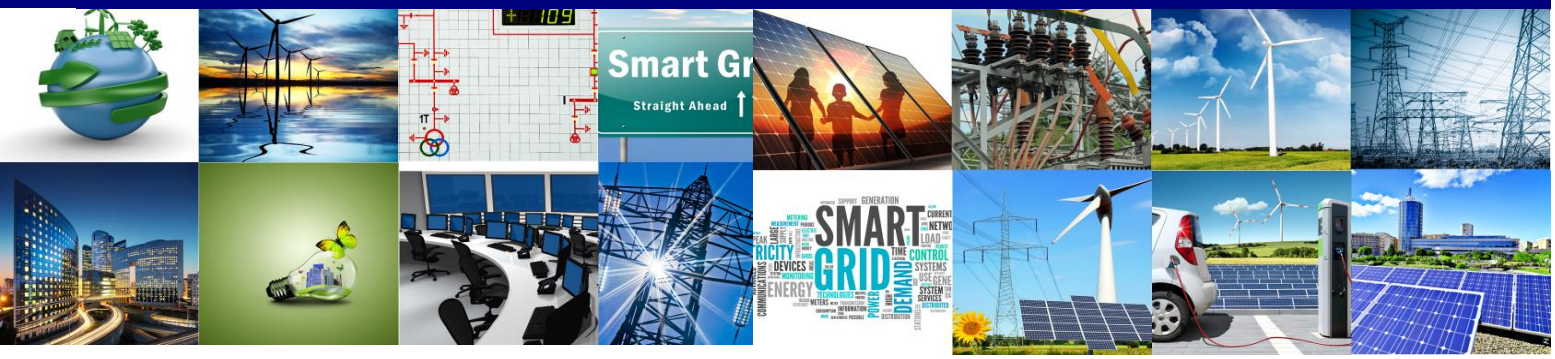
Project No. 609687

FP7-ENERGY-2013-IRP

ELECTRA

European Liaison on Electricity Committed Towards long-term Research Activities for Smart Grids



WP 4

Fully Interoperable systems

Deliverable D4.1

Description of security concerns and proposed solutions for the frequency and voltage control system

& Maturity model for smart grid risk assessment combining SGIS and NIST IR approaches

16/01/2015

ID&Title	**D4.1** Description of security concerns and proposed solutions for the frequency and voltage control system & maturity model for smart grid risk assessment combining SGIS and NIST IR approaches	**Number of pages:**	64

Short description (Max. 50 words):

This document consists of first ICT security related work in the ELECTRA project. The current Smart Grid security situation is discussed, along with most typical threats. The proposed high-level use cases are briefly reviewed concerning security aspects. Also, a novel maturity model and it's applicability to the project is discussed.

Version	Date	Modification's nature
V0.01	25/06/2014	First draft moved to ELECTRA template
V0.02	10/11/2014	Progress
V0.03	28/11/2014	Version ready for review, lacking the use case-review.
V1.00	15/12/2014	Submission for TOQA Review
V1.01	13/01/2015	Final corrections based on TOQA review
V1.02	16/01/2015	Submitted to ELECTRA Technical Committee

Accessibility

☒ PU, Public

☐ PP, Restricted to other program participants (including the Commission Services)

☐ RE, Restricted to other a group specified by the consortium (including the Commission Services)

☐ CO, Confidential, only for members of the consortium (including the Commission Services)

If restricted, please specify here the group:	

Owner / Main responsible:		
Chris Caerts (VITO)	WP4 Leader	
Reviewed by:		
J. Emilio Rodríguez (TECNALIA) Mihai Calin (DERLab)	TOQA assigned reviewer TOQA assigned reviewer	05/01/2015 05/01/2015
Final Approval by:		
ELECTRA Technical Committee		16/01/2015

Authors

Name	Last Name	Organization	Country
Sami	Noponen	VTT	Finland
Antonio	Del Giudice	ENEA	Italy
Özgür	Kahraman	TUBITAK	Turkey
Armağan	Temiz	TUBITAK	Turkey
Giovanna	Dondossola	RSE	Italy
Mathias	Uslar	OFFIS	Germany

Copyright

Consisting of:

Coordinator	
Ricerca Sul Sistema Energetico – (RSE)	Italy
Participants	
Austrian Institute of Technology GmbH - (AIT)	Austria
Vlaamse Instelling Voor Technologisch Onderzoek N.V. - (VITO)	Belgium
Belgisch Laboratorium Van De Elektriciteitsindustrie - (LABORELEC)	Belgium
Danmarks Tekniske Universitet - (DTU)	Denmark
Teknologian Tutkimuskeskus - (VTT)	Finland
Commissariat A L'Energie Atomique Et Aux Energies Alternatives - (CEA)	France
Fraunhofer-Gesellschaft Zur Förderung Der Angewandten Forschung E.V – (IWES)	Germany
Centre For Renewable Energy Sources And Saving - (CRES)	Greece
Agenzia Nazionale per Le Nuove Tecnologie, L´Energia E Lo Sviluppo Economico Sostenibile - (ENEA)	Italy
Fizikalas Energetikas Instituts - (IPE)	Latvia
SINTEF Energi AS - (SINTEF)	Norway
Instytut Energetyki - (IEN)	Poland
Instituto De Engenharia De Sistemas E Computadores Do Porto - (INESC_P)	Portugal
Fundacion Tecnalia Research & Innovation - (TECNALIA)	Spain
Joint Research Centre European Commission - (JRC)	Belgium
Nederlandse Organisatie Voor Toegepast Natuurwetenschappelijk Onderzoek – (TNO)	Netherlands
Turkiiye Bilimsel Ve Teknolojik Arastirma Kurumu - (TUBITAK)	Turkey
University Of Strathclyde - (USTRATH)	UK
European Distributed Energy Resources Laboratories (DERlab)	Germany
Institute for Information Technology at University of Oldenburg (OFFIS)	Germany

Executive summary

This deliverable discusses the security concerns related to a novel Smart Grid architecture that is proposed in the ELECTRA project. The main purpose of this work is to take cyber security into account from the very beginning of the project. The proposed high level architecture is for frequency and voltage control in the future power system (2030+).

ICT security is a major challenge in the Smart Grid, and developing a new architecture and features without taking security into account might result in serious consequences after deployment, such as grid instability. The main objective of the security work in the whole project will be to study the security of the proposed solutions and make recommendations on how to make them more secure. The proposed architecture and use case descriptions at this first stage of the project are high level, and therefore the security analysis work presented in this document is only the first step. A more detailed security analysis will be provided later on in the project. The main purpose of this document is to provide cyber security input for the design phase of ELECTRA.

This document also presents a summary of the current security threats facing the Smart Grid, specifically as frequency and voltage control is concerned, and lists mechanisms and countermeasures for mitigating these threats. Also, a novel maturity model that combines two well-known Smart Grid security approaches (NISTIR and SGIS) is presented and the applicability of this approach in ELECTRA is discussed.

Terminologies

Abbreviations

3DES	Triple DES, Triple Data Encryption Algorithm
ABAC	Attribute Based Access Control
AES	Advanced Encryption Standard
AVC	Automatic Voltage Controller
AVR	Automatic Voltage Regulator
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
COP	Common Operating Picture
DLMS/COSEM	Device Language Message Specification/Companion Specification for Energy Metering
DNP3	Distributed Network Protocol
DNS	Domain Name Server
DOS	Denial of Service
DSO	Distribution System Operator
ES-C2M2	Electricity Subsector Cyber Security Capability Maturity Model
ETSI	European Telecommunications Standards Institute
FRR	Frequency Restoration Reserve
GENCO	Any company doing electricity generation
HV	High Voltage
HAN	Home Area Network
HTTPS	Hypertext Transfer Protocol Secure
ICT	Information and Communication Technology
IED	Intelligent Electronic Device
IETF	Internet Engineering Task Force
IPSEC	Internet Protocol Security
IS	International Standard
ISMS	Information Security Management System
LAN	Local Area Network
LV	Low Voltage
MV	Medium Voltage
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
NVR	National Voltage Regulator
PLC	Programmable Logic Controller
PPVC	Post Primary Voltage Control

PV	Photovoltaic
PVR	Reactive Power (Q) Regulator of a single power plant
RABAC	Role Attribute Based Access Control
RBAC	Role Based Access Control
ROCOF	Rate of Change of Frequency
RVR	Regional Voltage Regulator
SCADA	Supervisory Control and Data Acquisition
SG	Smart Grid
SGAM	Smart Grid Architecture Model
SG-CG	Smart Grid Coordination Group
SGIS	Working Group Smart Grid Information Security
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
SSH	Secure SHell
TC 57	IEC Technical Committee 57
TFC	Tertiary Frequency Control
TLS	Transport Layer Security
TSO	Transmission System Operator
UCTE	Union for the Coordination of the Transmission of Electricity
VPN	Virtual Private Network

Table of contents

List of figures and tables

1 Introduction

This cybersecurity themed document presents the first results in the security task in the ELECTRA FP7 [1] project. The results are based on analysing the work done in the first year of the project. A second security deliverable will be released in 2017, when the ELECTRA concept and architecture are specified in more technical detail.

The ELECTRA project follows the European energy strategy through its Directive 2009/28/CE [2] that sets ambitious goals for the future. It is estimated, that in the future, electricity production will to a large extent be renewable energy coming from various distributed resources. This has a wide impact on the communication network topology and ever growing complexity as well. Integrating new information and communication technologies into Smart Grids are required when developing new functionalities.

Cybersecurity is one of the major challenges of any Smart Grid development. New information and communication technologies constantly increase the efficiency of the electric grid, but at the same time the new functionality causes new vulnerabilities and threats to arise and adds complexity. Smart Grids are part of a critical infrastructure and the massive deployment of IT-based components in the area of the electricity network also brings additional challenges to cybersecurity. These IT-based components are often required to implement the required properties in the communication infrastructure.

The planned mechanisms for managing the voltage and frequency levels in the ELECTRA architecture will widely utilise different communication infrastructures. Stability is a very critical property of the Smart Grid, and frequency and voltage are the essential properties for maintaining it. Therefore securing these operations is very critical, because the impact of successful attacks is very high. Cyber-attacks mainly come through communication networks and therefore this document is mostly focused on the security of related information and communication technology.

1.1 Scope

This document describes the initial cybersecurity analysis of the ELECTRA control system concept. The cybersecurity research in this document focuses on communication, security threats and countermeasures. Also the general situation in SG cybersecurity is discussed. Even though the term cybersecurity encompasses several issues such as physical access, this deliverable is mostly focused on ICT information security. Observing the state of the electricity network is a critical part of the ELECTRA project concept and it is required for making decisions for frequency and voltage control.

The aim of the work is to take cybersecurity into account from the very beginning of the project.

This is carried on by:

- Taking security as a design criteria when defining the high level functional architecture
- Surveying regarding available security technology
- Analysing the security of high-level use cases
- Identification of generic and domain specific security technologies
- Giving security input for and reviewing the design documents of the project

1.2 Structure

The document has been divided into 5 chapters that cover the different work done in the security task during the first year of the project.

Firstly, a general summary of current Smart Grid security and examples of potential threats, attackers and attack types are given in chapter 2. This is followed by a survey of security technologies and standards related to protecting the Smart Grid.

In chapter 3, we focus specifically on the security aspects related to voltage and frequency control. At first based on current control schemes, then based on the proposed ELECTRA architectural concept.

In chapter 4, a maturity model for smart grid risk assessment combining SGIS and NIST IR approaches is presented, and the applicability of this maturity model-approach for ELECTRA is discussed. Finally, conclusions are given in chapter 5

2 Smart Grid cybersecurity overview

2.1 Smart Grid cybersecurity

In recent years, the electric industry has started a process of integration of the electrical distribution systems with communication networks in order to form a new infrastructure called Smart Grid (SG). At the cost of adding distributed intelligence and new real time communication capabilities, the system gives back more energy efficiency, reliability and sustainability. The transition from the old distribution network to the new SG implies moving from a relatively small number of devices that exchange very few information and commands to a new environment with a high number of nodes that receive and send information in a real time fashion. This transition brings the traditional ICT and telecommunication sectors closely tied to the SG, because traditional components from the ICT world are applied. This also means that the security vulnerabilities and challenges from traditional ICT world are now relevant for the energy sector as well. The sophistication and volume of cyber-attacks are increasing every day.

The threats and risks that come from this intricate network of nodes have to be carefully handled. In the traditional electric grid a great effort have been done in order to reach a high level of safety. For safety mechanisms we intend all the countermeasures that have been taken to make the system not able to damage the environment or to put in danger the life or health. With SGs, this is still relevant, but not enough anymore.

The number of possible vulnerabilities arises when critical infrastructures are increasingly connected to the traditional ICT networks. More and more automation and remote monitoring/control are brought into the SG. Also, the ever growing complexity of the SG increases exposure to potential attackers. The SG can be considered secure and reliable only if the integrated control and communication system is reliable.

The concept of security in the information technology sector (usually referred to as cybersecurity) is divided into three main concepts: *confidentiality*, *integrity*, *availability*. Among the fundamental properties for cybersecurity, usually availability gets the highest priority when it comes to power systems. This differs from the ICT world, where the confidentiality is most often the top priority. One of the main reasons why availability is the top priority is that to most users, it is crucial to obtain the sufficient amount of power exactly when needed.

The second security attribute is confidentiality. Interconnected systems can increase the exposure of private customer information. Confidential information can be for example a collection of data about customer, personal information, consumption data and billing data. This data can reveal a lot of information about a customer's activity and behaviour. Utility companies need to rely on collected measures for both control purposes of the network parameters (voltage and frequency of the generated power) and to be able to produce the bill for customers without errors. Since there is the need to exchange confidential information and commands that regulate the grid, they have to be secure and it is important to adopt a secure encryption mechanism. The Triple Data Encryption Standard (3DES) is one example of encryption techniques that is used for exchanging data securely and in the NIST vision it will be used also in Smart Grids. But even so, NIST has stated that 3DES cannot be considered secure after 2030, yet the grid has a long lifetime. That's why another encryption algorithm, such as AES, would be preferred for new devices.

Finally, the third attribute, integrity, aims at delivering measures that are not corrupted during data transfer, for example from meters to data centres. The integrity attribute also applies to source reliability, in other words, the property that makes sure the receiver of the data really gets it from the correct sender and unchanged in transit.

Smart metering

Smart meters are briefly discussed here, because of their ever growing role in the Smart Grid deployments. Smart meter is a device based on a digital microprocessor capable to take precise measures and to communicate by means of a bi-directional channel so that it could send measures on request and receive commands (e.g disconnection of loads). During the '90s, energy operators started studies on mechanism to obtain temporally dense information about energy consumption of domestic and non-domestic (industrial) users. The basic idea was to design a system that is able to collect measures with a maximum period of 30 minutes. With the collected data the energy operators claimed to be able to improve the management of the power grid by minimizing the risk of discontinuity in the service. There are also other benefits that come from a bidirectional information flow integrated with the power grid: the meters are spatially scattered so it is easier to detect a bad functioning of a part of the grid and isolate it without compromising the working zones. The fine measures about consumption can be returned to the customers to improve the knowledge about the costs of consumptions during certain hours of the day so that people can be educated to use heavy loads only at more convenient times To obtain all these real time information there is the need of an integration between the energy grid and an bidirectional, real time information flow channel.

Cybersecurity is a major issue with smart meters, because of the bi-directional communication flow. Both hardware and software of the meters components have to be extremely reliable. Security can be compromised by a simple bad functioning of the hardware or by an intentional introduction of bugs into the software with the intent of tampering the grid or extort money from the energy operators. The role of smart meters in the ELECTRA project is not clarified yet, but they will likely have some role in the proposed architecture and use cases discussed later in the document.

2.2 Smart Grid threat landscape

Many electric sector infrastructures were built and designed at a time when cybersecurity attacks were not an issue. Through increased connectivity, software vulnerabilities in the SG network devices might open doors for serious attacks and result in serious consequences. Connecting common off-the-shelf ICT components to the nodes in the electric grid may cause vulnerabilities to spread. By abusing these vulnerabilities, attackers may penetrate the network, access control software, alter load conditions and cause instability to the electric grid.

To control the risk of the emerging SG, the utilities need to know and understand the vulnerabilities present in the system seen as a whole, the threats that could exploit them to penetrate into the system and manipulate some crucial parameters, and the consequences of a successful attack on the entire network.

A classification of the expected losses could be useful to take cost effective decisions on the security measures used to protect specific areas of the grid. In order to make reliable risk estimations and decide the security policies of the network, a risk assessment methodology which can estimate the adverse effects of the exploitation of a vulnerability, e.g. to get more privileges or to pass authentications firewalls, is needed.

There are three main potential threat classes in SG: manipulation, sabotage, espionage.

Manipulation attacks encompass a wide selection of threats. Manipulation attacks can target both hardware, and software. For example, through manipulation, attackers may affect the correctness

of the billing process or metering process or both. For manipulation attacks, the attacker needs to gain access to the network. The security manager has to rigorously define the authentication, privileges and other mechanisms for all network entry points. For example the access privileges for a domestic node have to be less powerful than those to a substation node. In an example manipulation attack, a modified software image is passed off as upgrade for meters (a requirement for smart meters is the possibility to update the software remotely) through which the programmer of the malicious software is able to change the tariff mechanism.

Sabotage; the main purpose of sabotage is to cause damage to equipment or people. For example, the attacker attempts to take over the control over systems that can be remotely controlled. Photovoltaic plants or wind generators can cause overvoltage at the end of a line, switching on or off at the wrong moment can cause serious damages to electrical equipment connected to the grid, and in case of an industry this can lead to heavy financial consequences.

Industrial Espionage happens when the attacker gains access to confidential information of the customer or the utility. This information contains company secrets, or in the case of metering it could be used to acquire knowledge of the habit of the customers and make deductions on the presence or absence of a person in a flat, or to specify the type of equipment in a house.

In addition to the previous, the communication protocols have to face different types of attacks. One simple attack is the replay attack. Once the communication channel between two entities of the grid has been located, an attacker is able to capture some messages (a load disconnection command for example) and retransmit it later; such time difference in the reception of message can cause great damages to the network. To avoid these types of attack every packet and every command sent to the grid must have a time reference by means of timestamps, which implies that entities in the grid have to be synchronized.

On the other hand, many control mechanisms are based on the services offered by the SG and the network exposes the grid to many vulnerabilities some of them even not known. In the SG there are many points from which an attacker can try to enter into the network. In recent years many cybersecurity reports related to SG have reported an increase in the frequency of attacks performed to the power grid. A good source for following the latest threats to industrial control systems, including the energy sector is ICS-CERT-group [3]. Based on ICS-CERT reports, attacks and malware towards the critical infrastructure has been on the rise especially after 2010.

The ENISA report makes a list of the cybersecurity attacks prioritized according to the number of occurrences of attacks in a fixed period of time [4].

- Drive-By Downloads:
  Web based attacks are the most frequent and the trend for these type of intrusion attempts is increasing. The increasing trend is explained by the fact that this attack is easy to perform. Typically attackers infect websites with malicious code, so that visitors of these web sites are scanned for entry points on their machines and operating systems, and once the weakness is found it is exploited to install a malware.

- Malicious Code:
  Spreading malicious programs is a practice that permits to attackers to obtain personal information by means of malware and Trojans. The malicious code must be installed on the target devices before it can be used. Creating malware variants based on existing code using the technique of polymorphism does not require a high level of competence.

- Code Injection:
  There are many tools available to attackers to produce Code Injection attacks: Cross-site scripting, SQL injection, Directory traversal are only few examples. And the proliferation of automated attack tools impacted the frequency of this threat.
- Exploit kits:
  These are tools that offer a large variety of functions. They have the ability to find a vulnerability of a device in order to abuse them and perform an ad hoc attack. The most successful exploit kit was “Blackhole”, and the developer of that tool has been arrested.
- Botnets:
  Botnets are collections of small programs performing a single task. In case of malicious intentions that task is most of the time to perform a denial of service attack or to send spam emails.
- Physical Damage:
  Data can be stolen by means of the techniques mentioned above but can be also destroyed causing big problems to the owner. This is the intention of the Physical Damage attack.
- Identity Fraud:
  This attack is very effective if well performed. It is about stealing the identity or credentials of a user that is allowed to bring modifications to a system or has access to sensitive data. The attacker could acquire all the privileges of an authorized person.
- Denial of Service (DoS):
  When an attacker is successful in performing a DoS attack, he will make the target unavailable for a certain period of time. The sophistication of DoS attacks is growing making them difficult to prevent and defend against. There are many variants; an interesting one is the DNS reflection effect. With this technique attackers can multiply the volume of their attacks by asking to DNS servers to send large replies to the victim. An interesting daily report on the activity of this type of threat in the world is depicted at http://www.digitalattackmap.com/.
- Phishing:
  This attack is intended to get sensitive information such as a password or personal data from the victim by means of a trick. This threat is not strictly technical rather is social and cultural, and is often based on the lack of information and knowledge of people about online operations and transactions.

There are several motivations that encourage malicious attacks, for example one could be interested in the energy activity of a domestic environment to study the times of presence in the house. Since the electric grid relies on an information network to keep the stability, a cybersecurity attack could result in catastrophic consequences for the energy operators. Unauthorised billing manipulation is not far-fetched example that can motivate somebody to hack the system for financial gain. The entities interested into the hacking of the information system of the electric grid are listed, but not limited to, the following:

- Insider threat
  Perhaps one of the most critical and difficult to detect is the insider threat. Insider threat comes from the people within the organisation, or for example through subcontracting. The threat arises from countless motivations such as personal financial difficulties, revenge, and disappointment. Human errors and accidents can also be counted within the insider threat.
- Corporations
  For example a corporation could benefit from the knowledge of confidential information on competitors. Corporations usually do not make attacks themselves, but rather they engage specialized groups to perform the intrusion.
- Nation States
  Nation States are often interested in intrusion because they want to acquire military secrets, State secrets or attempt to disrupt the reliability of an essential service of another State.
- Hacktivists
  Groups that are ideologically motivated could attempt to disrupt the security of other entities just to gain attention and exhibit their ideas.
- Cyber-Terrorists
  This group tries to influence the decision or actions of a State by mean of violence. Main targets are critical infrastructures.
- Script Kiddies
  Due to their large number, even if they lack deep technical knowledge, these groups can strongly compromise the security of an entity.

2.3 Security technologies related to Smart Grid protection

From the ICT security point of view of SG, there are three main areas to be dealt with, which are the **communication medium/system**, the **physical area** around the communication system and the **users**' privileges/access techniques to the system.

2.3.1 Physical protection and environmental security

Physical and environmental security techniques are mostly used to protect electrical equipment and buildings in generation, distribution, and transmission levels. It encompasses protection of physical assets from damage, misuse, or theft. Physical access control, physical boundaries, and surveillance are examples of security practices used to ensure that only authorized personnel are allowed to access SG information systems and components. Environmental security addresses the safety of assets from damage from environmental concerns. Physical and environmental security addresses protection from environmental threats. Methods to harden physical and environmental security are given below [5].

- Physical and Environmental Security Policy and Procedures
- Physical Access Authorizations
- Physical Access
- Monitoring Physical Access
- Visitor Control
- Visitor Records
- Physical Access Log Retention
- Emergency Shutoff Protection
- Emergency Power
- Delivery and Removal
- Alternate Work Site
- Location of Smart Grid Information System Assets

2.3.2 Access Control

Permissions, privileges, and access control are generally applied on the system which requires remote monitoring and control systems either with Internet based systems or dedicated private networks.

Since the planned voltage and frequency schemes include remote systems that have different access rights, these three aspects can be used to protect the control schemes. For the access control the general introduction is given about RBAC, ABAC, and RABAC, which are currently in use. Considering the complex smart grid topology, it may be a good option to develop specialized access control model for smart grid.

a. Role Based Access Control (RBAC);

A role is a collection of permissions that may be granted to a user. An individual user may be given several roles or may be permitted different roles in different circumstances and may thereby exercise different sets of permissions in different circumstances [5]. This access control model gives handling capability for management of many users. Role in RBAC is a collection of permissions [6]. A user is assigned to a role which has permissions for execution of certain operations. Access control system manages roles rather than each individual user for permission assignment. This feature makes management by the help of privileges depending on the role. However, in real cases, multiple and complex factors and number of roles may be needed to cover all factors and variables in the system.

b. Attribute Based Access Control (ABAC);

In ABAC, access rights are granted to users through the use of policies which combine attributes together. Attribute describes the identity or feature of a subject (e.g. user attributes, resource attributes, environment attributes). In ABAC, access is granted on the basis of attributes of the user [7]. To grant access, the user has to prove that his/her attributes are satisfying claims specified on the access control policy of the system. This model is more comprehensive when compared with RBAC.

c. Role Attribute Based Access Control (RABAC);

By adding attributes to role-based access control model, this RABAC model is created (Informal-Suggestion) [8]. RABAC has the advantages of RBAC and ABAC [9]. This model can be thought of as the combined model of RBAC and ABAC, thus it may be a good background for developing specialized access control modes for SGs [8].

2.3.2 Communication medium / System security

a. Host hardening

*H*ost hardening (security hardening) is widely used among the smart grid systems especially on servers, monitoring & control stations, and other computers included in the system. Host hardening must be applied to all computers especially which are connected to a LAN, HAN or Internet in the ELECTRA System. In general, a hardening process can be classified in three areas:

- *Operating System Hardening:*
  - Unnecessary services and ports should be closed in order to prevent any threats coming from them.
  - User authorization should be done to reduce vulnerabilities caused by the unauthorized users.
  - Log files which are located in C drive by default should be removed to D or different drive and access restriction should be made.
  - Windows or other firewall settings should be set to the high level restriction which does not block the normal operations.

- Login policies should be changed to prevent brute force attacks. Also, using more secure passwords, changing password after a certain time, and such precautions must be made compulsory to users.
- Windows or other operating system updates which are the crucial part of enhancing cybersecurity should be kept updated.

❖ *Database Hardening:*

- Most current database patches should be installed to avoid security gaps.
- Unused “guest” account should be removed from the "msdb" database.
- “Public” rights on important objects should be removed.
- Other technical arrangements should be made on the form of keeping database records.

❖ *IIS (Internet Information Services) Hardening:*

- Unnecessary services which comes from the default installation and may cause vulnerabilities to the system should be closed.
- The location of default IIS folders which can be a tool to manage important files should be changed from C drive to another drive to prevent cyber-attackers to get local manage folders.
- More current and secure protocols should be made to use.
- Location of the IIS log files should be changed from C drive to another location in order to prevent the cyber-attacks which create unnecessary logs on C drive to fill memory and block the operating system.

b. Anti-virus software

Anti-virus software is crucial to all computers and servers to prevent any cyber-attack or malwares.

c. Log review

In order to track the status of the system, make the maintenance process easier, and determine the exact cause of the errors, any important system or device in voltage and frequency control systems should have logging support. For operating the system successfully and considering maintenance of the system, logs should be taken and reviewed periodically.

d. Redundancy

Important devices and cables are designed considering the N-1 security criteria in electrical transmission and distribution networks. For instance, frequency and voltage control servers, some critically important RTUs and relays, main controller of a SCADA system, and communication mediums for these devices are designed with a back-up solution. If any component of the system at any critical level is broken or malfunctioning, the back-up device or component starts to operate in order to keep the system working as planned.

e. Network Security Monitoring

Network Security Monitoring is the collection, analysis, and escalation of indications and warnings to detect intrusions and respond to them.

f. Network segmentation

Segmentation is the act of splitting a computer network into subnetworks, each being a network segment or network layer. Advantages of splitting are primarily for boosting performance and improving security. If the attacker gains access into one part of the network, moving to another part of the network can be protected.

g. VPN

A Virtual Private Network (VPN) extends a private network across a public network, such as the Internet. A VPN is a virtual point-to-point connection through the use of dedicated connections and the connection is protected with encryption and authentication mechanisms. VPNs are widely used in critical infrastructure with remote management applications.

2.4 Smart Grid standards incorporating security technologies

In the following section an overview of the security standards for SGs, available or under development, is provided. To ensure the security and at the same time scalability of the SG it is important to work with standardization bodies or relevant research organizations such as ENISA, CEN/CENELEC/ETSI and NIST. The security of the entire grid depends on technologies used for privacy, authorization and authentication.

SG devices have to exchange information on the state of the grid continuously and on command requests implementing the control scheme. The selected protocol for communications must be based on existing standards so that the stakeholders can produce devices that are interoperable. Nevertheless the protocol should include security mechanisms that allow exchanging confidential information and commands to actuation devices that modify the status of the network. The grid may check in every moment the value of voltage and frequency and in case of values out of the boundaries the grid controllers have to be able to request/actuate actions that modify these values like the switching on or off of diesel generators. The control actuation on the physical system is enabled by means of communication packets that need to be secured by appropriate protocols.

The growing awareness of cyber-risks has pushed the smart grid actors to investigate into security standards currently applicable for the smart grid IED (Intelligent Electronic Devices).

Recently the international standardization committees have started the analysis of the current communication and security standards mapping them on the control use cases of SGs.

Since 2010, the US National Institute of Standards and Technology (NIST) provided a comprehensive guideline for smart grid cybersecurity analysing the risk levels, security requirements and measures of the main logical network interfaces [14]. This standard identifies a high level scheme (Figure 1) containing a set of 47 different actors distributed among 7 main smart grid domains: Transmission, Bulk Generator, Marketing, Operations, Service Providers, Distribution and Customer. Each actor interacts with others entities through logical interfaces (Figure 2) grouped in 22 categories, according to their scope and their security-related characteristics. These categories were defined based on attributes that could affect the security requirements.

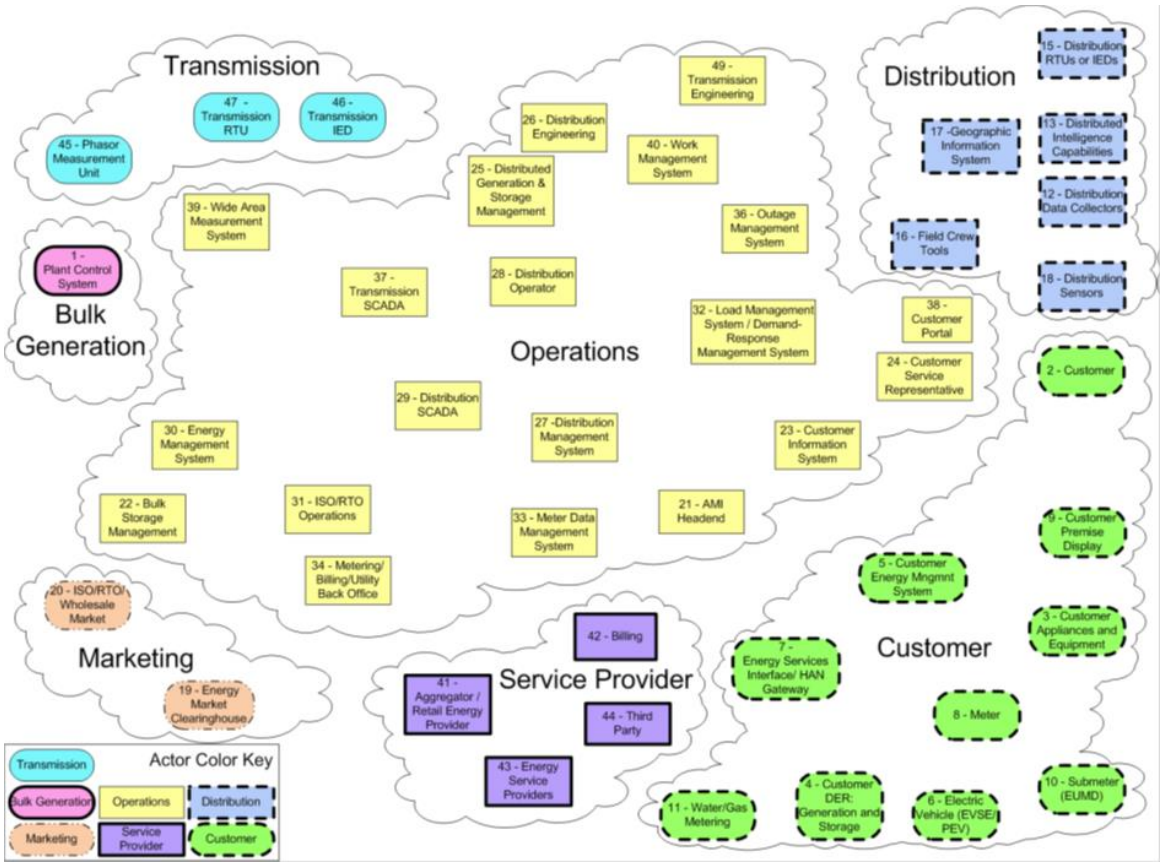


Figure 1: Smart Grid domains and actors - NIST IR 7628

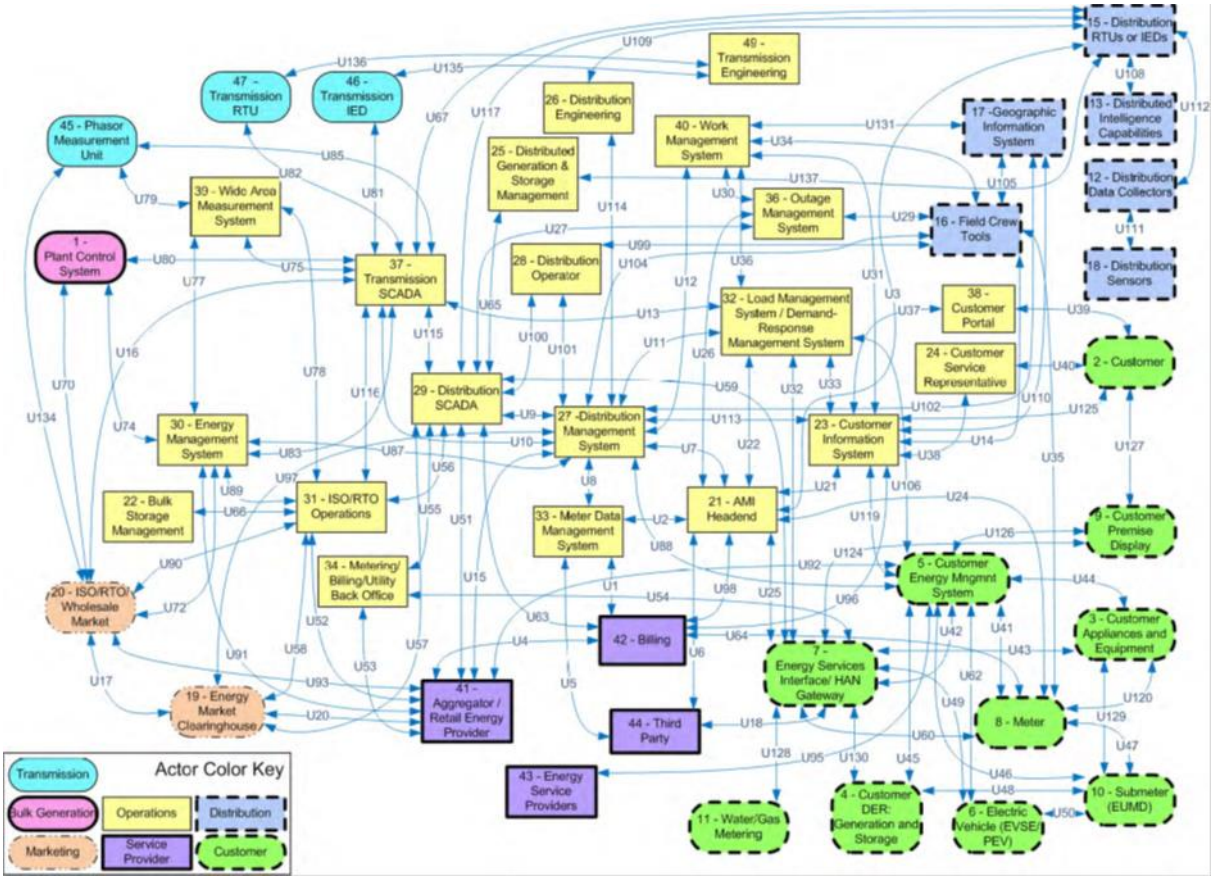


Figure 2: Smart Grid Logical Interfaces - NIST IR 7628

The recently launched NIST Cyber Security Framework [5], targeted to help critical infrastructures operators improving their cybersecurity, deserves special attention from the smart grid utilities.

The Working Group Smart Grid Information Security (SGIS) of the CEN/CENELEC/ETSI Smart Grid Coordination Group investigated a set of security standards supporting the SG reliable operation [15]. Besides the investigation into the coverage of selected standards (Figure 3), also the mapping of the set of security standards to SGAM is addressed, showing their applicability in the different smart grid zones and domains on a general level. The result is intended to enhance the SGIS toolbox with the considered standards to allow for the appropriate selection of security controls to address determined security requirements in the specific SGAM zone, domain, or layer. It has been acknowledged that the list of standards may not be complete and that there are certainly more standards contributing to SG security, which also needs to be investigated.

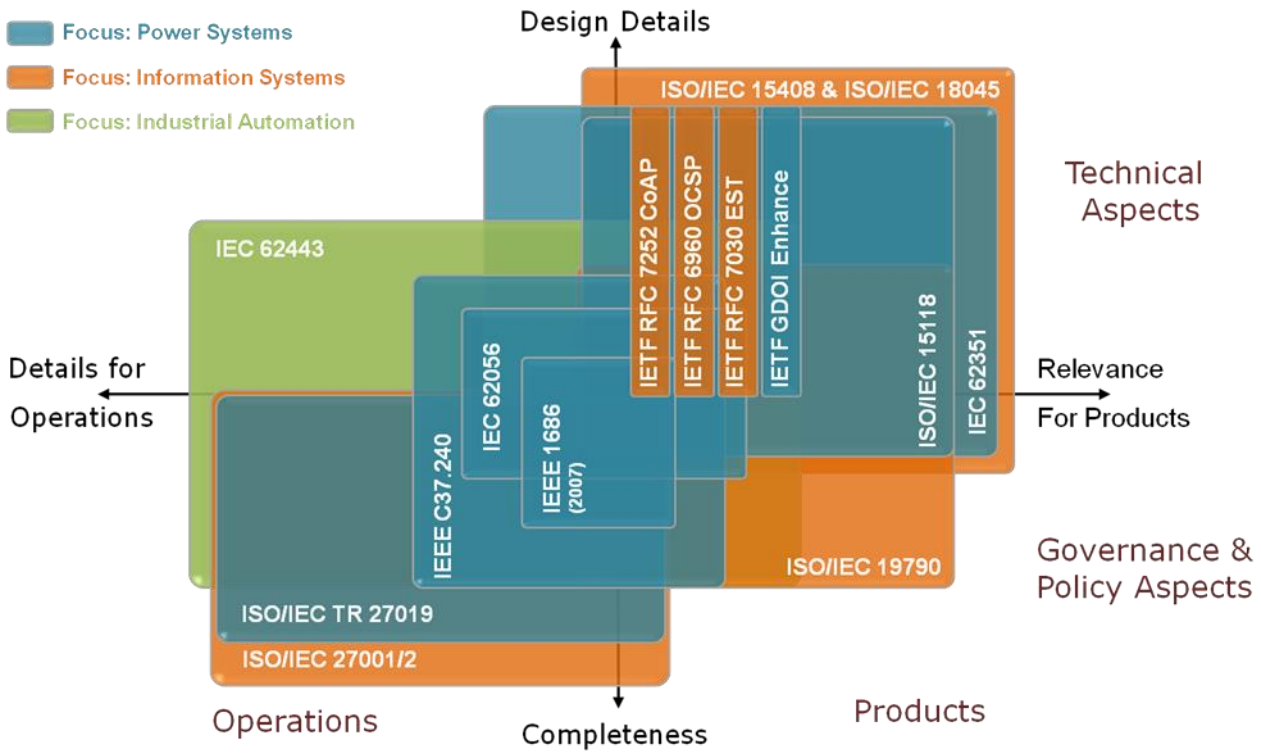


Figure 3: Standard coverage [SGIS Report]

With reference to the support provided to the power utilities for comprehensive security governance, three distinguishing security frameworks are noteworthy. The ISA99 committee, originated from the process industry, is quite active in developing process and product oriented specifications applicable to the industry at large, which could be used for the power industry. Their advanced drafts are used as input for the IEC Technical Committee 65 to turn them into IEC standards or technical reports (IEC 62443 series).

ISO/IEC have produced two standards that provide a general framework for information security management:

1. ISO/IEC 27001 Information technology – Security techniques – Information security management systems – Requirements
2. ISO/IEC 27002 Information technology – Security techniques – Code of practice for information security management

ISO/IEC 27001 provides a model for establishing, implementing, operating, monitoring, reviewing maintaining, and improving an Information Security Management System (ISMS). First, it is necessary to define the control objectives regarding the risks that have to be mitigated (rather than accepted, avoided or transferred). Then controls that are going to be used in controlling the risks must be identified or defined. This usually means that each control from a large control set has to be evaluated in the context of the scope. It uses a circular management structure based on the Plan – Do – Check – Act cycle. This management structure is common to several ISO management standards, most notably ISO 9001 and ISO 14001. ISO/IEC 27001 is very specific about how ISMS should be set up.

ISO/IEC 27002:2013 standard contains 14 security control clauses collectively containing a total of 35 main security categories and 113 controls. The security control clauses are:

1. Security Policies
2. Organization of information security
3. Human resource security
4. Asset management
5. Access control
6. Cryptography
7. Physical and environmental security
8. Operations security
9. Communications security
10. System acquisition, development and maintenance
11. Supplier relationships
12. Information security incident management
13. Information security aspects of business continuity management
14. Compliance

The ISO 27002 standard is designed for organizations to use as a reference for selecting controls within the process of implementing an ISMS based on ISO/IEC 27001 or as a guidance document for organizations implementing commonly accepted information security controls. In particular the set of controls is sector-agnostics, as the controls defined in the standard address overall issues, defining the objective of each control group and giving some high level guidance about the implementation that usually must be further defined to suit the peculiar security requirements of the organization and the business process.

For this reason, the ISO/IEC 27000 family also provides standards or technical reports addressing specific security requirements found in specific sectors. One of these documents addresses specifically the process control systems sector as used in the energy utility industry: the ISO/IEC TR 27019:2013 [29]. The technical report complements the set of controls contained in the

27002:2005 providing further guidance to implement the controls due to the specific requirement of the energy utility industry sector. The reason for such a document is that process control systems show increased requirements with respects to availability and integrity. Failures are not usually tolerated and the integrity can be crucial due to the nature of the business process. For example, failures and incorrect data cannot be tolerated in critical infrastructures like the energy ones and may imply danger for the personnel's health or cost human lives. Those specific requirements must be considered in the establishment and implementation of the ISMS.

The scope of the ISO 27019 Technical Report embraces the typical architectures and components of industrial control systems, and explicitly enumerates the following ones:

- The overall IT-supported central and distributed process control, monitoring and automation technology as well as IT systems used for their operation, such as programming and parameterization devices;
- Digital controllers and automation components such as control and field devices or PLCs, including digital sensor and actuator elements;
- All further supporting IT systems used in the process control domain, e.g. for supplementary data visualization tasks and for controlling, monitoring, data archiving and documentation purposes;
- The overall communications technology used in the process control domain, e.g. networks, telemetry, telecontrol applications and remote control technology;
- Digital metering and measurement devices, e.g. for measuring energy consumption, generation or emission values;
- Digital protection and safety systems, e.g. protection relays or safety PLCs;
- Distributed components of future SG environments;
- All software, firmware and applications installed on above mentioned systems.

A widely recognized solution standard in the SG arena is the IEC 62351 series, in charge to the IEC TC 57 (Power systems management and associated information exchange) WG15 (Data and communication security). The series provides security standards for the communication protocols defined by the IEC TC 57 (see Figure 4), specifically the IEC 60870-5 series, the IEC 60870-6 series, the IEC 61850 series, the IEC 61970 series, and the IEC 61968 series, and undertakes the development of standards and/or technical reports on end-to-end security issues.

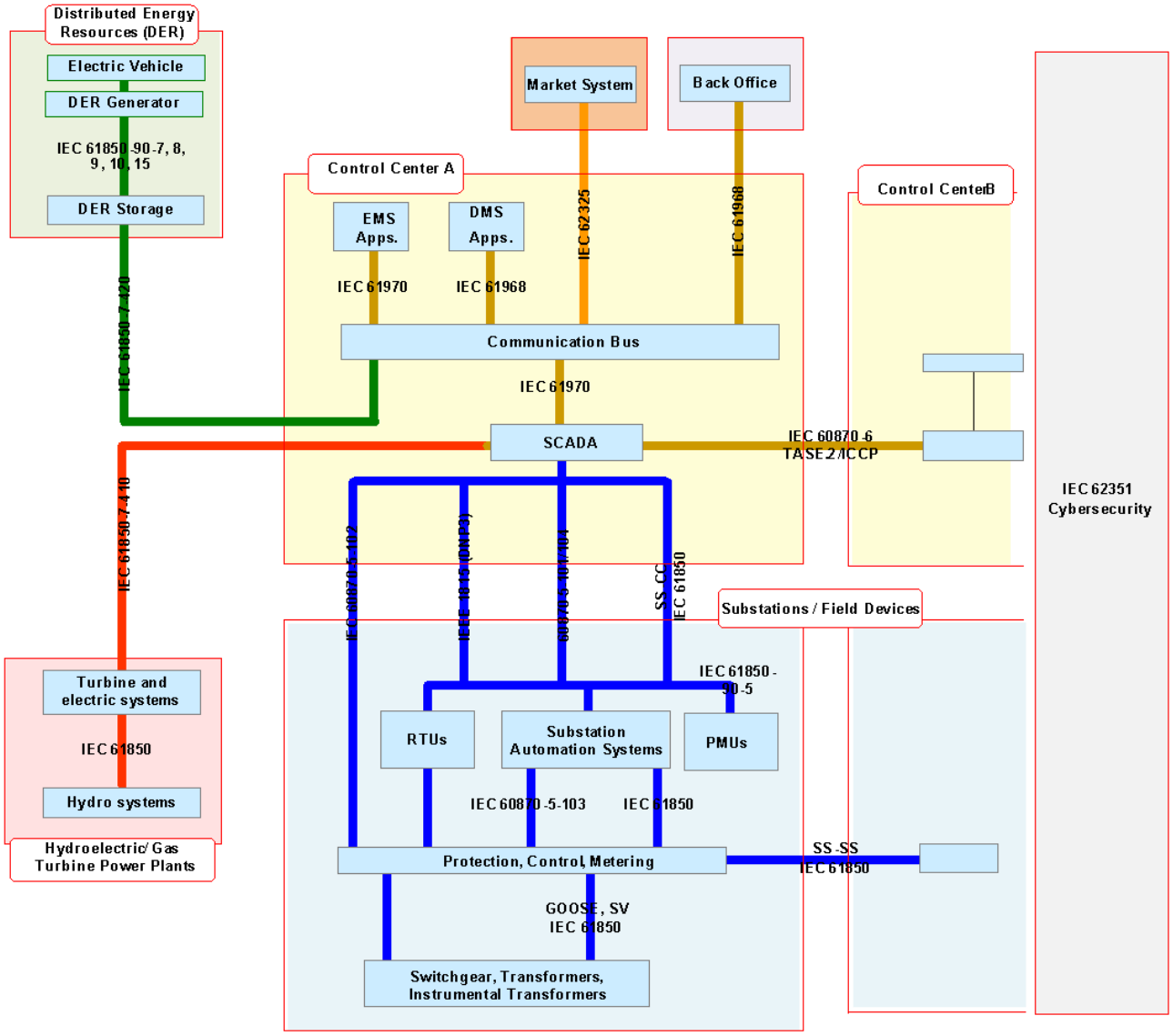


Figure 4: IEC TC57 communication standards [IEC 62351-1]

The approach is to build an end-to-end security system in order to ensure: authenticated access to sensitive devices of the remote control system, authorized access to sensitive data for the purposes of the electricity market, have reliable historical information on the operation and the malfunction of the equipment, perform the rescue and have at any time the data for the restoration of critical equipment (backup) and finally a reliable record of those data from which to reconstruct the crucial events at any time.

Figure 5 shows an overview of the IEC 62351 standard series parts, including the scope and the relationships with the TC 57 communication protocols that each IEC 62351 part aims to cover.

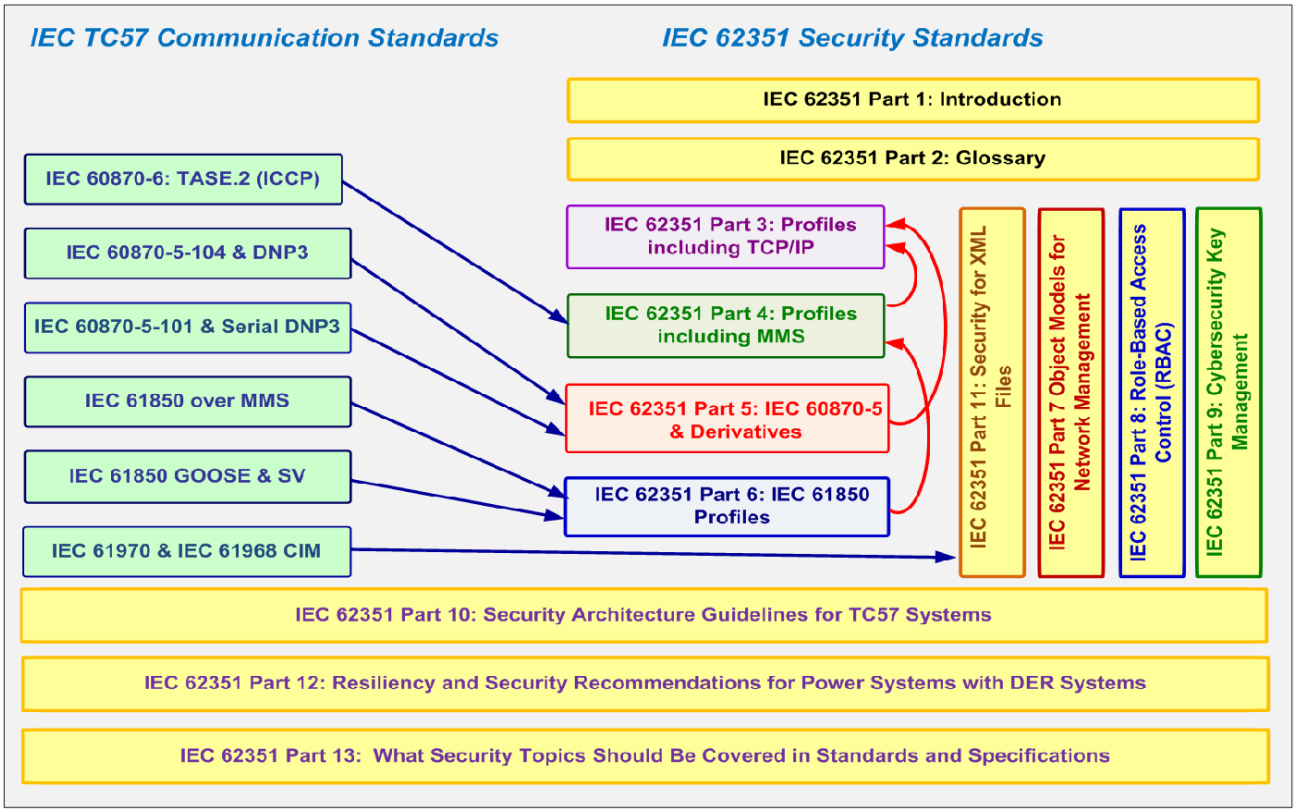


Figure 5: IEC 61351 linked to TC 57 communication standards

IEC 62351-1 and IEC 62351-2 define respectively the general standard scope and concepts and the glossary. IEC 62351-1 intends to address inadvertent and deliberate threats, underlying that the overall security of power system operations is threatened not only by deliberate acts of espionage or terrorism but by many other, sometimes deliberate, sometimes inadvertent threats that can ultimately have important impact. From a general perspective the security goal of IEC 62351 series are expressed in term of the following requirements:

- Availability of systems
- Integrity of systems and information
- Confidentiality of information
- Non repudiation of actions.

IEC 62351-3, IEC 62351-4, IEC 62351-5 and IEC 62351-6 address the security of specific protocols or entity protection.

IEC 62351-7, IEC 62351-8, IEC 62351-9 and IEC 62351-11 are no protocol specific parts but instead have the goal of covering the key enabling features, needed to operate the other more protocol/entity specific IEC 62351 parts, such as monitoring objects and protocols, role based access control, key management and XML security.

IEC 62351-10, IEC 62351-12 and IEC 62351-13 are guidelines documents, overviewing architectural and security requirements.

IEC 62351-10 targets the description of security architecture guidelines for power systems based on essential security controls. The relation and mapping of these security controls to the general

system architecture of power systems is provided as guideline to support system integrators to securely deploy available standards in power generation, transmission, and distribution systems. This guideline complements the detailed, specific technical aspects defined in the other parts. The issues related to the interoperable integration of security measures are also addressed in the technical report IEC 61850-90-12.

The first edition of IEC 62351 series have been released as TS (Technical Specification) according to IEC document classification. The latest and ongoing documents have been intended to be released as IS (International Standard). Further details on IEC 62351 can be found in [16].

Worth to be mentioned in the smart grid arena is the solution standard series IEC 62056 [30] for electricity meter data exchange: the international standard versions of the DLMS/COSEM specification. Data protection and information security in DLMS/COSEM is one of the topics that have reference in this standard. With the increase of computation power, the requirements for the use of a strong cryptographic mechanism are a priority, and DLMS/COSEM provides two main information security features for accessing and transporting data in a secure way. In DLMS/COSEM there are three data access security levels: no security, low level security and high level security. As a message security mechanism DLMS/COSEM specifies a data transport security system, a cryptographic protection that can be applied before sending a DLMS APDU (Application-layer Protocol Data Unit) with some security policies such as security not imposed, all messages authenticated, all messages encrypted, all messages authenticated and encrypted.

Three security contexts are defined:

- Security policy in force determining the kind of protection to be applied
- Security suite specifying the security algorithm(s)
- Security material relevant for the given security suite, including elements like block keys, authentication keys, initialization vectors, etc.

The security elements in this standard are a balanced cost-effective choice of security controls for equipment having resource limitations like smart meters.

Complementary to the security standards described above, that are specific to the power sector, there are several security standards (IETF and ITU-T) widely deployed in the general ICT context. VPN, IPSEC, TLS, SNMP, HTTPS, SSH are only some examples of such standards.

A quite comprehensive list of standards and guidelines describing security measures and technologies for smart grids can be found in [17].

3 Cybersecurity for voltage and frequency control

In this section, the frequency and voltage control strategies, and their associated communication requirements are presented, followed by an assessment of related cybersecurity threats and requirements. This is first done for the current - central - control approach. After that, the proposed ELECTRA control architecture is described in more detail.

3.1 Security concerns related to current frequency and voltage control systems

Nowadays voltage and frequency regulation systems belong to the first line of defence, which tries to keep the normal state of the interconnected power system (electrical security criterion N-1). This line of defence implies also the coordination with the neighbouring foreign TSOs because the power grids of some European countries are interconnected in wide regulation areas which constitute the UCTE interconnected system.

Each TSO control area adopts a hierarchical approach to frequency and voltage regulation [10]. The primary frequency regulation is performed by local controllers regulating the frequency of a single generator. The secondary frequency regulation has the goal to control the frequency of an interconnected power system. This coordination is obtained keeping the exchanges of energy among neighbouring countries to prefixed values. Each UCTE member realises this secondary frequency control using a different kind of control scheme. In the case of the Italian grid that has a longitudinal structure with only one area in direct contact with the European electric system, the grid is subdivided in one actual control area and two other virtual areas, which are organised in a decentralised adaptive scheme. This solution allows employing the energy reserves in a different way among the virtual control areas, every time the energy exchanges overcome the congestion values. It is up to the real control area to regulate the global exchanges of energy compensating the deviations of active power of the virtual areas, and to control the frequency of the whole electric power system.

The secondary frequency regulation has been implemented by a secondary frequency controller installed in a (national or regional) control centre which decides the reference frequency value (fref) to be sent to all the primary frequency controllers of those generators under the secondary frequency regulation regime. This is done in order to guarantee a right division of the load among the generators. This function which is described in Figure 6 through the secondary frequency regulators, changes the mechanical power for each generator in order to guarantee a good value of the grid frequency. In Figure 6 the secondary frequency regulator is called “Network Regulator” and modelled as a PI (Proportional Integral) type regulator.

It must be stressed that not all the generators of the grid are under to this secondary frequency regulation regime. There are some groups with only the primary frequency regulation, others with no regulation at all because they work at fixed load, and other with both primary and secondary controllers.

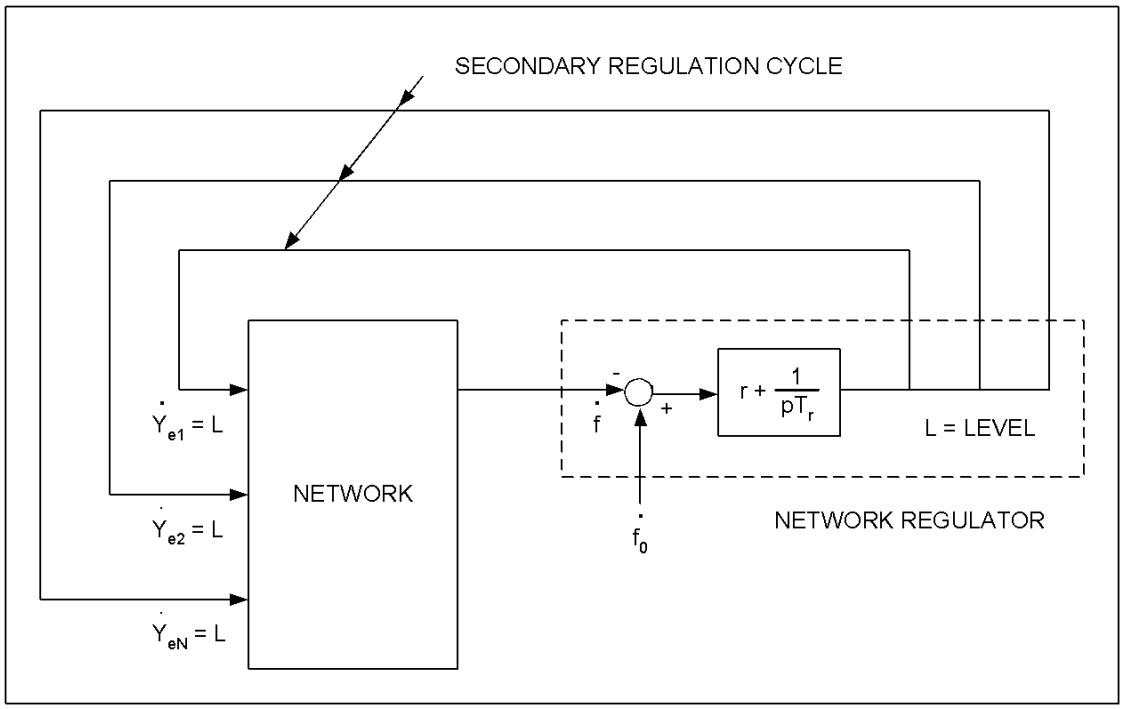


Figure 6: The secondary frequency regulation System – Crutial Project

To meet the quality of supply and voltage regulation objectives a hierarchical control structure has been developed and three control levels are used to regulate voltages of the transmission grid. This hierarchical control system is widespread along the nation, with the different controllers placed in different facilities (Figure 7): the power stations, the regional control centres and the national one:

- **AVR** – it is the Automatic Voltage Regulator which has the goal to perform the primary voltage control at the level of the single generator
- **PQR** – it is the reactive Power (Q) Regulator of a single power plant, a component of the secondary voltage control
- **RVR** – it is the Regional Voltage Regulator, it has the goal to control the voltages of the pilot nodes of its electrical region, receiving the measurements from the pilot nodes and deciding the values of the reactive power level, called q-level, for each power plant under its control
- **NVR** – this is the National Voltage Regulator at the top level, it receives the data from the field and, on the basis of an optimal voltage pattern computed by an optimisation algorithm, decides the voltage levels that have to be achieved for each controlled node of the grid.

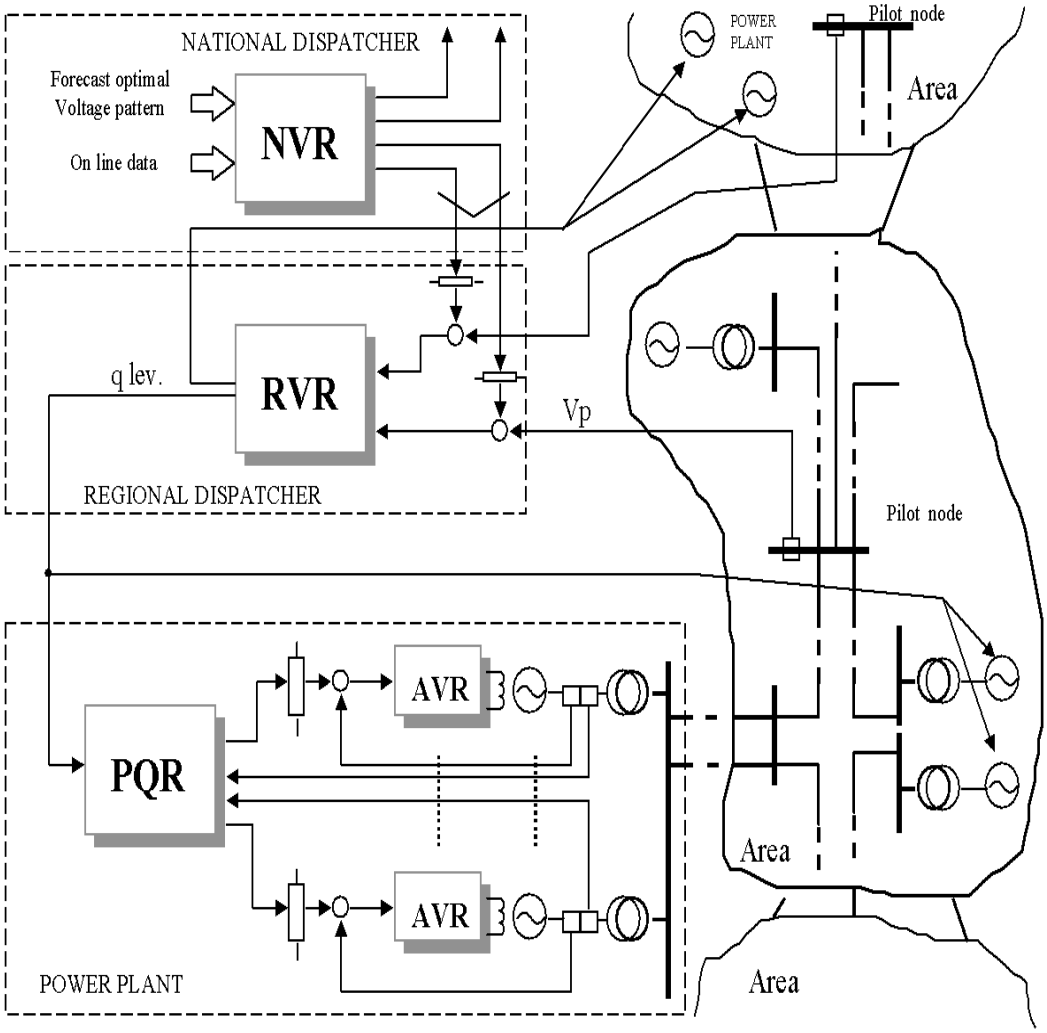


Figure 7: Hierarchical voltage control of a National Transmission Grid - Crutial Project

The cascading flow of information between NVR, RVR, PQR and AVR, and, finally, to the generator is described in the Voltage Regulation Activity Diagram of Figure 8.

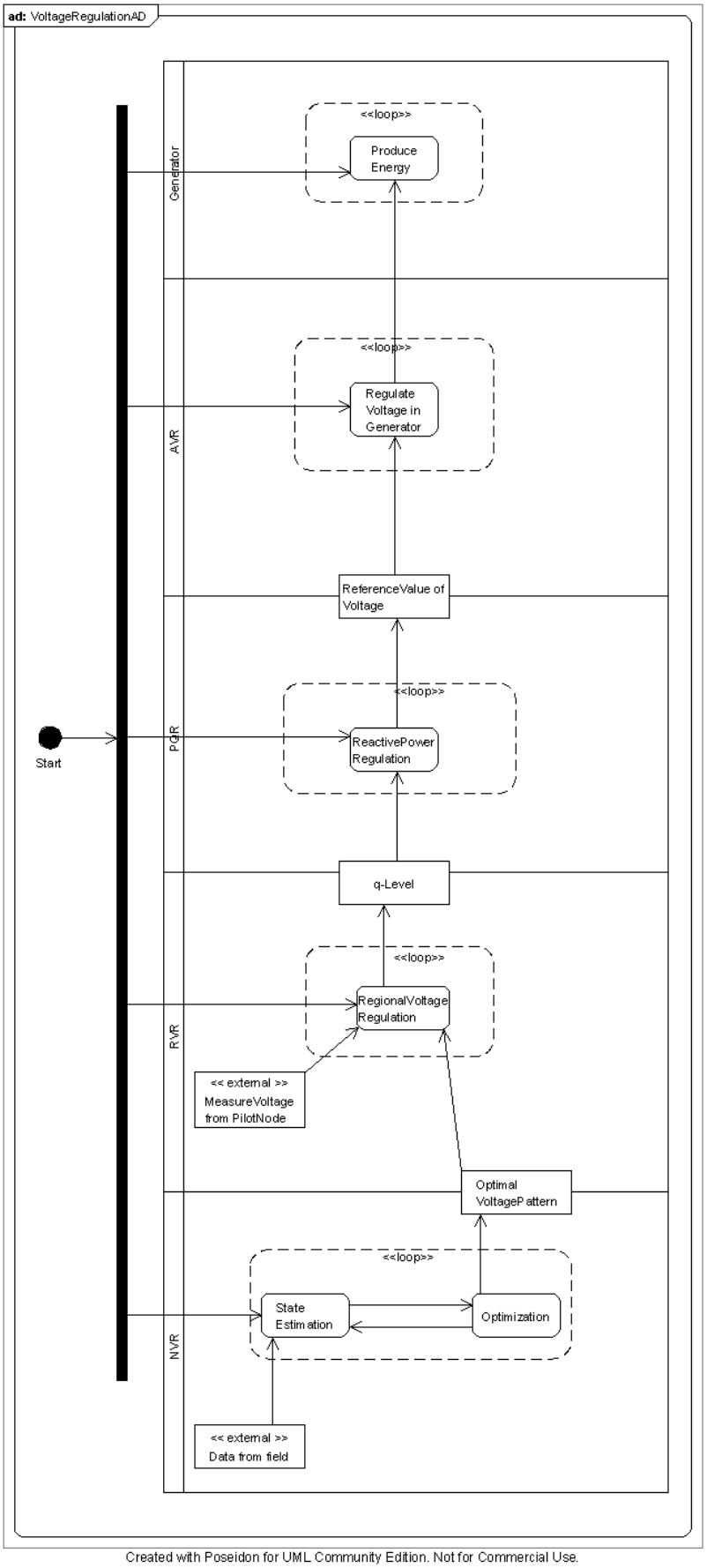


Figure 8: Activity diagram of the Voltage Regulation - Crutial Project

A different schematisation of the voltage control is shown in Figure 9 outlining the response times of the entire closed loop system, including communication times:

- 2-5 seconds for the AVR (UNIT CONTROLLER in Figure 9) placed in the power plant, one for each generator
- 20-50 seconds for PQR (POWER PLANT CONTROLLER in Figure 9)
- 100-200 seconds for the RVR (REGIONAL CONTROLLER in Figure 9) placed in each Regional Control Centre
- 400-500 seconds related to the last hierarchical control level, that is the NVR which has the goal to optimise the values of the Pilot Node voltages along of the grid.

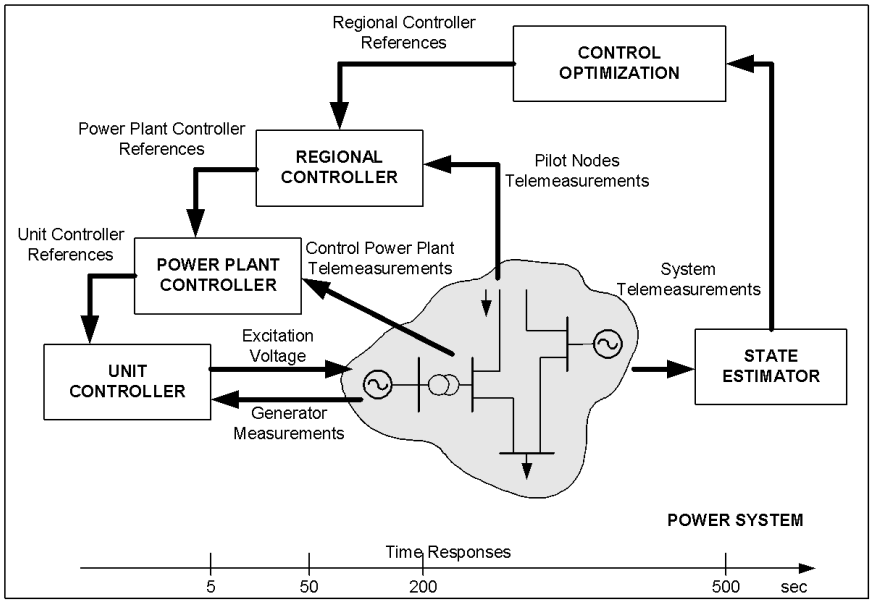


Figure 9: Response times and measurement flows for voltage regulations - Crutial Project

The main interactions of frequency and voltage regulators are depicted in Figure 9 where we can observe that the impact on the physical process of communication failures increases when moving upwards in the control chain. Interactions between TSO and GENCO (a company doing electricity generation) and between TSO and DSO are implemented for normal operation and in emergency cases.

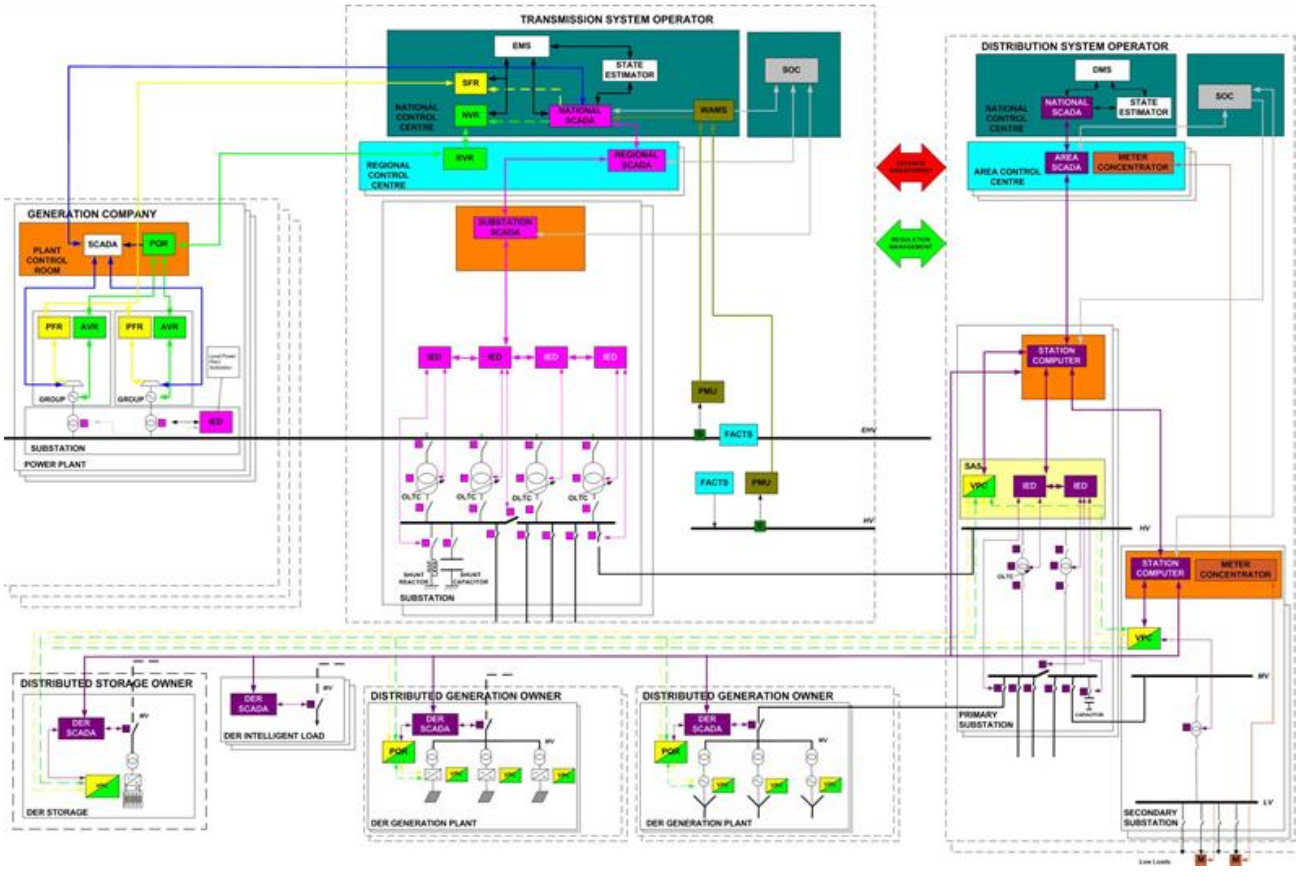


Figure 10: Hierarchical Control Scheme - Crutial Project

The data exchanges supporting the current hierarchical control functions are partially based on private communication networks and proprietary protocols, and partially deploy standard communications over IP connectivity services. Security in oldest communication systems is granted by security-by-obscurity principle, while more modern IP based networking is made secure through known best practices including network separation and access control, guaranteed by the use of intermediate gateways located in a Demilitarized Zone separated by Firewall technologies, and Virtual Private Network technologies, implementing standard authentication and encryption protocols, e.g. IPSEC.

In [10] a failure analysis of the frequency and voltage control has been performed and a set of scenarios have been identified considering possible cascading effects due to major cyber-threats and measurement failures.

This section has described the current technologies for controlling voltage and frequency through several examples. Traditionally, voltage and frequency control have not been considered a cyber-security issue. The control commands are transmitted through reliable independent infrastructure and monitoring is done at TSO, DSO and substation level. However, the integration of distributed resources poses several challenges for the frequency and voltage control, because public networks have to be used delivering the control commands. If the messaging is intercepted, denied or modified by an attacker, this can cause damage to personnel and equipment and power instability.

To address these communication related threats, ENTSO-E has written down guidelines. The Policy 6 of the ENTSO-E Operation Handbook [11] handles the requirements for the communication infrastructure that allows TSOs to exchange information, called Electronic Highway stating the following:

"A-S9.1. TSOs must take appropriate measures to protect the Electronic Highway and each connected TSO against any potential risks such as (a) operation disruption or data corruption and (b) disclosure of confidential data as defined by law, by regulatory bodies or by bilateral conventions

A-S9.2. TSOs shall protect against any unauthorized access to the Electronic Highway

A-S9.3. TSOs shall perform malware checks. It is the responsibility of each TSO to take care that all files it sends over Electronic Highway are valid and malware free

A-S9.4. TSOs shall monitor and ensure the availability of Electronic Highway components in their domain to reach the specified availability of the Electronic Highway

A-S9.5. TSOs shall ensure that their own local Electronic Highway network concept complies with the Electronic Highway requirements as defined in the Technical Reference Manual

A-S9.6. TSOs shall check redundancy of their physical lines and SCADA connections as defined in the Technical Reference Manual

A-S9.7. The above items must be verified through self-assessment by each TSO. These assessments shall be done periodically as detailed in the Technical Reference Manual

A-S9.8. The TSO shall respond to requests for proposed actions demanded by Entso-e

A-S9.9. Each TSO shall manage its own components of the network (routers, gateways, physical lines etc)".

The main focus of the Operation Handbook is the exchange of information between TSOs, but the scope should be updated in order to incorporate also the structural, real time and scheduled data exchanges between TSOs and DSOs, between TSOs, DSOs and Significant Grid Users required by the ENTSO-E Network Code on Operational Security [12].

In the European project SmartC2Net [13], a voltage control use case has been specified for medium voltage grids connecting DER (Figure 11): assuming that DSO are allowed to directly control DER such a voltage control function allows coordinating the set point requests from the TSO with the optimized voltage profiles of the underlying medium voltage grids connecting distributed generators, storage devices and flexible loads.

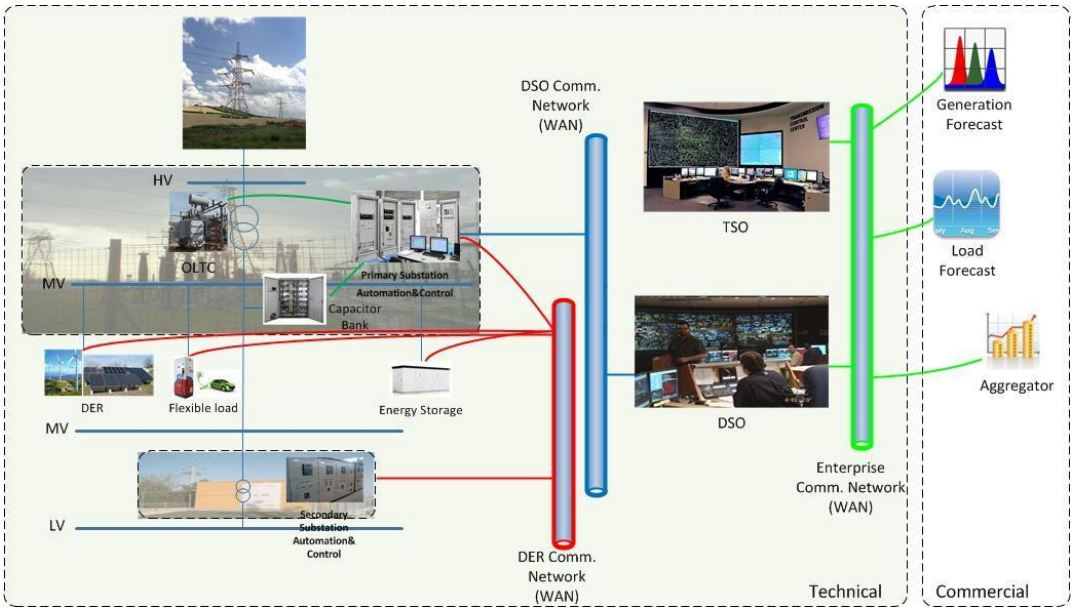


Figure 11: Medium Voltage Control in Active Distribution Grids - SmartC2Net Project

The reference communication standards of this voltage control function are reported on the SGAM layer mapping in Figure 12.

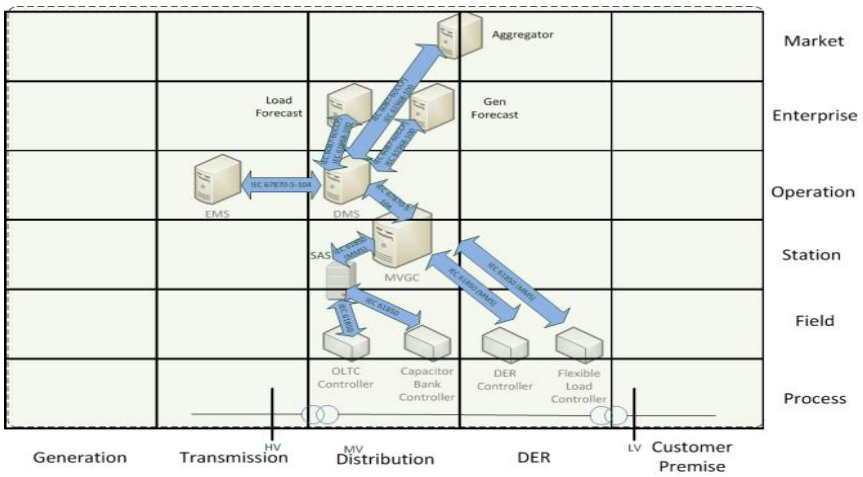


Figure 12: Medium Voltage Control - SGAM layer mapping SmartC2Net Project

Together with the specification of the expected control behaviours, some sequence diagrams have been provided illustrating the most critical effects of possible attack processes to the use case information assets, such as the intrusion of fake DER set points represented in Figure 13.

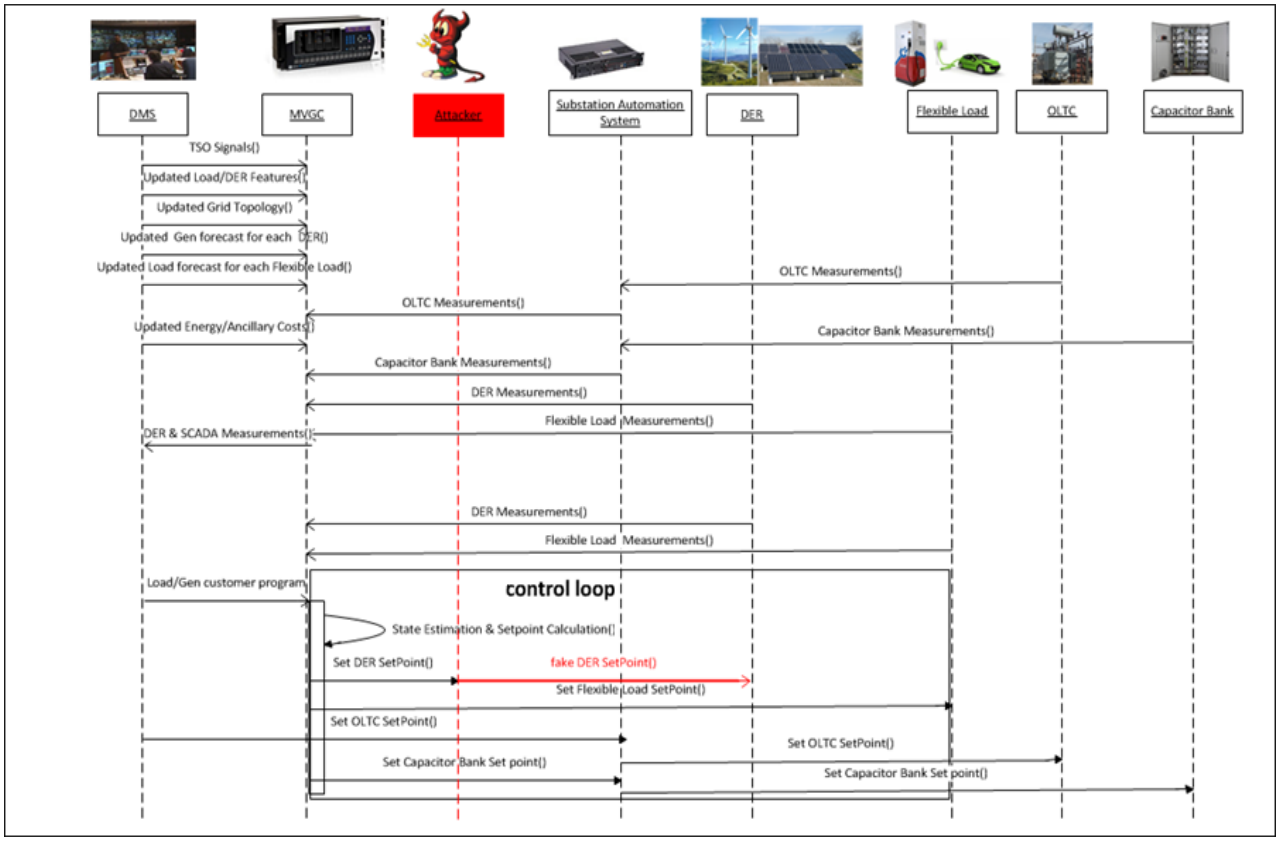


Figure 13: Medium Voltage Control – Intrusion of DER fake set points - SmartC2Net Project

3.2 Security review of ELECTRA high level architecture

This section introduces the ELECTRA proposed architecture and the high-level use cases. The use cases are reviewed in terms of cybersecurity.

3.2.1 ELECTRA scenarios and control schemes

ELECTRA does not present itself a unique scenario, but focuses its effort in designing control strategies for the provision of ancillary services that will be required to support the integration of large amounts of decentralized and intermittent generation, connected at all voltage levels of the electrical network. From this point of view it can be said that ELECTRA builds solutions to problems that will have to be faced by the kind of scenarios described in the e-highway 2050 project [31] and which could be expected to occur in the future. The high overall quality of the study and the wide scope of the results made the selection of 2050 scenarios as a starting point in ELECTRA project. Additionally, based on various reports and outlooks, some assumptions that possibly may occur in the future were made in ELECTRA Deliverable D3.1[23] to help determining the ELECTRA control schemes:

- Generation will shift from classical dispatchable units to intermittent renewables.
- Generation will shift from central transmission system connected generation to decentralized distribution system connected generation.
- Generation will shift from large units to many smaller units.
- Electricity consumption will increase significantly.
- Electrical storage will be a cost effective solution for offering ancillary services.
- Ubiquitous sensors will vastly increase the power system's observability.
- Large amounts of fast reacting distributed resources can offer reserves capacity.

The objective of the ELECTRA project is to develop advanced control techniques to fulfil the strategy of the European Union and the most possible future networks considering all possible assumptions. Therefore, two possible futures are evaluated by the ELECTRA technical team before proposing how to manage the ancillary services. The first one is a centrally managed future, where all ancillary services are still managed by the TSO in a central manner; but with vastly increased bi-directional information flows between TSO and DSO to ensure that distribution grid status is known to the TSO in order to allow him to effectively and safely dispatch reserves that are located at distribution grid level. The second one is a decentralized managed future, where the power system is divided in cells that are responsible for the local real-time balancing and voltage control.

The proposed conceptual architecture for ELECTRA is derived from the second design principle which is the cell based architecture. This structure combines 'manage locally' with 'connect globally' concept. Each cell has assigned a cell system operator who takes responsibility for the real time reserves activation and dispatching in his own cell. In principle, no global system state information is required for ancillary service operations. Thus, a "divide and conquer" way of tackling voltage and balancing issues is implemented. In this way, local problems resolved locally in a fast and secure manner.

According to the cell concept, the cells composing the grid infrastructure are heterogeneous with respect to their power grid scale and device type. Each cell is characterised by two main actor categories: a unique cell operator and multiple market parties, such as Balancing Service Providers (BSP) and Aggregators.

Another distinguishing feature of the ELECTRA control strategy is the key role of the monitoring functions which are expected to cover both power and cyber-assets. The use case specifications clearly distinguish locally acquired measurements and locally monitored variables from centrally received measurements/variables and centrally elaborated observables. In view of the future risk assessment, special attention should be given to the specification of the monitoring architecture, decoupling it from the control architecture whenever necessary.

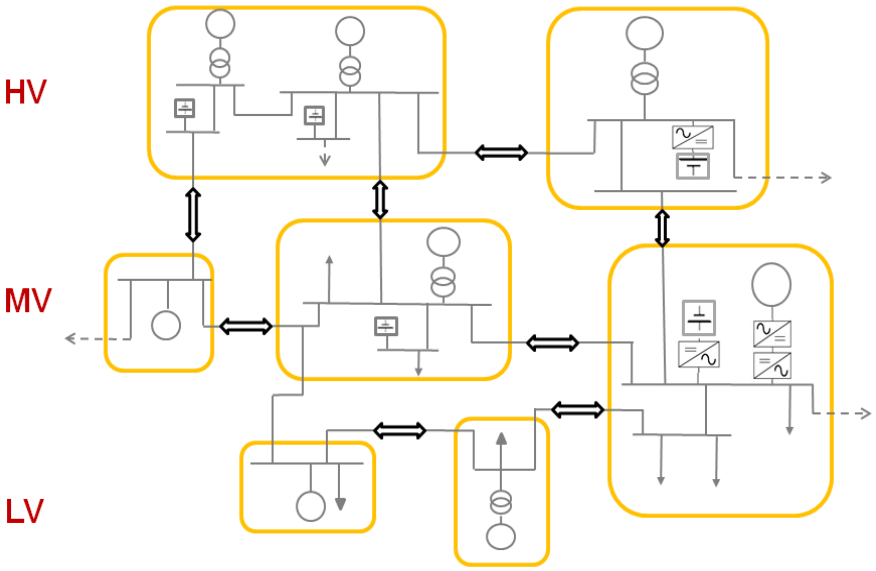


Figure 14: Cell based architecture

In ELECTRA, frequency and voltage control domains require data exchanges between:

- TSO and TSO
- TSO and large producers, storage providers, DSOs
- DSOs and cell operators, load aggregators, storage aggregators, DG aggregators, EV operator aggregators.

Many of these are most probably deploying commercial network services. In ELECTRA, frequency and voltage controllers will be in the DSO, DER and customer domains and the responsibility of those communication security rely on multiple operators. The ancillary services provided by widely distributed energy resources will play a significant role in the emergency management of the pan-European grid. The information flows among the smart grid actors depend on the regulatory frameworks that have not been defined yet.

3.2.1.1 Frequency/Balance control

Frequency/balance control can be described as the process that takes place to balance generation and consumption to stabilize the frequency. The ELECTRA project focuses on advanced frequency/balance control techniques with a cascade operation of inertia, primary (containment), secondary (balance restoration) and tertiary (balance steering) control operations. In the cell-based architecture, all principles are applied at cell level instead of a control area level, requiring novel observables and a novel control architecture. In the future, four frequency/balance control operations will be applied in each cell: inertia, Frequency Containment (primary), Balance Restoration (secondary), and Balance Steering (tertiary) control.

3.2.1.2 Voltage control

Voltage control is the process that prevents unbalanced voltage levels in order to eliminate the undesired reactive power flows. Generally, voltage stability is a slow and local issue. Since there is less time pressure on the corrective action, there is no need for a similar cascaded activation as for frequency control. In today's electricity grid, the voltage control process is divided into three main parts as primary, secondary and tertiary voltage control. However, in the cell-based architecture, the ELECTRA project proposes two voltage control operations; primary and post-primary voltage controls.

3.2.2 ELECTRA use case overview

The overall cell-based control strategy combines control algorithms local to a cell unit with coordinated controls for global optimizations. Six high-level use cases have been introduced in ELECTRA, namely:

- Inertia Control - IC
- Frequency Containment Control - FCC
- Balance Restoration Reserve - BRR
- Balance Steering Control - BSC
- Primary Voltage Control - PVC
- Post Primary Voltage Control - PPVC

In the following sections some initial security considerations are given per each ELECTRA use case.

3.2.2.1 Inertia Control

Inertia is needed within the overall power system so that the rate of change of the frequency (ROCOF) after a disturbance is kept within acceptable limits. In today's power system, the ROCOF is limited by the available stored kinetic energy in the rotating generators. When most generation is rotor based, as it is now, Inertia Control (IC) is not explicitly needed. On the other hand, in the future, two possible challenges will affect the total system inertia. First one is the increase of converter-coupled generation and load, which will cause a decrease in inertia and so in system stability. Second one is the time-variant generation mix, which will cause to change in the ratio of rotating and non-rotating generators.

In case of power imbalances within the limits of a reference incident, two requirements have to be guaranteed by the IC. First one is the limitation of rate of change (df/dt) to a maximum allowed value df_{max}/dt. Second one is supporting the assurance of a dynamic frequency deviation limit $\Delta f_{dyn,max}$. These two objectives are fulfilled using a sufficient fast change in active power contribution or consumption of generating units or loads.

The IC is intended to be a global optimisation use case coordinating intra-cell and inter-cell inertia provision. It is expected that there will be one inertia controller per each cell calculating the optimum inertia profile, communicating with other controllers in the same cell and with controllers in neighbouring cells when the available inertia within the cell is not sufficient. The IC functionality of each unit is switched on/off by the control cell operator. Therefore the control cell operator checks on a regular basis if enough inertia is present in his system.

In the cybersecurity sense, lots of monitoring and control messaging is required from the cell operator to plants, aggregators and units. There is also communication to the neighbouring cells. Probably, the communication channel used for IC messaging is used for other types of messaging as well. It is not yet defined how the inertia providers are registered or coupled to the cell control. Authentication is a critical issue, because feeding false measures about capacity or other values to the cell control as a “fake provider” should be made impossible. Relying on capacity that does not really exist, or false measurements causes system instability.

Although IC seems to be a local/internal control at the generation or flex-device level, remote information sharing is required between units and the cell operator. Moreover, as it is in post primary voltage control, inertia measurement from specific pilot points is required in order to

manage controlling inertia in a cell. Therefore, it is needed to use a secure channel and considering the three security criteria stated in section 2.1: confidentiality, integrity, availability.

3.2.2.2 Frequency Containment Control

The goal of Frequency Containment Control (FCC) is to stabilize the frequency deviation to a set safe band until the restoration control operation starts. The frequency is stabilized by activating the resources providing containment reserves automatically based on local frequency measurements. Operationally, it is not expected any fundamental change in future containment control compared to today's FCC , except the resources. The reserves will be much more distributed across the cell including load and storage units.

The FCC is understood as a global optimization use case controlling the frequency through large amounts of distributed sources within a cell. As shown in the sequence diagram in Figure 15, the FCC algorithm is operated by the Cell_Responsible. If all the requirements can be satisfied by the intra-cell FCC_Providers, then the required units are activated. On the other hand, if some parameters are violated, then coordination with the other intra-cell or inter-cell controls is performed.

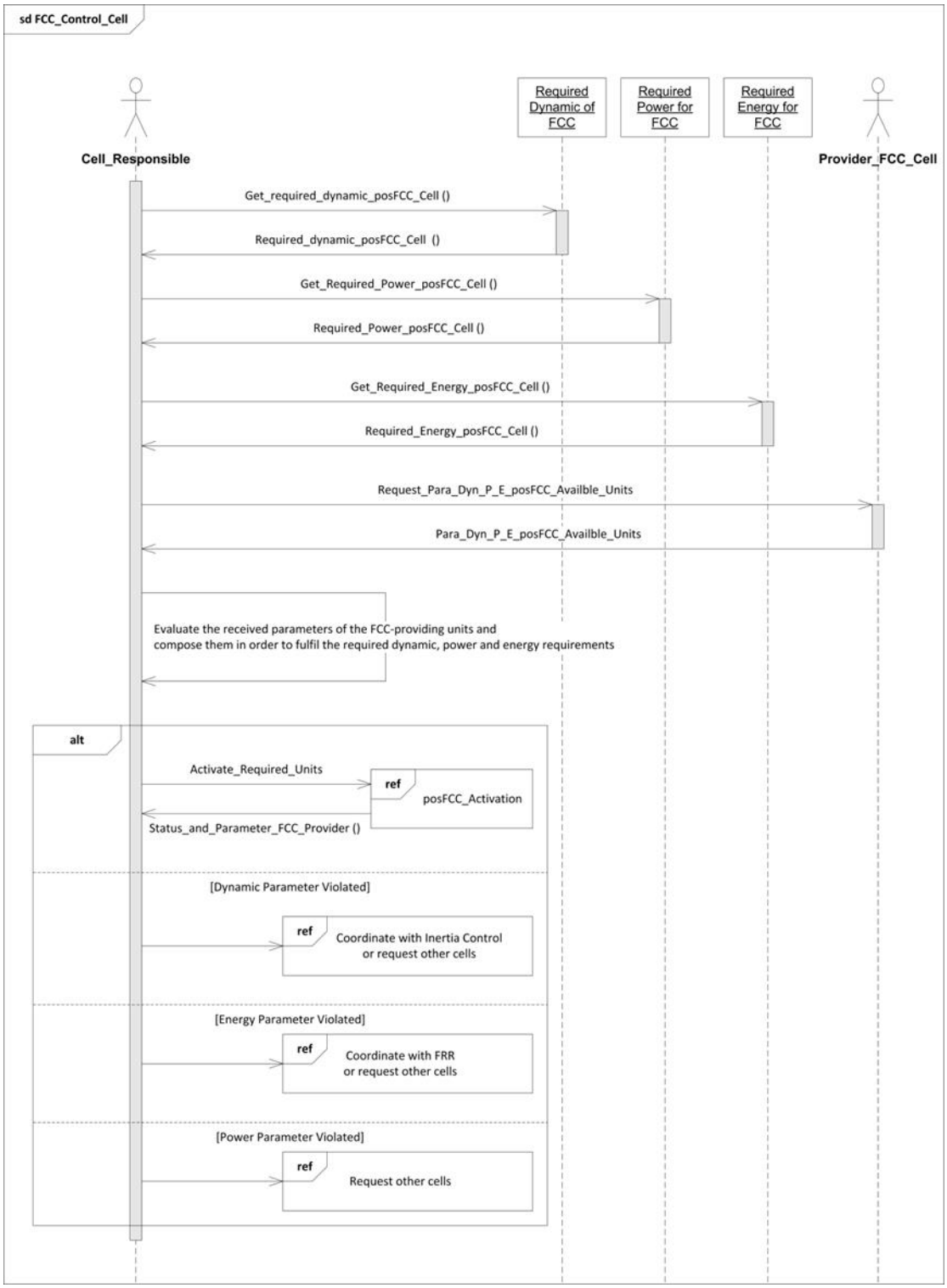


Figure 15: FCC – Optimization Sequence Diagram [23]

From the FCC_provider side (see Figure 16), three levels of control are defined: Provider control, Plant control and Unit control.

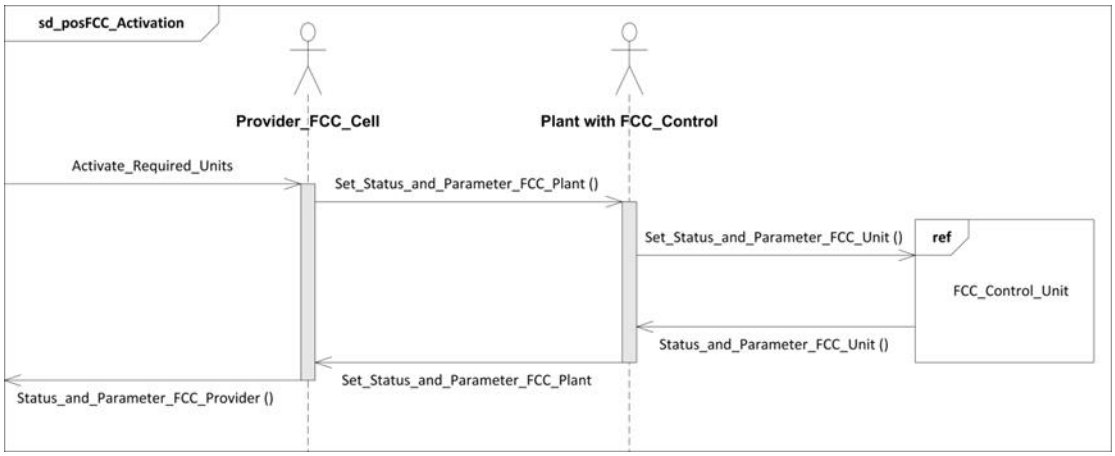


Figure 16: FCC – Activation Sequence Diagram [23]

Since no fundamental change is expected in the future, same cybersecurity issues considered in today's primary frequency control are also taken into account in future containment control. Although primary frequency control seems to be a local/internal control at the generation or flex-device level, remote information sharing may be required between actors. In other words, a secure communication infrastructure is needed either for remote communication or most importantly in local communication system.

From a security perspective this use case defines a closed control loop spanning from the Cell_Responsible towards the FCC_Units and involving intra- and inter-cell communications related to data and activation requests. The alternative branches of the FCC algorithm may involve communications with other use case controllers in the same cell, or may require interacting with external actors. The FCC process is automatic and local.

The resources providing containment reserves will be different: generating units as well as loads and storage. The resources will be smaller and more widely distributed. In the most extreme vision, every household could be having devices contributing to FCC. If the devices contributing to FCC are located to every household within a cell the devices are accessible by consumers at some level. This has to be taken into account when planning more specific functionality and security technologies to the FCC.

3.2.2.3 Balance Restoration Reserve

Balance Restoration Reserve (BRR) is to restore the cell balance to its nominal value within 30 seconds and 15 minutes. Restoration Reserves may be offered by loads, production units as well as storage units. In the future ELECTRA scenario, each cell operator will be responsible to fulfil the requirements of restoration control (contacting with the restoration reserve providers, dispatching the units, congestion management and re-dispatching units if necessary) in its own responsibility area.

In balance restoration operation, the cell operator takes the responsibility to operate the restoration control. The cell operator needs some information from the providers using the monitoring system. For instance, assuming that there is a market mechanism which will most probably be based on a software tool controlling the restoration reserves by supplying data information between the cell operator and service providers. Therefore, the market structure has to basically include some

security aspects such as access control and anti-virus software. If this action is carried out via Internet, there is a need for more security mechanisms to make the system work according to the confidentiality, integrity, and availability criteria.

The BRR use case is expected to have a distributed architecture crossing several domains and zones of the SGAM plane whose main actors are the Cell Operator and the Restoration Reserve Providers. According to the sequence diagram in Figure 17, this control algorithm is based on interactions between the Monitoring and Control functions of the Cell Operator, and between the Operator Control function and the Reserve Providers. Four critical information assets are exchanged by the use case devices: restoration reserve bids, restoration errors, restoration reserve activation orders and reserve activation measurements. The response time is 30 seconds counted from the detection time of the restoration error by the Monitoring function.

It is critical that the restoration providers are registered in a secure manner. The registration process has to be deployed in a way that malicious or false registration is not possible, because giving wrong values about restoration reserves capacity would result in errors in merit ordering and cause other error situations. Also, the communication channel between the cell operator and restoration reserve providers is critical in security and reliability sense, because probably the public communication infrastructure is to be used for delivering activation orders.

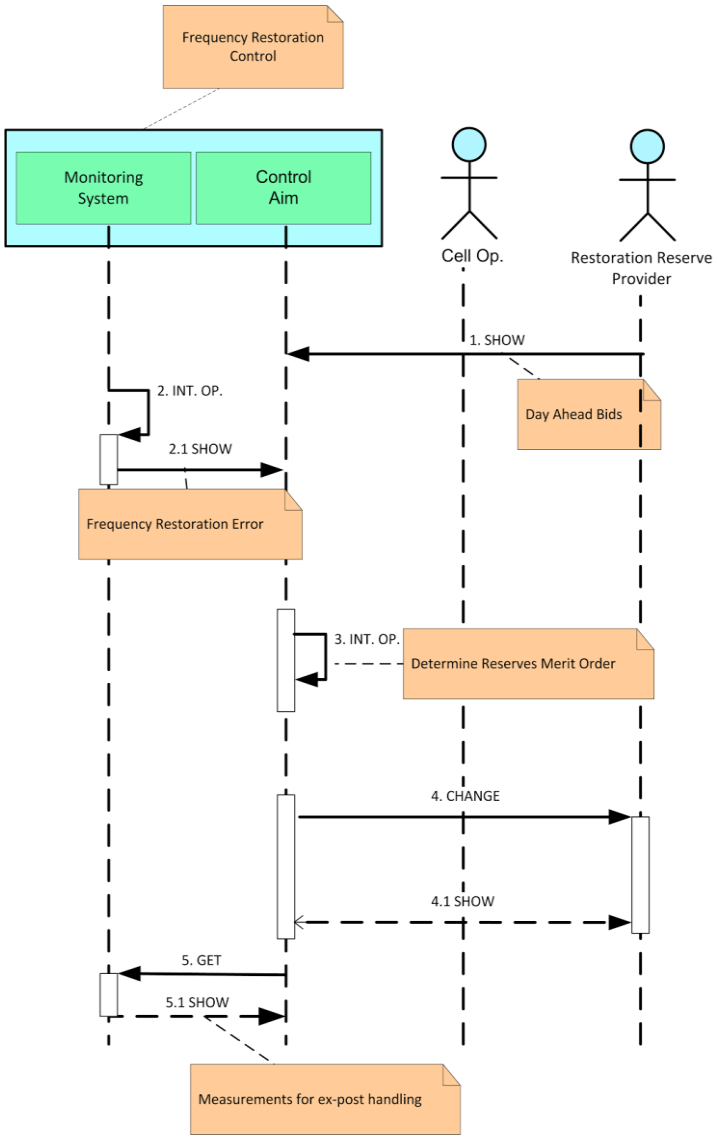


Figure 17: FRR – Sequence Diagram [23]

3.2.2.4 Balance Steering Control

The Balance Steering Control (BSC) use case is a very global optimization process performing the tertiary frequency control for the whole control area. The ultimate goal of BSC is to restore balance to a (new) set point. This is achieved either pro-actively or reactively by covering imbalances induced by forecast errors and other reasons, happening under normal conditions or contingencies. One major difference between steering and restoration control is that, in the first one, the cell operator deploys resources not only within the cell but also from adjacent cells.

The BSC can be distinguished into three main modes. In the proactive case, BSC has the responsibility of supervising the system, and based on short-term forecasting predict potential errors that may substantially affect the cell balance. In the substitution case, BSC is nominated with the responsibility of activating cheaper reserves replacing restoration reserves, or determining a new set point for the cell balance. In this latter case, a new set point is agreed upon, such as less reserve in cells with different signs of deviations must be activated. The timeframe of activation and operation of BSC in any of the above cases ranges from 15 minutes to 1 hour.

According to the BSC sequence diagram in Figure 18 three types of actors are expected to participate to this control loop: CA Operator, Cell Operator and BSC providers.

There will be information exchanges between actors while executing BSC operation and same security considerations indicated in FRR control can be also considered for BSC.

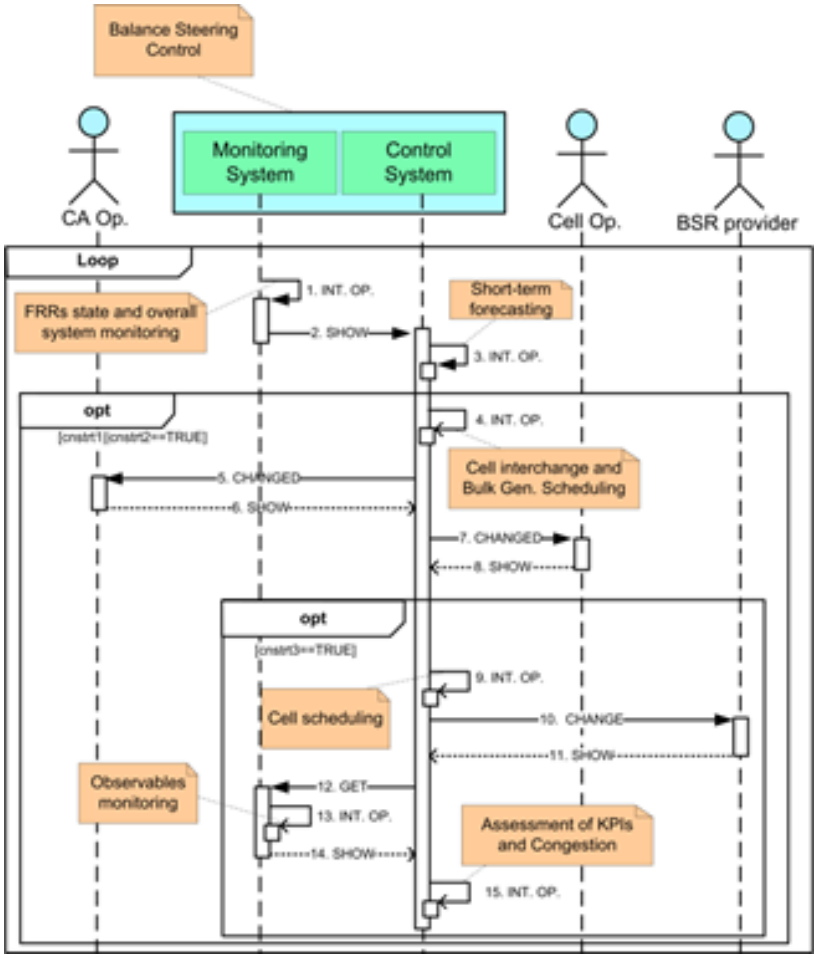


Figure 18: BSC – Sequence Diagram [23]

3.2.2.5 Primary Voltage Control

Primary Voltage Control (PVC) is a process executed locally concerning generating units: synchronous generators that are equipped with Automatic Voltage Controller (AVC), or other energy sources (photovoltaic, wind) with power electronics and control functionalities. PVC maintains the required voltage level of the feeder or busbar according to the current voltage set point and voltage droop. Operationally, no fundamental change compared to today's PVC is foreseen, except that the resources used for it voltage control will be located at the distribution grid as well, and may be of a different nature in the future.

The PVC use case described in the Figure 19 is local to a generating unit with limited communications for receiving a new voltage set point from local operators, remote operators or systems.

Although PVC operation is a local control, it needs set-points from the PPVC, which brings an obligation to provide this communication in a secure manner. Basically, same security aspects considered by inertia and primary frequency control can also be considered for securing this operation since all three have similar local operations using local communication and control infrastructure. Authorisation of generating unit to the cell operator is a security critical phase. Malicious or false generating units should be detected by the cell operator and not authorised.

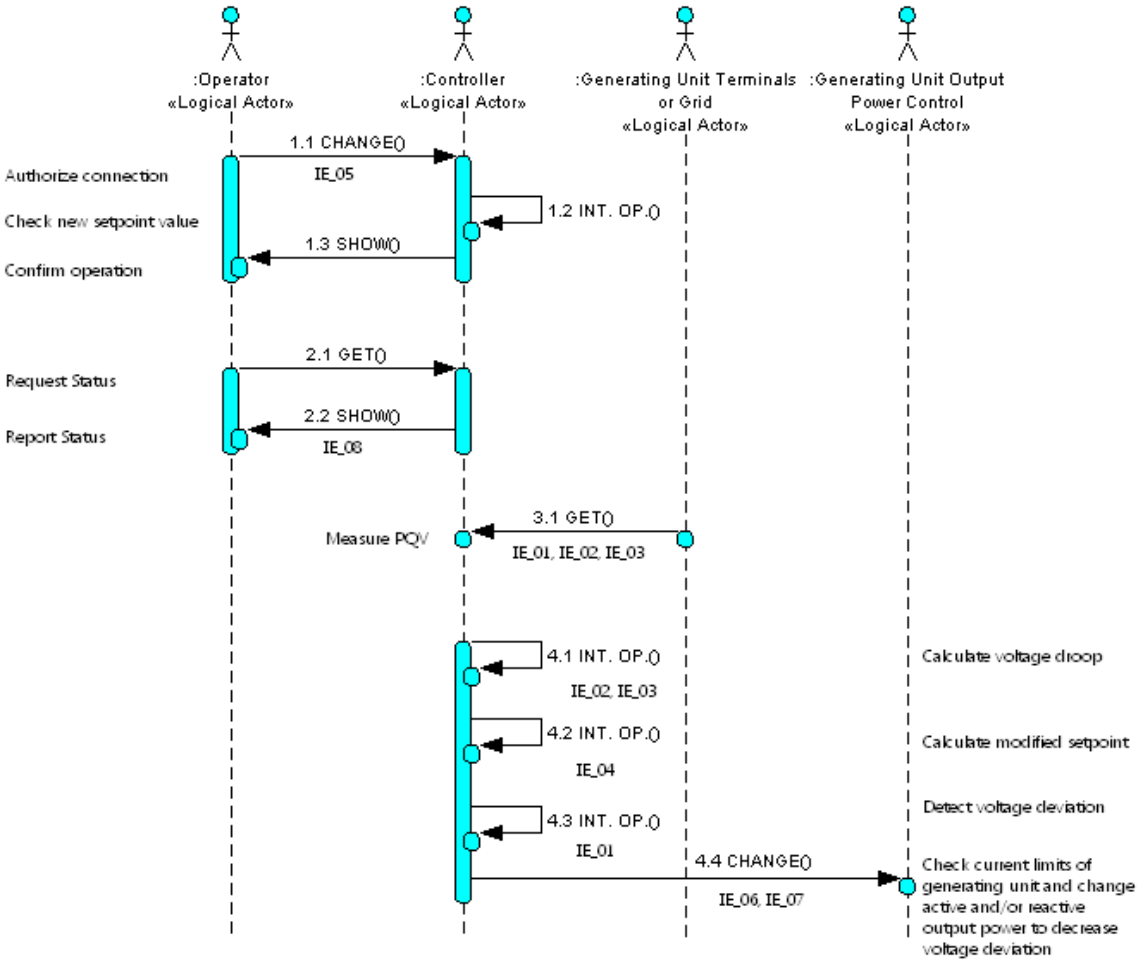


Figure 19: PVC – Sequence Diagram [23]

3.2.2.6 Post Primary Voltage Control

The cell-based grid architecture leads the ELECTRA team to merge the conventional secondary and tertiary voltage control under the new concept called Post Primary Voltage Control (PPVC) in order to manage the voltage control operation optimally. The objective of the PPVC is to provide an optimal and local voltage control for future electrical grids. PPVC, as a result of the coordination between the cells at different voltage levels, will restore the voltage in the nodes to nominal values, optimizing the reactive power flows in the system.

The PPVC is intended to replace the current secondary (local) and tertiary voltage control (global) schemes existing in power grids by a decentralized control, located a cell level. Each cell is responsible for its own voltage control while a close coordination between cells guarantees the provision of PPVC service between adjacent cells. Determining the unit set-points for PVC can be considered as a duty from the conventional secondary voltage control. Also, determining the set-points and measurement of the pilot nodes can be considered as a duty form the conventional tertiary voltage control. PPVC operation is a combination of conventional secondary and tertiary voltage control. A secure communication infrastructure is essential in this use case as well.

The PPVC is a decentralised control located at cell level and coordinated with neighbouring cells. The cell operator's controller interacts with the resource providers in its cell and with the operators of neighbouring cells (see Figure 20).

In PPVC operation, the cell operator has the main responsibility to maintain the voltage in its own area by managing the monitoring and control system. Since PPVC operation is a combination of conventional secondary and tertiary voltage control, it needs a good communication infrastructure to be able to manage the operation. Therefore, information security becomes important in this operation. Each cell may have different communication infrastructure or methods, but each different type of communication medium has to include security techniques on its scope of physical, electrical and IT properties. Once again, also the registration or authorisation of potential resource providers is important to do in a secure manner. Since PPVC requires also communication between cells, the communication channel has to be very reliable and there should be a mechanism to verify the reported capacity.

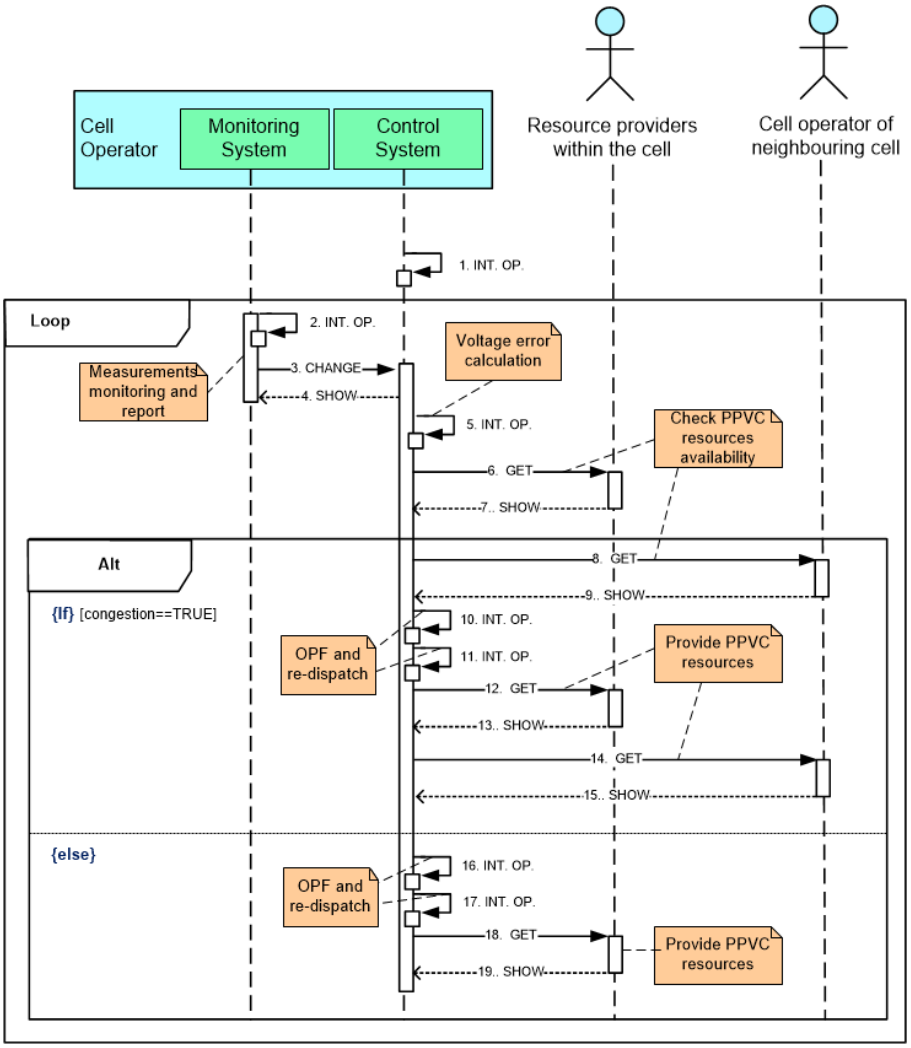


Figure 20: PPVC – Sequence Diagram [23]

3.2.3 Security concerns regarding the ELECTRA voltage and frequency control architecture

Based on the ELECTRA Use Cases review in the previous section, this section describes the derived security threats that are most relevant for the ELECTRA proposed architecture.

In the proposed architecture, the amount of communication will increase a lot, due to the shift of responsibilities from a few central controllers (at Control Areal level) to a large number of distributed controllers (at cell level). These distributed controllers will depend on a large amount of distributed sensors belonging to the monitoring system in each cell.

Next to that, the architecture describes how there is as well a shift from a small number of central reserves providing resources to a larger number of small distributed reserves providing resources. In an extreme case, consumer-class devices at every household might contribute to the frequency and voltage control schemes. One expected impact of this, is that such devices - due to their limited cost - will have reduced security related capabilities compared to today's industrial-grade systems. Besides, they will be located in easily accessible, non-secured locations. Finally, they most likely will be communicating through public communication infrastructure, instead of dedicated private communication lines. The reliability of public communication infrastructure is a major concern, because surprising downtimes at cellular operator's networks are not uncommon nowadays.

Finally, the proposed architecture has to be very open to enable such consumer-class devices to easily be added, or removed, from the list of reserves providing resources.

Because of the arguments above, the threats listed below are highly relevant to the ELECTRA's planned functionality for voltage and frequency control.

Injecting manipulated sensor data/parameters

Serious threats arise if an attacker gains access to a node or a communication path in the SG. An attacker may cause damage by manipulating sensor or meter data, sending disconnection commands and feeding incorrect values to destabilize the load.

Such attacks may be launched to several nodes (such as smart meters) simultaneously causing the state of the whole network to become unobservable by the control centre or cell operator. This may lead to incorrect actions based on false information which makes the situation even worse.

Denial of service attacks

When attackers have access to communication channels, they can jam these channels, attack networking protocols and flood the network traffic [18] in a way that valid messages (either measurements or control commands) cannot be delivered in a reliable manner.

Malware injection in monitor and controller networks

An example of sophisticated malware designed for injection in SCADA devices is the Stuxnet-worm [19]. Stuxnet was originally targeted at PLC (Programmable Logic Control) devices in

industrial networks and exploited vulnerabilities in Microsoft Windows and Siemens software. But it has been tailored to attack modern SCADA systems as well. The software was usually injected to the networks by means of USB flash drives. Such advanced threats are very difficult to detect once they have infected the system, and therefore such attacks have renewed long-standing concerns about whether the power grids can withstand targeted cyber-attacks.

Abusing vendor's remote control functionality

Often industrial control system manufacturers include a remote connection to their devices for updates and maintenance. In the worst case, such functionality is not well documented for the IT staff that cannot take proper action resulting in the service to be visible to the Internet. In the best case, the remote connections are only available on demand, and they are properly secured with VPNs and firewalls. Remote connections are a serious threat to all industrial networks, including SGs: they can be abused to falsify configurations, to inject falsified data, and to gain access to other devices.

Threats of wireless connections

Some parts of the SG communication network may use wireless techniques. For example, smart meters often use wireless communication channels. Security of wireless communications has always been difficult due to the fact that wireless signals cannot be isolated and they spread to the surroundings. Even if the communication is encrypted properly, the communication access points can be disrupted with wireless jamming devices and very little technical knowledge.

Vulnerabilities in end-user devices connected to the public Internet

Distributed generation and home automation brings several new smart devices into households. These devices may include software vulnerabilities that are exploitable through the Internet and can be used to disrupt the network or cause other problems.

Recently, a serious vulnerability from a solar panel monitoring kit was found [20]. This system runs globally on 229,300 solar plants. According to security researchers, attackers could break into the software causing significant damage, such as launching massive reconfigurations, changing user passwords, and manipulating specific power-generation related values.

Failure of devices and systems

The complexity and multiplicity of devices and systems interconnected in SG probably causes significant incidents due to malfunctioning devices, interoperability issues, and misconfigurations. These threats do not even require an attack. For example, device failure in an operator network would cause serious problems to the planned frequency and voltage control loops.

3.2.4 ELECTRA Security Recommendations and Architectural Constraints

This section contains a collection of recommendations and design constraints for the ELECTRA project's design phase.

3.2.4.1 Careful design specification

Good design documentation that describes the system with great detail, is a great help to perform a security analysis with associated cybersecurity threat and risk assessment. The ELECTRA system architecture description should provide clear answers to the following questions:

- Provide a detailed list of all components, their connections to other components (logical and physical), including their interfaces
- Which components, resources and added functionality are added specifically for the ELECTRA new functionality?
- What type of information is stored, used, and transmitted, and what is the sensitivity of each information type?
- Is the control system or some parts of it accessible to end users through e.g. smart meter or other devices located at households?
- Does the ELECTRA system transfer or store customer's or consumer's personal information (e.g. electricity consumption information)?
- Is the planned functionality and control scheme fully automated, or is there also a possibility for manual control?
- What communication protocols are planned to be used for different functionalities, e.g. control messages, power usage reports, metering, billing,...?
- What user access levels are defined: who will have what access rights to what parts of the system?
- What are the Electronic Security Perimeters (entry points to the system)?
- Identify all critical assets (facilities, systems, and equipment that if destroyed, degraded, or otherwise rendered unavailable would affect the reliability or operability of the bulk electric system [21]).
- What level of redundancy is required due to the risk of device crash or maintenance?
- What national cybersecurity regulations have to be applied and taken into account?
- How do all relevant actors engage with each other and with the electricity market in a secure manner (each private company may have different devices/security aspects)?

3.2.4.2 Specific Architectural guidelines

Secure all connections to the public Internet

In the proposed web-of-cells architecture, it is assumed that large amounts of small reserves providing resources, also possibly located at individual households, may offer ancillary services. It will be no longer conceivable to connect these through dedicated and private communication infrastructure. Instead, they most likely will be connected through public networks. Such decentralized devices and nodes that offer ancillary services must therefore be equipped with

adequate processing power to support the needed security mechanisms. Next to that communication protocols must be selected that include proper security mechanisms.

Add redundancy

Communication infrastructures in SG have very strict availability and response time requirements. Therefore considering a design with redundant communication paths is highly recommended. Depending on the criticality, even two physically independent lines can be a viable solution.

Introduce Network Segmentation

Segmentation can be considered as a protection mechanism that enhances security by splitting and dividing the communication network into multiple sub-networks. This way, the impact of successful attacks to a specific sub-network may be contained to that sub-network, without impacting the network as a whole.

Select interoperable standards with strong security provisions

Interoperability is very important for the SG development. All the devices of the grid should be able to communicate with each other through standard protocols and communication channels. The old security by obscurity approach using proprietary protocols and solutions only adds complexity and cannot be applied any more. Goal can only be accomplished by applying standards from organisations such as ISO/IEC, ETSI/CEN/CENELEC and NIST, and selecting well-known standard communication protocols.

3.2.4.3 Best practices and recommendations

The following issues are not restricted to the design phase, but relate to the whole lifecycle.

- As a general security rule, every user/node should have not more privileges than those that are necessary to perform the function expected.
- When designing new functionalities, always assume that someone will try to find and exploit security vulnerabilities.
- Encrypting data for communication and storage is a must-do for sensitive data.
- Strong authentication ensures that only authorized entities can request and obtain information from the actors of the grid.
- Identify critical assets (nodes, sensors, facilities, systems, and equipment that if destroyed, degraded, or otherwise rendered unavailable would affect the reliability or operability of the bulk electric system [21]) and make sure they reside behind a security protection.
- The system should be able to recognize random failures from malicious failures
- Proper prioritizing amongst the security goals is important. For example availability of power is more important than confidentiality of power flows. However, this does not mean that privacy issues should be ignored.
- Select proper standards (ISO/IEC 27001/2, SG-CG, NERC/CIP)
    - ISO/IEC 27001/2 sets rules of best practice to maintain a sufficient level of security in systems that need to exchange information such as SGs:

- Vulnerability management: once the communication network has been designed and built, the job of the security responsible is not over, and security policies and protection mechanisms have to be kept constantly updated to ensure an adequate security level also in the future.
- Threat modelling: an attack often is hardly discernible from a usage request, but if the communication network is trained to recognize possible threats, it is possible to implement an automatic self-protection mechanism.
- Penetration testing is a method to assess the security level of the network; periodically a third party organization should take some controlled attacks to the network to proof the validity of security mechanisms.

o SG-GC recommends the high/medium/low classification of data based on its criticality [15].

3.2.4.4 Conclusions and next steps

Based on the high-level functional architecture and use case descriptions of the ELECTRA Deliverable D3.1 [23], a number of high-level security guidelines and attention points have been described. These will be taken into account when further deriving the detailed functional architecture and use cases. This detailed architecture covering communication interfaces, specific protocol messaging, message sequencing of the control scheme and associated communication modes, traffic profiles and performance requirement, will then be analysed to perform a detailed risk assessment, and to provide remediation advices.

It has to be noted though that in order to perform a full evaluation of the impact and likelihood of attack scenarios, the detailed use cases must be instantiated on a specific network (section). A comprehensive list of specific network details that are needed for a full security analysis is provided in the table below.

Table 1: Use case details enabling cyber-risk analysis

Parameter	Description
Area	Geographical extension of the area covered by the grid service: multination, nation, region, province, city
Population density	# of people in the area
Regulation	Applicable regulations
DER penetration	Total amount of Power from Renewable Energy Sources (RES)
DER size	Installed DER capacity
Grid size	Installed grid capacity
Grid Topology	# HV/MV substations
	# MV loads
	# MV/LV substations
	# generators
	# storage devices
	# MV lines
Telecontrol Network Topology	# Control centres
	# substation links per centre
	# of DER links per substation
Communication Network Topology	# gateways per network
	# communication (internal and external) interfaces per device
Data exchanges	Information assets
	Message sequencing
	Communication protocols
	Data frequency
	Communication performance requirements

4 Maturity model for smart grid risk assessment combining SGIS and NIST IR approaches

The approach referred in this chapter is described in the ELECTRA internal report R4.2 [25].

Application for one individual use case of the maturity models described in [25] is desirable in the very context of this project. However, the current state of the use cases in ELECTRA, let alone template and systems identification postpones the very completion of this section within the scope of this deliverable. The next section provides a glimpse of the way to integrate the diverse technologies, and a more detailed use of maturity models will be presented later on the project.

The risk levels the SGIS group takes into account mainly deal with the critical loss of both load and generation in the UCTE grid. As incidents occur, the grid stability can become endangered by those incidents. However, one could argue that incidents with relevance to security will occur before the actual event of the outage or power loss. Therefore, topics like situational awareness for individual systems and interfaces have to be considered. Within the scope of ELECTRA, situational awareness shall be considered as a concept dealing with mainly four parts, namely logging the situational data in the RTU, monitoring the function in the distribution grid for the ELECTRA control-loops, maintaining an overall common operational picture and managing the day to day data activities for operations. For those four aspects, maturity models have been put in place in terms of one of the dimensions from the ES-C2M2 as described in R4.2 document. The Maturity sub-model for Situational Awareness takes into account those factors which shall be used alongside a proposed tool chain in ELECTRA as given in the next paragraph.

The following domain specific objectives and practices have been created as taxonomy in the model and been assigned certain maturity levels (called MIL X):

Domain-Specific Objectives and Practices

1. Perform Logging

MIL 1 a. Logging is occurring for assets important to the function where possible

MIL 2 b. Log data are being aggregated within the function

c. Logging requirements have been defined for all assets important to the function (e.g., scope of activity and coverage of assets, cybersecurity requirements [confidentiality, integrity, availability])

MIL 3 d. Log data support other business and security processes (e.g., incident response)

e. Logging requirements are based on the risk to the function management

2. Monitor the Function

MIL 1 a. Cybersecurity monitoring activities are performed (e.g., periodic reviews of log data)

b. Operational environments are monitored for anomalous behaviour that may indicate a cybersecurity event

MIL2 c. Monitoring and analysis requirements have been defined for the function and address timely review of event data

d. Alarms and alerts are configured to aid the identification of cybersecurity events (RESPONSE-1b)

e. Indicators of anomalous activity have been defined and are monitored across the operational environment

f. Monitoring activities are aligned with the function's threat profile (THREAT-1d)

MIL 3 g. Monitoring is integrated with other business and security processes (e.g., incident response, asset management)

h. Monitoring requirements are based on the risk to the function state for the function to enhance the common operating picture

i. Continuous monitoring is performed across the operational environment to identify anomalous activity

j. Risk register (RISK-2j) content is used to identify indicators of anomalous activity

k. Alarms and alerts are configured according to indicators of anomalous activity

3. Establish and Maintain a Common Operating Picture (COP)

MIL 1 No practice at MIL 1

MIL 2 a. Monitoring data are aggregated to provide near-real-time understanding of the operational state of the function (i.e., a common operating picture; a COP may or may not include visualization or be presented graphically)

b. Methods of communicating the current state of cybersecurity for the function are established and maintained

c. Information from across the organization is available to enhance the common operating picture

MIL3 d. Monitoring data are aggregated to provide near-real-time understanding of the cybersecurity

e. Information from outside the organization is collected to enhance the common operating picture

f. Pre-defined states of operation are defined and invoked (manual or automated process) based on the common operating picture

Common Objective and Practices

4. Manage SITUATION Activities

MIL 1 No practice at MIL1

MIL 2 a. Documented practices are followed for logging, monitoring, and COP activities

b. Stakeholders for logging, monitoring, and COP activities are identified and involved
c. Adequate resources (people, funding, and tools) are provided to support logging, monitoring, and COP activities

d. Standards and/or guidelines have been identified to inform logging, monitoring, and COP activities

MIL 3 e. Logging, monitoring, and COP activities are guided by documented policies or other organizational directives

f. Policies include compliance requirements for specified standards and/or guidelines
g. Logging, monitoring, and COP activities are periodically reviewed to ensure conformance with policy

h. Responsibility and authority for the performance of logging, monitoring, and COP activities is assigned to personnel

i. Personnel performing logging, monitoring, and COP activities have the skills and knowledge needed to perform their assigned responsibilities

Those requirements make for one dimension of the overall maturity of operating an asset, e.g. in ELECTRA. Certain dimensions of the maturity are architecture, interface or run-time based. This means, basic data for an assessment has to be gathered from various sources. The IntelliGrid Use Case template[27] usually comprises a sequence diagram and various information about the non-functional requirements as given for run-time operations phase. In addition, standards for security from the corresponding IEC 62559 annex can be annotated [27]. As depicted and described in [22], a combination of NISTIR and SGAM models is possible. Therefore, SGAM models from ELECTRA can be annotated with standards from the IEC Smart Grid Mapping tool, be assigned risks and threats to interfaces as well as mitigation strategies. So in addition to the use case, an SGAM model of the corresponding ELECTRA function would be beneficial for further analysis. The only thing still missing in the state-of-the-art is the link to a proper maturity model in terms of both information sources. This activity closes this open spot by adding the maturity model from the E-C2M2 to this spot. Based on the UML sequence diagrams e.g. data being logged and exchanged can be tracked for Set point 1: Perform Logging. We can see from the information flow (transitive) if this data is used in other systems or processes, which would lead to a MIL 3 assessment. However, the system does not name the standards applied. Therefore, we use the NISTIR 7628 [14] and SGAM modelling to assess the standards and the usual risk and mitigation strategies for this particular aspect. This enhances also our maturity model as it does not state explicitly standards to be applied at the maturity levels, e.g. ISMS based on ISO 27009 [28] (which would be need for Set point 4: manage SITUATIONS MIL 2). For the COP, we could identify the lack of MIL3 by finding out that the systems used do not cover an aggregator for real-time data. By carefully going through our individual ELECTRA use cases with the corresponding SGAM and Intelligrid models, we can easily set up a way in which those models interact to come up with a holistic tool chain to be used in context with ELECTRA.

5 Conclusions

With the increasing role of ICT in the Smart Grid environment, the importance of cybersecurity is becoming of the utmost importance. In the proposed ELECTRA architecture for voltage and frequency control, where responsibilities are distributed to decentralized cell controllers, this is even more so.

Next to the fact that there is a shift from a small number of central controllers (at Control Area level), to a larger number of decentralized controllers (in cells), there will be as well much more decentralized reserves providing resources that participate in frequency and voltage control schemes. Most likely, these will be communicating over public communication infrastructures requiring measures like strong authentication, integrity protection and encryption. Using public communication infrastructures as well is a concern, because of high availability and real-time requirements.

Besides, next to industrial- or utility-grade devices, also an increasing number of consumer-class devices will be included in frequency and voltage control schemes. In the most extreme view, these devices could be located at every household in a same manner as smart meters. Not only it can be expected that - because of cost - their security related capabilities will be more restricted than those of industry-grade devices, but also they will be located in non-secured, and easily accessible locations.

Based on the high-level functional architecture described in ELECTRA Deliverable D3.1, a number of guidelines and constraints have been formulated that will be taken into account while deriving the detailed functional architecture and specification. Ongoing cybersecurity reviews and advice will be provided during this detailed specification process and a full security review will be performed on the resulting architecture at the end of the project.

6 References

[1] "ELECTRA Project," http://www.electrairp.eu .

[2] EU, "DIRECTIVE 2009/28/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL," 2009.

[3] ICS-CERT, "The Industrial Control Systems Cyber Emergency Response Team," https://ics-cert.us-cert.gov/.

[4] L. Marinos, "ENISA Threat Landscape 2013 - Overview of current and emerging cyber threats".

[5] "NIST Cyber Security Framework," http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.

[6] D. F. et. al. Ferraiolo, "Proposed NIST Standard for Role-based Access Control," ACM, New York, 2001.

[7] L. et. al., "A Flexible Attribute Based Access Control Method for Grid Computing," Springer, 2008.

[8] "Xin, Jin; al., et. RABAC: Role-Centric Attribute-Based Access Control," Springer, 2012.

[9] "D. Richard Kuhn et al. Adding Attributes to Role-Based Access Control," ACM, Los Alamitos, CA, 2010.

[10] "CRUTIAL D2 "Analysis of new control Applications"," Crutial European Project, http://crutial.rse-web.it/content/files/Documents/Deliverables%20P1/WP1-D2-final.pdf.

[11] "Entso-e:Continental Europe Operation Handbook," https://www.entsoe.eu/publications/system-operations-reports/operation-handbook/.

[12] "Entso-e:Network Code on Operational Security," https://www.entsoe.eu/major-projects/network-code-development/operational-security/.

[13] "SmartC2Net D1.1 "SmartC2Net Use Cases, Preliminary Architecture and Business Drivers"," SmartC2Net European Project, , http://www.smartc2net.eu/public-deliverables.

[14] "Introduction to NISTIR 7628 - Guidelines for Smart Grid Cyber Security," The NIST Smart Grid Interoperability Panel Cyber Security Working Group. , 2010.

[15] "CEN-CENELEC-ETSI Smart Grid Coordination Group - Smart Grid Information Security," http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/xpert_group1_security.pdf, 2012.

[16] "Security of Energy Systems, D2 "International Standards and Policies – Map and Analysis" SoES European Project, http://www.soes-project.eu".

[17] "F. Cleveland, "List of Cybersecurity for Smart Grid Standards and Guidelines", May 2013. http://iectc57.ucaiug.org/wg15public/Public%20Documents/List%20of%20Smart%20Grid%20Standards%20with%20Cybersecurity.pdf".

[18] S. Liu, "Denial-of-Service (dos) attacks on load frequency control in smart grids".

[19] "Symantec Stuxnet Dossier," http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

[20] "The Register UK. Spotty solar power management platform could crash the grid.," http://www.theregister.co.uk/2014/05/12/hackable_solar_systems_spurt_free_money/, 2014.

[21] "NERC Glossary of Terms Used in Reliability Standards," www.nerc.com/files/glossary_of_terms.pdf.

[22] M. Uslar, "Security by Design for the Smart Grid: Combining the SGAM and NISTIR 7628," COMPSAC 2014.

[23] ELECTRA Deliverable D3.1 "Specification of Smart Grids high level functional architecture for Frequency and Voltage Control"

[24] ELECTRA Internal Report R3.1 "Problem description: specification of the requirements for the overall Smart Grid voltage and frequency control"

[25] ELECTRA Internal Report R4.2 "Maturity model for smart grid risk assessment combining SGIS and NISTIR approaches"

[26] G. Dondossola, R. Terruggia "Security of communications in voltage control for grids connecting DER: impact analysis and anomalous behaviours" Cigré Session 2014, Study Committee D2, Paper D2-104, Paris August 2014

[27] IEC/PAS 62559 ed 1.0. "IntelliGrid methodology for developing requirements for energy systems."

[28] ISO/IEC 27009 — Information technology — Security techniques — Sector-specific application of ISO/IEC 27001

[29] ISO/IEC TR 27019:2013 "Information technology — Security techniques — Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry"

[30] IEC 62056 "Electricity metering – Data exchange for meter reading, tariff and load control"

[31] The e-Highway2050 project. FP7. http://www.e-highway2050.eu/e-highway2050/

7 Disclaimer

The ELECTRA project is co-funded by the European Commission under the 7th Framework Programme 2013.

The sole responsibility for the content of this publication lies with the authors. It does not necessarily reflect the opinion of the European Commission.

The European Commission is not responsible for any use that may be made of the information contained therein.

ANNEX A: Background projects

Title	**CRUTIAL - Critical Utility InfrastructurAL Resilience**
Web site	http://crutial.rse-web.it/
Description	CRUTIAL is a European FP6 project addressing new networked ICT systems for the management of the electric power grid, in which artefacts controlling the physical process of electricity transportation need to be connected with information infrastructures, through corporate networks (intranets), which are in turn connected to the Internet. The objectives of the project have been: • Investigation of models and architectures that cope with the scenario of openness, heterogeneity and evolvability endured by electrical utilities infrastructures. • Analysis of critical scenarios in which faults in the information infrastructure provoke serious impacts on the controlled electric power infrastructure. • Investigation of distributed architectures enabling dependable control and management of the power grid.
Work relevant for ELECTRA	Control system scenarios and their ICT dependencies.

Title	**SoES – Security of Energy Systems**
Web site	www.soes-project.eu
Description	SoES is a European CIPS project designed to answer to the pressing demand of knowledge and best practices on the *cybersecurity* aspects in the Energy Smart Grids. It is conceived to raise the know-how of government bodies and operators by providing a multi-layered knowledge base on the ICT security matters grouping together information related to *reference architectures, international standards, vulnerabilities and countermeasures* of the Smart Grids. The analysis is developed along a three dimensional plan covering the technical issues, the policy aspects and inter-national/inter-organizational priorities.
Work relevant for ELECTRA	Use Cases, security risks and standards.

Title	**SmartC2Net - Smart Control of Energy Distribution Grids over Heterogeneous Communication Networks**
Web site	www.smartc2net.eu
Description	SmartC2Net is a European FP7 project that will develop, implement and validate robust solutions that enable Smart Grid operation on top of heterogeneous off-the-shelf communication infrastructures with varying properties. SmartC2Net objectives are: • To provide a reliable energy infrastructure at low infrastructure costs. • To position the capabilities of telecommunication operators and energy system integrators in the Smart Grid value chain creating benefits for all stakeholders. • To strengthen European research and industrial innovation in the area of Smart Grids via the combination of different research fields.
Work relevant for ELECTRA	Use Cases, security risks and standards, grid and ICT monitoring architectures.