Securing the Power System Information Infrastructure

IEC 62351 Application Notes

Volume 3: Application Examples of IEC 62351

December 2023

Contents

Figures

Tables

1 Introduction

1.1 Motivation

This document provides application examples for IEC 62351 [1] as Volume 3 of IEC 62351 application guidelines. It provides examples for using IEC 62351 functionality to secure the power system communication infrastructure as a dedicated target domain. The focus is placed on deployment environments which utilize IEC TC 57 defined communication standards like the telecontrol protocols IEC 60870-5 [2] or the control protocol IEC 61850 [3] and the corresponding data models, but the focus of IEC 62351 is not limited to these. The goal is to show the contribution of different IEC 62351 parts in the setup and operation of power system automation.

The term “secure power systems” can relate to many different aspects of operating the power systems securely. One aspect is the protection of communication for monitoring, control, and maintenance of a power automation system. A technical precondition for this protection is the distribution and application of cryptographic key material to support authentication and authorization of users. A further aspect relates to the security of data in transit or at rest (integrity, confidentiality). Besides securing the monitoring of the power system functions, monitoring by security tools during operation is also able to enhance the normal network management tools and to support the detection of threats based on an augmented view of the network.

Note that this volume concentrates on application examples of IEC 62351 as Technical “How” standards and does not address the derivation of security requirements from the Organizational “What” standards, as illustrated in Figure 1-1. It is expected that power systems as a critical infrastructure are operated in accordance with information security management such as ISO 27001 [4] and the IEC 62443 series [9]. Specifically, for power systems, ISO 27019 [5] provides an augmentation of the cybersecurity controls defined in ISO 27002 [6] to address the needs for the power system domain. Other examples targeting a security framework are provided by the NIST Cyber Security Framework [7] or the NISTIR 7628 for Guidelines on Smart Grid Security Controls [8]. In addition to the operation, an integrator may leverage parts of the IEC 62443 series to derive further security requirements for the overall system (by using the part 2-4 and part 3-3) in terms of technical security controls. The manufacturer may leverage further information for the development process. IEC 62351 in this respect specifies the necessary technology to address the derived requirements and to realize dedicated security controls.

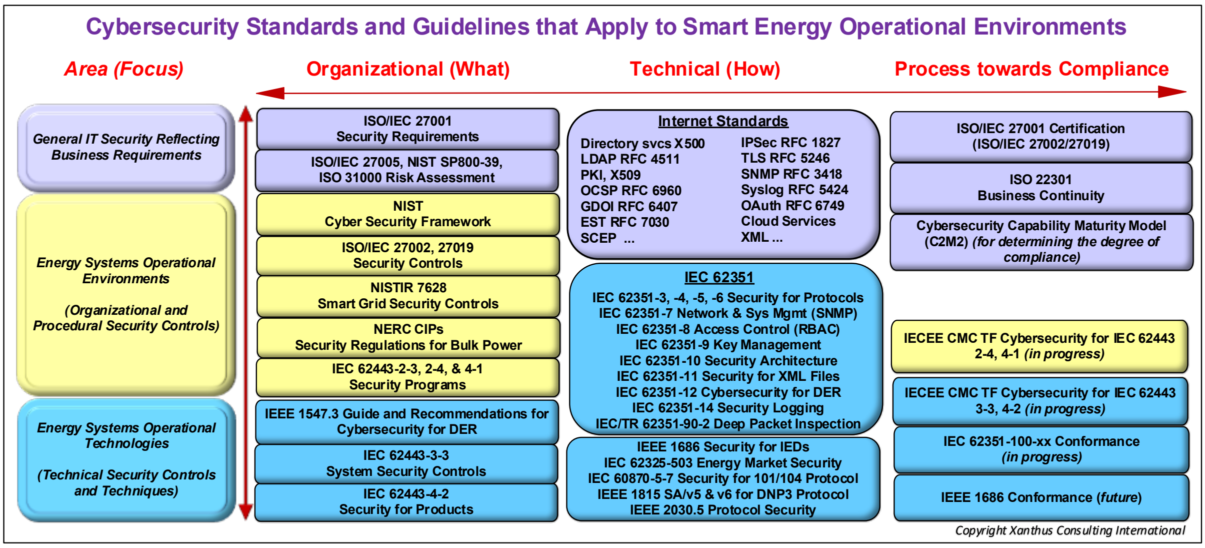

Cybersecurity Standards and Guidelines that Apply to Smart Energy Operational Environments
Area (Focus)
Organizational (What)
Technical (How)
Process towards Compliance
General IT Security Reflecting Business Requirements
Energy Systems Operational Environments
(Organizational and Procedural Security Controls)
Energy Systems Operational Technologies
(Technical Security Controls and Techniques)
ISO/IEC 27001 Security Requirements
ISO/IEC 27005, NIST SP800-39, ISO 31000 Risk Assessment
NIST Cyber Security Framework
ISO/IEC 27002, 27019 Security Controls
NISTIR 7628 Smart Grid Security Controls
NERC CIPs Security Regulations for Bulk Power
IEC 62443-2-3, 2-4, & 4-1 Security Programs
IEEE 1547.3 Guide and Recommendations for Cybersecurity for DER
IEC 62443-3-3 System Security Controls
IEC 62443-4-2 Security for Products
Internet Standards
Directory svcs X500
LDAP RFC 4511
PKI, X509
OCSP RFC 6960
GDOI RFC 6407
EST RFC 7030
SCEP ...
IPSec RFC 1827
TLS RFC 5246
SNMP RFC 3418
Syslog RFC 5424
OAuth RFC 6749
Cloud Services
XML ...
IEC 62351
IEC 62351-3, -4, -5, -6 Security for Protocols
IEC 62351-7 Network & Sys Mgmt (SNMP)
IEC 62351-8 Access Control (RBAC)
IEC 62351-9 Key Management
IEC 62351-10 Security Architecture
IEC 62351-11 Security for XML Files
IEC 62351-12 Cybersecurity for DER
IEC 62351-14 Security Logging
IEC/TR 62351-90-2 Deep Packet Inspection
IEEE 1686 Security for IEDs
IEC 62325-503 Energy Market Security
IEC 60870-5-7 Security for 101/104 Protocol
IEEE 1815 SA/v5 & v6 for DNP3 Protocol
IEEE 2030.5 Protocol Security
ISO/IEC 27001 Certification (ISO/IEC 27002/27019)
ISO 22301 Business Continuity
Cybersecurity Capability Maturity Model (C2M2) (for determining the degree of compliance)
IECEE CMC TF Cybersecurity for IEC 62443 2-4, 4-1 (in progress)
IECEE CMC TF Cybersecurity for IEC 62443 3-3, 4-2 (in progress)
IEC 62351-100-xx Conformance (in progress)
IEEE 1686 Conformance (future)
Copyright Xanthus Consulting International

Figure 1-1: Cybersecurity standards and guidelines: “What”, “How”, and “Compliance”

1.2 Parts of this application note volume 3

The examples in these application notes are grouped into three parts:

- Part I – IEC 62351 core services: includes examples applying IEC 62351 to securing power system communications for hydro and DER plant control, and to provide smart authentication for field devices;
- Part II – IEC 62351 support services: role-based access control, certificate and network management;
- Part III - IEC 62351 performance evaluations and security monitoring.

2 Target audience

Target audience for this document are system architects, operator, integrator, and manufacturer of power automation system components, who are in charge of planning and operating components of the digital grid. Note that this document only provides examples showing the application of IEC 62351 security measures.

3 Acronyms

Acronym	Description
AES	Advanced Encryption Standard
API	Application Programming Interface
CA	Certification Authority
CBC	Cipher Block Chaining
CEI	Comitato Elettrotecnico Italiano
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DER	Distributed Energy Resource
DES	Data Encryption Standard
DHE	Diffie-Hellman Ephemeral
DoS	Denial of Service
DSA	Digital Signature Algorithm
ECC	Elliptic Curve Cryptography
ECDHE	Elliptic Curve Diffie-Hellman Ephemeral
ECDSA	Elliptic Curve Digital Signature Algorithm
EMS	Element Management System
EST	Enrollment over Secure Transport
FIPS	Federal Information Processing Standards
GCM	Galois/Counter Mode
HTTP	Hypertext Transfer Protocol
ID	Identifier
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IP	Internet Protocol
IS	International Standard
ISO	International Organization for Standardization
LDAP	Lightweight Directory Access Protocol
MMS	Manufacturing Message Specification
OCSP	Online Certificate Status Protocol
OSI	Open Systems Interconnection
PCS	Power Control System
PKI	Public Key Infrastructure
RA	Registration Authority

Acronym	Description
RFC	Request for Comments
RSA	Rivest-Shamir-Adleman
RSE	Ricerca Sistema Energetico
RTU	Remote Terminal Unit
SCEP	Simple Certificate Enrollment Protocol
SHA	Secure Hash Algorithm
SoD	Separation of Duties
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TS	Technical Specification
UDP	User Datagram Protocol
VA	Validation Authority

4 Part I - IEC 62351 core services

4.1 Hydro generation telecontrol environment

4.1.1 Overview

Application of IEC 62351-5, IEC 62351-3, IEC 62351-8, IEC 62351-9 *by Marco Modica, Federico Bellio, Gigi Pugni*

Within the general context of the smart energy system security, this chapter specifically addresses the main cyber security requirement of control applications, namely the security of the communication protocols implementing the control data exchanges.

To provide an example grounded on reality, the application is presented considering the telecontrol environment of a Hydro generation facility which adopts IEC 60870-5-104 Transmission Protocols and symmetric and asymmetric cryptographic keys to protect the communications of the power systems.

4.1.2 Context

Hydroelectric power is generated by using gravitational or kinetic water energy according to the type of installation considered (i.e., reservoir or run of river). These water energies are then transformed into electrical power thanks to an alternator coupled to a turbine.

There are many opportunities for optimizing hydroelectric power plants. For example, it is possible to remotely control and operate a hydroelectric plant to achieve maximum economic benefit and minimum technical risk.

Telecontrol provides an integral operability of the telecontrolled hydro power plants from a control center sited at the power generation utility´s operation offices and permits the use of the strictest security standards that are required nowadays for this type of installations.

The most relevant examples of telecontrol are:

- Unit control (turbine, generator, power transformer and unit auxiliaries);
- Plant control (common plant auxiliaries, HV switchyard, spillway, intake and other hydraulic systems);
- Complex control functions, such as joint control, cascade control, flood and river control, plant frequency control, reactive and active power control;
- Remote control and dispatch center connectivity;
- Integrated electrical and mechanical protection throughout the hydro power plant;
- Automatic Generation Control (power schedules defined by traders in power exchange system sent to HPP and automatically actuated).

In a real hydro power plant (HPP) telecontrol infrastructure, several Generation Control Centers (assisted by a Disaster Recovery site) have the responsibility of controlling remotely hundreds of generation plants in turn connecting to hundreds hydro sub-plants (reservoir, dam, etc.). The Management Centers remotely operate OT based controls of Generation and Distribution operators, and networks devices/probes as well. This is carried out collecting data and events through monitoring objects and log reporting in a centralized correlation engine that is able to recognize the occurrence of anomalous situations from the complete view of the environment status and behavior.

A logical view of a Hydro Generation Telecontrol infrastructure is depicted in Figure 4-1, focused primarily on telecontrol and network management functions. The elements depicted in light blue are devoted to the SCADA operation of the generation plants. IEDs (RTUs) and remote/local SCADA are supposed to be fully available and reliable in providing their own services to the SCADA operators who have the responsibility of controlling the generation plants. The “Generation Network” cloud (depicted in light blue as well) is a logical network reserved to the telecontrol protocols transport, in our case the IEC 60870-5-104 protocol and its secure extension compliant with IEC 62351-3 and IEC 62351-5.

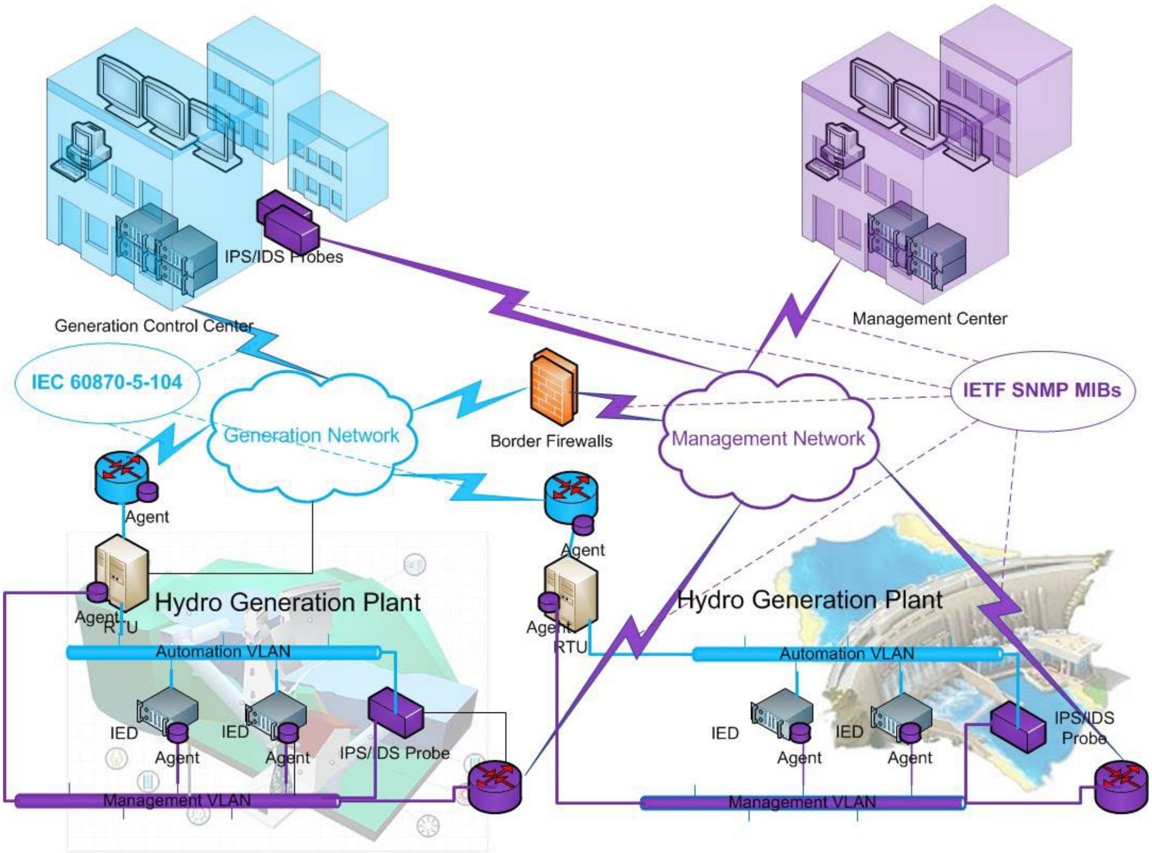


Figure 4-1: Hydro Power Plant Telecontrol Field – Logical View

4.1.3 IEC 62351-5 - the protocol - Secure 104 Key Change

IEC 62351-5 defines security mechanisms to protect serial communication (IEC 60870-5-101) and DNP3 (IEEE 1815). Additionally, this part utilizes IEC 62351-3 to protect the TCP based IEC 60870-5-104 communication (T-profile). The terms and definitions given in IEC/TS 62351-2 and in

Table 4-1 apply.

Table 4-1 - Naming Conventions

Name	Definition	Notes	Ref.
controlling station	station which performs the telecontrol of outstations	It is commonly called a “master” or “master station” in some specifications.	[IEC 60870-1-3]
control direction	direction of transmission from the controlling station to a controlled station		[IEC 60870-5-101]
controlled station	station which is monitored, or commanded and monitored by a master (controlling) station	It is commonly called an “outstation” or “slave” in some specifications.	[IEC 60870-1-3]
monitor direction	direction of transmission from a controlled station to a controlling station		[IEC 60870-5-101]

To protect the integrity of the communication layer and ensure mutual authentication between controlling and controlled stations the standard specifies a series of challenge and response protocols.

In summary, to secure the communication between the stations, the stations adopt a **symmetric Session Key** (actually two, one for each direction).

Each controlling station initialize the Session Keys upon establishing communications and when it detects the controlled station has restarted, furthermore it periodically changes the Session Keys as described in Table 4-2.

The controlling station uses a **symmetric Update Key** to encrypt the **Session Key** and transmit it to the controlled station.

An Update Key is separately assigned for each combination of user and controlled station. The Update Key is a symmetrical key, known by the station and the **User** administering it.

The process of changing Update Keys begins with changing the status of a **User**. The status of a user includes the user’s name, role, key and expiry interval.

Table 4-2 - Summary of symmetric keys usage

Type	Use	Change mechanism	Range of expected change interval
Monitoring Direction Session Key	Used to authenticate data transmitted in the monitoring direction by the controlled station.	The controlling station shall encrypt the Session Key in a Key Change message using the Update Key.	Minutes to weeks (for infrequent communications)
Control Direction Session Key	Used to authenticate data transmitted in the control direction by the controlling station.	The controlling station shall encrypt the Session Key in a Key Change message using the Update Key.	Minutes to weeks

Type	Use	Change mechanism	Range of expected change interval
Update Key	The controlling station shall use the Update Key to periodically change the Session Keys.	The Update Key may be pre-shared by the two stations, or it may be changed remotely using either symmetric or asymmetric cryptography.	Months or Years
Authority Certification Key (optional)	The authority shall use the Authority Certification Key to change Update Keys. The controlling station shall forward the Update Key encrypted by the authority to the controlled station.	The Authority Certification Key is pre-shared by the authority and the controlled station and can be changed only by means external to the protocol	Years, if ever

Instead of using the Authority Certification Key, the authority, controlling station and controlled station **may optionally use asymmetric cryptography**, also called public key cryptography, to remotely change Update Keys. Table 4-3 summarizes how these concepts may be used to change Update Keys remotely.

Table 4-3– Summary of asymmetric keys used (optional)

Type	Use	Change mechanism	Range of expected change interval
Authority Private Key	The authority shall use its Private Key to certify the User Public Key of a user.	The Authority Private Key is kept secret by the authority and may only be changed by means external to the protocol.	Years, if ever
Authority Public Key	The controlled station shall use the authority's Public Key to validate the Public Key of a User.	The Authority Public Key may be transmitted anywhere in the clear but must be securely installed in the controlled station by trusted personnel.	Years, if ever
User Private Key	The controlling station shall use the user's Private Key to digitally sign a new Update Key.	The User Private Key shall be generated by the user and ideally should be carried to the controlling station in a physical token by the user. In any case, the mechanism by which the controlling station accesses the user's private key must be secure.	Months or years
User Public Key	The controlled station shall use the user's Public Key to validate the Update Key of a user.	The User Public Key shall be generated by the user and may be transmitted anywhere in the clear, but the process by which the authority certifies it must be secure.	Months or years. Even if it is not changed, it shall expire periodically and its certification by the authority must be renewed.

Type	Use	Change mechanism	Range of expected change interval
Controlled Station Private Key	The controlled station shall use its Private Key to decrypt a new Update Key.	The Controlled Station Private Key shall be generated by the controlled station and stored securely on the controlled station.	Years if ever
Controlled Station Public Key	The controlling station shall use the Controlled Station's Public Key to encrypt a new Update Key for a user.	The Controlled Station Public Key shall be generated by the controlled station and may be transmitted anywhere in the clear, although it must be installed and stored securely in the controlling station by trusted personnel.	Years if ever

If the stations both permit remote change the controlling station may change the Update Key of a User at any time after after it has forwarded the Certification Data of the user in a User Status Change message or a certificate.

The controlling station shall do so by:

1. Sending an Update Key Change Request message containing the User Credentials and some random challenge data.
2. Upon receiving an Update Key Change Reply message from the controlled station, the controlling station shall send the Encrypted Update Key Data to the controlled station in an Update Key Change message.
3. The controlling station has to take different actions to obtain the Encrypted Update Key Data and to authenticate the transfer of this data depending on the Update Key Change Method in use:
   - If the Update Key Change Method is **symmetric**, the controlling station shall obtain the Encrypted Update Key Data from the authority. The method used to do so is outside the scope of this document, but the communication must be secured;
   - If the Update Key Change Method is **asymmetric**, the controlling station shall create the Encrypted Update Key Data as stated by the following paragraph.

4.1.4 Asymmetric update key change method

To exchange securely the Update Key both the User and the Stations require a pair of asymmetrical keys. The **asymmetric** Update Key Change Method is implemented as follows:

1. The controlling station create the Encrypted Update Key Data using the controlled station's Public Key.
2. The controlling station authenticate the transfer of the Encrypted Update Key Data by sending an Update Key Change Signature message with the Update Key Change message in its request.
3. In this way, the controlling station authenticates the transfer of the Encrypted Update Key Data by signing it with the User's Private Key.
4. The authority securely provided the controlled station with the User's Public Key in the User Status Change message, so the controlled station can verify that the controlling

station is authentic, and the controlling station and the authority agree on the new Update Key.

4.1.5 Public Key Infrastructure (PKI)

To enable the aforementioned **asymmetric** update key change, it is required that the various party involved agree on a series of asymmetric key.

The whole procedure requires an infrastructure that can provide each interested device with suitable credentials.

As said before, a PKI is an infrastructure wherein a set of roles, policies and procedures are needed for the creation, management, storage and revocation of digital certificates to facilitate public key encryption. The main purpose of PKI model is to enable secure communication between different entities involved in network activities.

The adopted underlying technology to realize the key management functionalities can be the same of the traditional Public Key Infrastructure, used for the emission of authentication certificates required by the present IT solutions (e.g., Secure Web, Transport Layer Security, etc.). A step up, however, is required to realize a series of additional functionalities that allow the solution to work within the strict requirement of a telecontrol environment.

Specifically, the solution should possess the following properties:

- adherence to the International Standard IEC 62351-9 [10] which specifies in detail the protocols required for the compatibility with the devices employed within the electric OT landscape;
- adherence to the International standard IEC 62351-8 which defines the rules for the implementation of Role Based Access Control model.

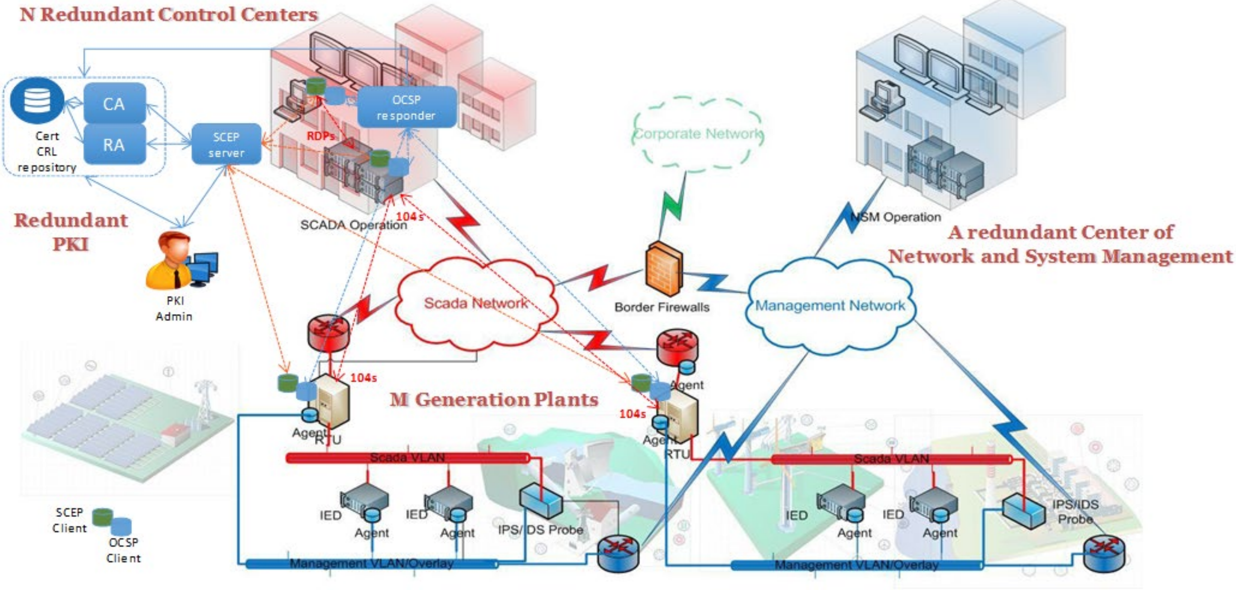


Figure 4-2: Relation between SCADA-RTU in secure connection and a PKI

Further information on key management and derivation may be found in section 5.2.

4.2 DER plant control

Application of IEC 62351-4, IEC 62351-3, IEC TS 62351-100-3, IEC 62351-8, IEC 62351-9, IEC 62443 *by Giovanna Dondossola, Roberta Terruggia, Mauro Giuseppe Todeschini, Marco Modica*

To guarantee the interoperability and security of communications for the remote access to the plant controllers by authorized parties, the Annex T of the Italian Norm CEI 0-16 specifies data and security profiles customizing the International standard profiles to the Italian context. For the definition of the DSO-DER data flows of authorized entities, the Norm utilizes communication services based on the TCP/IP transport protocol. In particular, the CCI interface for the DER-DSO communications is implemented by a data server mapping IEC 61850 data model and services on the ISO/OSI stack of the MMS protocol (Manufacturing Message Specification). The cybersecurity requirements of IEC 61850 communications are met by the implementation of cybersecurity profiles based on the ISA/IEC 62443 and IEC 62351 Standards (Figure 4-3).

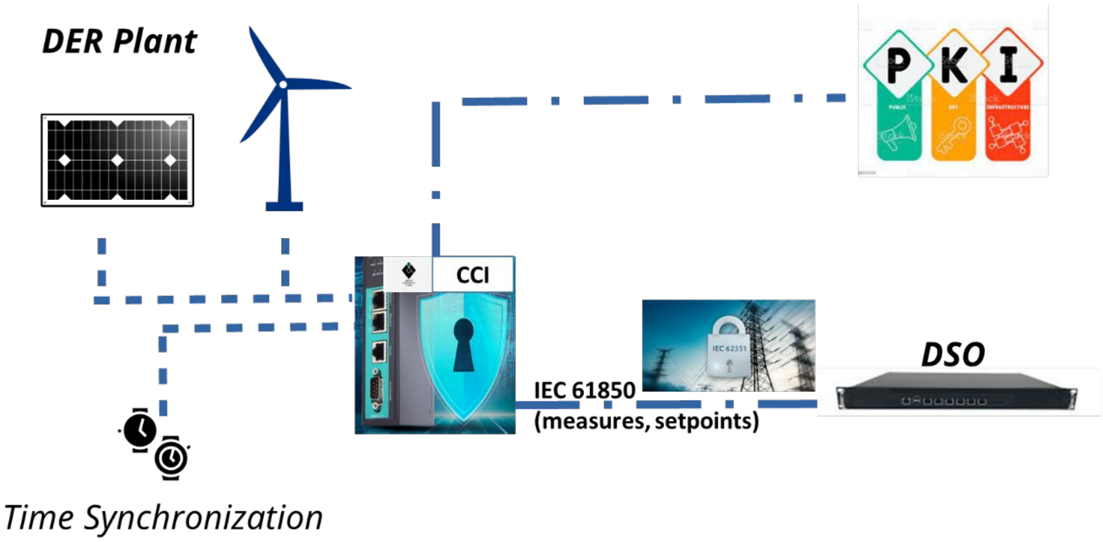


Figure 4-3: CCI communication interfaces

The following sections present the cybersecurity solutions and certifications required to the CCI devices to guarantee the identification of authorized users, the role-based access control, the mutual authentication of the communication terminal nodes, as well as the confidentiality, integrity, and availability of the information exchanges.

4.2.1 Identification, authorization, and authentication of communicating entities and devices

The secure access to CCI services and data by multiple remote entities in charge of different tasks (such as device configuration and maintenance, plant supervision, monitoring and control) is guaranteed through three distinct mechanisms:

- the identification of the remote entity connecting to CCI;
- the authorizations associated to the entity role;
- the authentication of the communicating peers.

The entity identification is performed by checking (the certificate of) the Certification Authority of the connecting entity that must be pre-configured on the CCI.

Once the remote operator has been identified as, for example, a DSO, the requested access roles will be checked against the CCI services and data authorised by the CCI plant owner, i.e., the producer, to the DSO. The specification of access roles to the IEC 61850 server is compliant with the Standard IEC 62351-8. More specifically two different roles will be authorised: the standard role VIEWER and the custom role DSO_OPERATOR, which gives DSO a set of permissions on the CCI dataset[1].

In IEC 61850 communications role control is applied at the data model level, i.e., to allow and to deny access to an ACSI (Abstract Communication Service Interface) service at each instance of the logical-device, logical-node, and data-object hierarchy. The assignment of a role to a specific subject allows to obtain specific responses to the requested services based on the privileges that have been assigned to that role (Figure 4-4). The “DSO_Operator” role information is contained in an access token transported, e.g., by an extension of the client identity certificate (see IEC 62351-8 [14]).

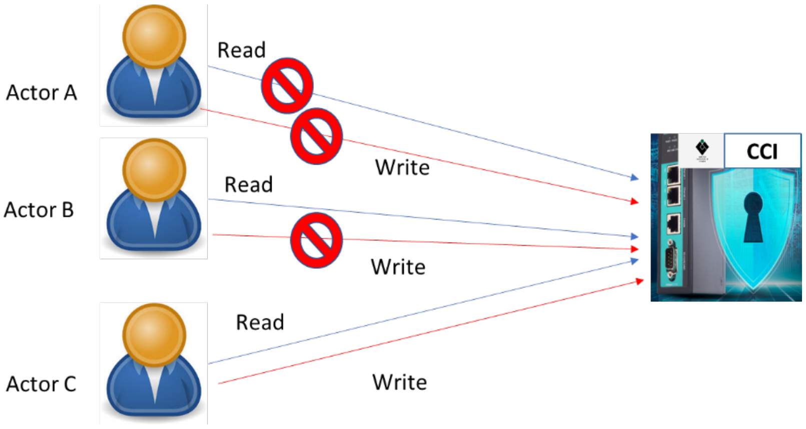


Figure 4-4 CCI roles

The authentication of the communicating peers is executed during the Transport Layer Security (TLS) protocol handshake. The TLS profile specified by IEC 62351-3 requires the mutual authentication of the communicating parties through digital certificates signed by recognized authorities. The CCI server must authenticate itself towards the DSO client so that the latter is certain of the device identity. Likewise, the client must authenticate against the CCI.

4.2.2 Data confidentiality and integrity

Data confidentiality concerns the impossibility for a third party to interpret the contents of the information exchange between the two parties and therefore to know the data content. Data integrity, on the other hand, concerns the impossibility of modifying the communication by replacing values or other contents, or by entering new contents both in encrypted and unencrypted form.

[1] Annex T of CEI 0-16 also defines the custom role AGGREGATOR_OPERATOR with specific permission and data sets.

The integrity and confidentiality of the communications between the CCI and the authorized Remote Operators is guaranteed through adequate security mechanisms at the various levels of the protocol stack.

As regards the IEC 61850-8-1/MMS communications adopted by the CCI for information exchanges with the DSO, the reference Standards for cybersecurity are IEC 62351-3 for the transport layer (layer 4, i.e., that of the TCP protocol), and IEC 62351-4 for the security of the MMS protocol (layer 7, mainly at the "application" level). Specifically, IEC 62351-3 defines security profiles for the TLS protocol suitable for applications in the field of electrical system control and IEC 62351-4 details and enriches them for the case of the MMS protocol.

The TLS profile of the CCI requires the usable configurations (among those allowed by IEC 62351-3), highlighting the most significant and characterizing parameters and incorporating some recent updates by excluding, for example, deprecated TLS versions and cipher suites as their usage is not justifiable for new devices like CCI and related telecontrol architectures.

To ensure the communication confidentiality and integrity, the TLS protocol is based on cryptographic algorithms, organized in suites that bring together algorithms for generating and exchanging session cryptographic keys, encrypting information, and applying cryptographic hashes. In the TLS v1.2 profile, the expression cipher suite is used to refer to combinations of encryption algorithms predefined by the IETF (the TLS protocol specification body), which are continuously updated in consideration of new vulnerabilities and advances in the computational capacity of devices (more performing devices can implement more complex and safer algorithms). For the CCI, minimum key sizes have been indicated with the aim of guaranteeing security for at least a decade.

However, in addition to the minimum values, the possibility of supporting keys with higher entropy and resistance to brute force attacks is suggested, as they are technologically not complex to implement and able to considerably lengthen the device operation over time. However, there shall always be the possibility of upgrading the CCI software/firmware, following the secure procedure specified by the Norm CEI 0-16 which involves both firmware authenticity and integrity verification by checking the manufacturer’s digital signature. Again, with a view to optimizing performance and security, the specifications for the session resumption and session renegotiation functions of TLS are indicated, which periodically renew the symmetric cryptographic keys to support individual sessions efficiently, while verifying the validity status of digital certificates.

In the installation phase of the CCI within the power plant environment the device configuration options will be selected in relation to the operational architecture and the security policies agreed upon by the organizations involved.

At the higher levels of the TCP/IP stack, The Norm CEI 0-16 specifies the E2E (End-to-End) security profile specified by IEC 62351-4, which guarantees the authentication of the parties together with encryption and integrity check of application messages. E2E security will be implemented to meet the CCI security requirements in segmented communication architectures, which involve intermediate hops in the server/client communication interrupting the TLS channel.

4.2.3 Key and certificate management

The cryptographic functions necessary to secure the operations require that the CCI is equipped with cryptographic keys and digital certificates, appropriately stored in a dedicated Hardware Secure Module that, as specified by Norm CEI 0-16, has to adhere to specific certifiable standards (i.e., Federal Information Processing Standards - FIPS 140-2 "Security Requirements for 1277 Cryptographic Modules").

The infrastructure responsible for managing the life cycle of cryptographic keys and associated digital certificates is the PKI (Public Key Infrastructure). A Public Key Infrastructure consists of various components among which the most significant is represented by the Certificate Authority. Certificate Authorities issue certificates to a client directly or, as in this case, authorize another entity to do so, thus creating a "certification chain" that can be trusted by other entities.

To make the CCI device operational and enable the IEC 61850 communications with remote operators, both DSO and Producer/CCI Owner have to exchange Certificate Authorities Public Certificates. This process enables each entity to authenticate certificate chain of the other and is referred to as "PKI Federation".

Afterwards the Producer/CCI Owner shall enroll the CCI through its own PKI (either managed or third party) thus recognizing the CCI as part of its authorized infrastructure. From this moment on, the PKI will manage the life cycle of the certificates necessary to enable its cryptographic functions (Figure 4-5), i.e., issuing the first certificate, checking its validity status, renewing the certificate before expiration and revoking the certificate in case of compromise of the CCI digital identity. For the procedures to follow for the keys and certificates management, the Norm CEI 0-16 refers to the IEC 62351-9 [10].

Once the CCI is enrolled and has received its first ID Certificate signed by CCI Owner Certificate Authority, it can be authenticated by the MMS Client of the DSO connecting entity.

In a similar way, DSO connecting entities are being enrolled by the DSO managed PKI and in turn receive an ID Certificate signed by DSO Certificate Authority.

Finally, during the TLS handshake, both entities send their own ID Certificates, which are validated by checking the Certificate Authority signature thus enabling mutual authentication and DSO identification/authorization.

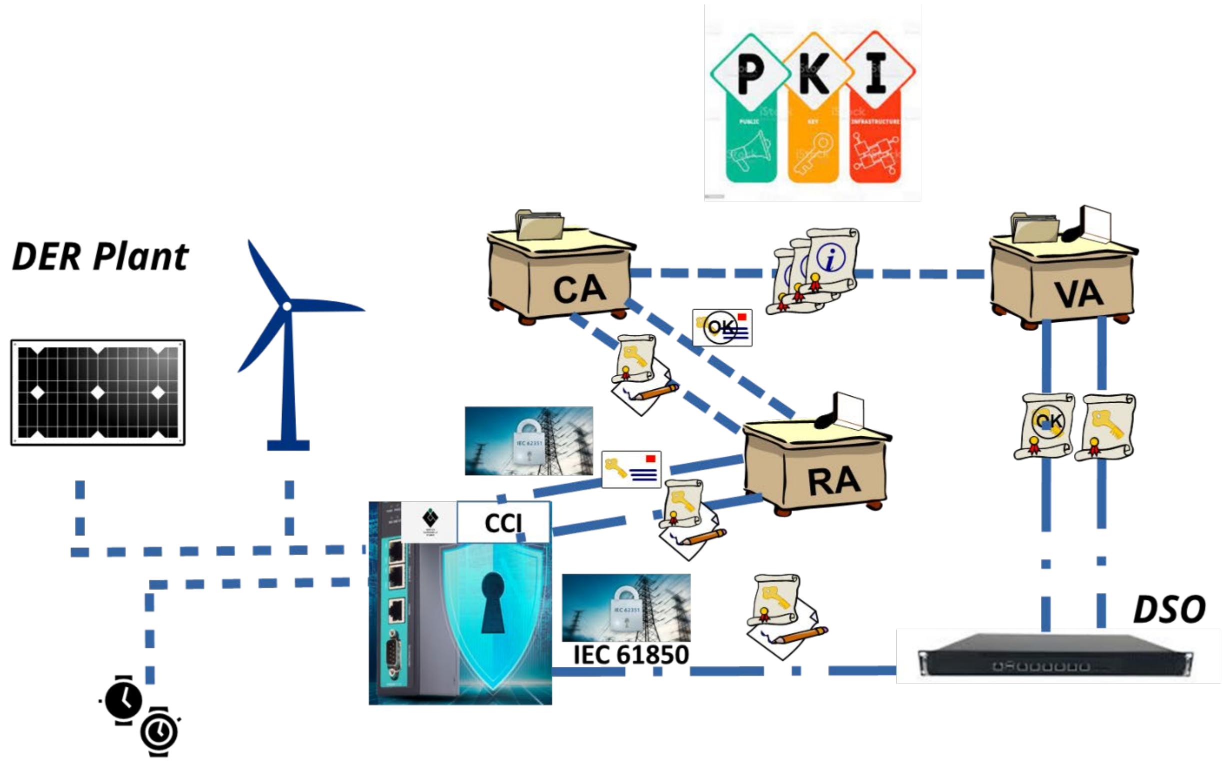


Figure 4-5: CCI communications with PKIs

4.2.4 Cybersecurity certifications

The correct implementation of the mandatory functions of CCI devices shall be verified by accredited certification bodies which, based on predefined and consolidated procedures, analyzes all the aspects characterizing the device itself, including the alternatives that the specification covers and which the manufacturer decides to implement, with the aim of drawing up a certificate of conformity to the reference standards. For the Standards IEC 62351, the technical specifications IEC 62351-100-x defines the conformity tests of security solutions. For the TLS profile, the Norm CEI 0-16 requires the certification of compliance with the Standard IEC 62351-100-3 for the CCI devices (Figure 4-6). IEC 62351-100-3 provides for the verification of the behavior of the CCI as regards the IEC 62351-3, both in expected circumstances and in possible but unusual circumstances.

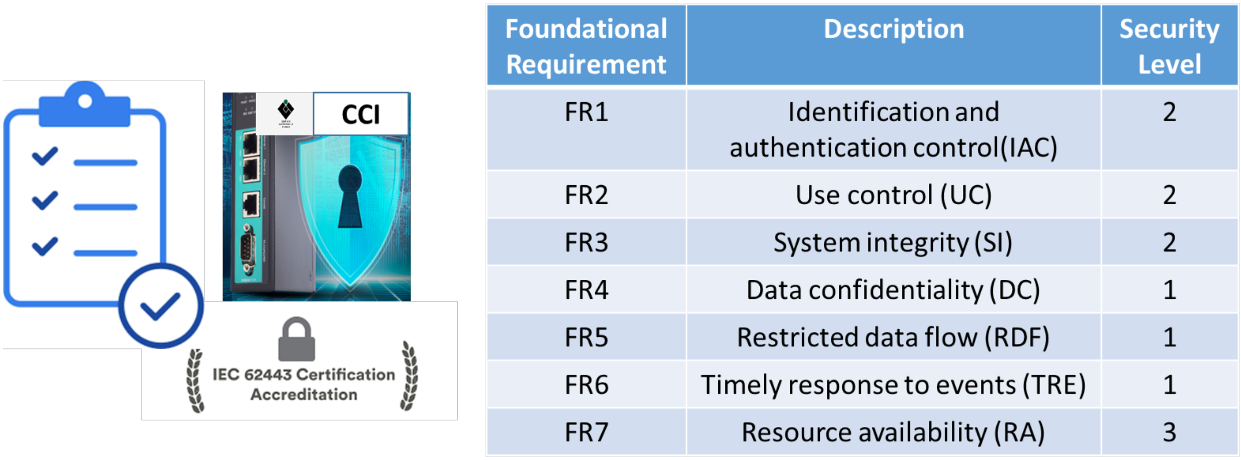
For example, with reference to the TLS communications, the IEC 62351-100-3 indicates to verify that the CCI checks the size of the cryptographic keys presented by the counterparty and that, if they do not comply with the minimum allowed, it issues a default log and end the session. In the case, however, of session resumption and session renegotiation, the checks concern compliance with the time limits specified by the Standard for the activation of these functions.

Also, for digital certificates tests are specified for the subsystems that verify their validity or revocation status and the overall size: in fact, all implementations shall be able to manage a range of sizes that does not set stringent limits to end users on the amount of information that can be stored in the certificate, but at the same time indicating a shared limit, which the parties should comply with for communication interoperability. However, it should be noted that the behavior required to CCI is indicated exclusively in the reference Standards of the Norm CEI

0-16, while the IEC 62351-100-x parts standardize the test procedure, the preliminary information required and the expected outputs, but they do not add further requirements to the device, at the most they suggest possible extensions and solutions that facilitate diagnostics.

Figure 4-6: Conformance testing of CCI communication security

Regarding the cybersecurity guarantees of the CCI device, the Norm CEI 0-16 requires certification of compliance with the Standard ISA/IEC 62443-4-1, related to the security of the CCI development process and with the Standard ISA/IEC 62443-4-2 with minimum Security Levels indicated in Figure 4-7. For each Foundational Requirement the appropriate Security Level has been chosen by selecting from the standard requirements those most appropriate for the CCI operational environment.


CCI
IEC 62443 Certification
Accreditation

Foundational Requirement	Description	Security Level
FR1	Identification and authentication control(IAC)	2
FR2	Use control (UC)	2
FR3	System integrity (SI)	2
FR4	Data confidentiality (DC)	1
FR5	Restricted data flow (RDF)	1
FR6	Timely response to events (TRE)	1
FR7	Resource availability (RA)	3

Figure 4-7: CCI security certifications

4.3 Secure remote access in fault recordings

4.3.1 Introduction and motivation

Application of IEC 62351-3/4/5, IEC 62351-8, IEC 62351-10 *by Steffen Fries*

There exist a variety of operative guidelines addressing security in power systems like the German BDEW white paper [13], IEC 62351-10 [15], or technical requirements like IEEE 1686:2022 or technical standards as IEC 62351-8 [14]. Common to all is that they consider role-based access control on a variety of interfaces. This also relates to the management of roles, their definition, the associated guidelines, as well as the assignment of subjects, which require a consistent and secure process.

For power system automation IEC 62351-8 defines different means to perform RBAC and specifies base roles to be supported in power systems. The standard also allows an interoperable exchange of customer defined specific roles in addition to the mandatory roles already defined in the standard. This allows the reuse of already defined roles. Note that the standard is currently revised to an Edition 2, which will address specifically the description of binding roles and permissions to IEC 61850 objects to ensure interoperability across different manufacturer implementations.

In addition to role-based access control measures on different levels, for the underlying network infrastructure architecture it is also recommended to support limitation of access. Especially for remote access, connectivity to internal parts of the network should only be allowed for authorized peers for authorized actions. In the network infrastructure the concept of network segmentation is therefore applied. This can be done in addition to RBAC as stated above.

4.3.2 Network architecture considerations

As stated above, RBAC within the power system protocols and application ensures that only authorized users can perform requested actions. To also support this from a network infrastructure point of view, there are guidelines like IEC 62351-10 recommending potential network architectures. The document details specific aspects like network segmentation, strong authentication, role-based access control, data security and communication security, as well as monitoring.

To also protect remote access, network segmentation is recommended defining separated zones using firewalls and demilitarized zones (DMZ) to prohibit direct access to an IED. Based on IEC 62351-10, Figure 4-8 depicts a potential network segmentation supporting remote access.

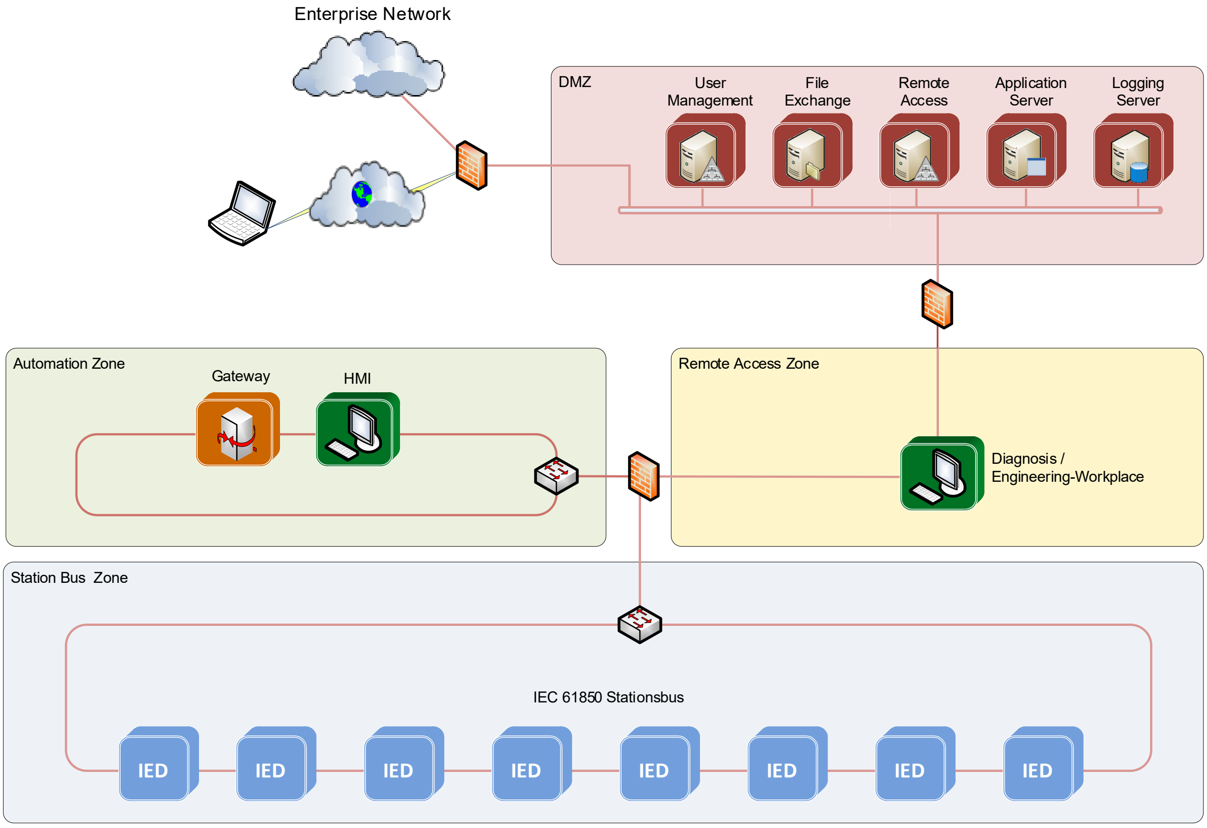


Figure 4-8: Network security architecture for remote access

The DMZ shown may be realized in a central place (e.g., a control center) or decentral in the substation itself or in both. If used in the substation, the DMZ may comprise the remote access zone. Important is the termination of remote access connection within the DMZ to prohibit direct connectivity to an IED. Using a dedicated workplace for diagnosis and engineering can avoid connecting mobile equipment to the substation network. Note that to support also access control of equipment there are further standards available allowing network access only for authenticated and authorized devices. Moreover, it may also be checked if a devices copes with certain security requirements like a dedicated operation system version or a specific patch level. Devices not matching may be placed in quarantine and be updated before allowing access. The shown approach can be used for greenfield installations, but also in existing deployments.

4.3.3 Utilized communication protocols

If fault recordings are distributed via standardized protocols like IEC 61850 or IEC 60870-5-104, communication security can be provided as defined in IEC 62351 parts 3, 4, and 5 to protect the transport layer. IEC 62351 employs TLS with mutual authentication based on certificates and defines allowed cipher suites as well as TLS session management. Using the RBAC extension in the certificates as specified in IEC 62351-8 enables a more fine-grained access control either on transport level or on application level or both.

4.4 Smart authentication: RBAC PMI using attribute certificates in power systems

IEC 62351-8, IEC 62351-90-1 *by Marco Modica*

4.4.1 Introduction and motivation

In power system automation, the typical access control scenario is a Human-Machine Interface (HMI), which allows supervision and control of a sub process, protected by a login interface. Secure access to computer-based applications involves authentication of the user to the application. After authentication, the types of interactions, which the user can perform with the application, are determined.

The use of local mechanisms for authorization creates a patchwork of approaches difficult to administer uniformly across the breadth of a power system enterprise. Each application decides with its own logic the authorization process. However, if applications can access a network to help manage authentication, a database can serve as a trusted source of user's group or role affiliation. Thus, the access to a shared user base can be controlled centrally. Each application can then examine the rights listed for a subject and corresponding role and determine their level of authorization.

From this perspective, a traditional Access Control system, based on the login/password dichotomy, can add a point of failure, slow or disrupt the process and render maintenance more difficult especially in an emergency context. This could lead users to try to avoid or bypass authentication, adopting bad practices and violating company security policies. Moreover, Separation of Duty (SoD) is not completely enforced.

Rethinking the authorization system represents an opportunity to help workers while also enforcing accountability and separation of duty to achieve increased security of the automation systems in the energy industrial domain.

Within this case scenario, we define a novel approach to implement role-based access control (RBAC) in the power systems automation environment using X.509 Attribute Certificates for enterprise-wide use in power systems. It supports a distributed or service-oriented architecture (Figure 4-9) where security is a distributed service and applications are consumers of distributed services. The identity and role of a user are transported in an X.509 Attribute Certificate, associated to the HMI X.509 Public Key Certificate, to act as an authorization token of that user to the object (e.g., IED).

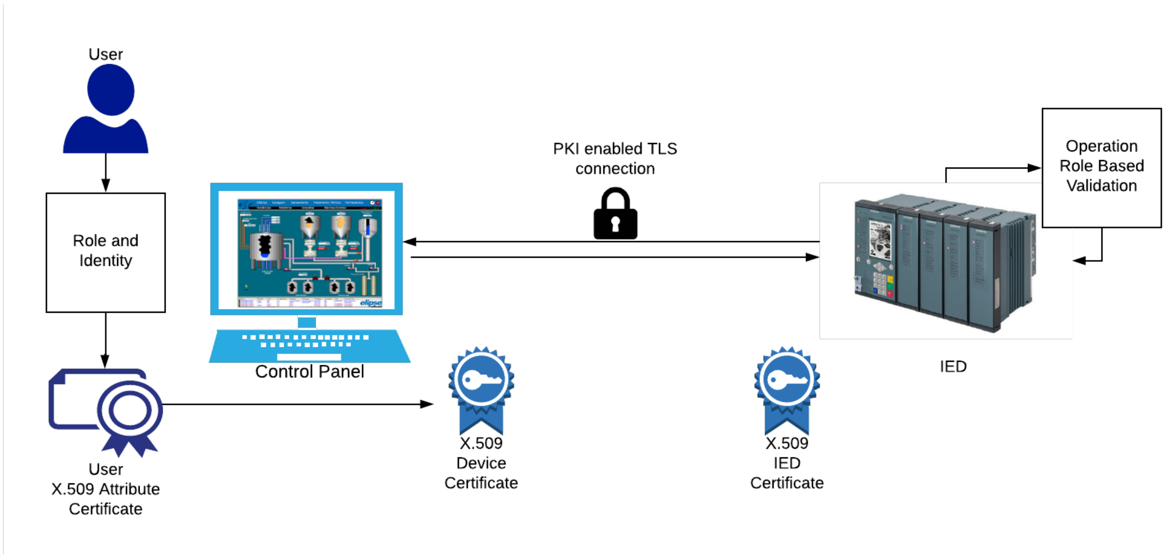

User
Role and Identity
User X.509 Attribute Certificate
Control Panel
PKI enabled TLS connection
X.509 Device Certificate
X.509 IED Certificate
IED
Operation Role Based Validation

Figure 4-9: Overview of the Smart Authentication components

Attribute Certificates are administered via a (possibly federated) identity management tool. The user has to authenticate to a workstation in his working Domain and receive a Certificate Attribute with a properly defined Area of Responsibility (AoR). To enable local verification of the Attribute Certificate validity at remote sites without the need to access a centralized repository (e.g., a centralized revocation list a.k.a. CRL) Attribute Certificates have a limited lifetime and are subject to expiration. Prior to verification of the Attribute Certificates itself, the HMI transmitting the Attribute Certificates must be authenticated by the object (i.e., IED). The object trusts the management tool to issue Attribute Certificates with a suitable duration.

To support an efficient management of user's roles and identities, suitable for the power system domain, IEC 62351-8 and 62351-90-1 define solutions for a PKI based access control. The focus for this section lies on the Attribute Certificate based approach. Among those mentioned, the PUSH model approach (as outlined in section 5.1.2.3) has been selected because it allows us to best adapt to the emergency requirements expressed by the safety policies. The user, should an emergency arise, must be able to retain the ability to access the IED remotely with proper authorization even though for example the connectivity between the client device and Attribute Authority cannot be established.

At the end of the procedure, the output is to have the bonded certificates (User Attribute Certificate & Device Identity Certificate) available on the various appliances (e.g., HMI & IED).

4.4.2 Smart authorization sequence

Following, we describe an ideal authorization sequence (Figure 4-10). Considering the scope of this example it is assumed that the authentication phase is already been completed and the subject is logged into a session on the client machine (i.e., Control Panel) according to the security policies of the Operator. This allows to retrieve and verify the subject name from the Active Directory Domain, the unique security identifier (SID) and the Ticket Granting Ticket (assuming that the authentication is executed using the Kerberos Protocol).

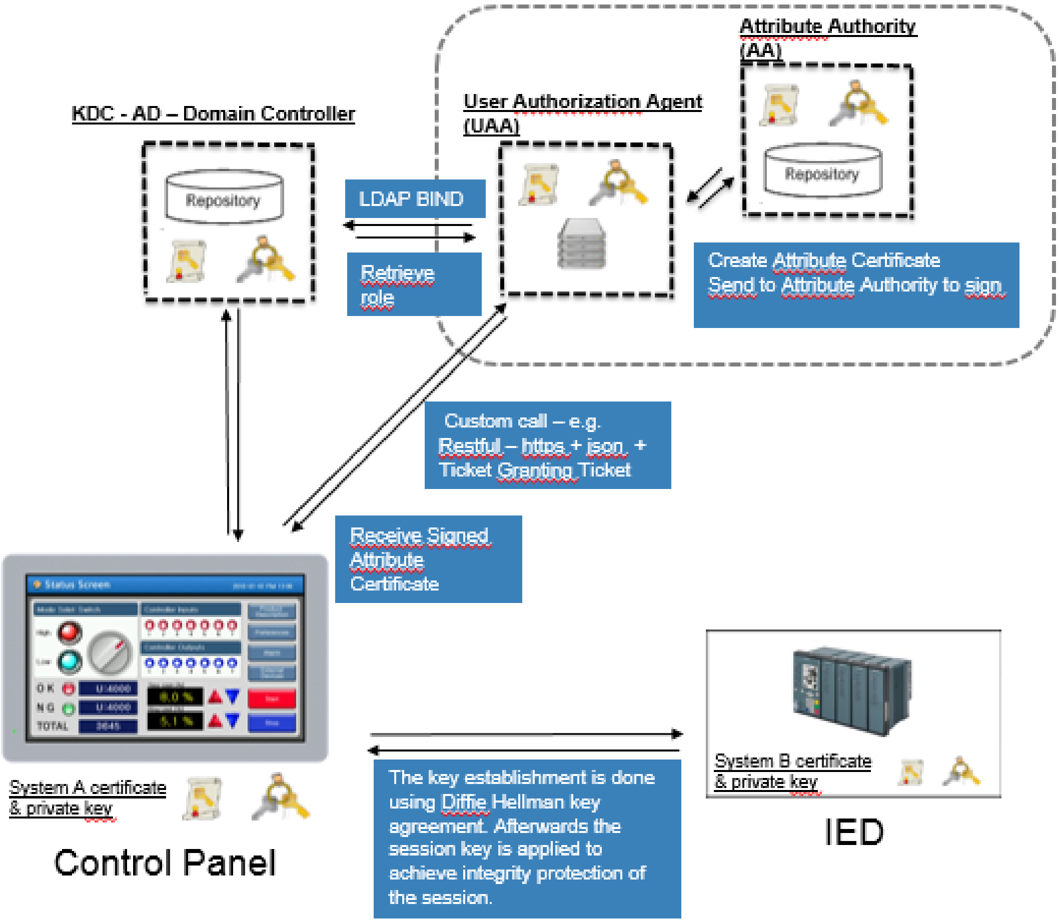

Attribute Authority (AA)
Repository
User Authorization Agent (UAA)
KDC - AD – Domain Controller
Repository
LDAP BIND
Retrieve role
Create Attribute Certificate
Send to Attribute Authority to sign
Custom call – e.g. Restful – https + json + Ticket Granting Ticket
Receive Signed Attribute Certificate
System A certificate & private key
Control Panel
The key establishment is done using Diffie Hellman key agreement. Afterwards the session key is applied to achieve integrity protection of the session.
System B certificate & private key
IED

Figure 4-10: Authorization sequence view

Following, we list the proposed sequence, in which a subject is trying to access an IED (system B) through a Control Panel (System A):

1. After successful authentication of the subject, the repository provides the subject with the access token (e.g., Kerberos Ticket) containing the user identity.
2. System A submits the access token along with the device identity Certificate to an entity known as User Authorization Agent (UAA).
3. The UAA verify the subject identity and retrieve the subject role(s) from the LDAP directory. Then requests the appropriate Attribute Certificate to the Attribute Authority specifying subject identity, subject role(s) and device identity Certificate.
4. Attribute Authority verifies legitimacy of the request authenticating the UAA and submits appropriate authorization token (attribute certificate associated with the device identity certificate).
5. System A receives the appropriate authorization token and forwards it to System B along with authentication request.
6. System B verifies the identity certificate of the device associated with the authorization token(s) of the subject and gives the subject authorized access to the object according to the right(s) associated with the role(s) specified by the access token.
7. After successful verification of the authorization token, system B acknowledges access to system A.

5 Part II - IEC 62351 support services

5.1 Access control and management in power systems

5.1.1 Overview on Access Control Systems (ACS) and Role Base Access Control (RBAC)

Application of IEC 62351-8) *by Steffen Fries*

Role-based Access Control (RBAC) is a proven concept in IT systems, which is typically known from operating systems for controlling access to system resources. It is a clear improvement compared to the often-used single administrator-guest-model. Instead of providing specific access rights on a per user base, RBAC supports the least privilege principle to assign a user only the necessary permissions for an administrative action. It is used to group dedicated permissions to specific roles. These roles can then be assigned to a user, which entitles him to perform only his specific tasks (Figure 5-1).

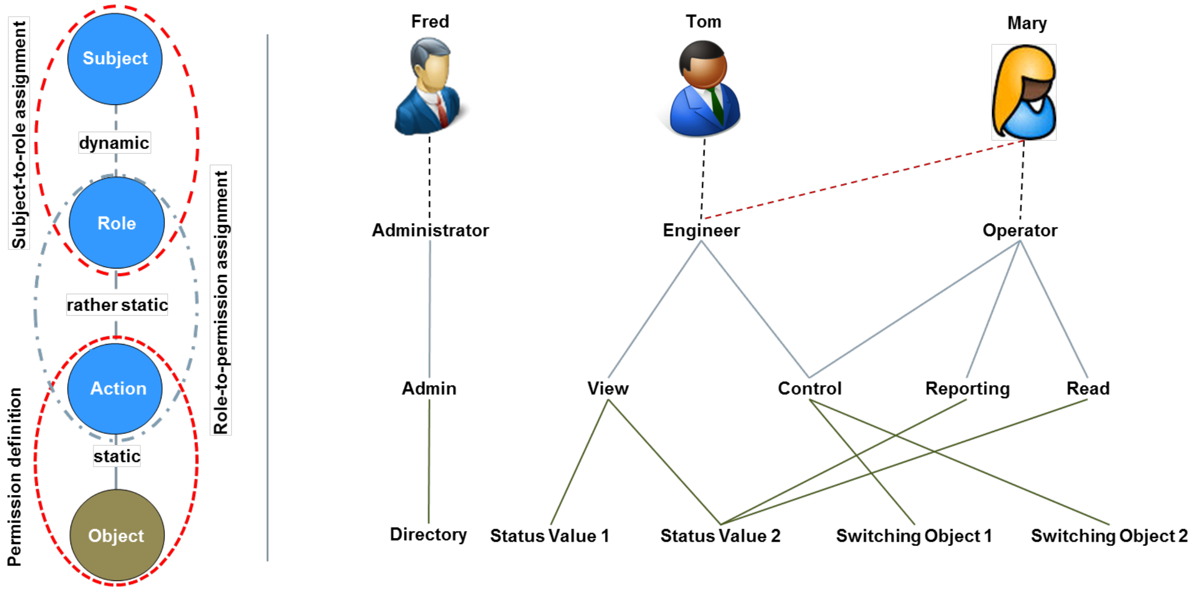


Figure 5-1: Role-based access control example (see also [14])

RBAC reduces complexity and costs for the security administration in networks and systems for a larger number of subjects. Subjects may be user applications, or devices. The basic approach assigns subject to roles to avoid the assignment of individual permissions. Figure 5-1 shows the general RBAC concept and the assignment of subjects to roles and roles to permissions. Permissions in turn constitute actions on objects. As shown, Tom is assigned the engineer role, which entitles him to view and control certain objects. The objects shown here are status values and switching objects.

An access control system can be defined as a system that restricts access to a resource to a authorized users. It builds on two main steps: authentication and authorization. When a user requests access to a physical resource it claims an identity and the authentication process will verify the validity of this claim. Authentication in access control typically involves the authentication of a person. Authorization is determining what a user is allowed to do. In the context of information security, access control mechanisms ensure that subjects are allowed to perform only authorized operations on objects in question. In other words, access control mechanisms enforce confidentiality, integrity and indirectly availability of a given protected object. Separation of Duty (SoD) is a key concept of internal controls (Figure 5-2). SoD, as it relates to security, has two primary objectives:

- Prevention of conflict of interest (real or apparent), wrongful acts, fraud, abuse and errors.
- Detection of control failures that include security breaches, information theft and circumvention of security controls.

SoD is designed to ensure that individuals do not have conflicting responsibilities or are not responsible for reporting on themselves or their superior. To these purposes RBAC for the energy automation environment is already considered in several requirements standards, guidelines, and in regulatory requirements to ensure a reliable operation of power systems.

RBAC enables an organization to subdivide super-user capabilities and package them into specific user accounts termed roles for assignment to dedicated individuals according to their job needs. This subdivision enables security policies to determine, who or what systems are permitted access to which resources (e.g., data) in other systems. RBAC thus provides a means of reallocating system controls as defined by the organization policy. In particular, RBAC can protect critical system operations from inadvertent (or deliberate) actions by unauthorized users. Clearly RBAC is not confined to human users though; it applies equally well to automated systems and software applications, i.e., software parts operating independent of user interactions.

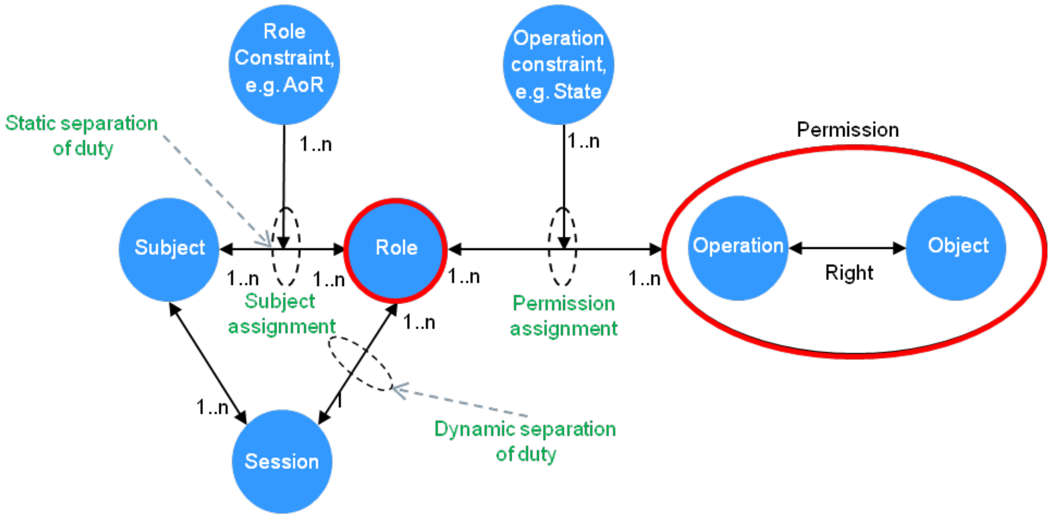


Figure 5-2: Diagram of RBAC with static and dynamic separation of duty (enhanced version of [ANSI INCITS 359-2004])

The main components of RBAC are: subject, role, session, right for operations, and objects.

- Subjects include human users, automated systems, and software applications. Examples for users or entities connected to RBAC in the power management system domain include a system engineer, SCADA system, outage management system, power flow application in an EMS, maintenance test application in a maintenance laptop.

- Roles can be associated with job functions within the context of an organization with some semantics associated regarding the authority and responsibility conferred on the subjects assigned to the role. Examples include transmission system operator, power scheduler, RTU maintenance, protection engineering.
- Sessions are the mapping of one subject to one or possibly many roles, thus indicating which roles a subject is allowed to take on. Each session is associated with a single subject and each subject is associated with one or more roles. One example is a human user allowed to act as system operator, a power scheduler, or a supervisor. Another example is a power flow application allowed to access a real-time dataset or to access a set of historical data in a database.
- Operations are the set of actions (verbs) that can be permitted or denied. Examples include get, set, report, log, create, or delete.
- Rights are the operations that are assigned to specific objects (e.g., data, services) within a particular object. Examples include viewing data (information on a screen), reading data (monitoring data, downloading documents), writing data (setting parameters, updating protection settings, updating assignment of subjects to roles), issuing control commands (issue trip command, enable function), configuring (updating firmware), and managing files (create and delete files)

Objects are the resources which separate the different rights that may be invoked. Examples include protective relays that separate the rights for reading protective parameters, for updating protective parameters, and for configuring the firmware.

5.1.2 Overview about role-based access control support in IEC 62351-8

5.1.2.1 Roles

IEC 62351-8 defines a minimum set of roles to be supported, but also allows a potential operator to define their own roles. The role information associated with a user is part of an access token, which can have different form factors like part of a public key certificate, or attribute certificate, a JSON web token, or part of a RADIUS response.

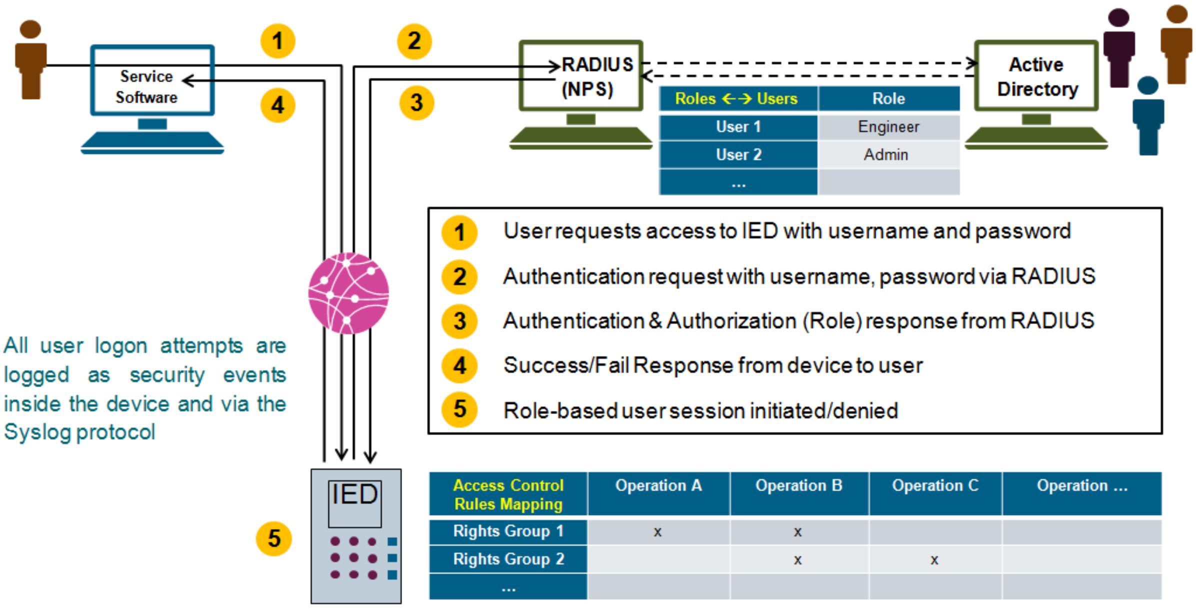
To ease the introduction of RBAC in operative power system networks, IEC 62351-8 allows to integrate RBAC using already established login process using username and password combinations. This approach relates in IEC 62351-8 to the PULL procedure and allows the accessed device to query the necessary RBAC information from, e.g., a central repository, like a LDAP or RADIUS server. It allows to utilize the access tokens in the backend communication, associated with users, without involving the user in the access token handling itself. As the access token is pulled by the IED this case is called “PULL”

In contrast IEC 62351-8 describes the fetching of role information by the user upfront delivering the RBAC information already as part of the request towards the accessed device. This approach is called PUSH. Note that PUSH cannot be done using RADIUS.

Both approaches, PUSH and PULL are described further in the next sub clauses on the example of remote access to a substation to query for instance fault recordings. Remote access needs specific security considerations as it provides an interface, to query information from a substation and to control properties of the substations. These actions need to be protected against unauthorized access, ideally through RBAC.

5.1.2.2 PULL

The PULL model defined in IEC 62351-8 allows a user to provide his credentials to the accessed supply (device or application or service), which in turn utilizes this information to query a central repository for the RBAC credentials of the accessing user. The approach is depicted as example in Figure 5-3.



Roles <-> Users	Role
User 1	Engineer
User 2	Admin
...	

1 User requests access to IED with username and password

2 Authentication request with username, password via RADIUS

3 Authentication & Authorization (Role) response from RADIUS

4 Success/Fail Response from device to user

5 Role-based user session initiated/denied

All user logon attempts are logged as security events inside the device and via the Syslog protocol

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

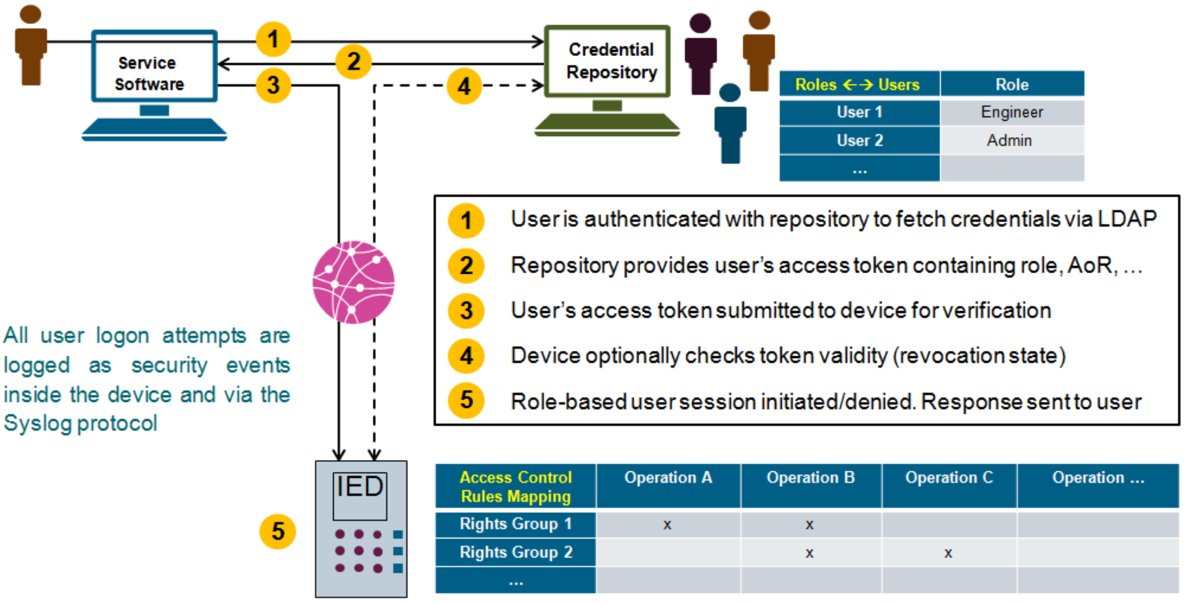
Figure 5-3: Example application of the RBAC PULL model

It is expected that system resources (devices and applications) will support the verification of RBAC credentials provided during remote access or also via the local HMI. To enable a unified interpretation of RBAC information IEC 6351-8 defines the format and the content of RBAC access token as stated above.

In the example in Figure 5-3 RBAC is achieved by using a RADIUS repository in the substation, here in combination with a Network Policy Server. After the user provides his credentials to the IED, the IED establishes a connection with the RADIUS server secured with IED specific credentials and queries the user related RBAC information. As shown, the user authentication may be performed against an active directory allowing the separation of user login information and RBAC to distinct domains. In the example shown, the user management can be done in the standard IT, while the specific RBAC handling is managed in the associated OT environment. This allows for IEC 62351-8 compliant RBAC, without requiring the user to change the currently used authentication approach.

5.1.2.3 PUSH

The PUSH model defined in IEC 62351-8 allows a user to fetch his credentials before accessing a device or application on a central repository and to provide these credentials to the device or application directly. This is shown in Figure 5-4.



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

1 User is authenticated with repository to fetch credentials via LDAP

2 Repository provides user's access token containing role, AoR, ...

3 User's access token submitted to device for verification

4 Device optionally checks token validity (revocation state)

5 Role-based user session initiated/denied. Response sent to user

All user logon attempts are logged as security events inside the device and via the Syslog protocol

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

Figure 5-4: Example application of the RBAC PUSH model

When using certificates this requires an existing PKI at the operator's side, which can be accessed by the users in contrast to the PULL model described above. Using the PUSH model also allows for RBAC, even if the controlled device is offline and has no connection to a central repository.

5.2 Certificate management in power systems

5.2.1 Overview

Application of IEC 62351-9 *by Marco Modica*

The planning of the PKI design is one of the most important aspects of PKI implementation since design influences the way certificates are validated and used by the solutions and equipment enabled to use them.

The design should include a certification chain that will contain a single internal root Certificate Authority (CA), which will use a self-signed CA certificate, at the top of the chain and several CAs subordinate, which will use CA certificates generated by the internal root CA (Figure 5-5).

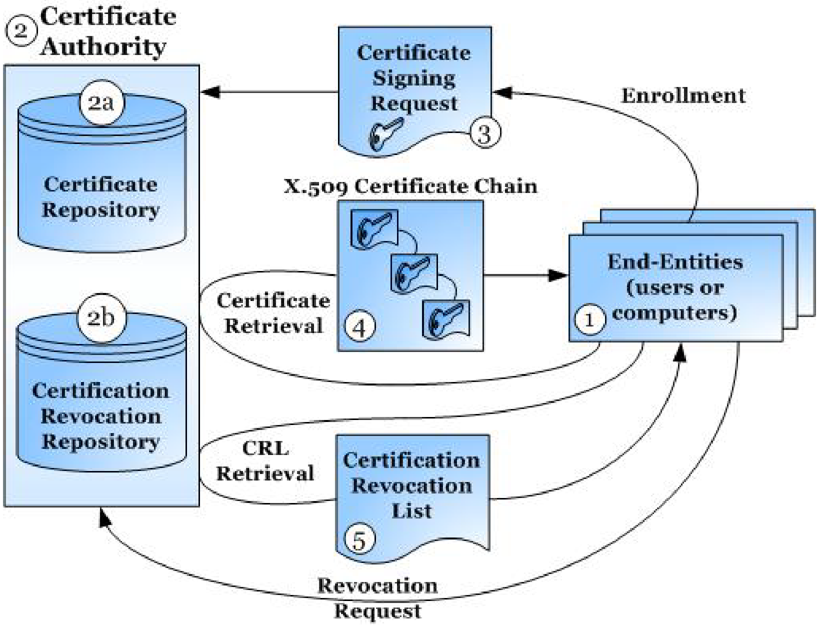


Figure 5-5: Logical-functional scheme of a CA

The solution requires the following components / features:

- Certification Authority for
  - generation of certificates for users, devices, Devices manufacturers and subCAs (with RSA keys);
  - generation of Certificate Revocation Lists (CRLs);
  - revocation of the certificates generated by the Certification Authority and / or its own subCAs;
  - generation of certificates for Attribute Authority (with RSA keys);
  - generation of Attributes Certificates;
  - CRLs available for use by users and devices through HTTP and LDAP protocol.
- Registration Authority
  - A registration authority (RA) is a subject to whom the CA has given specific mandate for carrying out one or more typical activities of the registration process, such as: identification of the applicant, registration of data, request to the CA, distribution of the certificate, etc. creation and distribution of Trust Anchor lists via RFC 7030 protocol [11](optional RFC 5934).

5.2.2 Operation

5.2.2.1 PKI operation schema

Figure 5-6 illustrates the PKI operation schema.

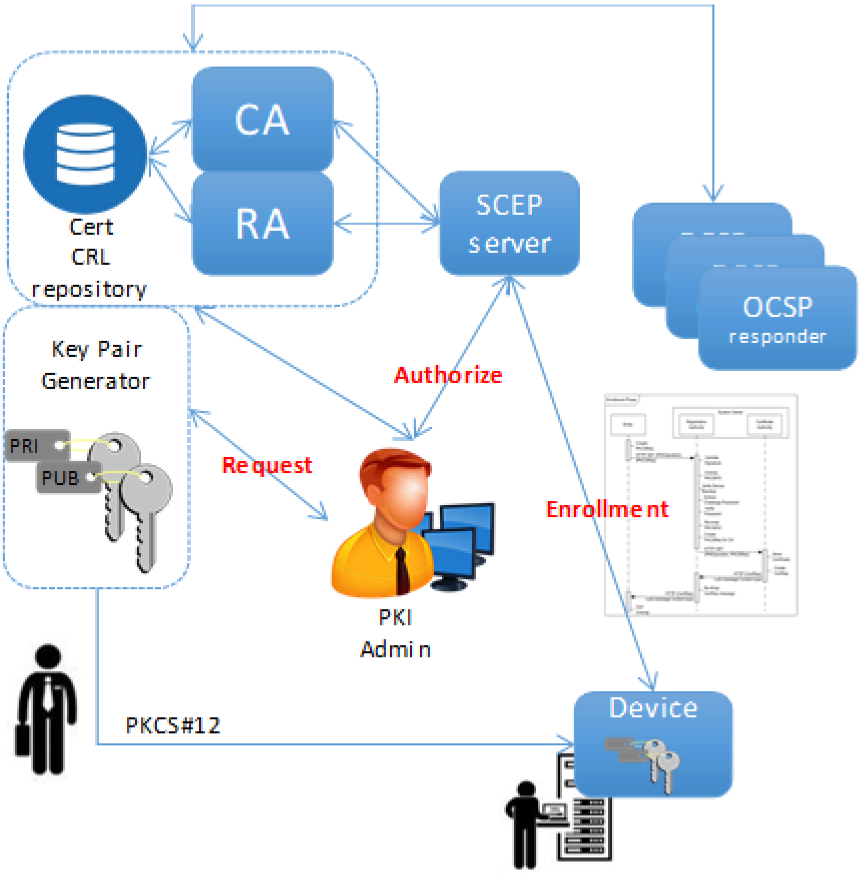


Figure 5-6: PKI operation schema

5.2.2.2 Enrollment of the device

This security procedure describes the process of generating the cryptographic keys associated with the certificate and the process of certification of the public key by the Certification Authority (CA).

Objective

Upon installation, the device must be equipped with one or more digital identities that will allow it to authenticate itself against the PKI infrastructure when connected. This digital identity is made up of Public Key Certificates in accordance with the X509v3 standard.

This security procedure describes the process of generating the cryptographic keys associated with this certificate and the process of certification of the public key by the Certification Authority (CA).

Prerequisites

The operations to be carried out for the completion of the enrollment procedure require the preparation of a PKI (Public Key Infrastructure) infrastructure equipped with a relative Registration Authority capable of exhibiting the standard enrollment services in accordance with the provisions in IEC 62351-9 [10] and in particular SCEP (Simple Certificate Enrollment Protocol) [12] and EST (Enrollment over Secure Transport) [11] services.

A coding process must also have been defined during the installation (or pre-installation on the device at the factory) of an enrollment key capable of activating the enrollment of the device itself. The enrollment key is a one-time password, every time this procedure must be performed a new enrollment key is required.

This procedure can be requested in the act of installing the device for the purpose of connecting to the network with authentication towards the remote management system.

Procedure Steps

1. The device is equipped in the factory with a shared enrollment key or the same key, communicated to the installer via a secure channel, is installed upon activation in the system. This key is associated with the identity of the device (Unique identifier of the device).
2. Once the device is connected to the telecommunications network, it checks the reachability of the Registration Authority end-point by sending a query message required by the protocol.
3. The device generates a pair of asymmetric keys (private key and public key) and generates a Certification request (CSR) by including the public key in the request itself.
4. The device sends the certification request to the Registration Authority via one of the enrollment protocols (SCEP or EST) and also enters the enrollment key in the data. If the request is malformed, the Registration Authority will reject this request.
5. The Registration Authority verifies the validity of the request (in turn using the enrollment key) and forwards the request for the signature of the Certificate containing the public key of the device to the Certification Authority.
6. The Certification Authority publishes the certificate and returns it to the Registration Authority.
7. The Registration Authority sends the Certificate to the device through the same enrollment protocol (SCEP or EST).

5.2.2.3 Certificate renewal

This procedure describes the certificate renewal process which consists of the generation of new cryptographic keys associated with this certificate and the public key certification process charged to the Certification Authority.

Objective

With adequate advance with respect to the expiry of the Certificate which represents the digital identity of the device, and which is used for TLS authentication, the device must send a renewal request to the same Registration Authority that issued the Certificate in expiry phase.

Prerequisites

The operations to be carried out for the completion of the certificate renewal phase require the availability of a PKI (Public Key Infrastructure) equipped with a related Registration Authority capable of exhibiting the standard enrollment services in accordance with the provisions of IEC 62351- 9 and in particular the SCEP

(Simple Certificate Enrollment Protocol) and EST (Enrollment over Secure Transport) services.

For the renewal request, the device will use the existing certificate, in a valid condition. It is therefore not necessary to prepare a new shared enrollment key. Particular attention should be paid to the time alignment between device and RA because this allows correct synchronization on the expiration of the certificate.

The recognition by the device of the condition of proximity to the expiration of the certificate (the expiry date is a field of the certificate itself) activates this safety procedure.

Procedure Steps

1. The device acknowledges that the certificate in use is nearing its expiry by comparing the current date with the expiry date and assessing whether the difference is less than expected.
2. The device verifies the reachability of the end-point of the Registration Authority.
3. The device generates a pair of asymmetric keys (private key and public key) and generates a Certification request (CSR) by including the public key in the request itself.
4. The device sends the Certification request to the Registration Authority using one of the enrollment protocols (SCEP or EST) using the current certificate that is still valid.
5. The Registration Authority verifies the validity of the request and forwards the request for signature of the certificate containing the public key of the device to the Certification Authority.
6. The Certification Authority publishes the certificate and returns it to the Registration Authority.
7. The Registration Authority sends the certificate to the device using the same enrollment protocol (SCEP or EST).

5.2.2.4 Certificate revocation

This security procedure describes the certificate revocation process.

Objective

In the event of a suspected compromise of the digital identity of the device (e.g., tampering) or in the event of transfer of ownership or control to another remote management system, it is necessary to revoke the possibility of access of the device to the previous remote management system.

Prerequisites

The device has a valid certificate. This safety procedure is activated when there is a notification of the condition of compromise or change of responsibility regarding the control of the device.

Procedure Steps

1. The Registration Authority receives a request for revocation of the device certificate from an authorized manager directly or via the API interface of the remote management system.

2. The Registration Authority verifies that the manager is authorized to revoke the specific certificate, if it is not, this procedure is interrupted.
3. In the event of a positive verification, the Registration Authority requests the Certification Authority (CA) to revoke the certificate and insert the relative Serial Number (serial number that identifies the device's certificate) in the Certificate Revocation List – CRL.
4. The CRL is published by the CRL Issuer or the CA, with a predefined frequency (minimum every 24 hours).
5. In the face of each new realtime verification (via OCSP protocol) the certificate will be reported as revoked.

5.2.2.5 Checking the validity of the certificate through revocation lists

Revocation lists include:

- Internet-connected (CRL - Certificate Revocation List)
- Realtime (OCSP - Online Certificate Status Protocol)

This safety procedure is activated during periodic verification, with a frequency consistent with the publication of new CRLs.

Objective

This security procedure describes the process of verifying the certificate (which represents the digital identity of the device) or the certificate of the remote management system.

Prerequisites

To activate this safety procedure, the device must be equipped with a valid certificate or if the remote management system is being verified, the remote management system must be equipped with a valid certificate.

Procedure Steps

1. The device checks (optional) that the certificate of the remote management system is not present in the latest version of the revocation list referenced in the certificate itself. This verification can take place by:
   a. Periodic download of the CRL
   b. OCSP request to the OCSP responder (specific server of the OCSP protocol) of the PKI.
2. The remote management system checks that the device certificate is not present in the latest version of the revocation list referenced in the certificate itself. This verification can take place by:
   a) Periodic download of the CRL
   b) OCSP request to the OCSP responder (specific server of the OCSP protocol) of the PKI
3. Depending on the option chosen for each of the previous steps:
   c) The CRL is examined, and the certificate is not revoked or revoked.

d) The OCSP responder returns the status of the certificate: valid or revoked.

4. In case of certificate revoked, if an over TLS connection is active, it is deactivated. If, on the other hand, this procedure is carried out when an attempt is made to establish a connection, in the case of a certificate revoked, it is not established.

The CRL is published on a predefined basis (minimum every 24 hours).

5.3 Network and system management

Application of IEC 62351-7 by Moreno Carullo and Gigi Pugni

The remote control systems of the energy generation and transport systems are based on the use of a series of tools:

- Geographic telecommunications networks;
- Local plant networks;
- Intelligent Electronic Devices (IED);
- Local SCADA system systems;
- Central SCADA systems.

Each of these objects contributes to the remote control of the real infrastructures of the electrical system. Through this system, SCADA is able to reliably control the automation system, providing that the operativity of the system is always available and working well, and also that there is no anomalous state or behavior during the automation process. We must remember that the communication between different networks, the growing power and interaction capacity of the new generation remote control systems exposes them to a series of risks, for example:

- Software errors, which can occur spontaneously in the form of malfunctions;
- Software vulnerabilities;
- Communication Problems (packet loss, delays, periodic disconnections), which can cause the loss of the equipment visibility;
- Hardware anomalies (for example power supplies, batteries, memory) that become evident only at the time of the failure;
- Malware, which can cause abnormal use of device resources.

In many cases the recognition of an event or a potential risk situation is possible through the correlation of monitoring information from more than one element, mostly in presence of intrusion attempts, which often occur progressively first towards the network devices and then towards the end-points. These are minor cases where the anomaly or an event is an individual situation that is not related to other anomaly behaviors.

For this reason, it is appropriate and necessary to collect and correlate by a unified infrastructure the events and the status of the systems, capable of collecting, classifying, and correlating the events and identifying the operating status of each device. It doesn´t matter if it belongs to the domain remote control systems (IED, SCADA, etc.) or to the domain of communication and support infrastructures (firewall, IDS / IPS, router, switch etc.).

Integrated monitoring of systems through a Network and System Management infrastructure (NSM) have long been a cornerstone for telecommunications operators and ICT providers, who have equipped themselves with adequate monitoring tools and protocols and also have organizational processes aimed at this purpose.

This fact suggests the use of technological solutions to integrate the monitoring of the events and states of the systems at Enterprise level, in a high profile NSM infrastructure to manage the network and IT systems. The adoption of integrated NSM systems at Enterprise level offers the possibility to obtain the correlation of security events not only from the process environment, but also from the management environment, with which moreover, recently the process systems are used to interact to respond to the business needs of an open market.

5.3.1 The IEC62351-7 standard

The entire remote control infrastructure must be protected and reliable to guarantee the safety and reliability of operations on electrical systems. This also involves the implementation of the monitoring actions required to recognize the symptoms of the anomalies and associate them with a possible threat, adopting the appropriate countermeasures as far as possible.

From an operational point of view, safety can be implemented according to several levels of intervention:

- Deterrence and delay, trying to avoid attacks, or at least delay them long enough to prepare adequate countermeasures.
- Detection of attacks: detection is essential for all other security measures because when you are not able to recognize a possible attack, you cannot prevent it. IDS solutions can perform an important role in helping with attack detection.
- Risk Evaluation of the attack, to determine the nature and severity of the attack. For example, it is necessary to assess and analyze if the attack compromises the availability, confidentiality or integrity of the environment, or whether the attack is just a nuisance.
- Communication and notification, so managers and systems can be aware of the attack in a timely manner.
- Attack Response strategy, which includes actions by those responsible for mitigating the effect of the attack in a timely manner. This response can then prevent or delay a subsequent attack.

In this context, the NSM infrastructure has an important role implementing the following:

- Monitoring the status of software applications, hardware devices and communications. This monitoring action can provide notification of status changes, such as equipment failures, abnormal configuration changes, software errors or failures, temporary communication interruptions and permanent communication failures.
- Monitoring the performance of systems and communications. This data collection and correlation of information is able to record the conditions of data traffic, changes

in the performance of software applications, changes in the flow of data (in volume and type), communication performance results, etc.

- Intrusion Detection. Not only the obvious intrusions, but this detection must be sensitive to "normal" conditions, to attempt to detect even the slightest changes in the context that could be a symptom of an intrusion. This intrusion detection naturally uses the information obtained through status monitoring and performance monitoring (e.g., identify if an DDOS is a UDP flood, ICMP flood, NTP amplification, Zero-day-based exploit attack, etc.).
- Configuration Management. The configuration of equipment, communication networks and systems can be managed, either by defining automatic changes based on events (for example by activating new rules on firewalls in case of an attack recognized by a virus), or by manually selecting a new configuration, or when a new component/equipment is activated.

NSM infrastructures are already constantly used for the monitoring and control of telecommunications infrastructures, including those supporting the process networks, but the information collected is unfortunately limited to the operativity of the network systems (router firewall and IDS). The monitoring is carried out by the operators who manage the telecommunications system and often this monitoring does not include the network equipment belonging to the LAN plant, and all this information could contribute to the information gathering.

Part 7 of the IEC 62351 standard intends to fill this gap by first introducing the concept of monitoring the remote control network, also including the part related to the automation system and then also assigning an active role to the remote control and automation components, as a source of information for monitoring.

According to part 7, the components of the remote control systems (SCADA, RTU, IED ...) must be able to use the values already stored in their own software and share this information with NSM infrastructure when requested. To do that, providers must develop monitoring and control objects inside the hardware devices to permit NSM to monitor these devices and analyze this information, using MIBs, in spontaneous generation of events or when information is requested by NSM. In addition, spontaneous generation of events is similar to what has already been prepared for IT network equipment. When implemented, remote control devices can alert the NSM infrastructure even when a particular critical situation is in progress.

The standard introduces the concepts related to the definition of specific objects intended for the monitoring of remote control and automation systems, detailing specific classes of quantities and values that can be controlled by the NSM system.

This definition takes place according to an abstraction criterion, independent of the utilized protocol, to permit monitoring solutions based on different objects.

However, the standard is inspired by the monitoring systems based on the SNMP (Simple Network Management Protocol) protocol, which represents the classically used tool for monitoring computer networks, but in this case mapping and monitoring objects belonging to the process network, for example based on IEC 61850.

SNMP has the advantage of allowing rapid integration of new objects within the existing NSM infrastructure, which is responsible for monitoring network communications and ICT systems.

The aim is to implement a demonstration in the field of the integrated monitoring solution of remote control systems and network systems, obtaining a more exhaustive correlation of events and a more complete system status, while enhancing the investments already made in NSM systems existing.

5.3.2 Data object model

To obtain integrated monitoring of the entities involved in the field of remote control systems, standard 62351-7 uses an abstract object model, which can be simple, i.e. associated for example with a Boolean or numerical value, and more frequently structured objects that are recursively made up of simple objects or additional structures. The standard provides that each object, in addition to the values associated with it, includes some essential fields (Figure 5-7) including:

- the "ID" of the “data object” to be monitored, which represents the unique identifier of the element being monitored (IED, Communication channel or other);
- the "object name", which represents the identity of the "data object";
- Quality indicator of the Data value, essential for assessing the reliability of the “data object”;
- the time stamp of the event.

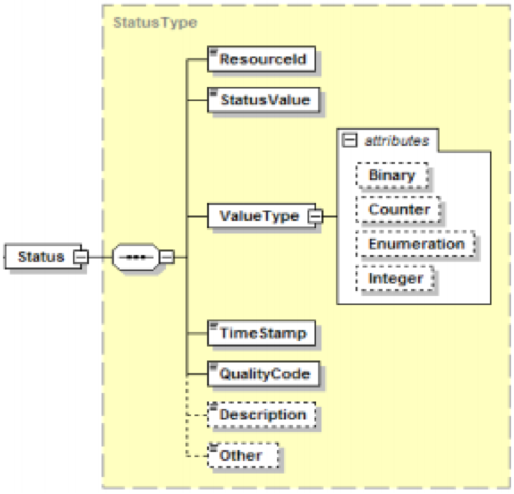


Figure 5-7: object fields

Objects can be read-only or read-write.

The standard introduces some categories of objects organized in three main levels. The first level includes the monitoring of the “Networks and Protocols” and it is aimed at observing the behavior of the communication with attention to the following aspects:

- Network Configuration Monitoring and Control, which concerns the monitoring and management of the network intended as an entire infrastructure and as individual components, including endpoints, routers, switches, etc.

- Network Backup Monitoring, meaning that the state of health of the backup infrastructures must be kept under constant observation.
- Network Communications Failures and Degradation Monitoring. This class of objects is aimed at highlighting changes in the performance and reliability of network components even when these anomalous behaviors do not typify a failure. The aim is to recognize in a preventive way a state of potential degradation and to intervene promptly with the appropriate countermeasures.
- Communication Protocol Monitoring, with the aim of recognizing anomalous situations that may derive from malformed or tampered messages, attempts to Denial of Service (perhaps with the intention of causing buffer overflow). In concrete terms, the purpose is to collect the "health status" of the application communication, to collect the statistics on communication and the information on anomalous situations that can be surprisingly numerous.

The second level concerns the monitoring of the "End Systems", to get information on the operating status of the endpoints. They can be the IED or the SCADA:

- Monitoring End Systems. For each of these entities, a series of objects is defined in the standard which allows evaluating the coherence of the actual state and values of the device and the values previously defined.
- Security Control and Management of End Systems. Standard values are given to endpoint security objects, which like the others are subject to collection, control and consistency checks.

The third level concerns to the Intrusion Detection:

- Reporting of "Unauthorized Access", the recognition of unauthorized access attempts to a resource.
- Recognition of Resource Exhaustion due to a Denial of Service (DoS) attack.
- Recognition and reporting of Buffer Overflows following DoS attacks.
- Recognition and counting of altered or malformed PDUs.
- Reporting of physical access attempts included tampering in an energy meter.
- Reporting of not allowed accesses from Network Addresses.

These series of information, collected by the endpoints and network systems, make up the remote control infrastructure, represent a real valuable information that can and must be used to recognize the health of the entire system as well as individual components.

It means that each element of the infrastructure, in accordance with IEC 62351-7, has a sort of internal image of its status and performance, compared to a certain variable number of monitoring and control objects that describe its status, performance and which can be used (when writable) to change some of its behaviors.

5.3.3 Architecture of the network monitoring system

Each element of the system brings a significant potential complexity, so it becomes difficult to manage when considering the whole system. The amount of information available can be so much to easily overcome the amount of information classically exchanged for the exercise of the functions of the remote control systems.

For this reason, it´s so important to define the best interrogation technique of these objects and the most efficient architecture of the monitoring system adopted by the central monitoring system.

The objects described in section 5.3.2 can be received in different times and ways:

- **unsolicited manner**. The “data object” send spontaneous information to the central monitoring system, when the value of the variable exceed the specific value previously defined (for example in case of alarm, high temperature, dangerous, etc.);
- **interrogation by the Central System**. Through interrogation by the central system, with long (daily) intervals. However, for many objects a constant collection of values is not necessary, especially if a complementary solution of unsolicited sending messages has been adopted;
- **frequent interrogation by the Central System**. This method is used to obtain a detailed trend over time of some values associated with specific objects. This method assumes more intense network traffic (and a greater commitment of resources on the endpoint) and is usually used as a technique for deepening the information collected with other methods.

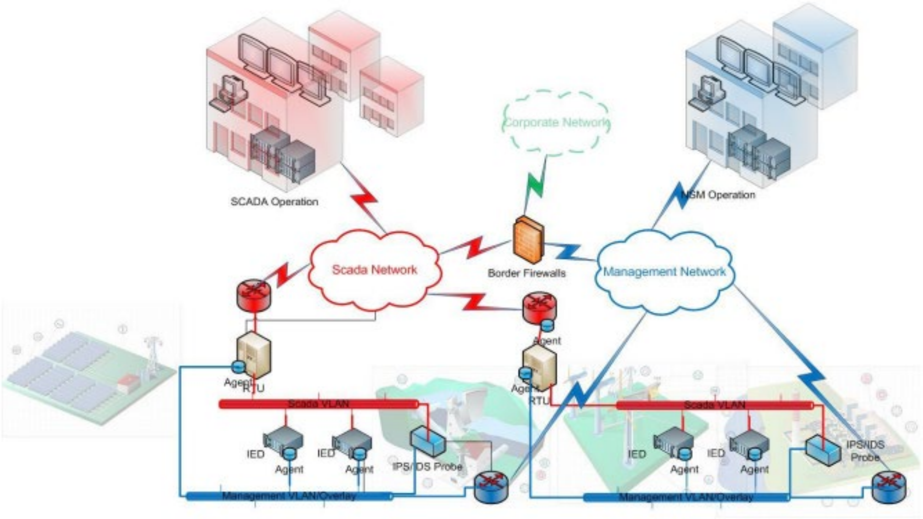


Figure 5-8: Monitoring System Architecture

Figure 5-8 shows the hierarchy of collection of events and variables from the various elements of the remote control system.

The upper hierarchical level is represented by the central NSM system which has the task of collecting information from the different components of the telecommunications network and from the devices belonging to the remote control system.

As previously mentioned, the choice of protocols used for communication is, according to standard 62351-7, open with the intention of mapping objects using different protocols. For this reason, the NSM central system can monitor and assume the physiognomy of technological objects from both the world of telecommunications/ICT systems and from the SCADA world.

The telecommunications infrastructure assigned to the NSM is logically segregated from the remote control support network to underline the different “responsibility” and business strategy of the two services.

Even for reasons related to the Separation of Duties and to increase the resilience, the monitoring and control of the health state of the infrastructure, it should be delegated to managers (and potentially to control centers) other than those who are responsible for the exercise of the remote control (this aspect is also highlighted in the diagram). Within the telecommunications network, in addition to the remote control objects, numerous elements belonging to the network itself (router, switch) are also represented, as well as devices that are responsible for managing security network (firewall, IDS / IPS).

5.3.4 Monitoring protocols

The "agent" is that software / hardware entity responsible for the management of monitoring objects (at a single end point lever, for example, those in the class of network interfaces). Each endpoint (or other network element) can host different types of agents to manage classes of objects belonging to the different logical levels (from the network communication level to the application level).

The agent constitutes the translation point between the logical objects (NSM data objects) described in the standard in the specific elements provided by the management protocol.

The SNMP and IEC 61850 protocols are structured according to an object paradigm that goes naturally with the logic of the IEC 62351-7 standard and represent a natural display of the central monitoring functionality towards two NSM worlds: the classic Telco / ICT and SCADA

Both protocols offer advantages and points of attention. The IEC 61850 protocol is designed to monitor electrical infrastructure objects by collecting information quickly and efficiently from a large number of distributed devices and allows the well-timed execution of commands. Its adoption as a monitoring protocol will become natural when its diffusion is adequate at central SCADA systems level, keeping separate the role of NSM central system.

SNMP is universally adopted in the Telco / ICT field and the Utilities normally use an NSM infrastructure for monitoring and control through this protocol. The mapping of NSM data objects of the 62351-7 standard can be performed negotiable and manageable on SNMP MIBs. In addition to the possibility of inheriting the monitoring of existing network and security devices, SNMP also allows to inherit the logical objects relating to the network components which are already well described in the related MIBs, allowing focusing attention on the definition of the necessary MIBs to define the specific objects of IEC 62351-7.

So, the approach that has been considered will involve the use of the SNMP protocol.

We have also considered some limitations and possible critical issues that the use of SMNP in a remote control environment can involve:

- **Protocol Security**: only the latest version (SNMPv3) of the protocol provides an encryption and authentication mechanism and therefore the adoption of this version is mandatory.

- **Resources use and scalability:** It is necessary to define a correct sizing of the architecture and monitoring processes (to identify the resources used at the endpoint level and for the potential network traffic generated)

Based on the needs expressed, the IEC 62351-7 standard will have to be revised to include the mapping to the monitoring protocols mentioned and the whole of the monitoring objects will also be refined.

5.3.5 Security and priority between monitoring and remote control traffic

Based on the considerations expressed in the previous chapter, regarding the possible invasiveness of monitoring, certain precautions should be provided, to avoid that remote control traffic could be penalized by a possible intrusion of the systems monitoring.

It is already known the problem of the segregation of the NSM protocols concerning to the “application protocols” (in our case are the ones specific of remote control)

In the telecommunication network, it is often adopted the transportation of many logic networks utilizing the same physical infrastructure. For example, in a LAN network, it means that the traffic can be segregated configuring different VLANs, and in a geographic network, it is possible to segregate the MPLS network. Alternatively, it is possible to fix it by adopting solutions of encryption network connections to protect the network communication.

5.3.6 Integrating the remote control and network monitoring systems

The activation of monitoring via SNMP facilitates the integration of the components of the telecontrol infrastructures within the monitoring system already used for network and ICT infrastructures.

Because of the synoptic tradition and the similarity of the structure, it is possible to obtain an almost automatic integration of new objects within the network management and correlate all the generated security events and alarms utilizing the already existing correlation systems tool.

This integration does not only concern aspects of the technological nature, but also valorizes and makes use of the organizational processes that are already well-established for the management of the central NMS. The adoption and the implementation of an NSM structure configure, in addition to the technical aspects, the preparation of an organizational and process-related structure (including risk and crisis management processes).

When you already have an implemented NSM system in the ICT Network, the convergence of the system can accelerate the monitoring system implementation on the remote network system. It can also bring a consolidated and integrated view of all cybersecurity issues, vulnerabilities and risks inside the company (OT and IT). It required it could be possible to organize the integrated dashboards with different views according to eventually necessity, from technical to managerial, giving an integrated and homogeneous view of risk for all company systems.

It represents the possibility of using SCADA protocols (for example IEC 61850) for monitoring functions, with a longer-term perspective, and contribute to add the vision of “what happens in the plant”, giving to the user a more detailed series of information regarding the remote control systems, in operational and cybersecurity levels.

6 Part III: IEC 62351 performance evaluations and security monitoring

6.1 Performance evaluation of DER – substation communications

6.1.1 Voltage control in active grids

Application of IEC 62351-10, IEC 62351-4, IEC 62351-3 by Giovanna Dondossola, Mauro Giuseppe Todeschini, Roberta Terruggia

The connection of DERs to medium voltage grids can influence the state of the power grid, affecting the capacity of the DSO to comply with the terms contracted with the TSO (Transmission System Operator) and can have an impact on the quality of service of their neighbor grids. To maintain stable voltages in the distribution grids a Voltage Control (VC) function has been designed to monitor the grid status acquiring field measurements and to compute optimized set points for the available flexible assets such as DERs, flexible loads and power loads communicate with the controller via the DER/Flexible loads communication network, possibly deploying heterogeneous communication technologies. The system level outlay of the voltage control function is shown in Figure 6-1. The VC function is performed by a controller that is a node of a HV/MV substation control network. To compute an optimized voltage profile, the algorithm needs to communicate both with components inside the DSO area, and with systems outside the DSO domain.

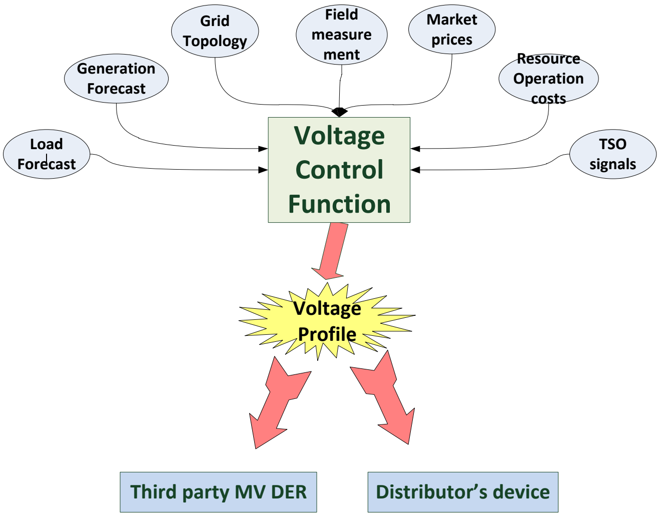


Figure 6-1: Voltage Control Function

The ICT infrastructure required for the operation of the Voltage Control functionality has to be secured implementing different secure measures (IEC 62351-10). In Figure 6-2 an overview of the secure architecture is presented.

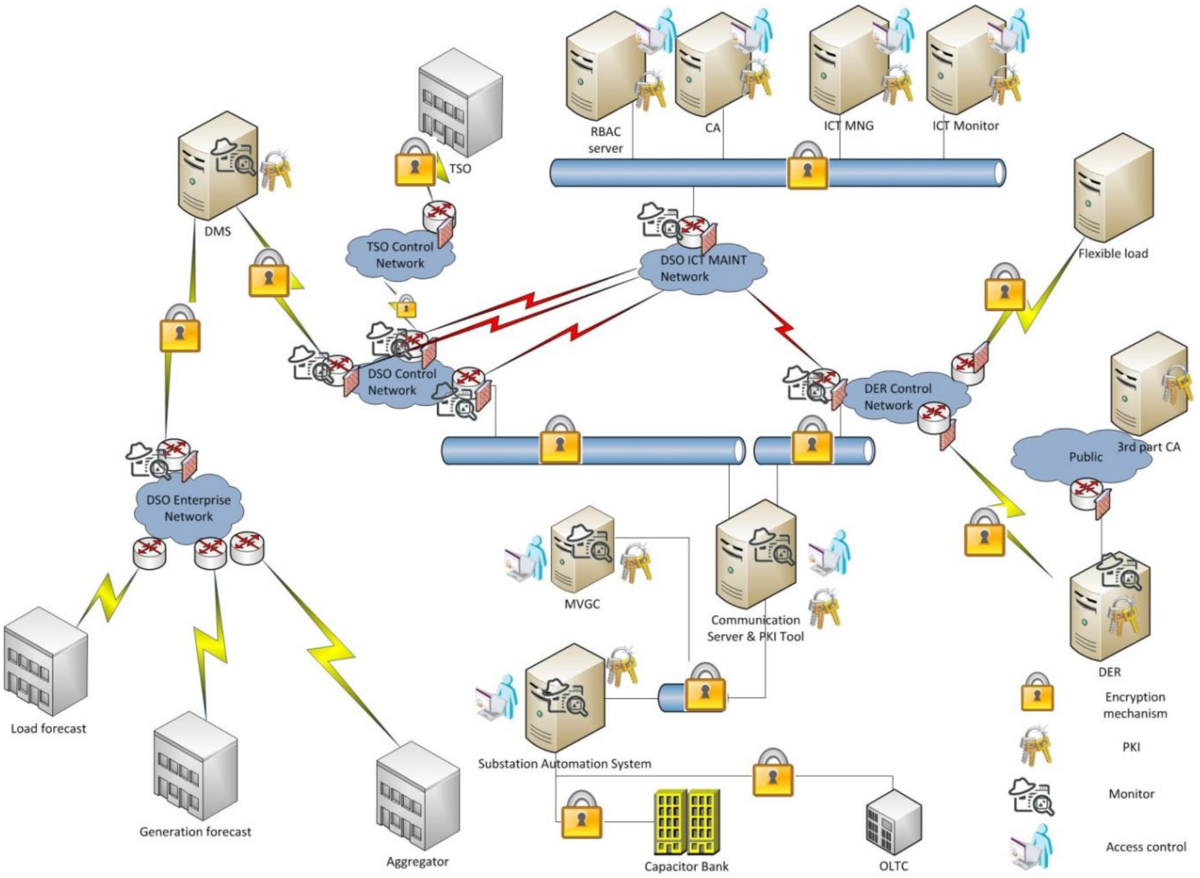


Figure 6-2: Secure Architecture

6.1.2 Test bed layout

To evaluate the applicability of the IEC 62351 series a test platform has been set up in RSE PCS-ResTest Lab (Power Control Systems – Resilience Testing Laboratory) for running cyber security experiments over realistic VC scenarios in the operation of active grids. Figure 6-3 illustrates the simplified view of the physical setup deployed for the experimental analysis. At the logical level the test bed consists of a set of software building blocks including in particular:

- **HV/MV substation network:** each substation includes automation, communication, SCADA and Operator HMI functions. At each substation the behavior of the electrical process is simulated by a Field Simulator application that cyclically reads and updates a virtual I/O interface. The substation hosts the client module managing substation-DER communications.
- **DER sites:** 4 large DERs sites connected to the HV/MV substation through the server module.
- **DER control networks** connecting each DSO substation with multiple third party DER sites located in different geographical areas deploying heterogeneous communication technologies.

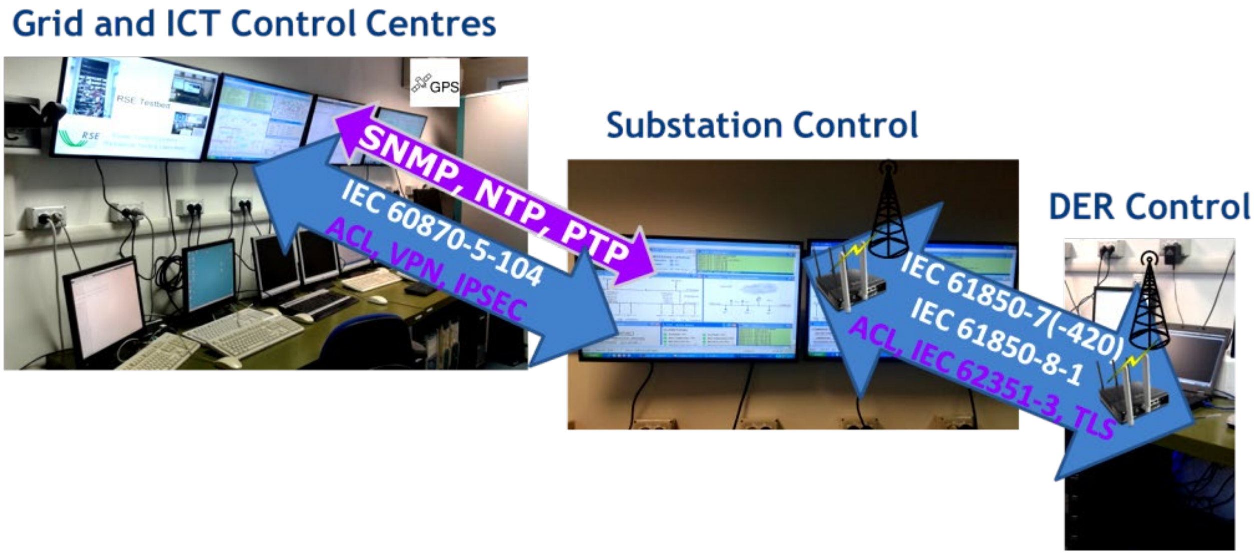


Figure 6-3: Test Bed Layout

6.1.3 Security tests with mobile communications

To evaluate the performance of cellular M2M network technologies (e.g., LTE/4G, 3G and 2G) that enable the connection of DER sites with the DSO substations, one DER site in the test bed is connected to the substation through a wired Ethernet VLAN (Virtual Local Area Network) as the baseline test, and three DER sites (located in the RSE test facility and in other places in the Milan area) are connected via a cellular network. Data from substation and DER move in and out being routed through the M2M LTE network, by proper LTE SIM cards inside 4G routers configured with private static IP addresses. Both the primary substation and the DER rely on their own Ethernet based LAN and connect to the mobile access network via LTE routers, through a GRE (Generic Routing Encapsulation) tunnel configured on both sides (Figure 6-4).

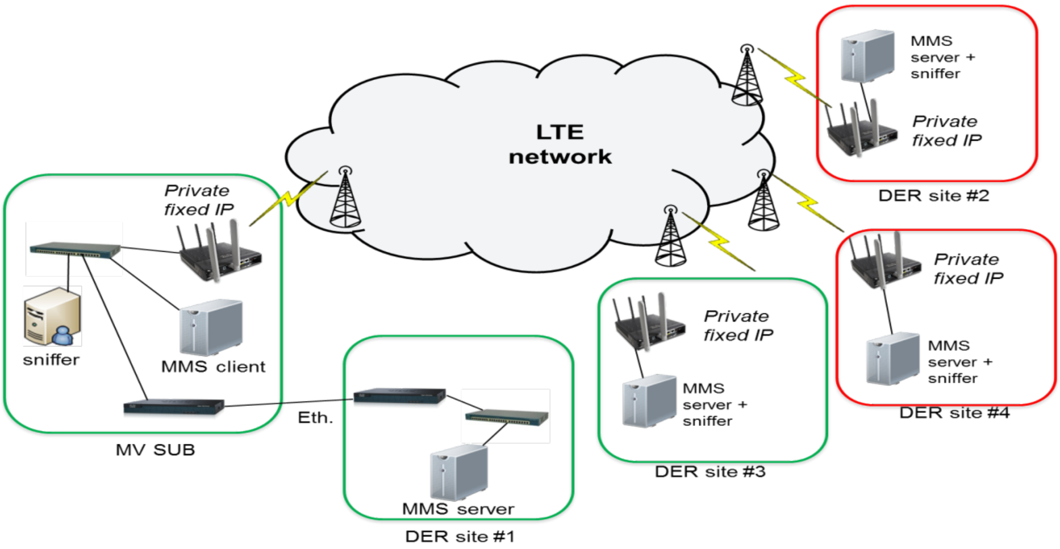


Figure 6-4: 4G network configuration

6.1.4 Client and server test application based on IEC 61850

MMS information exchange between DERs and substations, related to the VC scenarios, is provided by a test client-server application: the server application is associated to the DER site while the client resides on the substation SCADA. The client establishes an MMS session with the server, requests the transmission of the IED's profile (as specified by IEC61850), then enables a report control block provided by the server requiring the transmission of periodical information reports. The number of reports to be sent by the server and the interval between the emission of two consecutive reports are configurable. Report transmission causes the information flow from the server towards the client. To generate the information flow in the other direction, from the client towards the server the test client can be instructed by the user, to send setpoints on a periodic basis. Also, in this case the period is configurable. The client-server application is implemented on top of the API provided by the libIEC61850 library [9] to implement the most important MMS services needed by IEC 61850 and the secure T-Profile compliant with IEC 62351-4.

6.1.5 Test cases

The medium voltage control test bed focusses on the core control and communication components for the voltage control use case. Also, the components supporting ICT maintenance and monitoring functions are integrated in the test bed. Up to now, the tests carried out on our test bed as described in the above sections, can be grouped into two comparable test classes verifying the behavior of communication under the following security measures:

- **Plain Security**: tests verifying the VC communications with basic security measures, i.e., access control to communication gateways. These tests aim at checking the plain communications among DSO substations and DER sites. Both Ethernet and cellular technologies are tested to be compared with each other according to several performance criteria.
- **Standard Security**: tests verifying the VC communications with enhanced security measures as suggested by IEC 62351 Part 4 in T-Profile (currently including TLS profile recommended by IEC 62351-3).

6.1.5.1 Methods and results

To stress the various aspects of the protocols involved, two scenarios have been setup:

- **short tests**: repeated runs (i.e., 10 runs) of relatively short test (50 reports sent from MMS server and setpoints sent from MMS client);
- **long tests**: a single run of MMS where thousand (i.e., 2000/50000) of reports and setpoints are emitted by the MMS server and setpoints by the MMS client respectively.

These different scenarios are used to obtain relevant estimation of the metrics described in the next subsection. The first scenario is used to evaluate the mean time of the indicators related to the handshake and session setup, the second one provides report and setpoints statistics.

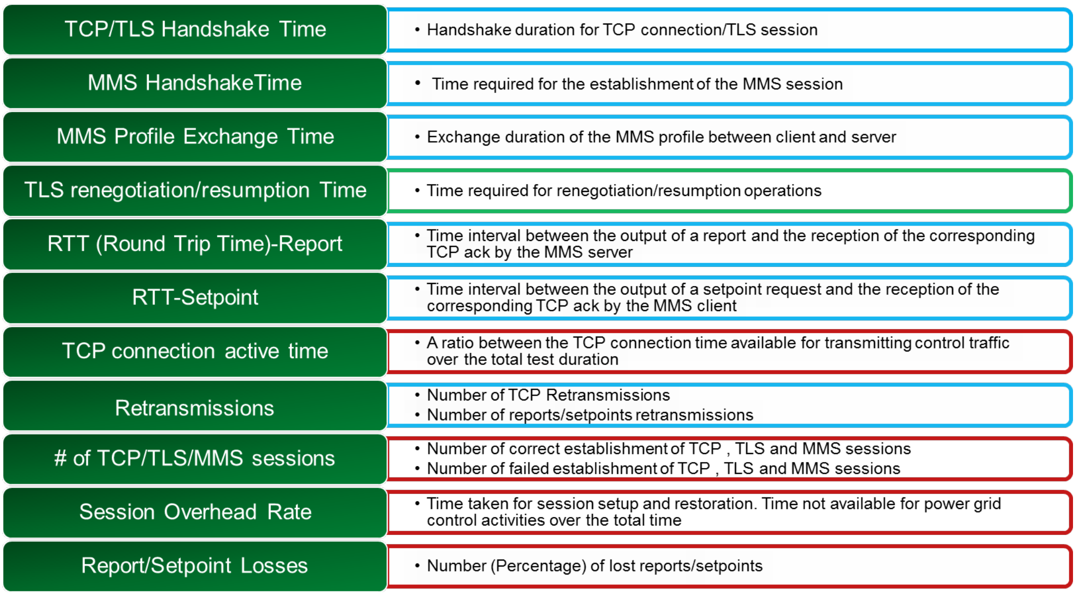
6.1.5.2 Metrics

The traces achieved during the test session have been analyzed through a customer-built tool that is able to extract and calculate several interesting indicators. The trace Analyser is used to obtain the values of the following performance indicators:

- TCP/TLS Handshake Time: handshake duration for TCP connection/TLS session.
- TLS renegotiation/resumption Time: the time required for renegotiation/resumption operations.
- MMS handshake Time: the time required for the establishment of the MMS session.
- MMS Profile Exchange Time: the exchange duration of the MMS profile between client and server.
- RTT (Round Trip Time)-Report: the time interval between the output of a report and the reception of the corresponding TCP acknowledgment by the MMS server.
- RTT-Setpoint: the time interval between the output of a setpoint request and the reception of the corresponding TCP acknowledgment by the MMS client.
- Inter-Report Time or Inter-Setpoint Time: the time interval between each two consecutive reports or setpoints, respectively.
- Number of TCP Retransmissions for a report or a setpoint.

The Standard Security test trace analysis required a way to perform the deep packet inspection. The tool implements the “Private key sharing” solution referred in part 90-2 of the IEC 62351 for deep packet inspection operation on encrypted channels.

From this base set of indicators more others can be evaluated. In Figure 6-5 some of them used in the evaluation are presented.



TCP/TLS Handshake Time	• Handshake duration for TCP connection/TLS session
MMS HandshakeTime	• Time required for the establishment of the MMS session
MMS Profile Exchange Time	• Exchange duration of the MMS profile between client and server
TLS renegotiation/resumption Time	• Time required for renegotiation/resumption operations
RTT (Round Trip Time)-Report	• Time interval between the output of a report and the reception of the corresponding TCP ack by the MMS server
RTT-Setpoint	• Time interval between the output of a setpoint request and the reception of the corresponding TCP ack by the MMS client
TCP connection active time	• A ratio between the TCP connection time available for transmitting control traffic over the total test duration
Retransmissions	• Number of TCP Retransmissions • Number of reports/setpoints retransmissions
# of TCP/TLS/MMS sessions	• Number of correct establishment of TCP , TLS and MMS sessions • Number of failed establishment of TCP , TLS and MMS sessions
Session Overhead Rate	• Time taken for session setup and restoration. Time not available for power grid control activities over the total time
Report/Setpoint Losses	• Number (Percentage) of lost reports/setpoints

Figure 6-5: Performance Evaluation Metrics

6.1.5.3 Analysis

Table 6-1 lists the average values for time metrics, e.g., TCP/TLS handshake time, MMS profile exchange time or RTT-Report etc., for the test scenarios. The values are extracted from the two test groups. Short tests provide the best approximation for the metrics considering handshake and session/profile exchange because in these tests we have different runs. Long tests have been used to estimate Renegotiation time, RTT- Setpoint and RTT-Report thanks to the thousands of reports and setpoints included in the test. The packet size has a strong impact on the time value of the indicators. The profile size influences the handshake times. The profile size is 2914 byte, the report packet size is 230 (259 with TLS).

6.1.5.3.1 TLS performance

The inclusion of the security of communication allows to achieve a lot of benefit in terms of integrity and confidentiality, but it is also important to evaluate the impact on availability: test the overhead of the inclusion of the TLS allows to have a clearer view of the effects of the IEC 62351-4 T-Profile integration.

The overhead brought by TLS on the different metrics can be easily taken from Table 6-1 considering the Ethernet network as base case. The results show that the inclusion of the TLS causes the increase of the time for each single communication phase and introduces an extra time of 0.047849 sec for the TLS handshake. We can conclude that the total time for the initial handshake and session phases is 0.107455 sec without TLS and 0.155647 sec including TLS security which means an overhead of 0.048192 sec corresponding to an increment of 44.84% of the total time. Considering only the MMS Handshake and Profile Exchange Time indicators the impact of TLS is not so consistent. Also considering the RTT-Report and RTT-Setpoint indicators it is possible to note that the impact on the time is irrelevant (0.000004 sec and 0.000293 sec). Similar results may be inferred analyzing the trace from the 4G cellular test. Here it is important to consider the bias due to the unpredictability typical of the mobile networks for the presence of variable background traffic.

Table 6-1 Analysis results

Test Case	Network	Metrics (time in seconds)								
		TCP Handshake Time	*TLS Handshake Time*	*TLS Renegotiation Time*	*MMS Handshake Time*	*MMS Profile Exchange Time*	*Total Handshake Time*	*RTT-Report*	*RTT-Setpoint*	*Retrasmission*
Plain Security	ETH	0.000986	-	-	0.002477	0.103992	0.107455	0.001153	0.001411	0
	4G	0.04966	-	-	0.115076	0.308075	0.472811	0.12716	0.107341	3
Standard Security (TLS)	ETH	0.001159	0.047849	0.044036	0.002729	0.103911	0.155647	0.001157	0.001704	0
	4G	0.054625	0.132415	0.176210	0.076725	0.343444	0.607209	0.101212	0.107154	1.877778
	3G	0.390826	1.229483	0.431360	0.54844	2.451566	4.620315	0.506906	0.498593	2.885417
	2G	2.003555	5.64858	4.568160	3.694058	11.99704	23.34323	2.293466	2.293621	8.066667

6.1.5.3.2 Cellular technology performance

The applicability of the IEC 62351 series depends also on the impact considering different communication technologies, in particular the mobile ones. It is important to evaluate the performance considering different technologies.

The aim of this subsection is to compare the baseline technology (Ethernet) performance with the ones obtained considering different types of cellular access networks. We focus on Standard Security scenarios, but an Ethernet vs 4G comparison considering Plain Security could also be performed.

The magnitude of the total handshake time (see Figure 6-6 and Table 6-1) in Ethernet tests is of 100 ms; considering the 4G/LTE technology, we have a value of 500/600 ms, but if we change the cellular technology we scale up of one order of magnitude with 3G (4600 ms) and of two orders with 2G (23300 ms). The values in Figure 6-6 refer to the mean value over the three DER sites for each of the run in the short tests. Considering 2G not all the DER values are available for all the run (means of the * symbol in the legend). The cellular results are deeply influenced by the TCP retransmissions occurring during the tests over the mobile network.

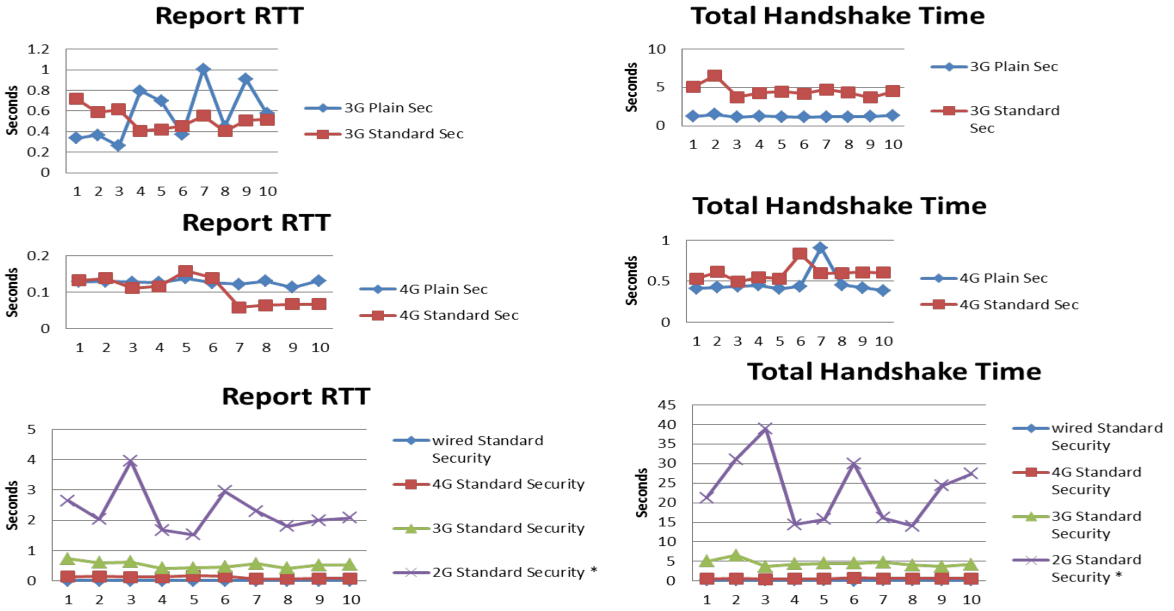


Figure 6-6: Results of the mobile communication evaluation

If we focus on RTT values (see Figure 6-6 and Table 6-1), we see that the gap between 4G and 3G is less evident (100 ms with 4G and 500 ms with 3G). The main step is between the Ethernet solution (1 ms) and 4G (100 ms) and between 3G (500 ms) and 2G (2290 ms). In Figure 6-6 the means over the three DERs for each run is plotted. Also, in this case for 2G test not all the DER values are available for all the run (marked with * symbol). From the test results it is clear that the 2G technology does not meet the availability and delay requirements of the VC application (neither those of the DER protection applications most probably sharing the same communication link). The 4G radio transmission seems to provide acceptable performances.

In case the 4G mobile coverage is not able to guarantee the service due to the DER site geographical position or the mobile network condition is degraded, the 3G technology can be a valid backup solution. Another important aspect to consider for the right interpretation of the test results is the dependency of the evaluated indicators on the cellular network topology and condition: the size of the mobile cell, the relative position of the DER site within the mobile cell, the background traffic changing with the daytime and the weekday are all key parameters that influence the QoS results. We have to underline that the 4G/3G/2G network equipped for this test bed is a prototypal solution, to be improved also using the trial results here gathered to build a more satisfying implementation to meet theoretical RTT values of less than 20ms.

The same test methodology for the performance evaluation is applicable to communication deploying IEC 60870-5-104 protocol, considering IEC 62351-5 instead of IEC 62351-4.

6.2 Cypher suites impact evaluation in DER control (Application of IEC 62351-4 and IEC 62351-3) *by Mauro Giuseppe Todeschini*

6.2.1 Introduction and motivation

In power system automation IEC 61850 MMS communications security should be made compliant with IEC 62351-4 and IEC 62351-3 whenever possible. IEC 62351-3 specifies the adoption of specific cypher suites and defines if a cypher suite is mandatory or optional and which one should be supported to ease backward compatibility.

In principle newer cypher suites should provide stronger security at the cost of a bigger impact on performance (slower computations, slower data transfers) and/or requirements (faster hardware is needed to counterbalance computational and communications performance loss) if compared to legacy ones.

The choice of supported and adopted cypher suites is not the only parameter an operator has to make in order optimize system cybersecurity and performance; as an example, IEC 62351-3 recommends a minimum key-length of 2048 bits and a TLS 1.2 protocol version; in both cases the operator is allowed to use other values if they fit well with specific use case considered and if the standard allows such values for the use case.

Cyber security operators can be supported in design and implementation choices by software tools which evaluate the impact of TLS parameters to the communication performance; such a tool (the Cybersecurity Impact Measurement Tool) and the results which were measured with it are described hereafter along with the results in a lab environment.

6.2.2 Cybersecurity impact measurement tool

The chosen reference use case consists in the telecontrol of four Distributed Energy Resources (DERs) connected to a primary substation. Remote control was achieved using IEC 61850 MMS (MMS) communication, where the DERs sent MMS reports containing data on their current energy production to a central controller. This central controller then performed operations on the DERs and implemented necessary adjustments by sending MMS setpoints. To facilitate this communication, software components were developed, specifically the endpoints for MMS communication: the 61850-server on the DER side and the 61850-client on the central controller side. Both components were implemented as Linux-x86 applications using open-source libraries supporting IEC 61850 communications and TLS communication protection.

This architecture was deployed in a laboratory reference scenario comprising four separate hosts running the *61850-server* component for each DER to simulate their geographical distribution. These hosts were connected to four distinct Local Area Networks (LANs). On the other side of the telecontrol communication, the *61850-client* endpoints for the four MMS telecontrol streams were executed by a single host, representing the command and control unit of the architecture. This host was also connected to a dedicated LAN. The five LANs mentioned above were implemented in the laboratory scenario as Ethernet networks and interconnected through a sixth network representing an intermediate WAN, accessible through five routers. This architecture is depicted in Figure 6-7.

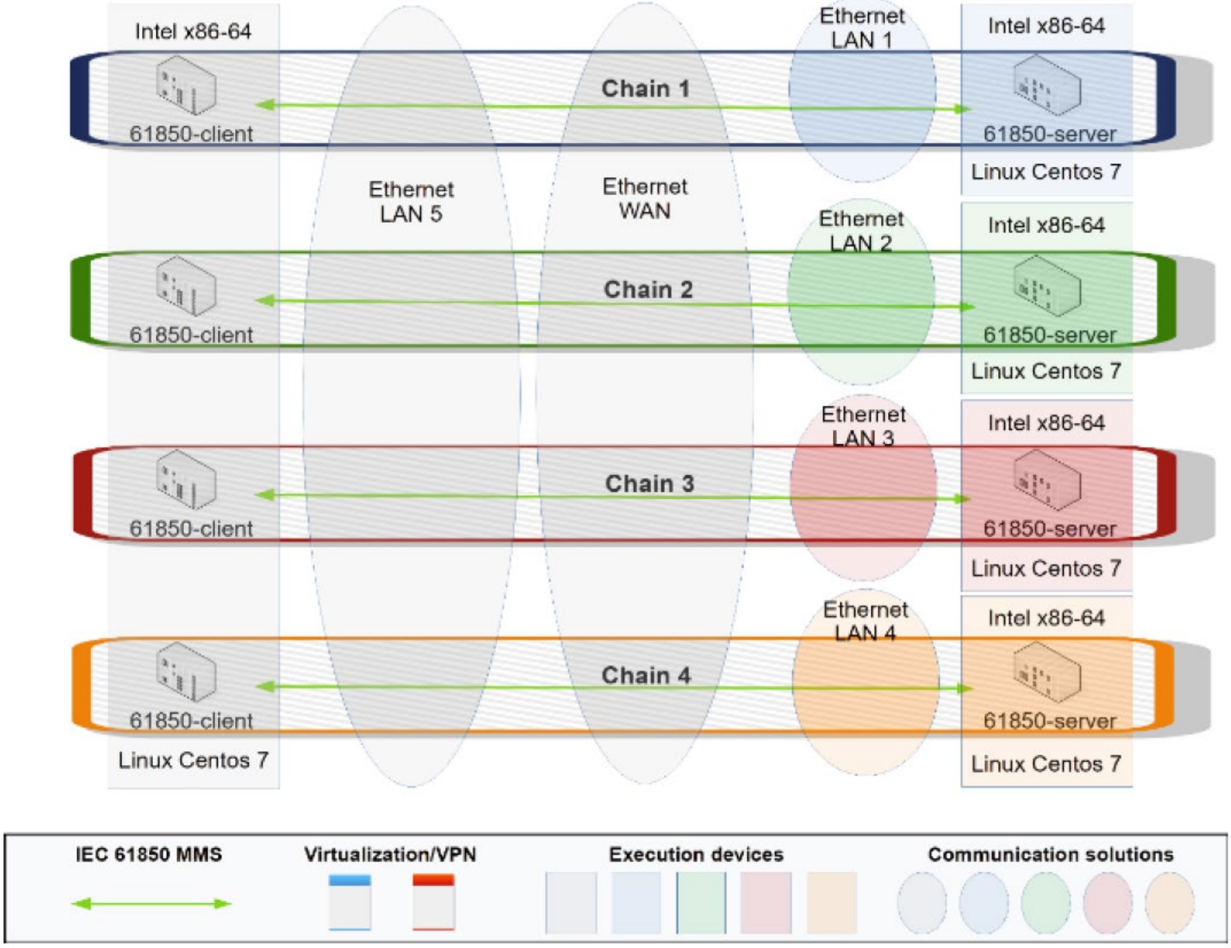


Figure 6-7: Architecture of the reference telecontrol scenario for the Cybersecurity Impact Measurement Tool

6.2.3 Test scenarios

Several derived scenarios were generated from the above reference scenario, incorporating architectural variations in terms of:

- processing solutions: the impact of virtualization and physical hosts was considered;
- communication solutions: wired and wireless LAN and WAN communication solutions were considered;
- Cybersecurity profiles: IEC 62351-3 TLS v1.2 profiles were considered.

In summary, the following scenarios were established (Figure 6-8):

- REFERENCE: this is the reference scenario described earlier;
- VIRTUALIZATION: architecturally identical to the REFERENCE scenario, but all processing and routing devices were implemented as virtual machines (VMs) within an hypervisor;
- WIRED TELECOMM: characterized by the adoption of an ADSL wired communication protected by a VPN network-to-host solution. An Ethernet LAN network was employed at the 61850-client side. The 61850-client endpoint operated in a virtual environment, while its counterparts run on physical machines, designed for heavy-duty loads;

- WIRELESS TELECOMM: characterized by the adoption of a 4G LTE WAN wireless communication protected by a VPN network-to-host solution. A Wi-Fi wireless LAN network was employed at the 61850-client side. The 61850-client endpoint operated in a virtual environment, while its counterparts run on physical machines, designed for heavy-duty applications.

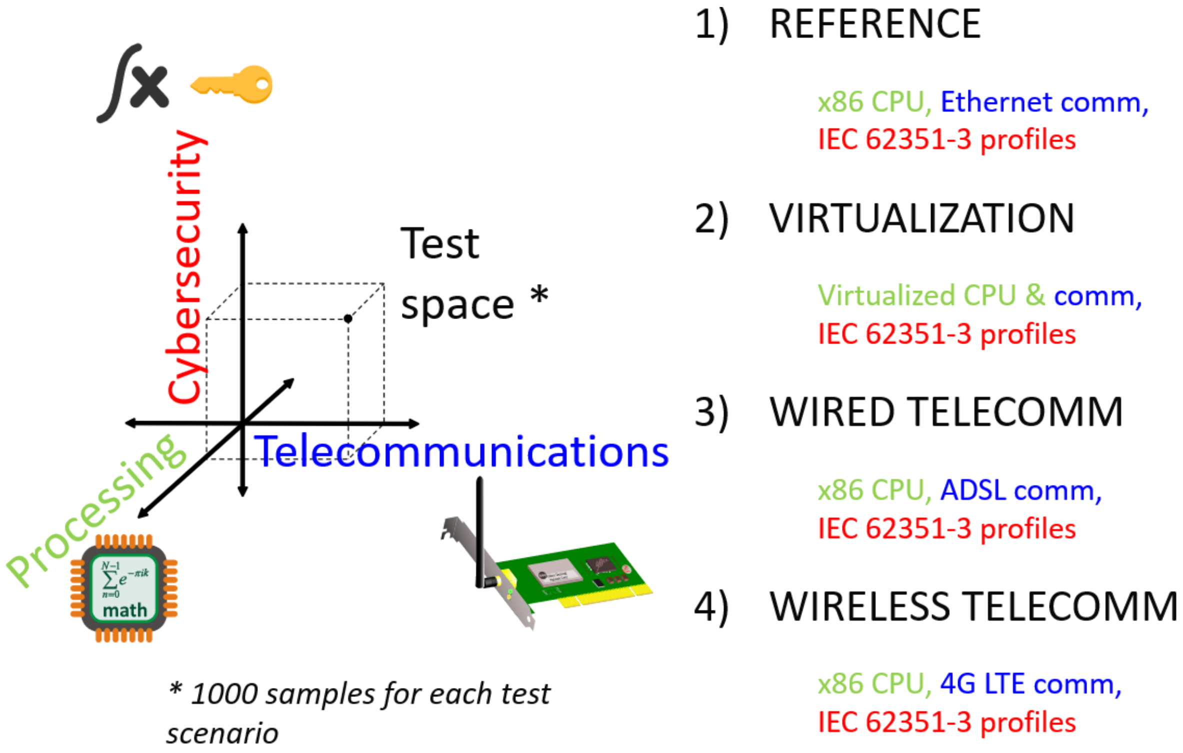

Cybersecurity
Processing
Telecommunications
Test space *
math
* 1000 samples for each test scenario
1) REFERENCE
x86 CPU, Ethernet comm, IEC 62351-3 profiles
2) VIRTUALIZATION
Virtualized CPU & comm, IEC 62351-3 profiles
3) WIRED TELECOMM
x86 CPU, ADSL comm, IEC 62351-3 profiles
4) WIRELESS TELECOMM
x86 CPU, 4G LTE comm, IEC 62351-3 profiles

Figure 6-8: The additional test scenarios which were derived from the reference scenario

TLS profiles considered

IEC 62351-3 defines specifications for protecting electrical system telecontrol communications over TCP/IP communication channels. The prescriptions concern algorithms that can be used, the data and parameters that must be supplied to these algorithms and the best practices about how they could be generated or selected.

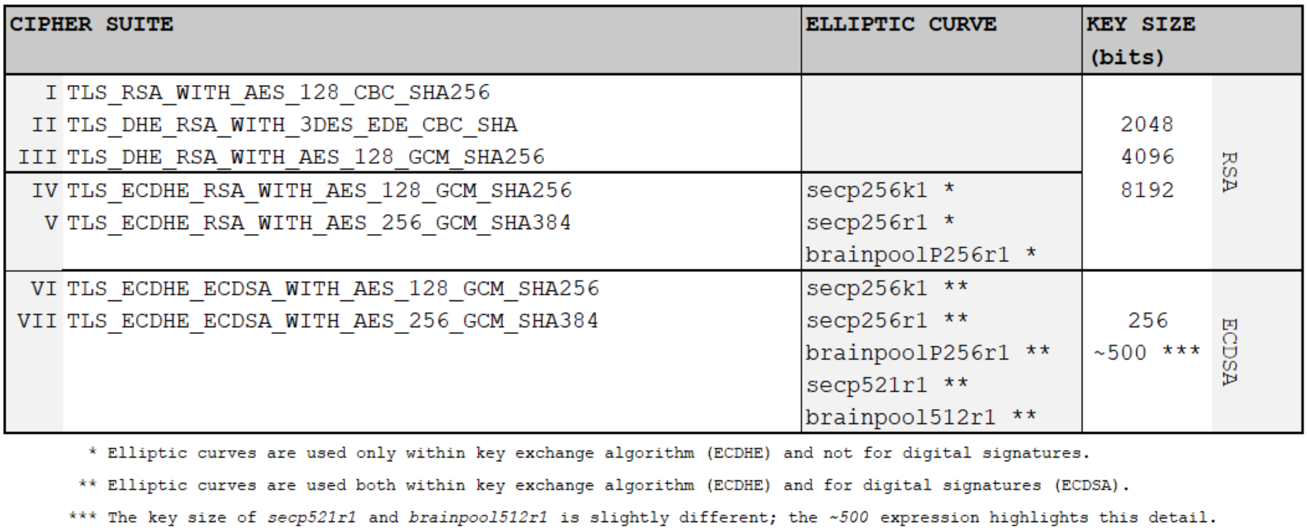
The cipher suites that have been considered in the tests have been selected among the mandatory or recommended by IEC 62351; mainly future proof cipher suites have been considered. However also a legacy cipher suite has been considered to verify possible performance advantages.

The size of 2048 bits cryptographic RSA keys and 256 bits ECDSA keys were considered as a baseline as those are the minimum sizes recommended by the standard. Larger keys were also considered in the tests, as they are already being used in the field.

As far as elliptic curves are concerned, the secp256r1 curve was mainly considered as its support is required by IEC 62351-3. The brainpoolP256r1 curve was also considered, as it is indicated as optional in IEC 62351-3. Moreover, elliptic curve secp256k1, was also included for comparison as it is supposed to achieve better performances than the previous ones, but it is unrelated to IEC 62351-3.

A combination of the parameters shown in Table 6-2 represents a cybersecurity profile that protects the cybersecurity of telecontrol communications. All possible combinations of these parameters have been applied to the test scenarios, but only the most significant results are reported hereafter. The roman number on the left of the table sometimes replaces the cipher suite name in the rest of the chapter for compactness.

Table 6-2: The parameters which define a TLS profile



CIPHER SUITE		ELLIPTIC CURVE	KEY SIZE (bits)	
I	TLS_RSA_WITH_AES_128_CBC_SHA256		2048 4096 8192	RSA
II	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA			
III	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256			
IV	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	secp256k1 * secp256r1 * brainpoolP256r1 *		
V	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384			
VI	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	secp256k1 ** secp256r1 ** brainpoolP256r1 ** secp521r1 ** brainpool512r1 **	256 ~500 ***	ECDSA
VII	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384			

* Elliptic curves are used only within key exchange algorithm (ECDHE) and not for digital signatures.

** Elliptic curves are used both within key exchange algorithm (ECDHE) and for digital signatures (ECDSA).

*** The key size of *secp521r1* and *brainpool512r1* is slightly different; the *~500* expression highlights this detail.

6.2.4 Key performance indicators

To quantify the performance differences among profiles and solutions, three different KPI have been considered:

- CET (Connection Establishment Time): measures the latency which is experienced by 61850-client since it attempts a connection to 61850-server and when it receives a confirmation of a successful conclusion of the connection phase (Figure 6-9);
- RTT (Report Transmission Time): measures the latency of the transmission of a MMS report from 61850-server to 61850-client (Figure 6-10);
- STT (Setpoint Transmission Time): measures the latency of the transmission of a MMS report from 61850-client to 61850-server.

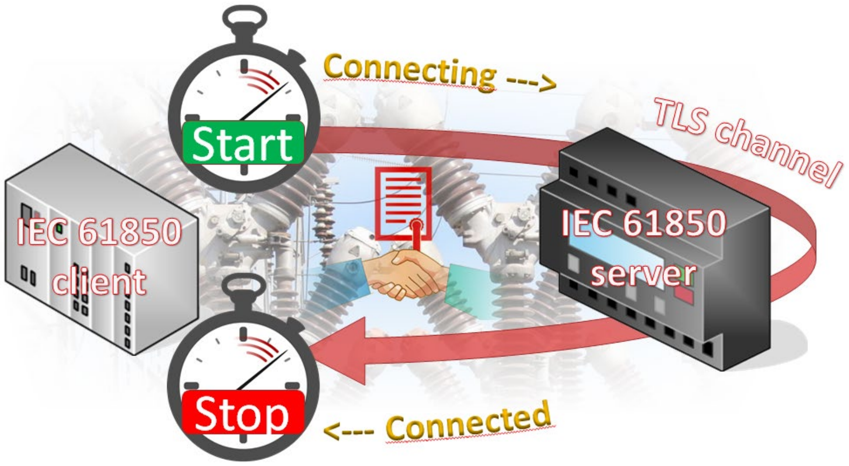


Figure 6-9: The Connection Establishment Time KPI

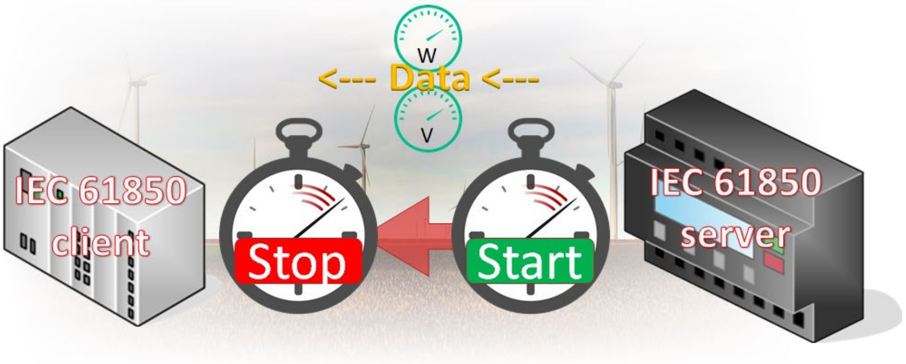


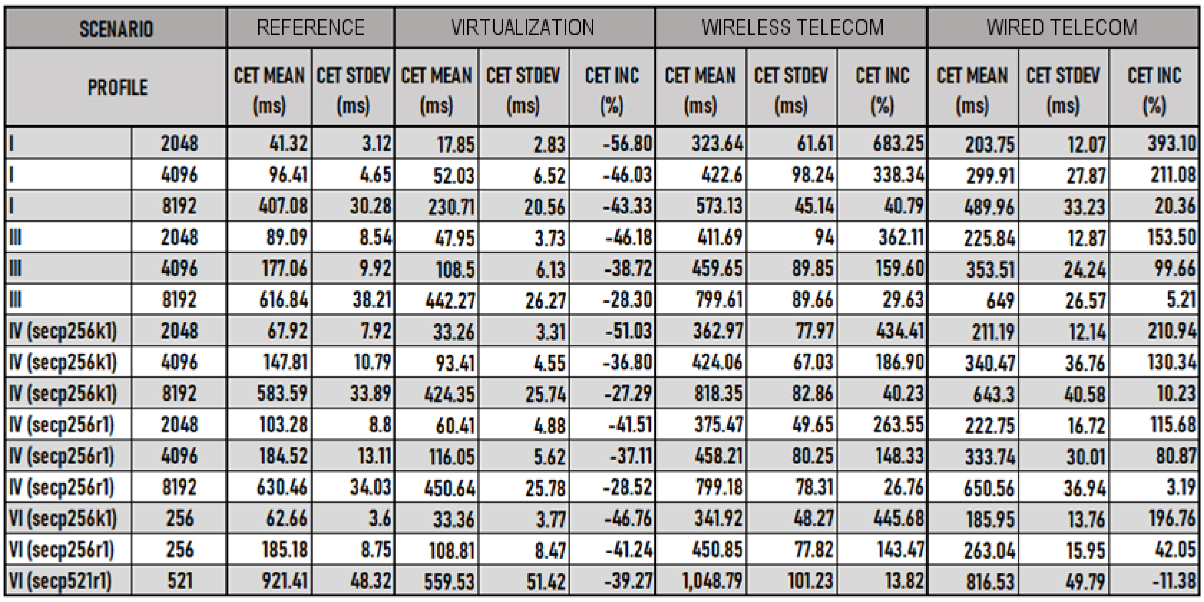
Figure 6-10: The Report Transmission Time KPI

6.2.5 Tests results

The performance of the cipher suites in the TLS handshake phase is determined by the key exchange and digital signature algorithms. In fact, in the tests carried out, the performance of the cipher suites that share the same algorithms show analogous performances, regardless of the bulk encryption and message authentication algorithms.

The measurements show that the incidence of the size of the cryptographic keys has a consistent impact on the performance of the communications (Table 12-2). Considering the reference scenario, the transition from 2048 bit keys to 4096 bit keys resulted in a 78%-134% increase in the CET indicator, while the further step towards 8192 bit keys resulted in a further increase in the range of 241%-323%. The cipher suites based on elliptic curves are usually regarded to have better performances; in principle this is supported also by the fact that they are characterized by smaller cryptographic keys for the same level of security. In our tests, the performance advantage was not detected, which can be attributed to implementations which are not yet been completely optimized. Instead, the performance advantage of the *secp256k1* curve, compared, for example, to *secp256r1* was verified.

Table 6-3: Summary of the CET PKI results



SCENARIO		REFERENCE		VIRTUALIZATION			WIRELESS TELECOM			WIRED TELECOM		
PROFILE		CET MEAN (ms)	CET STDEV (ms)	CET MEAN (ms)	CET STDEV (ms)	CET INC (%)	CET MEAN (ms)	CET STDEV (ms)	CET INC (%)	CET MEAN (ms)	CET STDEV (ms)	CET INC (%)
I	2048	41.32	3.12	17.85	2.83	-56.80	323.64	61.61	683.25	203.75	12.07	393.10
I	4096	96.41	4.65	52.03	6.52	-46.03	422.6	98.24	338.34	299.91	27.87	211.08
I	8192	407.08	30.28	230.71	20.56	-43.33	573.13	45.14	40.79	489.96	33.23	20.36
III	2048	89.09	8.54	47.95	3.73	-46.18	411.69	94	362.11	225.84	12.87	153.50
III	4096	177.06	9.92	108.5	6.13	-38.72	459.65	89.85	159.60	353.51	24.24	99.66
III	8192	616.84	38.21	442.27	26.27	-28.30	799.61	89.66	29.63	649	26.57	5.21
IV (secp256k1)	2048	67.92	7.92	33.26	3.31	-51.03	362.97	77.97	434.41	211.19	12.14	210.94
IV (secp256k1)	4096	147.81	10.79	93.41	4.55	-36.80	424.06	67.03	186.90	340.47	36.76	130.34
IV (secp256k1)	8192	583.59	33.89	424.35	25.74	-27.29	818.35	82.86	40.23	643.3	40.58	10.23
IV (secp256r1)	2048	103.28	8.8	60.41	4.88	-41.51	375.47	49.65	263.55	222.75	16.72	115.68
IV (secp256r1)	4096	184.52	13.11	116.05	5.62	-37.11	458.21	80.25	148.33	333.74	30.01	80.87
IV (secp256r1)	8192	630.46	34.03	450.64	25.78	-28.52	799.18	78.31	26.76	650.56	36.94	3.19
VI (secp256k1)	256	62.66	3.6	33.36	3.77	-46.76	341.92	48.27	445.68	185.95	13.76	196.76
VI (secp256r1)	256	185.18	8.75	108.81	8.47	-41.24	450.85	77.82	143.47	263.04	15.95	42.05
VI (secp521r1)	521	921.41	48.32	559.53	51.42	-39.27	1,048.79	101.23	13.82	816.53	49.79	-11.38

The behaviors described above were registered in all the scenarios that were considered.

The WIRELESS TELECOMM scenario showed the worst performance for CET indicator. Wireless communications introduce a considerable latency, significantly impacting communications adopting smaller cryptographic keys. In the case of larger key sizes, the effect of the higher latency is masked by the latency in processing bigger cryptographic keys.

In the WIRED TELECOMM scenario, on the other hand, the latencies are lower than in WIRELESS TELECOMM. In the case of large cryptographic keys, the higher processing power of the hosts was, in one profile, able to more than compensate for the latency increase.

The VIRTUALIZATION scenario highlighted consistent benefits for CET measurements, probably linked to the fact that communications are also virtualized and implemented with fast memory transfers within the hypervisor instead of physical transfers through network cables and equipment.

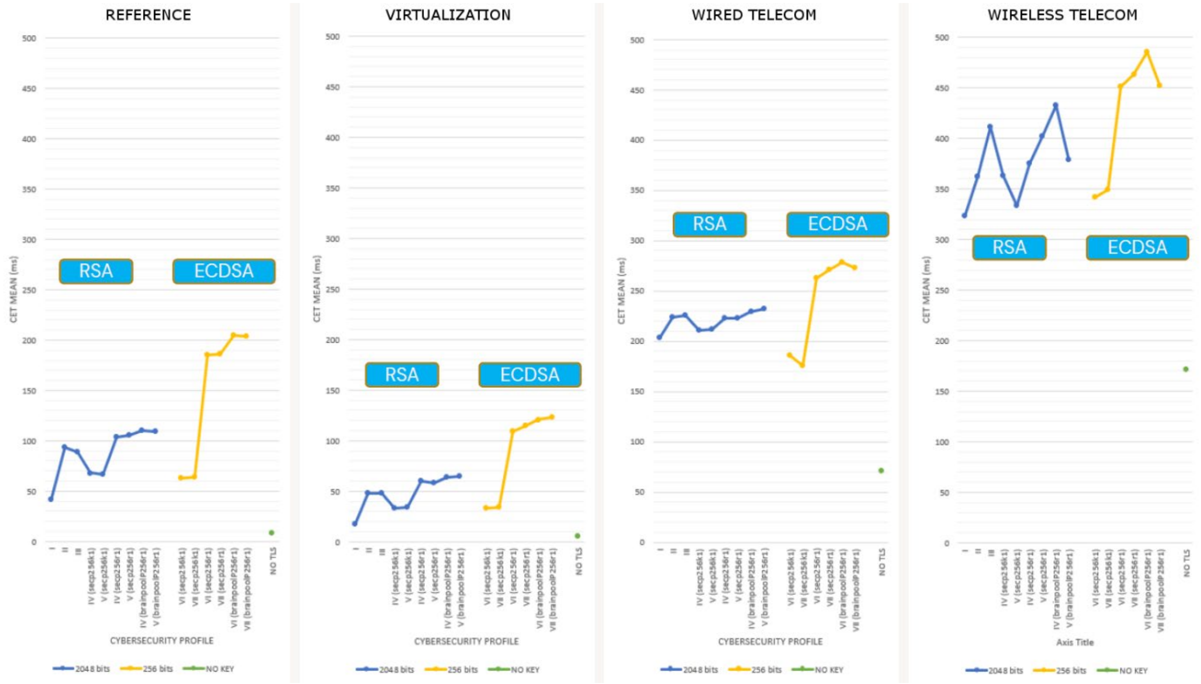


Figure 6-11: Charts representing and correlating the results for CET KPI

The measurements of the RTT and STT indicators, associated respectively with the transmission of reports and setpoints, showed a significantly different behavior compared to those of CET. No differences resulting from the cybersecurity profiles were measured; this phase of the TLS communication uses symmetric key algorithms, which are significantly more efficient than public key cryptography used during TLS handshake. The relevant algorithms in this phase are those of bulk encryption and message authentication, which require smaller keys and can often benefit from hardware acceleration by modern microprocessors; in our scenarios the transmission of reports always required just milliseconds to tens of milliseconds. This makes the performance differences among algorithms insignificant with respect to the latencies introduced by communication of network. The differences highlighted by the chart in Figure 6-12 are therefore due to the different communication solutions that characterize the scenarios. The chart highlights also that the performance of encrypted reports and setpoints transmission, and therefore of remote control in general, is equivalent to that of unencrypted transmissions, reported as NO TLS in charts, demonstrating the efficiency achieved in the implementation of modern cryptographic algorithms.

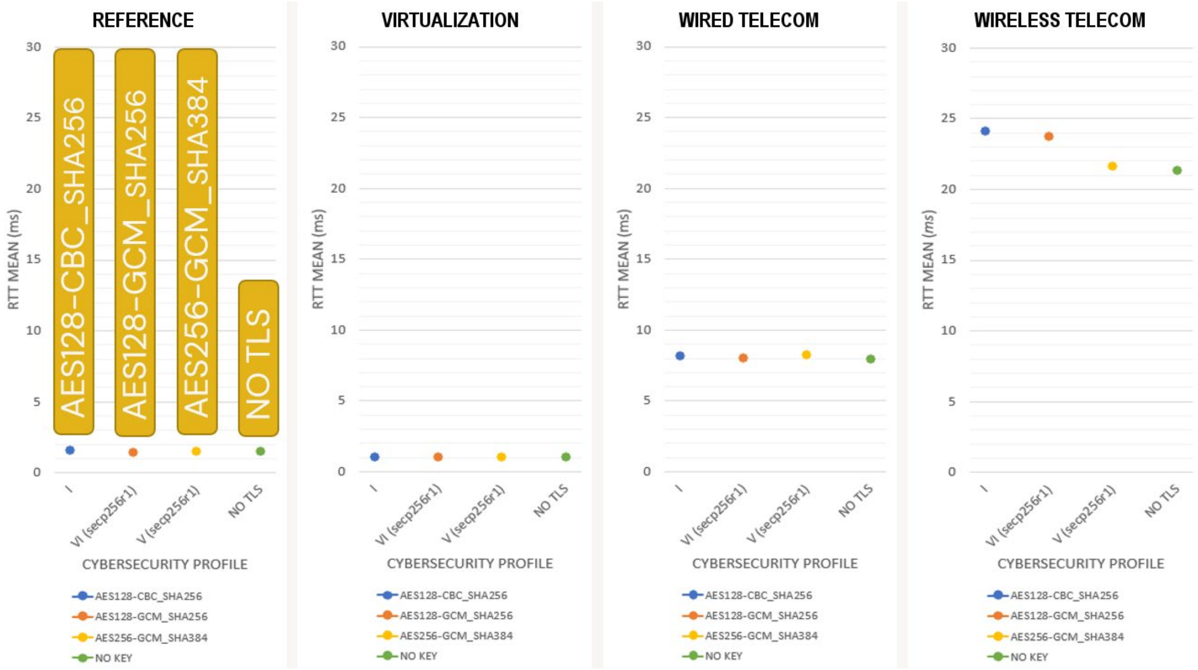


Figure 6-12: Charts representing and correlating the results for RTT KPI

The results and/or the methodology presented in this chapter might be of interest to operators or system integrators in charge of upgrading existing architectures for connecting DER installations.

6.3 Security monitoring for threat analyses

6.3.1 Security monitoring framework

Application of IEC 62351-7) *by Roberta Terruggia and Giovanna Dondossola*

The monitoring infrastructure represents a valid instrument to support the response capabilities to ICT anomalies and to increase the system resilience. The traditional preventive security measures (e.g., network segregation, access control, authentication, end to end data encryption) have to be complemented by a smart monitoring infrastructure. Indeed, real time monitoring is able to highlight vulnerabilities and timely respond to the residual risks not covered by the preventive measures applied in the system. Moreover, the outcomes of the monitoring data analysis can be used as input data for the configuration of power control strategies to be able to adapt the optimization function to the real time status of the ICT infrastructure.

The smart monitoring can be performed implementing and configuring a Network and Application Security Monitoring platform where several monitoring agents are installed in key control infrastructure points at communication and IED devices, to observe and correlate not only the IT aspects as the traditional network monitoring frameworks, but also OT power control communication specific events addressing for example the objects defined in the IEC 62351-7 standard. The traditional Security Information and Event Management (SIEM) collects IT information coming from different sources and can correlate and perform some sort of analysis for maintenance and security purposes. In the scope of smart grids this paradigm needs to be expanded to involve information coming from the IT (Information Technology) world, but also values specific of OT (Operation Technology) devices. Figure 6-13 presents a schema of possible information sources which could provide useful measures for a wide comprehensive analysis.

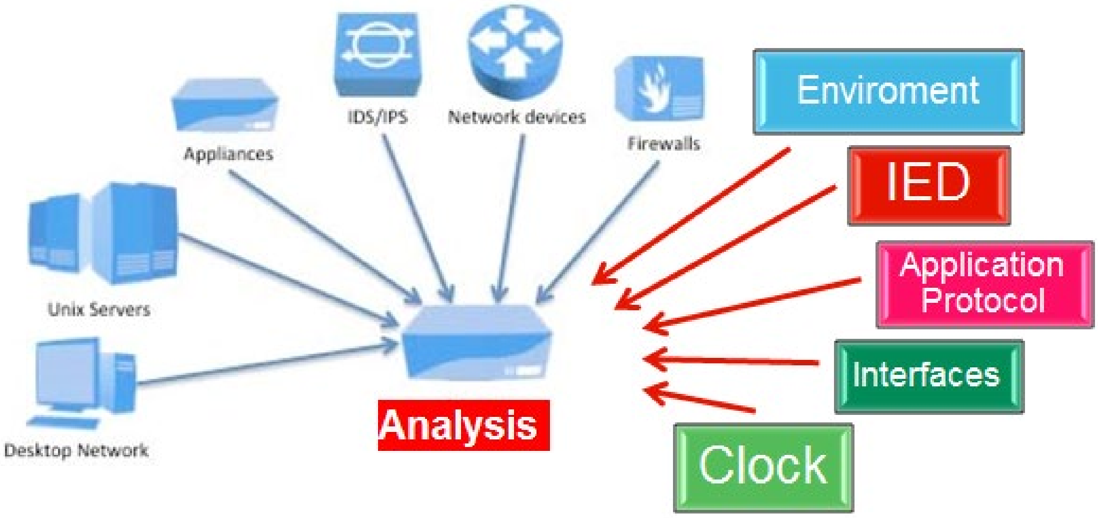


Figure 6-13: Data sources for Smart Grid monitoring analysis

The smart platform manages indicators of different nature, IT as well as OT objects to perform an integrated IT/OT monitoring. The platform allows analysing in detail the key role of monitoring in attack prevention, detection, and effect mitigation. The monitoring information coming from heterogeneous devices (communication components as well as power grid IEDs) need to be collected and analysed by a central system correlating data at different stack layers to recognise the type of occurring anomaly (see Figure 6-14).

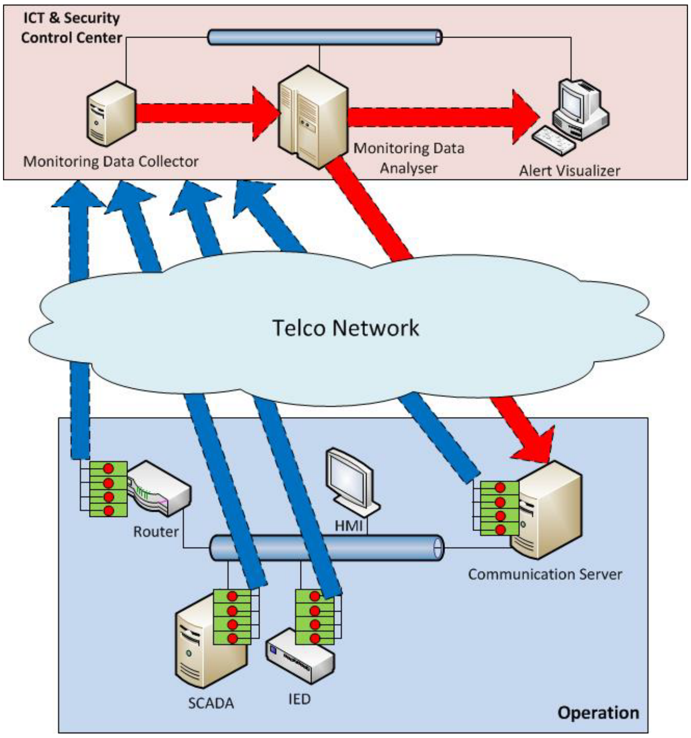


Figure 6-14: Smart Monitoring Conceptual Layout

The alerts coming from the analysis of collected data can reveal the existence of vulnerabilities or give an indication that a given attack process has started. In the first case the data are used to identify potential threats and address possible corrective actions. In the case of detected attacks, the alerts allow the execution of automatic or manual recovery actions. Moreover, the outcomes of the monitoring data analysis are used as input data for the configuration of power control strategies adapted to the real time status of the ICT infrastructure.

The ICT monitoring framework is based on performance measures specific for energy applications and communication/security protocols. In Figure 6-15 the framework logical steps are presented. Starting from the online analysis of the network traces, an Analysis Tool placed at device machine (i.e., substation controller) evaluates and extracts the different measures of interest. The indicator values are mapped on data objects of the IEC 62351-7 standard and transmitted by means of the SNMP protocol to the ICT monitoring centre that eventually generates security alerts.

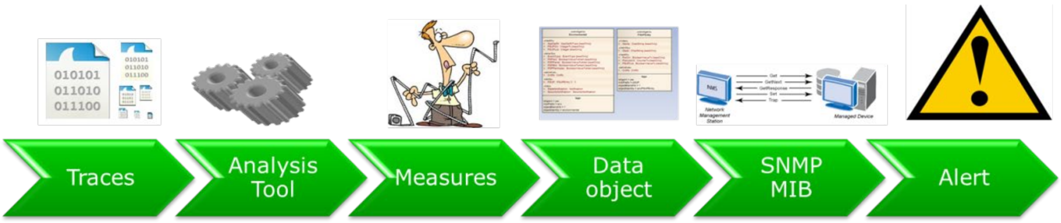


Figure 6-15: Monitoring flow steps

The Smart Monitoring Platform (see Figure 6-16) comprises several components: the agents are placed into different device and have to be able to capture IT but also OT evidences.

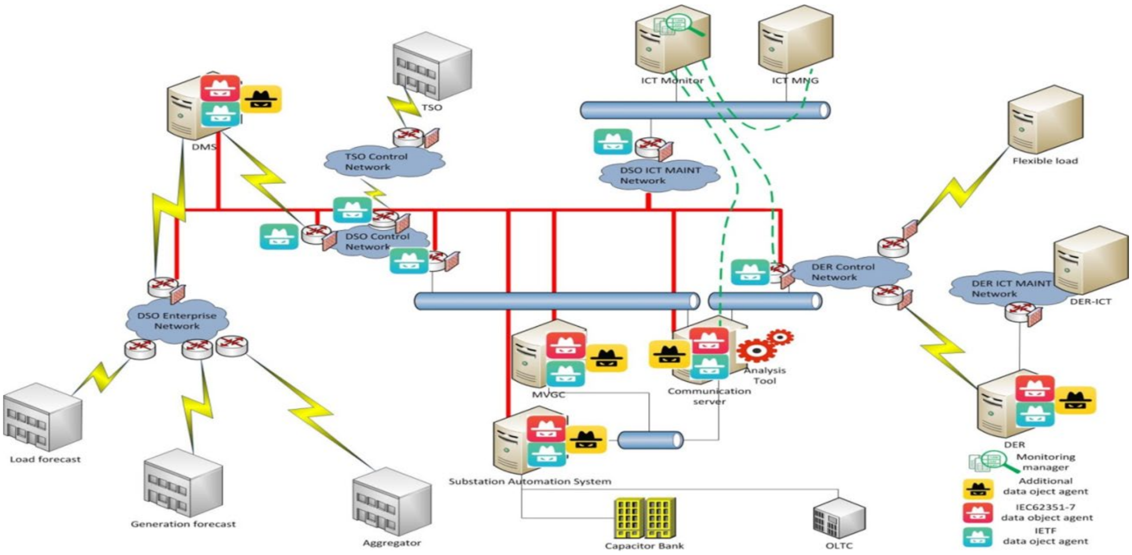


Figure 6-16: Smart Monitoring Platform

6.3.2 Monitoring platform

The assessment of the security monitoring functionality described above is carried out by the setup of a lab platform, shown in Figure 6-17 and physically located at RSE premises, implementing the ICT components of the distribution grid domain with different standard communication modules: as introduced in the previous section, the focus is on the communications between a DSO (Distribution System Operator) primary substation and third party DER (Distributed Energy Resources) sites, required for the optimization of the medium voltage grid management in presence of renewable generation. These communications are implemented by MMS (Manufacturing Message Specification) information flows, compliant with the IEC 61850 data model and communication profile and secured in compliance with the IEC 62351-4 T-profile. The lab platform deploys the monitoring infrastructure implementing the monitoring agents (related to ICT and IED objects) that provide data to the Security Control Center via standard protocols (i.e., SNMP, Syslog). Here the information coming from the agents are collected, correlated, and analyzed.

Figure 6-17: Experimental security assessment – RSE PCS-ResTest Lab

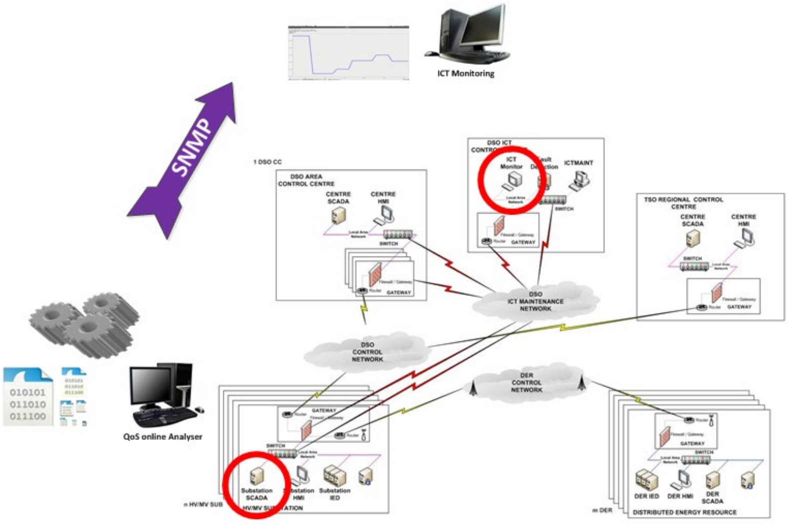


Figure 6-18: Monitoring Architecture

A dedicated machine at ICT monitoring centre (ICT Monitor in Figure 6-18) receives the measures from the different sources (the substation controller, but also devices as routers and switches) and plots the main indicators to allow operators monitoring the values.

The SNMP architecture (see Figure 6-19) currently implements data requests from the monitoring manager (proxy) towards the monitoring agents in polling operation mode. However, in a full-scale infrastructure the monitoring architecture shall use the most efficient implementation mixing monitoring traps from the agents towards the manager with data rates of polling requests in the opposite communication way.

To secure the monitoring information flow and be compliant with the IEC 62351-7 standard [4], the SNMP version 3 TSM security profile is implemented to provide authentication and encryption for the communications between the Analysis Tool and the ICT Monitor.

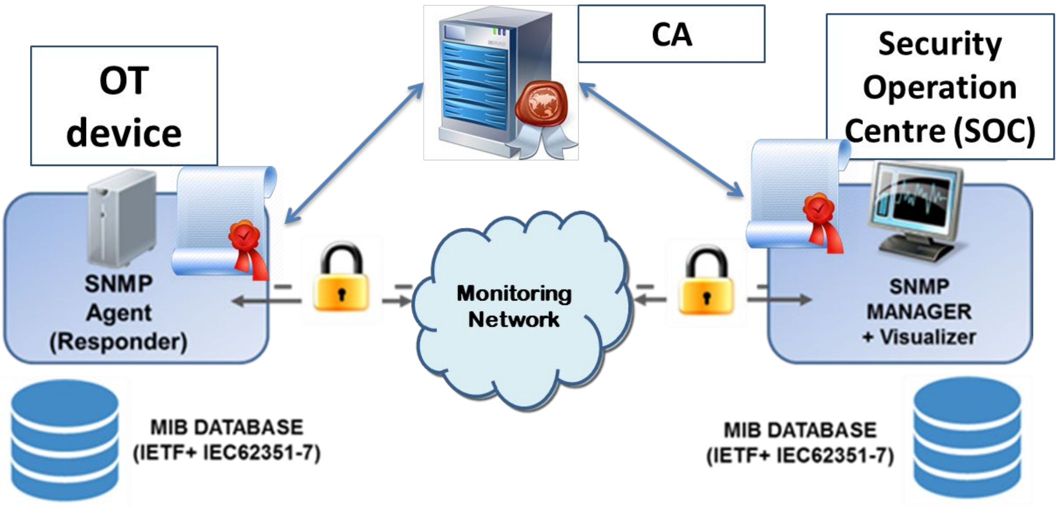

OT device
CA
Security Operation Centre (SOC)
SNMP Agent (Responder)
Monitoring Network
SNMP MANAGER + Visualizer
MIB DATABASE (IETF+ IEC62351-7)
MIB DATABASE (IETF+ IEC62351-7)

Figure 6-19: SNMP architecture

In case of cyber-attacks, the performance indicator values might vary significantly, thus an online evaluation of such indicators supports the analysis of the attack effects and the correlation of monitoring data related to network and control devices. In the reported examples two types of Denial-of-Service attacks (UDP Flooding Attack and TCP Reset Attack) have been considered and the effect of the injected attacks on the communication performances are recognizable through the indicators' values. As these types of attack are not prevented by the IEC 62351-3 and IEC 62351-4 deployment, they represent interesting residual risks to analyze by means of the IEC 62351-7 monitoring framework.

6.3.3 Results

This section provides the combination of monitoring performance indicators (Table 6-4) that are meaningful for analysing the behaviour of IEC 61850 DER communications under attacks.

In the presented scenarios the remote maintenance interface of the substation router in the DER wireless network is under a packet flooding attack. Considering the whole set of collected indicators it is possible to highlight anomalous values for the indicators in the following table.

Table 6-4: Security indicators

SOURCE	**MIB (OBJECTS)**	**DESCRIPTION**
IEC 62351-7	*mMSRtxCnt*	Number of MMS message retransmissions
	mMSRptReceptionDelay	MMS report Delay
IETF	*UdpInErrors*	Number of UDP datagrams discarded
	UdpNoPorts	Number of UDP datagrams addressed to a not open port
	UdpInDatagrams	Number of UDP datagrams correctly received

The values of monitoring objects are obtained from devices of different types (substation IED and router) and refer to various layers of the communication stack. The IEC 62351-7 objects in the list, collected from the substation IED, are related to IEC 61850 communications, while those from the substation router are typical network objects of the transport layer.

Figure 6-20 presents the plot of the end-to-end transmission Delay indicator for 4 DERs (1 DER is wired connected, 3 DERs communicate by mobile links) and highlights the effects of the attack on the communications with the different nodes. The top left plot is related to the wired DER, that is not involved in the attack process, indeed its communications present a normal trace. The other 3 plots refer the wireless DERs through the wireless router in the substation (the target of the attack). As it is possible to note the under attack communications are subject to delays, some orders of magnitude higher than the wired one (the plots use different scales). Another issue is related to the capability of the monitoring platform to provide the measures coming from the agents to the manager: from Figure 6-20 is clear that some monitoring data are lost, this is due to the attack process within the maintenance network.

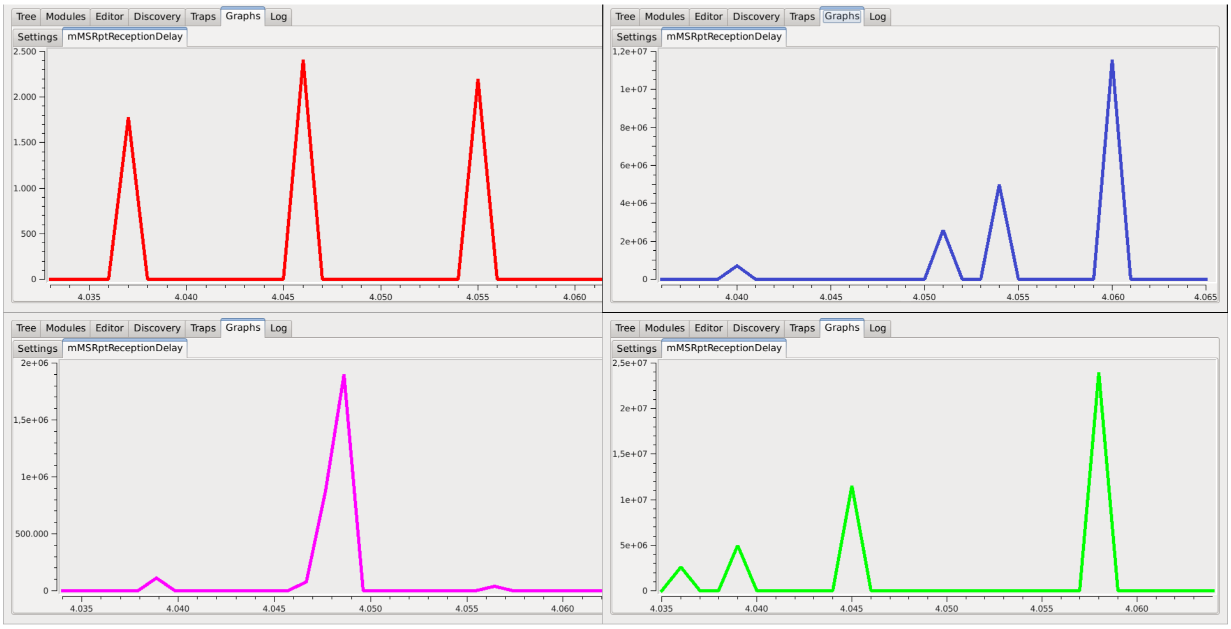


Figure 6-20 : Delay plots for4 DERs – 1 wired (top-left), 3 wireless

Only the information coming from the Delay indicator is not enough to establish that the bad performance is caused by an active attack. Indeed, the performances of the cellular network are not deterministic, and delays may occur also in other circumstances related to the status of the radio links. Further information is needed to discriminate the source of the communication anomaly: for example, observing the IETF UdpNoPorts indicator from the substation router (whose values are plotted in Figure 6-21) it is possible to see the value increase signing that some malicious activity is running. Correlating the values of these two indicators it is possible to promptly detect the presence of the anomalies and locate the criticality before the connection drop, so to apply an appropriate mitigation action to rapidly recover from the bad performance of the control communications.

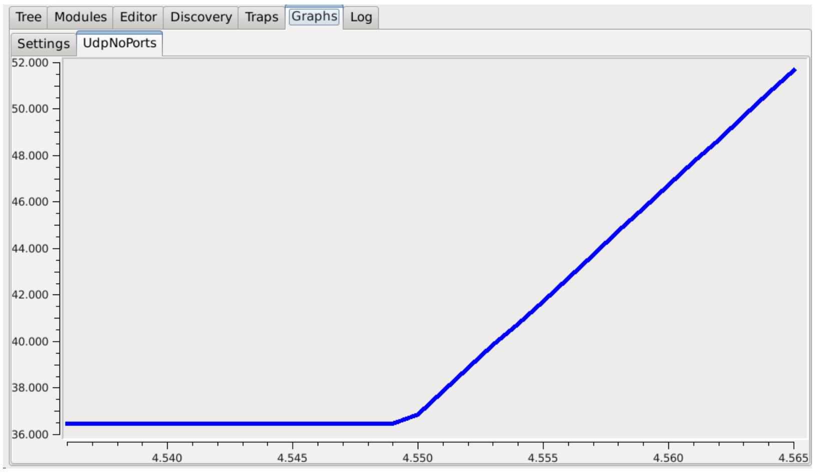


Figure 6-21: UdpNoPorts indicator plot

The outcomes of the analyses coming from the monitoring platform support also a second level of resilience, i.e., the information on the communication status is an input of the control algorithm that shall adapt its optimisation function to the actually controllable resources and select the most appropriate control strategy for maintaining the grid stability and operation efficiency.

In the next pictures it is possible to see some screenshots displaying selected indicator plots as visualised by the ICT Monitor HMI.

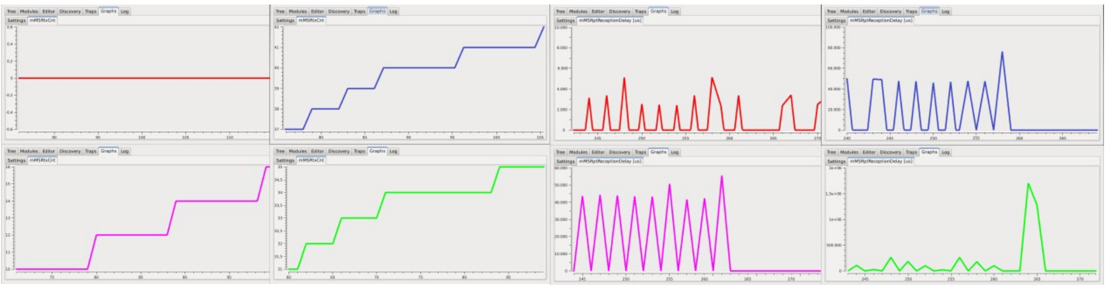


Figure 6-22: MMS Retransmission (left); MMS Report Delay (right) [4 DERs]

Figure 6-22 depicts the graphs, with different scales, of the MMS Retransmission and MMS Report Delay Times of the 4 DERs when the flooding attack is active. As this attack process targets the cellular connected DERs, the red plots on the top left about the wired connected DER show normal performances (there are neither retransmissions nor perturbed report delays). On the other hand, the wireless DERs manifest increased Report Delay values, particularly relevant in the green line at bottom right plot. The attack can block the SNMP message exchange of all wireless DERs, as visible in Figure 6-22 by the Delay plots for cellular connected DERs (blue, purple and green lines), thus denying the monitoring service at the Management Center.

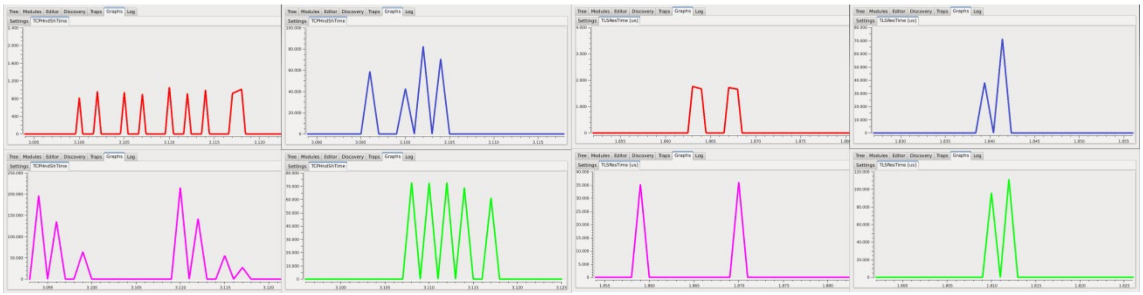


Figure 6-23: TCP Handshake Time (left); TLS Resumption Time (right) [4 DERs]

Figure 6-23 shows, with different scales, the plots of TCP Handshake Time and TLS Resumption Time indicators during a TCP Reset attack targeting all the DER communications. Indeed, it is possible to note that all the 4 DERs manifest a perturbation in the performance values. When the attack causes the TCP connection drop, a new TCP handshake is started from the application recovery mechanism (left side plots) and, with MMSs communications, also the TLS resumption mechanism is activated to recovery the TLS session (right side plots).

Furthermore, the outcomes obtained from the implemented monitoring components can be combined to obtain more complex indicators for detection purposes and to perform more focused analysis aimed at restoring a normal communication situation. Some examples of complex indicators considered in different UDP Flooding attack scenarios are presented in Figure 6-24.

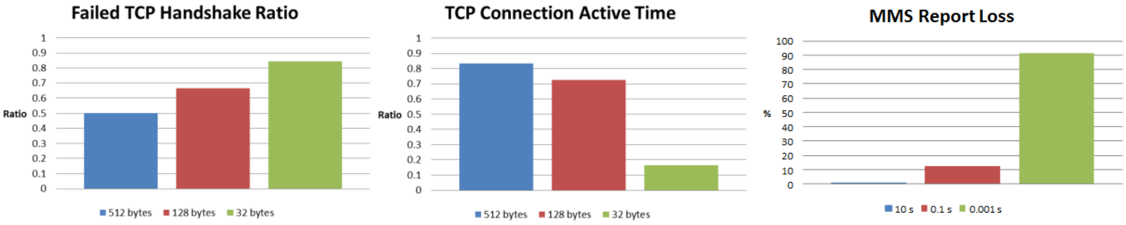


Figure 6-24: Analysis of Flooding Attack Indicators

The first histogram compares the ratio of the failed TCP Handshake over the total number of started TCP Handshake, by changing the UDP flood datagram size. In the second one the TCP Connection Active Time (i.e., the estimation of the time available to the control traffic, not used for connection setup or recovery, over the total observation time) is plotted, here as well changing the malicious datagram size. The third and last one shows the percentage of lost packets with DER measurements changing the malicious packet rate.

The monitoring results obtained from the experimental activity, bear out that the advancements in the cyber security defense are supported by the implementation of standard monitoring functions in both the communication and control devices of the smart energy systems. They also support the specification of an adaptive monitoring infrastructure that manages the trade-off between the monitoring overhead and the actual limits of device controllability.

6.3.4 Integrated platform

The monitoring platform has to be integrated with the log infrastructure (Figure 6-25) following the specification of IEC 62351-14 in order to be able to have an overall integrated monitoring framework (IEC 62351-90-3).

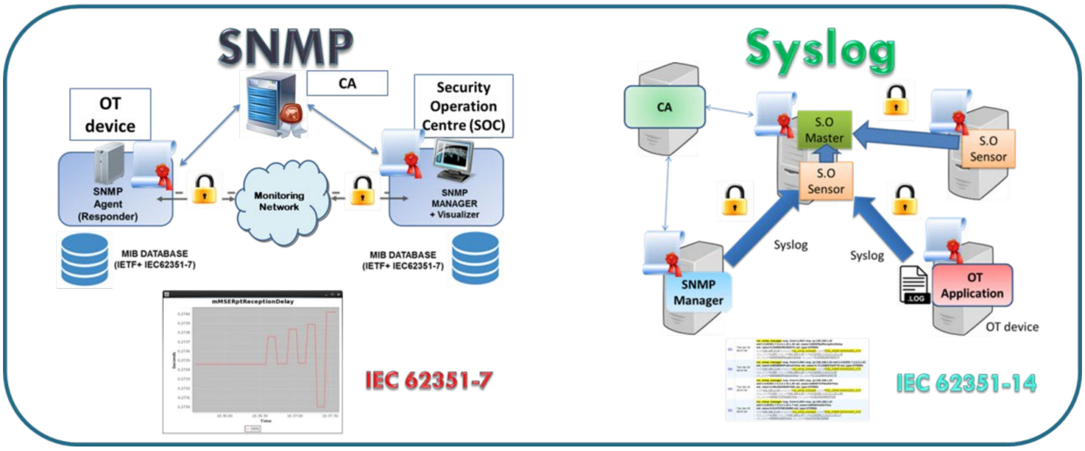


Figure 6-25: Integrated platform

Figure 6-26 shows the applicability of the different event log categories with reference to the architecture of the operating environment. Categories that apply to the entire architecture are indicated in red (generic log events, and the ones related to part 8 and part 9 of IEC 62351), in blue the categories specific to IEC 60870-5-104 communications (log events 60870-5-104 and 62351-5 and 62351-3) and those relating to IEC 61850-8-1 (MMS) communications in green (log events relating 62351-4 and 62351-3).

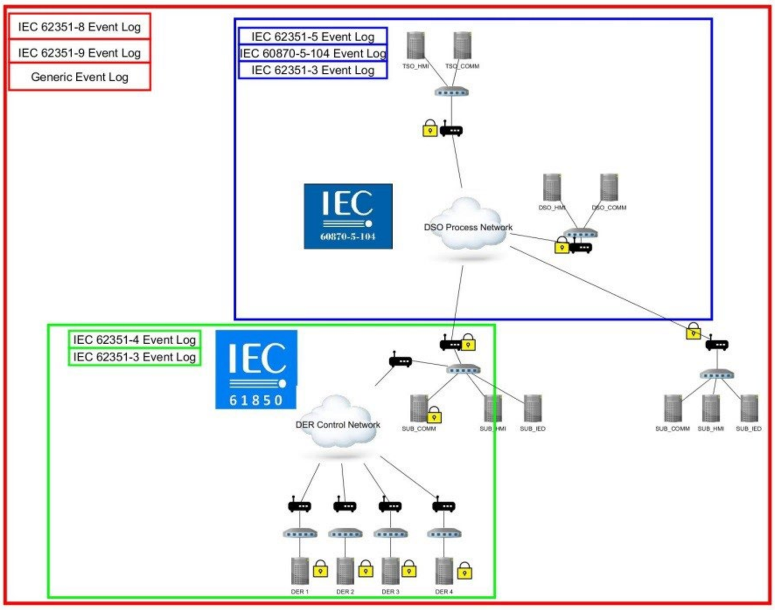


Figure 6-26: Significant event logs

Focusing on the IEC 61850-8-1(MMS) communications implemented between the primary substation and the DERs, developed through an MMS client that communicates with the MMS servers on DER control devices. The log categories that can be taken into consideration to implement security measures, to detect possible active attack processes and implement recovery measures, are those specific to the MMS protocol, in addition to the generic ones. Events relating to part 4 of 62351 may be also of interest, as they may provide indication of specific events relating to the MMS protocol.

MMS communications between the primary substation and the DERs are secured through channel encryption and mutual authentication provided by the TLS (Transport Layer Security). For this reason, it may be of interest to select the log events that are significant for the transport layer.

If an infrastructure for role management is implemented, the events relating to part 8 can signal important evidence of anomaly.

The end-to-end security of communications between the primary substation and the DERs is based on the use of certificates. In a complete configuration there is a PKI (Public Key Infrastructure) to manage public/private key pairs and certificates. This can be implemented through differently complex platforms. Whatever is the implementation choice, the events relating to PKI management provide useful information to identify cyber security problems.

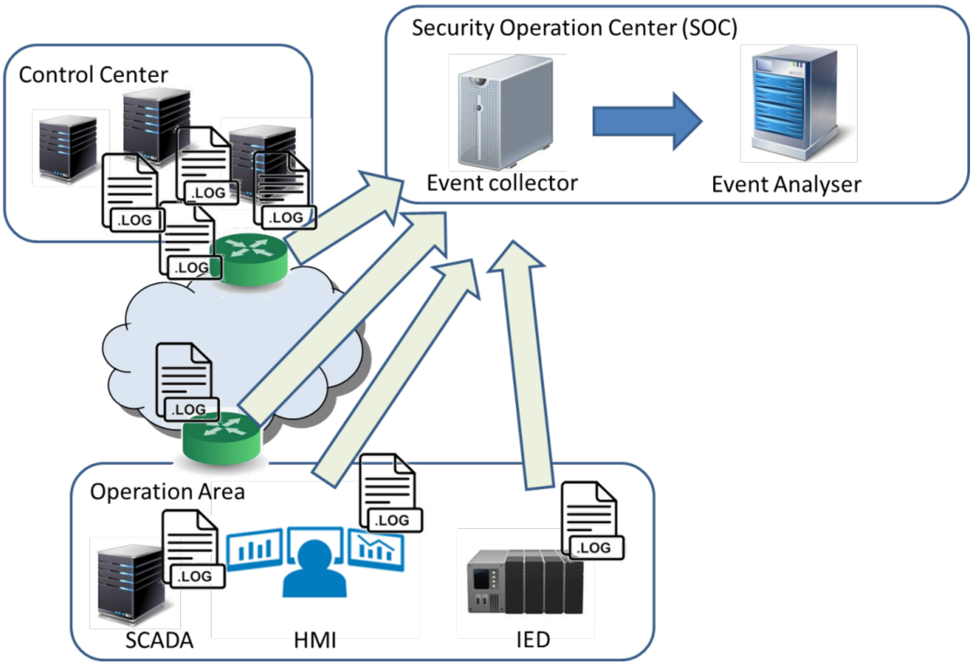


Figure 6-27: Collection and analysis platform

To develop advanced anomaly detection environment, it is necessary to implement an infrastructure for collecting and processing events from different sources, be they IT network devices and OT nodes. Figure 6-27 represents the main elements of the architecture implemented in the PCS-ResTest laboratory. This infrastructure allows collecting logs from operational areas such as, for example, primary substations or distributed generation sites (represented in the figure as Operation Area). Furthermore, evidences of anomalies can be collected from local or central control areas (represented in the figure as Control Center). Information from logs can refer to OT events, such as communication protocol logs, or IT one, such as information on the status of network components. The logs come from both communication devices and control end-nodes, both belonging to OT domains. The Syslog protocol has been used for transmitting logs from operation areas to central and security management domains.

7 References

[1] IEC 62351-Series: “Power Systems Management and associated information exchange – Data and Communication Security, https://webstore.iec.ch/publication/6912

[2] IEC 60870-5: “Telecontrol equipment and systems - Part 5: Transmission protocols”, https://webstore.iec.ch/publication/3755; focus here are 101 and 104

[3] IEC 61850: “Communication networks and systems for power utility automation”, https://webstore.iec.ch/publication/6028

[4] ISO 27001: “Information technology - Security techniques - Information security management systems - Requirements”, https://webstore.iec.ch/publication/11286

[5] ISO 27019: “Information technology - Security techniques - Information security controls for the energy utility industry”, https://webstore.iec.ch/publication/61906

[6] ISO 27002: “Information technology - Security techniques - Code of practice for information security controls”, https://webstore.iec.ch/publication/11288

[7] NIST Cyber Security Framework, https://www.nist.gov/cyberframework

[8] NISTIR 7628: Guidelines for Smart Grid Cybersecurity, https://doi.org/10.6028/NIST.IR.7628r1

[9] IEC 62443 Series: “Industrial communication networks - Network and system security”

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

[11] Enrollment over Secure Transport – EST, RFC 7030, https://tools.ietf.org/html/rfc7030, 10-2013

[12] Simple Certificate Enrollment Protocol – SCEP, RFC 8894, September 2020, https://tools.ietf.org/html/rfc8894

[13] Whitepaper, Requirements for Secure Control and Telecommunication Systems, Version 2.0, 05/2018, BDEW - Federal Association of Energy and Water Industries and Energy Austria, Berlin, https://www.bdew.de/media/documents/Awh_20180507_OE-BDEW-Whitepaper-Secure-Systems.pdf

[14] IEC 62351-8, Power systems management and associated information exchange – Data and communications security – Part 8: Role-based Access Control

[15] IEC/TR 62351-10, Power systems management and associated information exchange – Data and communications security – Part 10: Security architecture guidelines, Edition 1.0 2012-10