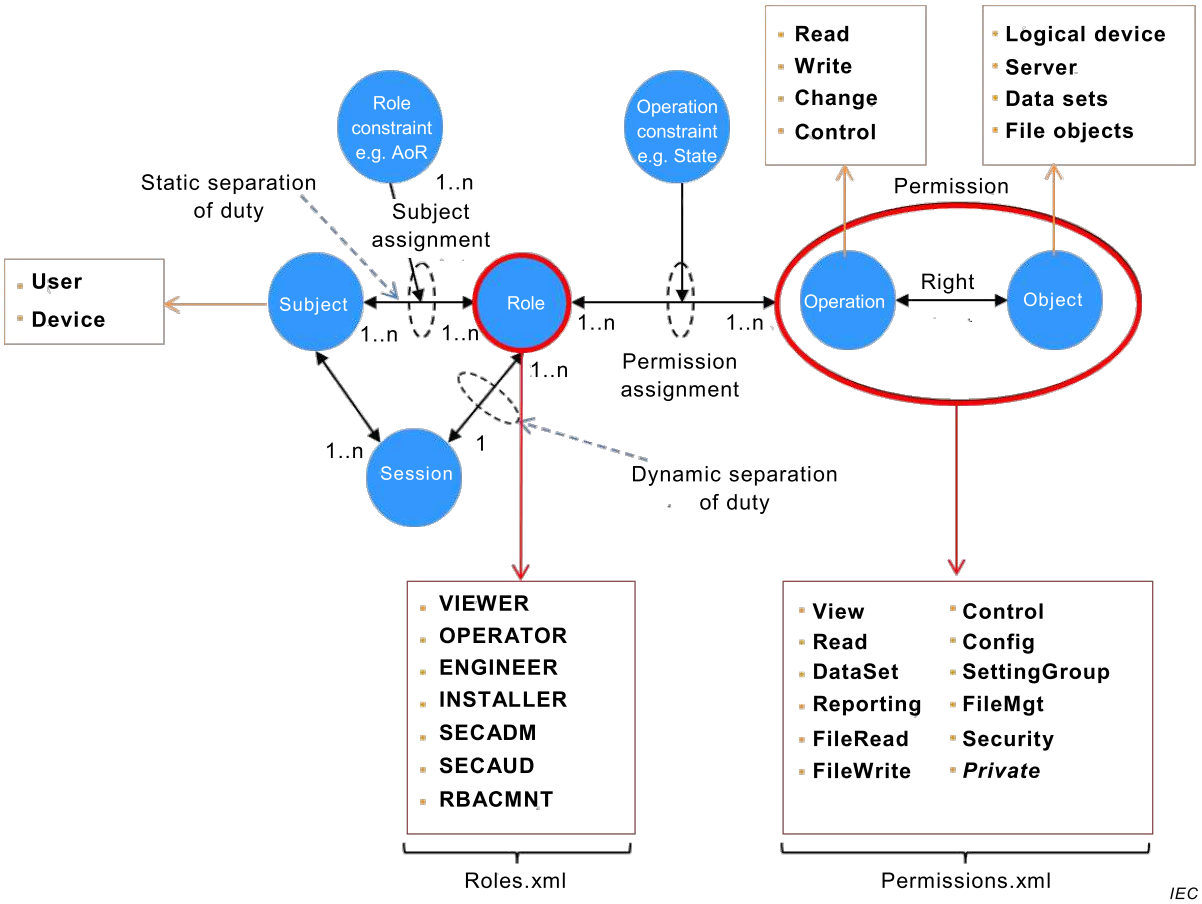

Figure 9 – XACML policy file mapping

The XACML policy files are:

– roles.xml lists all roles and their decomposition into permissions

– permissions.xml file lists all permissions and their decomposition into objects/actions

The role constraints and operation constraints (such as AoR, state of devices, etc.) are encoded in the roles.xml file. XACML offers a polymorphism capability to allow the decomposition of roles into permissions tight to the environment of the decision point.

Although the data in the XACML representation of the IEC 62351 security model needs to be refined, the XACML representation fits clearly the needs in terms of configuration.

It is very easy to create such a model as a basis to ensure interoperability between devices, and on top of existing roles, allow vendors or customers to create their own roles and own set of rights while keeping a complete interoperability.

Both files are utilized to show the mapping of IEC TS 62351-8 defined roles in 7.3.

7.3 Encoding and exchange of IEC TS 62351-8 defined roles

A complete encoding of the IEC TS 62351-8 security model is given along with this document. Some parts are extracted to explain the XACML philosophy.

In the following extract from roles.xml, the definition of a role is shown.

<CODE BEGINS>

```
<PolicySet PolicySetId="" PolicyCombiningAlgId="urn:oasis:names:tc:xacml:1.0:policy-combining-
algorithm:permit-overrides">
  <Target>
    <Subjects>
      <Subject>
        <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal">
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#anyURI">
            Role:VIEWER
          </AttributeValue>
          <SubjectAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role"
                                      DataType="http://www.w3.org/2001/XMLSchema#anyURI"/>
          </SubjectMatch>
      </Subject>
    </Subjects>
  </Target>
  <PolicySetIdReference>PPS:VIEWER</PolicySetIdReference>
</PolicySet>
```

<CODE ENDS>

A role is a `PolicySet` element, identified by its `SubjectMatch` element that defines both the identifier: “Role:VIEWER”, and its type “anyURI”. The important element is the `PolicySetIdReference` element at the end: It refers to another `PolicySet` that will contain the list of the permissions associated to the role.

To allow for a plain definition of the role, the permission `PolicySetIdReference` is neglected to be able to map this information to a later point in time. The plain definition of VIEWER allows already an association with a user, without taking the associated rights into account.

The following example represents the permission `PolicySet` associated to the role VIEWER.

<CODE BEGINS>

```
<PolicySet PolicySetId="PPS:VIEWER" PolicyCombiningAlgId="urn:oasis:names:tc:xacml:1.0:policy-
combining-algorithm:permit-overrides">
  <Target/>
  <PolicySetIdReference>Permission:VIEW</PolicySetIdReference>
</PolicySet>
```

<CODE ENDS>

In this very simple case, the role is associated with only a single permission: VIEW.

A further example, which is more complex: OPERATOR. As defined in IEC TS 62351-8, an operator is associated with four rights: VIEW, READ, REPORTING, and CONTROL.

Because VIEW and READ are common to most of the role, a “62351-8:minimal” permission `PolicySet` is defined to which all the roles refer (except VIEWER). This results in the following.

<CODE BEGINS>

```
<PolicySet PolicySetId="" PolicyCombiningAlgId="urn:oasis:names:tc:xacml:1.0:policy-combining-
algorithm:permit-overrides">
  <Target>
    <Subjects>
      <Subject>
        <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal">
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#anyURI">
             Role:OPERATOR
          </AttributeValue>
          <SubjectAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role"
                                      DataType="http://www.w3.org/2001/XMLSchema#anyURI"/>
        </SubjectMatch>
      </Subject>
    </Subjects>
  </Target>
  <PolicySetIdReference>PPS:62351-8:minimal</PolicySetIdReference>
  <PolicySetIdReference>PPS:OPERATOR</PolicySetIdReference>
</PolicySet>
```

<CODE ENDS>

Here the role refers to two `PolicySets`: “PPS:62351-8:minimal” and “PPS:OPERATOR”. These two `PolicySets` are represented below.

<CODE BEGINS>

```
<PolicySet PolicySetId="PPS:62351-8-minimal"
PolicyCombiningAlgId="urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:permit-
overrides">
  <Target/>
  <PolicySetIdReference>Permission:VIEW</PolicySetIdReference>
  <PolicySetIdReference>Permission:READ</PolicySetIdReference>
</PolicySet>

<PolicySet PolicySetId="PPS:OPERATOR"
PolicyCombiningAlgId="urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:permit-
overrides">
  <Target/>
  <PolicySetIdReference>Permission:REPORTING</PolicySetIdReference>
  <PolicySetIdReference>Permission:CONTROL</PolicySetIdReference>
</PolicySet>
```

<CODE ENDS>

The result will be the role OPERATOR associated with its 4 rights. This mechanism avoids the repetition of identical permissions association in the file.

The permission.xml file contains the breakdown of permissions into object and actions. One or several objects can be associated with one or several actions.

A permission is also a `PolicySet` identified by its `PolicySetId`. The following example is the FILEMNGT permission, in which the object “File” is associated with the actions “Create”, “Delete”, “Read”, and “Write”.

<CODE BEGINS>

```
<PolicySet PolicySetId="Permission:FILEMNGT"
PolicyCombiningAlgId="urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:permit-
overrides">
  <Target/>
    <Policy PolicyId="" RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-
algorithm:permit-overrides">
      <Target/>
      <Rule RuleId="" Effect="Permit">
        <Target>
         <Resources>
           <Resource>
              <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                  File
                </AttributeValue>
                <ResourceAttributeDesignator
                  AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
                  DataType=http://www.w3.org/2001/XMLSchema#string
                <ResourceAttributeDesignator/>
              </ResourceMatch>
            </Resource>
          </Resources>
         <Actions>
           <Action>
             <ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
               <AttributeValue
                 DataType="http://www.w3.org/2001/XMLSchema#string">
                 Create
               </AttributeValue>
               <ActionAttributeDesignator
                 AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
                 DataType="http://www.w3.org/2001/XMLSchema#string" />
             </ActionMatch>
           </Action>
           <Action>
             <ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
               <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                 Delete
               </AttributeValue>
               <ActionAttributeDesignator
                 AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
                 DataType="http://www.w3.org/2001/XMLSchema#string" />
             </ActionMatch>
           </Action>
           <Action>
             <ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
               <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                 Read
               </AttributeValue>
               <ActionAttributeDesignator
                 AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
                 DataType="http://www.w3.org/2001/XMLSchema#string" />
             </ActionMatch>
           </Action>
           <Action>
             <ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
               <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                 Write
               </AttributeValue>
               <ActionAttributeDesignator
                 AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
                 DataType="http://www.w3.org/2001/XMLSchema#string" />
             </ActionMatch>
           </Action>
         </Actions>
        </Target>
    </Rule>
  </Policy>
</PolicySet>
```

<CODE ENDS>

7.4 User defined roles

7.4.1 Usage

IEC TS 62351-8 defines a set of seven predefined roles. However, users should have the capabilities to create their own roles, because:

- Some security policies can be already in place, and do not comply to IEC TS 62351-8 pre-defined roles
- Predefined roles cannot be expected to cover all cases and needs.

It is therefore necessary to be able to add easily new roles to the system in order to adapt the security model to the needs.

Using XACML files and their respect of the RBAC theoretical model (roles → rights → actions/objects) simplifies this operation. A new role can be created from a list of existing rights that can be picked in the existing security model of an IED.

For custom roles, the IEC TS 62351-8 “RoleID” needs to be defined in the role definition, as it is the primary key used in authentication profiles. IEC TS 62351-8 describes the number ranges for the definition of custom based roles. In addition, the “roleDefinition” as part of the RBAC credential allows for description of the path to the role to right definition.

7.4.2 Example

In this example, in addition to default roles a new operator role is created that will have the rights to perform configuration operations, and have file access. This role is called “super operator".

Table 6 shows the list of rights of the roles “OPERATOR” and SUPER_OPERATOR:

Table 6 – User defined role definition

Right / Role	VIEW	READ	DATASET	REPORTING	FILEREAD	FILEWRITE	FILEMNGT	CONTROL	CONFIG	SETTINGGROUP	SECURITY
OPERATOR	X	X		X				X			
SUPER_OPERATOR	X	X		X	X			X	X		

First of all, this new role and its link to the permission list must be defined. Since it is equivalent to the OPERATOR role, its definitions can simply be reused, and add a `PolicySet` for its particularities.

<CODE BEGINS>

```
<PolicySet PolicySetId="" PolicyCombiningAlgId="urn:oasis:names:tc:xacml:1.0:policy-combining-
algorithm:permit-overrides">
  <Target>
    <Subjects>
      <Subject>
        <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal">
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#anyURI">
               Role:SUPER_OPERATOR
          </AttributeValue>
          <SubjectAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role"
                                      DataType="http://www.w3.org/2001/XMLSchema#anyURI"/>
        </SubjectMatch>
      </Subject>
    </Subjects>
  </Target>
  <PolicySetIdReference>PPS:62351-8:minimal</PolicySetIdReference>
  <PolicySetIdReference>PPS:OPERATOR</PolicySetIdReference>
  <PolicySetIdReference>PPS:SUPER_OPERATOR</PolicySetIdReference>
</PolicySet>
```

<CODE ENDS>

Based on this, the new `PolicySet` specific to the SUPER_OPERATOR, with the additional rights has to be defined:

<CODE BEGINS>

```
<PolicySet PolicySetId="PPS:SUPER_OPERATOR"
 PolicyCombiningAlgId="urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:permit-
 overrides">
  <Target/>
    <PolicySetIdReference>Permission:FILEREAD</PolicySetIdReference>
    <PolicySetIdReference>Permission:CONFIG</PolicySetIdReference>
  </PolicySet>
```

<CODE ENDS>

This leads to a new role resulting of a combination of the OPRATOR role, with 2 new rights, while keeping a complete interoperability with IEC TS 62351-8 defined roles.

7.5 Role polymorphism

7.5.1 Encoding in XACML

The RBAC concept defines that one (or several) roles are associated to a user. At the same time, this association can have limits (Area of responsibility, time), and the content itself of a role can change depending on the operational state of a device.

These constraints can be expressed in the roles.xml file using conditions that can be defined in XACML.

As seen in Subclause 7.4, the definition of a role was defined in a `PolicySet` element. A `PolicySet` element can refer eventually to several sub `PolicySet` elements through a `PolicySetIdReference`. At the end, the XACML decision point will treat all these references as a single `PolicySet`.

One feature of a `PolicySet` is its capability to be conditional, depending on a `Target` element. As defined by the XACML standard, a Policy Decision Point will check the match between the target and the environment (in our case) and apply or not the `PolicySet`.

Using this mechanism, it is enabled to “re route” the evaluation of the rights attached to a role, or to apply or not a complete `PolicySet`.

7.5.2 Examples

Two kinds of conditions and their implementation as examples will be developed:

- Area of responsibility (AoR).
- System access / roles capabilities depending on device state.

Area of responsibility

Definition from IEC TS 62351-8:2011:

The area of responsibility (AoR) restricts the applicability of a subject's role to a set of objects. [...]The AoR is an identifier and should define a hierarchical name space or a reference to the namespace. Note that these identifiers are typically alphanumeric. The relying party / IED shall validate the complete AoR and shall ignore any UserRoleInfo definition which includes an unrecognized AoR.

Therefore an AoR (which is part of the credential of an agent) restricts the access of this agent to the objects (devices, applications, i.e. decision points) that belong to this AoR.

It is a global restriction that applies to the whole RBAC of a decision point, therefore a top level decision. Figure 10 represents the organisation of a device security model, and the point of decision.

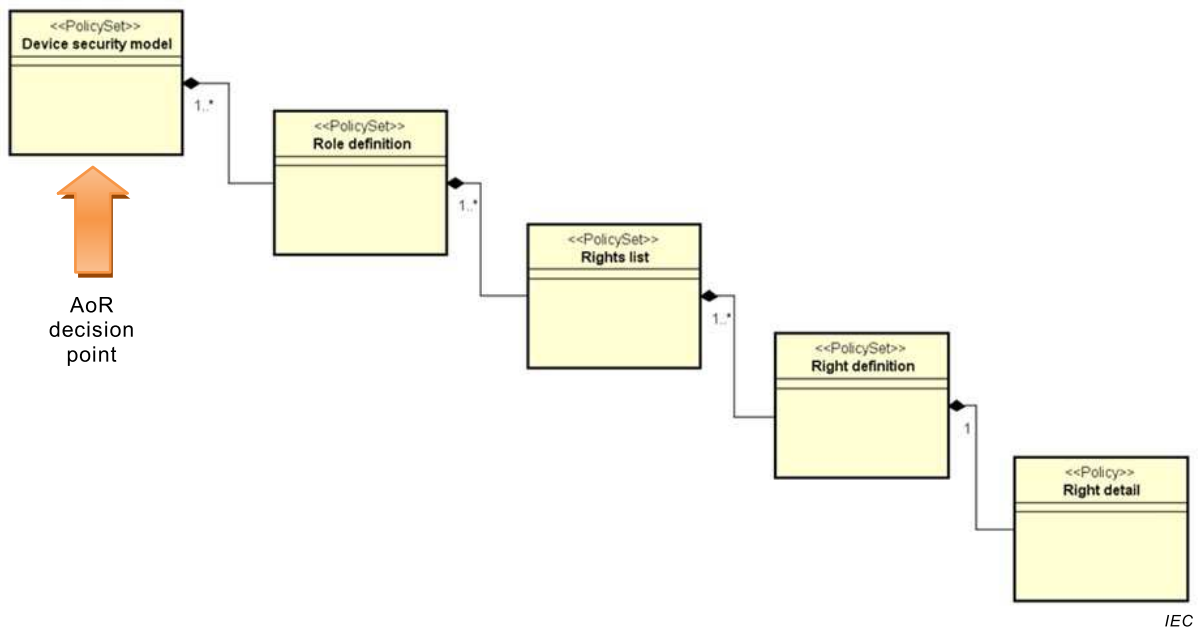

Figure 10 – AoR decision point

Since the top level of a roles.xml file is a `PolicySet`, a global decision at this level can be applied that will invalidate all the roles assignment for an agent that does not belong to the proper AoR.

In XACML, each subject can be associated with one or several attribute. One of these attribute fits with the AoR concept: The subject id qualifier. Here is its definition:

urn:oasis:names:tc:xacml:1.0:subject:subject-id-qualifier

This identifier indicates the security domain of the subject. It identifies the administrator and policy that manages the namespace in which the subject id is administered.

This attribute will be used to make a top level decision in order to restrict the access to a device for a specified AoR.

<CODE BEGINS>

```
<PolicySet xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" Version="1"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" PolicySetId="RPS:Roles-list"
PolicyCombiningAlgId="urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:permit-
overrides" xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os">
  <Target>
    <Subjects>
      <Subject>
        <SubjectMatch MatchId="function;string-equal">
          <AttributeValue DataType="xml;string">France-SouthWest</AttributeValue>
          <SubjectAttributeDesignator
            AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id-qualifier"
            DataType="xml;string"/>
        </SubjectMatch>
      </Subject>
    </Subjects>
  </Target>
  <PolicySet PolicySetId="" PolicyCombiningAlgId="urn:oasis:names:tc:xacml:1.0:policy-
combining-algorithm:permit-overrides">
    <Target>
      <Subjects>
        <Subject>
          <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#anyURI">
              Role:OPERATOR
            </AttributeValue>
            <SubjectAttributeDesignator
              AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role"
              DataType="http://www.w3.org/2001/XMLSchema#anyURI"/>
          </SubjectMatch>
        </Subject>
      </Subjects>
    </Target>
  <PolicySetIdReference>PPS:62351-8:minimal</PolicySetIdReference>
  <PolicySetIdReference>PPS:OPERATOR</PolicySetIdReference>
</PolicySet>
```

<CODE ENDS>

The red part is the “classical” beginning of an XACML roles.xml file. The yellow part restricts that application of all the roles only to users having belonging to the “France-SouthWest” AoR.

Roles depending on device state:

The goal of this example is to show how the permissions associated to a role for a device can be modified by the device status. Let us take as an example a device that can have three operational states:

- Normal
- Lockout
- Maintenance

For each of these states, the capabilities associated with the roles can change: i.e. some permission can be added or removed.

Here also the capability of a `PolicySet` to be conditional will be used. The security model organization, Figure 11 shows the point where the decision will be made:

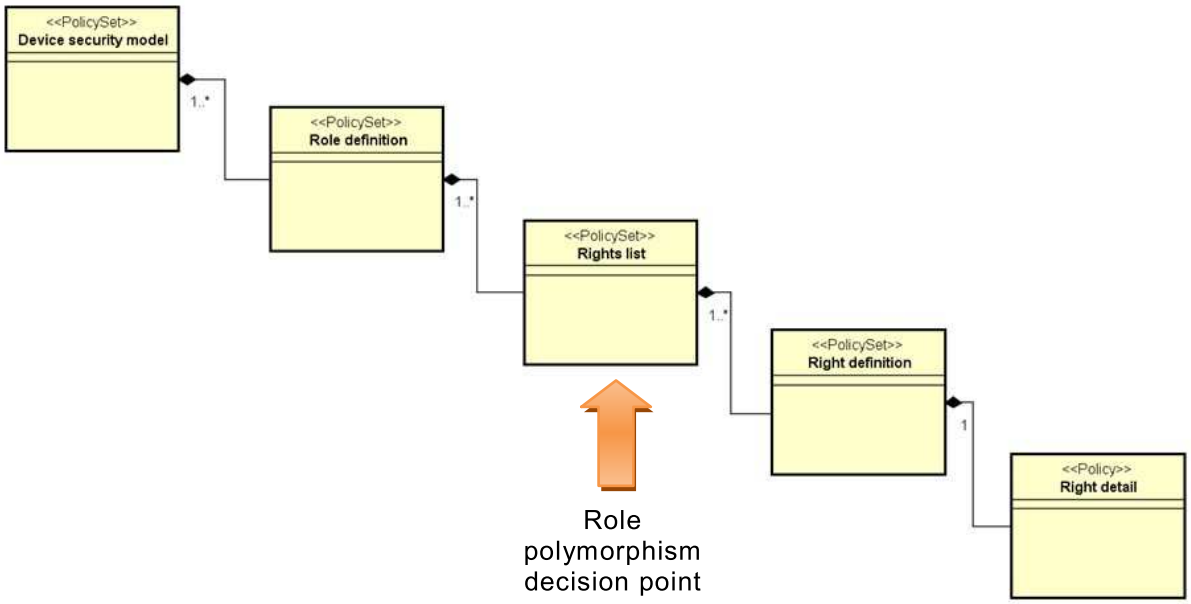

Figure 11 – Role polymorphism decision point

Basically, for each role, several right lists will be defined, each of them conditioned to the status of the device.

In order to encode this status, another concept of XACML will be used: A decision can be made on a `Subject`, as seen for the AoR, but can be conditioned by two other kinds of constraints:

- `Resource`
- `Environment`

The Environment constraint is of course the obvious one. Up to now, only date and time are defined by IEC TS 62351-8:2011. Therefore own attribute will be defined. The following XML file shows how to encode three different modes for the role “ENGINEER”.

<CODE BEGINS>

```
<PolicySet xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" Version="1"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" PolicySetId="RPS:Roles-list"
PolicyCombiningAlgId="urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:permit-
overrides" xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os">
  <Target/>
    <PolicySet PolicySetId="" PolicyCombiningAlgId="urn:oasis:names:tc:xacml:1.0:policy-
combining-algorithm:permit-overrides">
      <Target>
        <Subjects>
          <Subject>
            <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal">
              <AttributeValue
                DataType="http://www.w3.org/2001/XMLSchema#anyURI">
                Role:ENGINEER
              </AttributeValue>
              <SubjectAttributeDesignator
                AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role"
                DataType="http://www.w3.org/2001/XMLSchema#anyURI"/>
            </SubjectMatch>
          </Subject>
        </Subjects>
      </Target>
    <PolicySetIdReference>PPS:62351-8:minimal</PolicySetIdReference>
    <PolicySetIdReference>PPS:ENGINEER_state:Normal</PolicySetIdReference>
    <PolicySetIdReference>PPS:ENGINEER_state:Lockout</PolicySetIdReference>
    <PolicySetIdReference>PPS:ENGINEER_state:Maintenance</PolicySetIdReference>
  </PolicySet>
  < PolicySetId="PPS:62351-8-minimal"
    PolicyCombiningAlgId="urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:permit-
overrides">…</PolicySet>
  <PolicySet PolicySetId="PPS:ENGINEER_state:Normal"
    PolicyCombiningAlgId="urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:permit-
overrides">
    <Target>
      <Environments>
        <Environment>
          <EnvironmentMatch MatchId="function;string-equal">
            <AttributeValue DataType="xml;string">Normal</AttributeValue>
            <EnvironmentAttributeDesignator
              AttributeId="urn:IEC:names:tc:62351:1.0:environment:device-status"
              DataType="xml;string"/>
          </EnvironmentMatch>
        </Environment>
      </Environments>
    </Target>
    <PolicySetIdReference>Permission:DATASET</PolicySetIdReference>
    <PolicySetIdReference>Permission:REPORTING</PolicySetIdReference>
    <PolicySetIdReference>Permission:FILEWRITE</PolicySetIdReference>
    <PolicySetIdReference>Permission:FILEMNGT</PolicySetIdReference>
    <PolicySetIdReference>Permission:CONFIG</PolicySetIdReference>
  </PolicySet>
  <PolicySet PolicySetId="PPS:ENGINEER_state:Lockout"
    PolicyCombiningAlgId="urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:permit-
overrides">
    <Target>
      <Environments>
        <Environment>
          <EnvironmentMatch MatchId="function;string-equal">
            <AttributeValue DataType="xml;string">Lockout</AttributeValue>
            <EnvironmentAttributeDesignator
              AttributeId="urn:IEC:names:tc:62351:1.0:environment:device-status"
              DataType="xml;string"/>
          </EnvironmentMatch>
        </Environment>
      </Environments>
    </Target>
    <PolicySetIdReference>Permission:DATASET</PolicySetIdReference>
    <PolicySetIdReference>Permission:REPORTING</PolicySetIdReference>
  </PolicySet>
  <PolicySet PolicySetId="PPS:ENGINEER_state:Maintenance"
    PolicyCombiningAlgId="urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:permit-
overrides">
    <Target>
      <Environments>
        <Environment>
          <EnvironmentMatch MatchId="function;string-equal">
```

```
            <AttributeValue DataType="xml;string"> Maintenance </AttributeValue>
            <EnvironmentAttributeDesignator
              AttributeId="urn:IEC:names:tc:62351:1.0:environment:device-status"
              DataType="xml;string"/>
          </EnvironmentMatch>
        </Environment>
      </Environments>
    </Target>
    <PolicySetIdReference>Permission:DATASET</PolicySetIdReference>
    <PolicySetIdReference>Permission:REPORTING</PolicySetIdReference>
    <PolicySetIdReference>Permission:FILEWRITE</PolicySetIdReference>
    <PolicySetIdReference>Permission:FILEMNGT</PolicySetIdReference>
  </PolicySet>
</PolicySet>

<CODE ENDS>
```

The decision points are colored in red, the associated permissions in yellow. It is visible that to the role “ENGINEER”, has four rights lists associated:

- IEC TS 62351-8:minimal
- ENGINEER_state:Normal
- ENGINEER_state:Lockout
- ENGINEER_state:Maintenance

The last three rights lists are actually conditioned to the environment status of the device, and define a different list of rights. Only one of these conditional rights lists can apply, therefore modifying the definition of the ENGINEER role.

7.6 Roles to rights mapping data

Roles to rights mapping is achieved by specifying, which actions or which subcategories or categories of actions is a role allowed to perform.

By default a new role has no permissions at all. It is the task of the organizations to define their needed roles and the corresponding permissions.

Different vendors will provide tools for the easy management of RBAC including the management of new custom roles and their permissions following the concepts described in this document, for example following the categorization as described in Clause 5.

When all organizational roles have been defined, an xml file is generated, e.g.,*”IEC_62351_90_1_roles.xml”*, which should be distributed to all IEC TR 62351-90-1 compliant devices.

The standard xsd file “*access_control-xacml-2 0-policy-schema-os.xsd*” serves to validate the *IEC_62351_90_1_roles.xml* generated files for compliance with this part, besides enforcing a few rules such as no role names duplication, no role-id duplication, and others.

Note also that OASIS already defined a profile for RBAC in [20].

Bibliography

[1] IEC 62351-9, *Power systems management and associated information exchange – Data and communications security – Part 9: Cyber security key management for power system equipment*

[2] IEC/ISO 9798-2, *Information technology – Security techniques – Entity authentication – Part 2: Mechanisms using symmetric encipherment algorithms*

[3] ANSI X.9.69-2006, *Framework for Key Management Extensions*

[4] ANSI X.9.73-2002, *Cryptographic Message Syntax*

[5] IEEE 1518:2010, *Distributed Network Protocol (DNP3)*

[6] IEEE P1689, *Trial Use Standard for Retrofit Cyber Security of Serial SCADA Links and IED Remote Access*

[7] NIST: SP 800-82, *Guide to Industrial Control Systems (ICS) Security*

[8] XACML, *Extensible Access Control Markup Language (XACML)* v2.0, February, 2005

[9] PKCS#12, *Personal Information Exchange Syntax Standard*

[10] RFC5246, *The Transport Layer Security (TLS) Protocol* Version 1.2

[11] RFC5280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*

[12] RFC5878, *Transport Layer Security (TLS) Authorization Extensions*

[13] NERC CIP-001 – CIP-009, *North American Electric Reliability Corporation: Critical Infrastructure Protection*, NERC CIP-001 – CIP-009

[14] ANSI INCITS 359-2004, *Role Based Access Control*

[15] BDEW White Book Requirements for Secure Control and Telecommunication Systems, https://www.bdew.de/internet.nsf/id/232E01B4E0C52139C1257A5D00429968/$file/2008-06-10_Whitepaper_Sichere%20Steuerungs-_Telekommunikationssysteme.pdf

[16] ISO 27019, *Information technology – Security techniques – Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry*

[17] IEEE 1686, *IEEE Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities*

[18] IEC 62443 (all parts), *Industrial communication networks – Network and system security*

[19] BSI TR 03109, *Technical guidelines for intelligent metering systems and their secure operation*

[20] XACML v3.0, *Core and Hierarchical Role Based Access Control (RBAC) Profile* Version 1.0, https://docs.oasis-open.org/xacml/3.0/xacml-3.0-rbac-v1-spec-en.html

[21] IEC 61850-7-3, *Communication networks and systems for power utility automation – Part 7-3: Basic communication structure – Common data classes*

[22] IEC 60870-5-104, *Telecontrol equipment and systems – Part 5-104: Transmission protocols – Network access for IEC 60870-5-101 using standard transport profiles*

[23] IEC TS 60870-5-7, *Telecontrol equipment and systems – Part 5-7: Security extensions to IEC 60870-5-101 and IEC 60870-5-104 protocols (IEC 62351-5 secure authentication)*

_____

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

3, rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland

Tel: + 41 22 919 02 11
Fax: + 41 22 919 03 00
info@iec.ch
www.iec.ch