Role-based Access Control in Power Systems

Introduction

Role-based Access Control (RBAC) is a proven concept in IT-Systems, which is used by many (operating) systems to control access to system resources. It is an improvement to the popular but insecure single-administrator/guest model. Instead of granting users specific access rights, RBAC goes into a different direction by supporting the principle of least privilege. This enables the association of a subject (a user) with a role, which has only those rights necessary to perform a certain task. Thus, RBAC enables an organization to define dedicated rights and package them into specific roles for assignment.

RBAC for the energy automation environment is already considered in several requirements standards, guidelines, and also in regulatory requirements to ensure a reliable operation of power systems. Besides the requirements supporting this functionality, technical standards ensuring interoperability have been developed.

Basic Concept

RBAC reduces complexity and cost of security administration in networks with a large numbers of subjects. These subjects may be users, applications, or devices. The basic idea is to assign subjects to roles in order to separate them from assignment of individual rights. The following figure shows the general concept of RBAC.

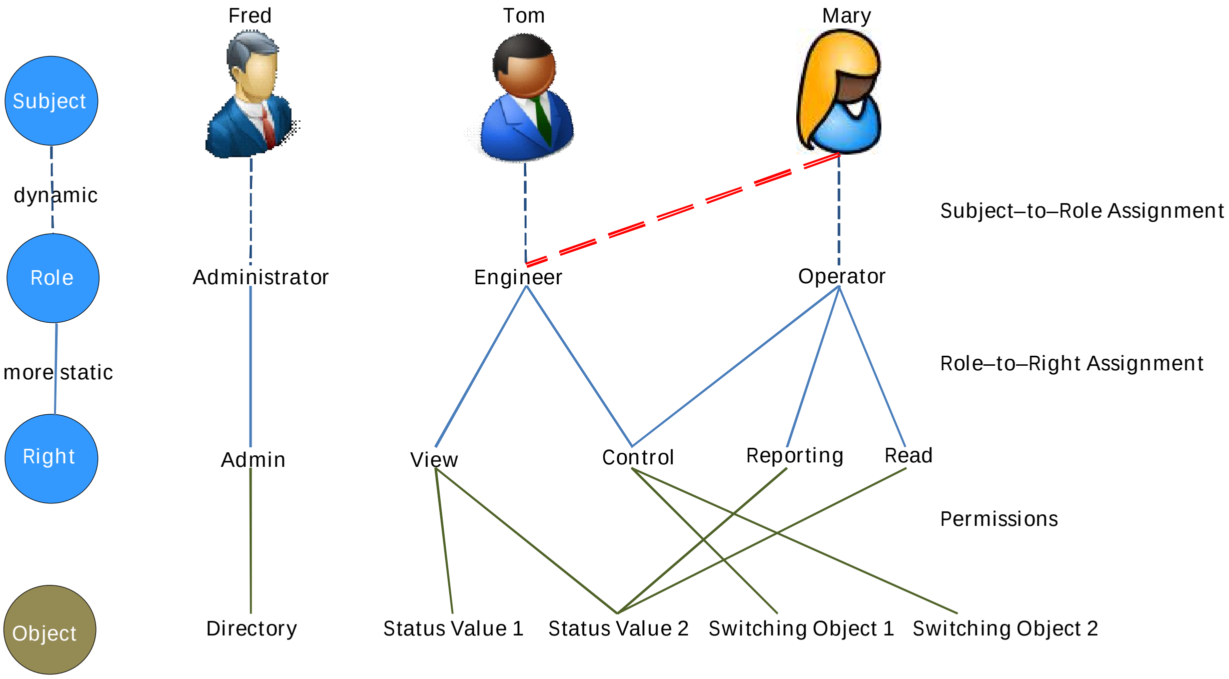


Figure 1: Association (1) of subjects to roles (and associated rights)

Figure 1 illustrates the basic concept of subject-role-right association. In this illustration “Tom” is assigned the role “Engineer”. Acting in this role “Tom” is entitled to “view” and “control” objects. Objects may include status values or switching objects.

This concept allows the separation of subject administration and role-to-right assignment. This enables a flexible and centralized management of subject-to-role assignment that tends to be dynamic. At the same time it allows the combination with well-defined role-to-right-assignment that has usually a more static character.

Figure 1 also shows the dynamic and static assignments between subjects, roles and rights. The example illustrates that granting the right ”view” to “Mary” can be added by assigning the role “Engineer” to “Mary” without changing the associated rights on objects.

Security administration is simplified through the use of roles and constraints to organize subject access levels. Constraints in this context may connected directly with a given role like a validity time or a specific location in which the role can be used. Other constraints may be given through the operational environment and may change the effectively of a role, e.g., in emergency cases. RBAC in general can reduce costs within an organization, as it accepts that (especially) employees change roles and responsibilities more frequently than the rights within roles and responsibilities have to be changed.

RBAC applied in Energy Automation

In order to protect the power grid from the increasing onset of cyber attacks, it is necessary to establish preventive, detective and corrective controls, in order to achieve accountability and traceability of all actions involved in operating the grid: manual or automated, local or remote. This is where RBAC, security event logging, and user management come into play.

For access control, security logging and user management in the energy industry to be effective, the specific constraints of the sector need to be addressed.

- Many substations to operate
- One user, multiple roles
- One substation, multiple secondary technology vendors
- External contractors and vendor specialists requiring access to substation equipment

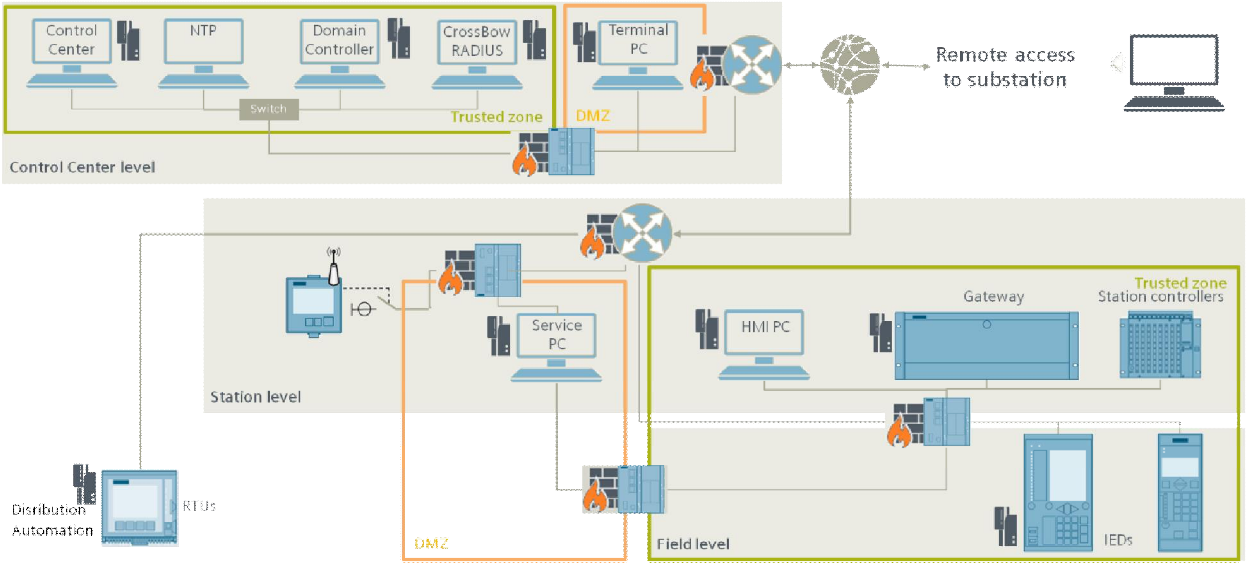


Figure 2: Exemplary Implementation of RBAC in the power industry

Although RBAC plays a role in all lifecycle phases of a digital substation – from commissioning to its total renovation – access control during the daily operations is the most crucial phase to focus on. This section lists some of the common user interaction scenarios that pertain to digital substation operations. It must be noted that it is imperative to log all user actions that are relevant from a system security point of view, across all access control scenarios. Some of the common scenarios are discussed here.

HMI access:
During normal operations in a substation an operator monitors and controls the process automation using the PC-based human machine interface (HMI) software, which allows the viewing and modifying of the states of both primary substation equipment (e.g. circuit breaker, disconnector, etc) and secondary substation equipment (e.g. bay controller, protection device, etc) that control them. Unauthorized and anonymous access to HMIs must therefore be prevented. These considerations also apply to PC-based runtime applications that handle communication gateway and station controlling and automation tasks.

IED access:
Viewing and modification of settings belonging to IEDs (e.g. protection relays) in the substation is achieved normally using the engineering tool connected with the IED (typically over IP or also over serial connections in case of legacy IEDs). This is also achieved over the IED's on-board HMI panel. A similar user-interactive scenario is that of managing automation- and communication-intensive intensive secondary devices such as RTUs and related networking equipment in the substation.

Access for data retrieval:
Collecting data for offline diagnostics and grid optimization is another scenario: operational logs and sequence of events, as well as retrieval of non-operational logs and fault-/disturbance records. Today's power quality devices capture sensitive information about the grid's topology and the nature of settings that led to a fault (e.g. transformer settings, monitored feeders, lines, etc stored in the internationally accepted COMTRADE format for disturbance records.) In this scenario the active user can mostly carry out his tasks with "read-only" access to the IEDs and data archival systems. A more liberal, potentially harmful set of access rights should be avoided.

Access for carrying out updates and backups:
National regulations expect power system operators to actively implement security patch management of all deployed grid automation products. The access rights required for firmware and software updates to be carried out by an operator in the field can be misused by anonymous malicious parties to install corrupt/obsolete/manipulated firmware and software into secondary equipment.

Access for managing backups:
The parallel-running recurring activity of creating regular backups of secondary equipment settings needs to be covered by access control as well. In this scenario the active user is able to mostly carry out his tasks with "read-only" access to the system.

Temporary access:
Special consideration is required for providing temporary access to secondary equipment in the substation for external technicians such as contractors and vendor specialists. It should be possible to restrict the validity of such user accounts and to keep these accounts inactive or non-existent until the need arises.

Flexibility with roles:
Apart from the aforementioned exemplary scenarios, there are of course other user-interactive scenarios, where an establishment of a customized set of roles and rights would best fit the organizational structures of power system operators, especially if they have a large operations staff. The need for flexibility in supporting user-defined roles that can be consistently applied across multiple secondary equipment vendors is foreseeable.

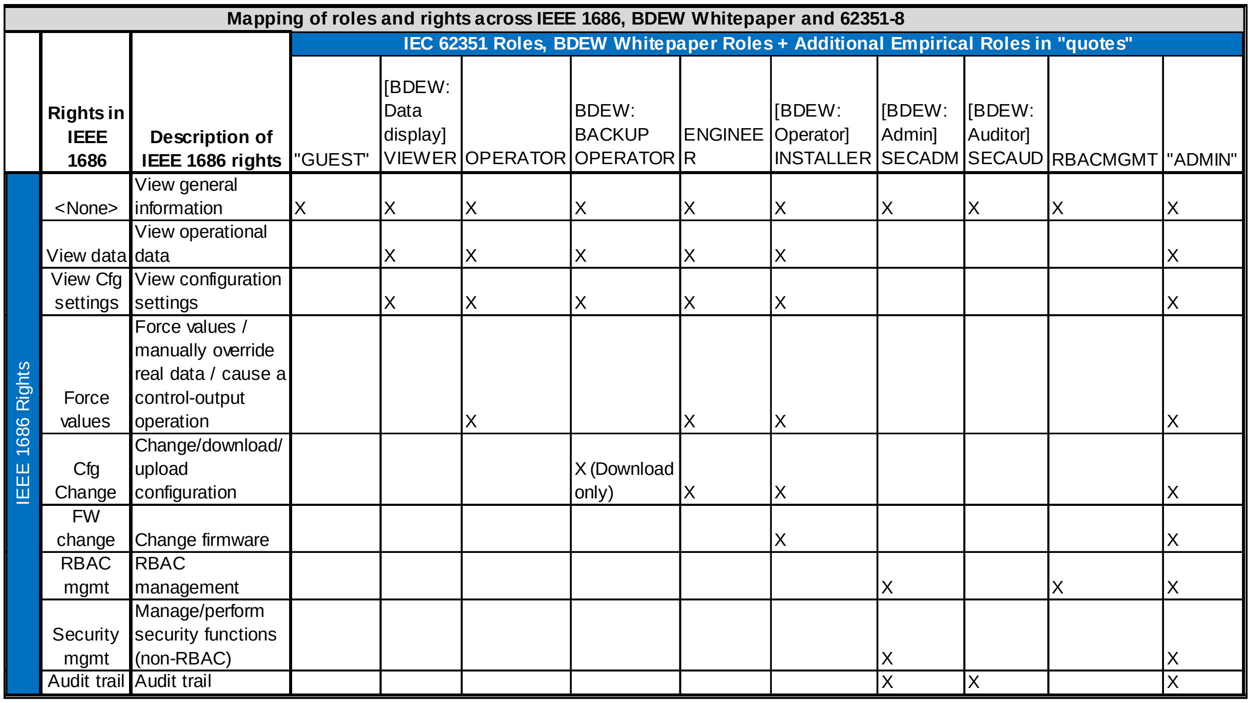
Administering security:
As covered in the BDEW Whitepaper requirements and in the IEC 62351-8 standard, applying access control and user management requires continuous administration of the supporting infrastructure and policies. To this end, the access control system should support roles for administering the security settings in secondary equipment, centrally administering users (i.e. adding and removing user accounts), and managing user roles and rights required to carry out the aforementioned operational user-interactive scenarios. An additional scenario is the retrieval of security logs from secondary equipment and from centralized security log servers for purposes of audit trail. While inspecting suspicious activity, external or dedicated security auditors might be engaged, who solely have the privilege to access security logs from their sources and archives for analysis purposes.

Availability comes first – emergency access:
Finally, with user management and RBAC in place, it must still be possible in emergency cases for operators to access critical secondary substation components, even if, for some reason the operator is unable to access the secondary equipment with his/hear user credentials. It is unacceptable to have a secure substation at the cost of system availability.

An Approach towards RBAC with Basic Interoperability

Over the past decade, there have been concerted efforts in the power grid markets internationally to raise awareness about IT/OT security, driven by standards such as IEC 62351 and IEEE 1686, and regional organizations of energy operators such as NERC in North America and BDEW in Germany.
Currently, however, the RBAC guidance provides no alignment among the set of roles, which are required by the different standards and recommendations referenced here. For instance, due to the fact that the IEC 62351-8 standard currently specifies minimum roles aligned with operations covered by the IEC 61850 standard alone, some or all of its rights cannot be translated to operational activities that are not in the purview of IEC 61850 (e.g. consideration of firmware update). As seen in Figure 3, a mapping of the roles as specified in IEC 62351-8 and BDEW Whitepaper to the different IEEE 1686 rights would address this gap, so as to:

- holistically address basic interoperability for RBAC and not just from the viewpoint of a singular standard
- address all markets driven by the aforementioned associations and standardization committees



Mapping of roles and rights across IEEE 1686, BDEW Whitepaper and 62351-8												
			IEC 62351 Roles, BDEW Whitepaper Roles + Additional Empirical Roles in "quotes"									
	Rights in IEEE 1686	**Description of IEEE 1686 rights**	"GUEST"	[BDEW: Data display] VIEWER	OPERATOR	BDEW: BACKUP OPERATOR	ENGINEER	[BDEW: Operator] INSTALLER	[BDEW: Admin] SECADM	[BDEW: Auditor] SECAUD	RBACMGMT	"ADMIN"
IEEE 1686 Rights	<None>	View general information	X	X	X	X	X	X	X	X	X	X
	View data	View operational data		X	X	X	X	X				X
	View Cfg settings	View configuration settings		X	X	X	X	X				X
	Force values	Force values / manually override real data / cause a control-output operation			X		X	X				X
	Cfg Change	Change/download/upload configuration				X (Download only)	X	X				X
	FW change	Change firmware						X				X
	RBAC mgmt	RBAC management							X		X	X
	Security mgmt	Manage/perform security functions (non-RBAC)							X			X
	Audit trail	Audit trail							X	X		X

Figure 3: Mapping of roles and rights across international standards and recommendations

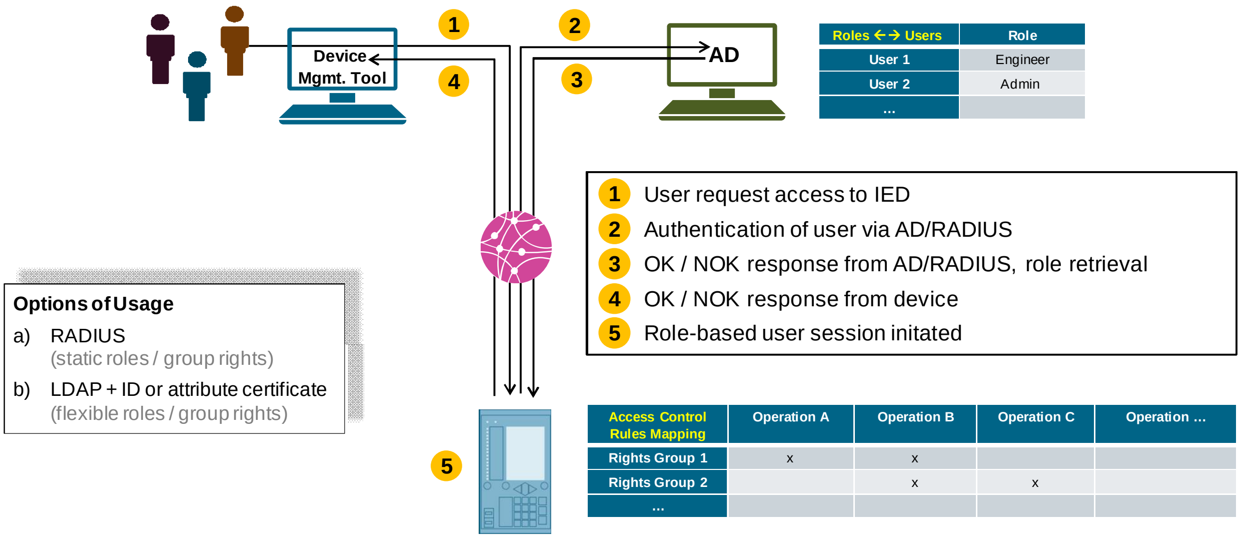
In addition to these mandatory standard roles, it should be noted that interoperability of user-defined roles and rights definitions, which would help better align the roles with an operator's environment, is being currently addressed in the standardization groups.

RBAC Outlook

With the increasing number of secondary equipment directly supporting RBAC come the challenges of scalability and interoperability. An interoperable, scalable and secure solution to apply RBAC across different secondary equipment from different vendors, across substations and beyond, needs to be established. It should ultimately be possible for power system operators to implement and operate RBAC effectively and at reasonable operative expenses.

To address this requirement and similar scalability requirements concerning operational IT security, the IEC 62351-9 standard is defines the necessary cryptographic key management. This essentially covers the handling of cryptographic key material using a public key infrastructure (PKI) for precisely the aforementioned scenarios and is based on the handling of X.509 based certificates.

The application of certificates for RBAC is covered in the IEC 62351-8 standard. Essentially, a centralized certificate authority (CA) will be employed to issue X.509 certificates to identify each user and to indicate the user's attributes such as user role, area of responsibility, etc. These user certificates will be stored related to the associated user accounts in the central LDAP server (e.g. AD domain controller.) To illustrate an example deployment scenario; when a user wants to interact with an IED that can handle user certificates, he presents his user name and password to the IED. The IED then establishes a secure connection to the AD domain controller, forwards the user credentials to the AD server in order to authenticate the user. If the user account is valid, then the IED receives the user's attribute certificate containing among other details also the user's role. With the user's role(s) now available to the IED, the IED creates a new user session in order to apply the role restrictions, and finally allows the user to proceed with interactions. This approach supports also migration from IEDs not featuring an interface over which the user can provide his own certificate directly. This would be the consequent next step.



Roles ←→ Users	Role
User 1	Engineer
User 2	Admin
...	

1 User request access to IED
2 Authentication of user via AD/RADIUS
3 OK / NOK response from AD/RADIUS, role retrieval
4 OK / NOK response from device
5 Role-based user session initated

Options of Usage

a) RADIUS
(static roles / group rights)

b) LDAP + ID or attribute certificate
(flexible roles / group rights)

Access Control Rules Mapping	Operation A	Operation B	Operation C	Operation ...
Rights Group 1	x	x		
Rights Group 2		x	x	
...				

Figure 4: Usage of User Authentication and Authorization Based on Open Standards

Access control will continue to be a cornerstone of operational security in the energy sector. Preventive measures based on RBAC, detective measures based on audit trail of user-triggered events and alarms, and corrective measures based on effective user account management provide the necessary controls for a power grid operator in minimizing the attack surface and impact of cyber attacks, internal and external, local and remote. Secondary technology vendors and standardization committees must continue to work hand-in-hand with the power grid operators in defining and implementing pragmatic, future-enabling and interoperable products that leverage existing and openly available technologies. In the interim, it is important to consider transitional technologies and tools that address the restrictions of the generation-old secondary equipment that will continue to represent the majority installed base along the years to come.

Dipl.-Ing. Steffen Fries,
Principal Key Expert
IT-Security,
Corporate Technology,
Siemens AG, München

Dipl.-Inf. Chaitanya Bisale,
Product Manager, Senior Key
Expert Cyber Security,
Siemens-Division Energy
Management,
Business Unit Digital Grid,
Siemens AG, Nürnberg

chaitanya.b@siemens.com
www.siemens.com/gridsecurity