Project no.:	**IST-FP6-STREP - 027513**
Project full title:	**Critical Utility InfrastructurAL Resilience**
Project Acronym:	**CRUTIAL**
Start date of the project:	**01/01/2006 Duration: 36 months**
Deliverable no.:	**D2**
Title of the deliverable:	**Analysis of new control applications**

Project co-funded by the European Commission within the Sixth Framework Programme (2002-2006)

Contractual Date of Delivery to the CEC:	31/12/2006
Actual Date of Delivery to the CEC:	17/01/2007
Organisation name of lead contractor for this deliverable	CESI RICERCA
Author(s): F.Garrone[1] (Editor), C. Brasca[1], D. Cerotti[6], D. Codetta Raiteri[6], A.Daidone[3], G.Deconinck[5], S. Donatelli[6], G.Dondossola[1], F. Grandoni[3], M. Kaâniche[4], T.Rigole[5]	
Participant(s): [1]CESI, [3]CNR-ISTI, [4]LAAS-CNRS, [5]KUL, [6]CNIT	
Work package contributing to the deliverable:	WP1
Nature:	R
Dissemination level:	PU
Version:	005
Total number of pages:	193

Abstract:

This document reports the results of the activities performed during the first year of the CRUTIAL project, within the Work Package 1 "Identification and description of Control System Scenarios".

It represents the outcome of the analysis of new control applications in the Power System and the identification of critical control system scenarios to be explored by the CRUTIAL project.

Keyword list: critical control system scenario, interdependency, electrical infrastructure, ICT infrastructure, threat, power system operation and maintenance

DOCUMENT HISTORY

Date	Version	Status	Comments
19/09/2006	001	Int	First table of contents
17/10/2006	002	Int	Agreed table of contents
30/11/2006	003	Int	Integration of major contributions
22/12/2006	004	Int	Integration of comments and contributions
17/01/2007	005	Apr	Integration of final comments and contributions

Table of Contents

Table of Figures

List of Tables

1 EXECUTIVE SUMMARY

This document reports the results of the activities performed in the Work Package 1 “Identification and description of Control System Scenarios” of the “CRitical UTility InfrastructurAL resilience (CRUTIAL)” project, as described in the Annex 1 to the EC contract n° 027513. It represents the outcome of the analysis of new control applications in the Power System and the identification of critical control system scenarios to be explored by the CRUTIAL project.

The Work Package 1 plan is structured into three tasks:

- T1.1, which is dedicated to the definition of requirements for architectural patterns including both the Electrical Infrastructure (EI) and the control structures, by emerging applications and technological renewal of existing applications. Two important evolutions are taking place nowadays. Firstly, the need to exchange process information among different operators/departments is forcing the adoption of standard IP based protocols over shared/connected wide and local area networks. Secondly, centralised control is not sufficient to exploit the opportunities of e.g., Autonomous Electricity Networks based on distributed generation, and decentralised control is required.
- T1.2, in which new control applications were investigated, related to autonomous electricity networks with distributed resources and interactions among power operators based on regulation and teleoperation hierarchical systems.
- T1.3, concerned the scenario representation. The UML (Unified Modelling Language) standard modelling notation has been selected for describing the infrastructures and control scenarios.

As a working methodology, considerable effort has been devoted in WP1 to collect information from existing systems, their renewal plans and emerging evolutions from the scientific and technical literature. Considering the largeness and complexity of the amount of systems and devices falling under the umbrella of power system control, the acquired knowledge is certainly partial and the power system picture derived has the only ambition to support the identification of sample control scenarios highlighting critical interdependencies among E.I. and ICT (Information, Communication Technology) services infrastructures.

The specification of the (portion of) Electrical Power System that is of interest for CRUTIAL is given in the form of natural language with the support of picture with drawings and symbols that are commonly used by electrical people, as well as in the form of a collection of UML diagrams, a language with whom computer science people are more familiar.

In the context of power system control, the ICT applications supporting the remote control of the equipments located in both generation stations and transformation substations are commonly called SCADA (Supervision Control And Data Acquisition) systems. Recently the meaning underlying the term SCADA system has been extended to refer to all the information, communication and control devices located in control and (sub)station sites.

These SCADA systems play a central role in the definition of CRUTIAL scenarios.

The document is organized into seven chapters and an appendix:

- Chapter 2 summarises background information and terminology used within the electrical system community that help in constructing a common set of concepts within the CRUTIAL consortium. For more detailed explanations, the reader is referred to specialised literature.
- Chapter 3 introduces a model of the Operational States and the Defence Plan of the Power System. There are summarised the technical and organisational counter-measures taken to prevent the propagation of a power system incident and the degradation of the state of service, and to avoid a collapse. The main regulations

constituting the first defence line are presented together with the hierarchical structure of the other defence actions.

- Chapter 4 overviews the identified control system scenarios, their main functions and ICT components. Also, it deals with configuration and security issues in current and future SCADA systems.
- Chapter 5 describes a set of scenarios that covers emerging themes involving ICT for Power System bulk generation, transmission and distribution infrastructures including:
    - the security of the remote supervision and control functions for grid and generation operators
    - the impact of attacks in emergency conditions
    - the possible breaches caused by the interconnections between the corporate and the process networks
    - the possible problems related to the ICT Systems' remote maintenance.
- Chapter 6 describes a set of scenarios that covers emerging themes involving ICT for Power System Distributed Generation.
- Chapter 7 reports the conclusions of the activities performed in the Work Package 1 of the CRUTIAL project and finalizes the results to the other Work Packages.
- Chapter 8 collects in an appendix the UML specification of the (CRUTIAL point of view on) Electrical Power Systems: a few UML diagrams are also included in the previous chapters, mainly to provide more structure to some concepts and to give a flavour of which aspects of the Electrical Power System can be captured through the UML diagrams.

The Italian power grid is used as an example to illustrate throughout the document.

1.1 Abbreviations

ACC	Area Control Centre
AEG	Autonomous Electricity Grid
ATS	Area Telecontrol System
AVR	Automatic Voltage Regulator
CC	Control Centre
CCT	Critical Clearing Time
CHP	Combined Heat and Power Cogeneration
CNM	Central Network Management
COTS	Commercial Off-the Shelf hardware or software component
DG	Distributed Generation
DoS	Denial of Service
DSO	Distribution System Operator
EHV	Extra-High Voltage
EI	Electrical Infrastructure
EMS	Energy Management System

EPS	Electrical Power System
FACTS	Flexible Alternating Current Transmission Systems
FTP	File Transfer Protocol
GENCO	GENeration COompany
HMI	Human-Machine Interface
HV	High Voltage
ICT	Information Communication Technology
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Device
IP	Internet Protocol
LAN	Local Area Network
LV	Low Voltage
MC	Marginal Cost
MCD-TU	Monitoring Control and Defence Terminal Unit
MV	Medium Voltage
NIC	Network Interface Card
NTP	Network Time Protocol
NTS	National Telecontrol System
NVR	National Voltage Regulator
OSI	Open System Interconnection
P2P	Peer-to-peer network
PFR	Primary Frequency Regulator
PMU	Phasor Measurement Unit
PQR	Reactive Power (Q) Regulator
PS	Primary Substation
PSAS	Primary Substation Automation System
PSS	Power System Stabiliser
RCC	Regional Control Centre
RPC	Remote Procedure Call protocol
RTS	Regional Telecontrol System
RVR	Regional Voltage Regulator
SAS	Substation Automation System
SCADA	Supervisory Control and Data Acquisition
SFR	Secondary Frequency Regulator
SQL	Structured Query Language
SS	Secondary Substation
TCI	TeleControl Interface

TCP	Transmission Control Protocol
TMI	TeleMonitoring Interface
TSO	Transmission System Operator
TSP	Telecommunication Service Provider
UCTE	Union for Co-ordination of Transmission of Electricity
ULTC	Under Load Tap Changer
UML	Unified Modelling Language
UPS	Uninterruptible Power Supply
VPN	Virtual Private Network
WAMS	Wide Area Measurement Systems
WAN	Wide Area Network
WAP	Wide Area Protection
XML	eXtensible Markup Language

1.2 Definitions

Term {Synonym}

Definition / explanation, cross-reference

Control System Scenario

A CONTROL SYSTEM SCENARIO is a reference structure and behaviour of (a portion of) the Power System, its related Monitoring, Control and Maintenance Networks and devices, including communication, host and server devices, in an environment exposed to threats that may jeopardise the operation of the power system services.

The Control System Scenarios explored in CRUTIAL are derived from state of art power control systems and their envisioned evolution.

Defence Plan

The DEFENCE PLAN summarises all technical and organisational measures taken to prevent the propagation or deterioration of a power system incident in order to avoid a collapse.

Disturbance

A DISTURBANCE is an unplanned event that produces an abnormal system condition.

Electrical Contingency

ELECTRICAL CONTINGENCY is an unexpected failure or outage of an electrical system component such as a generator, transmission line, circuit breaker, switch or another element. An ELECTRICAL CONTINGENCY may also include multiple components, which are related by situations leading to simultaneous component outages.

Electrical Power System {Electrical System}

The term ELECTRICAL POWER SYSTEM covers all the electrical, the control and automation, information and communication infrastructures and, generally speaking, all the necessary devices to produce and to transport the electric power towards the final users.

Island

An ISLAND represents a portion of a power system or several power systems that is electrically separated from the main interconnected system (separation resulting e.g. from the disconnection failure of transmission systems elements).

Marginal Cost

In economics and finance, MARGINAL COST is the change in total cost that arises when the quantity produced changes by one unit. The MARGINAL COST may change with volume, and so at each level of production, the MARGINAL COST is the cost of the next unit produced.

Power Grid

The infrastructure used to transport the electric power from the production plants to the final customers is called POWER GRID. The entire POWER GRID may be considered the sum of two subsystems: the transmission and distribution grids.

Regulation {Control}

The REGULATION of the electrical system is the process to obtain the desired behaviour of a continuous variable. In the case of the electrical power the main regulated variables are voltage, frequency, active and reactive power.

Security

The term SECURITY is used with different meaning in electric, information and communication communities. Within the electric power community SECURITY means the availability of energy supply in different operating condition in face of contingencies and disturbances. Meanwhile in information and communication communities the SECURITY is the resilience to malicious threats and attacks.

In order to avoid ambiguity in the following we will use the term SECURITY when the context is ICT and we will specify ELECTRICAL SECURITY in the power context.

Teleoperation

The term TELEOPERATION refers to actions performed at a distance and provoking a change in the configuration or setting of power components. Examples of teleoperation are the reconfiguration of the grid topology or maintenance operations.

Threat

The term THREAT refers to a potential violation of security, which exists when there is a circumstance, capability, action or event that could breach security and cause harm.

1.3 UML Formalisms

The UML (Unified Modelling Language) standard modelling notation [OMG 2002a] [OMG 2002b] [Pender 2003] [Flower 2003] has been selected for describing the infrastructures and control scenarios. The choice of adopting UML is mainly motivated by the fact that UML graphical notations are becoming widely accepted within some industrial communities like those in charge of developing standards for power control systems (IEC 61970, IEC 61850, IEEE C37.115 etc.) and UML diagrams normally support the documentation in their standard reports.

Different (meta)classes of UML diagrams have been used to provide a (close to) formal description of the control scenarios.

UML *class diagrams* are used to represent the structure of the electric power system in terms of class stereotypes. Each diagram focuses on particular aspects of the system. The class diagrams presented in this document show a static view of the system. Such diagrams may be refined and other types of UML diagrams such as sequence diagrams, may be derived from the class diagrams and used to represent the dynamic behaviour of the system in each scenario.

1.3.1 Class Diagrams

In UML a system is seen mainly from an object-oriented point of view, and therefore class diagrams play a central role. In a class diagram the system is considered as a collection of interacting objects corresponding to the system components. Objects are independent entities characterized by attributes and methods: the values of the attributes describe the state of the object; methods describe the behaviour of the object, e.g.: the operations that the object can perform.

The class diagram indicates the classes of the system, where a class acts as a template defining the common features of a set of identical objects, e.g.: objects with the same attributes and methods. An example of class diagram is reported in Figure 2-2.

A *class* is graphically represented by a box composed by three compartments containing the name of the class, its attributes and its methods respectively. When the attributes and the methods of a class are not specified, the class will be graphically represented by a box showing only one compartment (containing the name of the class).

Besides attributes and methods of the classes, the class diagram shows the relationships among the classes, in form of arcs; these are the types of relationship used in this document: association, generalization and aggregation.

An *association* is a logical relationship between two classes and is graphically indicated by an arc connecting such classes; if the association is in both directions, the arc has no verse, else its verse indicates the direction of the association. For instance, in Figure 8-1, the class *Application* is associated with the class *AutomationFunction*; in this example, the association holds only in one direction: from the class *Application* to the class *AutomationFunction*. The label of such association is “performs”, therefore we express that an application performs an automation function (not vice-versa).

The associations of the same class are mutually exclusive when only one of them can hold for an object (instance) of the class; mutually exclusive associations are represented by using the XOR operator.

The *generalization* is used to express that a class inherits the attributes and the methods from another class (parent class); this relation is graphically indicated by an arc with a white closed triangle pointing the parent class. For instance, in the class diagram in Figure 8-2, the class *LVLine* inherits the attributes of the class *Line* (parent class).

The *aggregation* indicates that the objects of a certain class (container class) are composed by objects of other classes; this type of relationship is indicated by an arc with a diamond pointing the container class. In the class diagram in Figure 8-4, the objects of the class *Site* are composed by objects of the class *PhysicalHost*.

A cardinality can be indicated on each end of an arc, in order to express the number of objects involved in the relationship; a cardinality can be a constant or a value varying over a certain limited or unlimited range. A range can be defined in this way: *a..b*, where *a* and *b* are the lower and upper limit of the range respectively: *a* must be a constant, while *b* can be set to a constant or to the infinite value. In UML, the symbol * used inside a range indicates +∞ (for instance, 3..*). The range 0..* can be indicated simply by ***.** For instance, in the class diagram in Figure 8-4, we express by means of the cardinality 1..* indicated on the aggregation arc connecting the class *PhysicalHost* to the class *Site*, that a site is composed by at least one physical host.

1.3.2 Use Case Diagrams

Use case diagrams are used to identify and partition system functionalities. Use case diagrams are composed by two types of elements: use cases and actors.

Actors represents roles that can be played by the user of the system; a user can be a human user or another system; in any case, a user is external to the system we are representing, and a user must supply stimuli to the system. An actor is graphically represented by the stick figure of a man.

A use case represents the behaviour of the system when a particular stimulus is sent to the system by a certain actor. Such behaviour is described textually by a “scenario” associated with the use case. A use case is graphically represented by an oval with the indication of the name of the use case.

Associations between actors and use cases are indicated in use case diagrams by solid lines. An association exists whenever an actor is involved with an interaction described by a use case. Associations are modelled as lines connecting use cases and actors to one another, with an optional arrowhead on one end of the line. For instance, in the use case diagram in Figure 8-10, the actor *LocalOperator* is associated with the use case *Primary*. The arrowhead is often used to indicate the direction of the initial invocation of the relationship or to indicate the primary actor within the use case.

There are three types of relationships between use cases: extends, includes, and inheritance as well as inheritance between actors.

An *extend* relationship specifies that the behaviour of a use case may be extended by the behaviour of another use case. The extension takes place at one or more specific extension points defined in the extended use case. However the extended use case is defined independently of the extending use case and is meaningful independent of the extending use case. On the other hand, the extending use case typically defines behaviour that may not necessarily be meaningful by itself. Instead, the extending use case defines a set of modular behaviour increments that augment an execution of the extended use case under specific conditions. An extend relationship is graphically represented by a dashed oriented arc going from the extending use case to the extended use case. The label of this arc is. <<extend>>. An example of extend relationship is present in the use case diagram in Figure 8-10, from the use case *SetupParameter* (extending use case) to the use case *Primary* (extended use case); this means that the use case *SetupParameter* is eventually perfomed when the use case *Primary* is perfomed. The condition determining the invocation of the extending use case is called “point of exception” and is defined in the “scenario” describing the behaviour of the extended use case.

An *include* relationship between two use cases means that the behaviour of a use case (including use case) includes the behaviour of another use case (included use case). The include relationship is intended to be used when there are common parts of the behaviour of two or more use cases. This common part is then extracted to a separate use case, to be included by all the use cases having this part in common. An include relationship is graphically represented by a dashed oriented arc going from the including use case to the included use case. The label of this arc is <<include>>. An example of include relationship in the use case diagram in Figure 8-11, involves the use case *Secondary* (including use case) and the use case *Communication* (included use case); this means that the behaviour of the use case *Secondary* includes the behaviour of the use case *Communication*; in other words, the use case *Communication* is executed whenever the use case *Secondary* is executed.

An *inheritance* relationship between two actors indicates that an actor inherits the use cases associated with another actor (pointed by the “triangle-headed” inheritance arc). An inheritance relationship between two use cases expresses that a use case is a specialization of another (pointed by the inheritance arc); for instance, in the use case diagram in Figure 8-10, the use case *Primary* is a specialization of the more general use case *VoltageRegulation*.

1.3.3 Interaction Diagrams

Interaction diagrams model the behaviour of use cases by describing the way groups of objects interact to complete the task. The two kinds of interaction diagrams are *sequence* and *collaboration* diagrams (communication diagram in UML 2.0). Interaction diagrams are used when you want to model the behaviour of several objects in a use case. They demonstrate how the objects collaborate for the behaviour. Sequence diagrams, collaboration diagrams, or both diagrams can be used to demonstrate the interaction of objects in a use case. Sequence diagrams generally show the sequence of events that occur, collaboration diagrams demonstrate how objects are statically connected. Both diagrams contain similar elements: the objects and the messages they exchange.

In sequence diagrams *objects* are shown as boxes at the top of vertical lines representing the object life time. *Messages* between objects are represented as arcs between vertical lines. This diagram is read left to right and descending.

There are a number of mechanisms that do allow for adding a degree of procedural logic to diagrams and which come under the heading of combined fragments. A combined fragment is one or more processing sequence enclosed in a frame and executed under specific named circumstances. Some of the fragments available are:

- *Alternative fragment* (denoted “alt”) models if…then…else constructs;
- *Option fragment* (denoted “opt”) models switch constructs;
- *Parallel fragment* (denoted “par”) models concurrent processing;
- *Loop fragment* encloses a series of messages which are repeated.

Example of sequence diagrams are present in the appendix.

In collaboration diagrams objects are listed as icons and arrows indicate the messages being passed between them. The numbers next to the messages are called sequence numbers. As the name suggests, they show the sequence of the messages as they are passed between the objects. There are many acceptable sequence numbering schemes in UML. A simple 1, 2, 3... format can be used, as the example below shows, or for more detailed and complex diagrams a 1, 1.1 ,1.2, 1.2.1... scheme can be used.

1.3.4 State Diagrams

A collection of state diagrams can be used to describe the behaviour of a system, of a component, or of an object. State diagrams describe all of the possible states of an object (or a component or a system), as events occur. The nodes of a state diagram are rounded boxes representing the *states*; arrows in a state diagram are used to indicate *state transitions*. The box representing a state may contain the activity section indicating the *activities* that the object will be doing while it is in that state. A state diagram includes an *initial state*:, this is the state of the object when it is created. The initial state is identified by a black dot connected to the initial state by an arc. For instance, in the state diagram in Figure 8-24, the state *Idle* is the initial state.

The dynamics of the state diagram is determined by the events associated with the transitions (arrows). A state transition is triggered by several kinds of event such as a certain Boolean condition becoming true, the receipt of an explicit signal, or the passage of a designated period of time after a designated event.

State diagrams can include super-states. A super-state is a particular state containing an inner state diagram composed by sub-states. A super-state is useful when the description of a single state needs a further state diagram instead of a simple activity. In the state diagram in Figure 8-24, the super-state *Sending* is present; its sub-states are *Delivery* and *FailedDelivery*; *Delivery* is in turn a super-state whose sub-states are *Normal* and *Delayed*.

A particular node consisting of a circle containing the symbol H, is used to indicate the sub-state holding the first time we enter the super-state. The sub-state inside a super-state can change as the time elapses; when we leave the super-state, we implicitly leave the current sub-state. The symbol H (history) indicates that if we return in a certain super-state, we return in the sub-state we had previously left. Such symbol is present in the state diagram in Figure 8-24, and it points the sub-state *Normal* inside the super-state *Delivery*.

2 POWER SYSTEM INFRASTRUCTURE AND CONTROL

We use the term *Electrical Power System* (EPS) or *Electrical System* to cover all the electrical, the control and automation, information and communication infrastructures and, generally speaking, all the necessary devices to produce and to transport the electric power towards the final users. Electric power is obtained transforming several kinds of energy available in nature by means of machines called generators, situated inside power plants. The energy produced by the generators is then adapted, for voltage levels, by components called transformers, to be conveyed with minimal dispersion, to the different types of end users (civil, industrial, military, etc).

The infrastructure used to transport the electric power from the production plants to the final customers is called *Electric Power Grid* (or *Electric Power Network*). The entire power grid may be considered the sum of two subsystems: the transmission and the distribution grids.

From now on this document the term network will be used only to refer to Information and Communication Network, in order to avoid any type of misunderstanding with the Electric Power Network.

While the Electrical Power Grid is the most important part of the electrical system, other subsystems are necessary to guarantee the continuity of power supply and the structural integrity of the components of the electrical infrastructure: the automation and control systems of the power equipments and its protection system. The distinction between the two infrastructures is not always obvious, because only their combined action ensures the correct operation of the electrical system.

Another important subsystem is the so called *Energy Management System* (EMS) whose function consists in maintaining the correct balance between load and generation.

The Figure 2-1 represents a simple scheme of the electrical system. As illustrated by the scheme, the electrical system is subdivided into three main subsystems: generation, transmission and distribution, whose components are physically connected through the power lines.

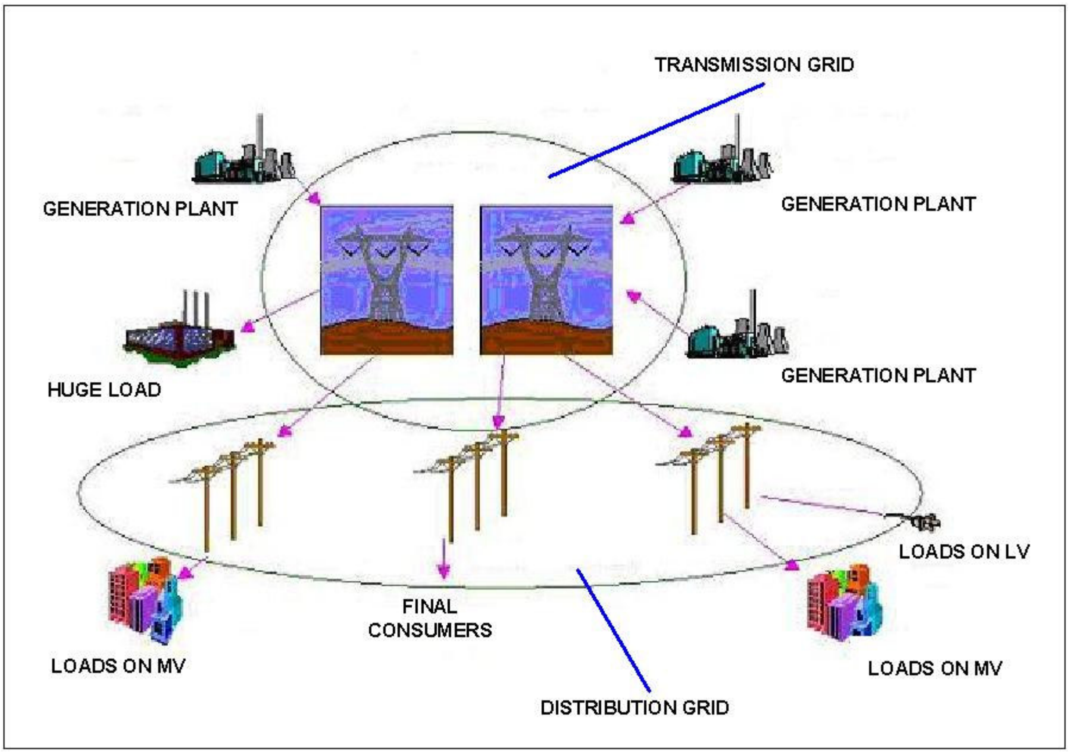


Figure 2-1: Scheme of the electrical system

The logical organization of the EPS as UML class diagram (CD) is shown in Figure 2-2, where dotted points means that other components are present, but are not relevant at this point.

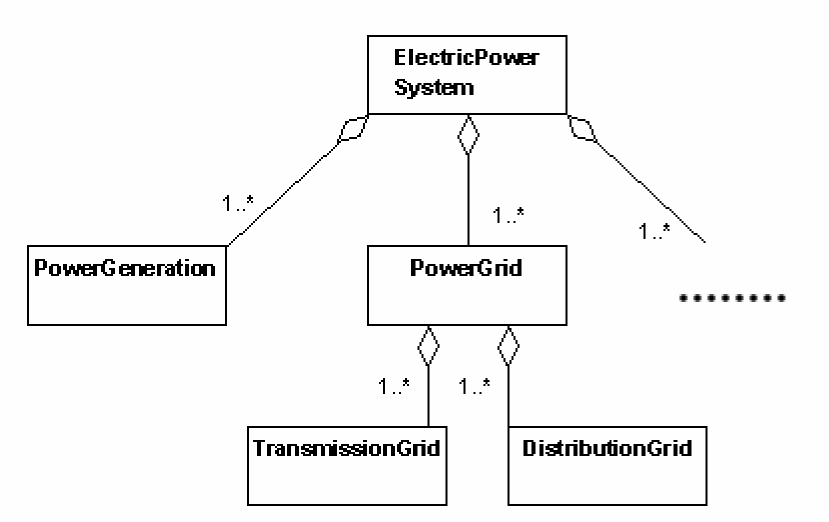


Figure 2-2: Class Diagram of EPS main components

Each macro-subsystem is equipped with its own components of protection and control that constitute the ICT (Information Communication Technology) infrastructure.

The logical organization of the ICT infrastructure as UML class diagram is shown in Figure 2-3. The CD also highlights the relationships between the ICT infrastructure and the EPS.

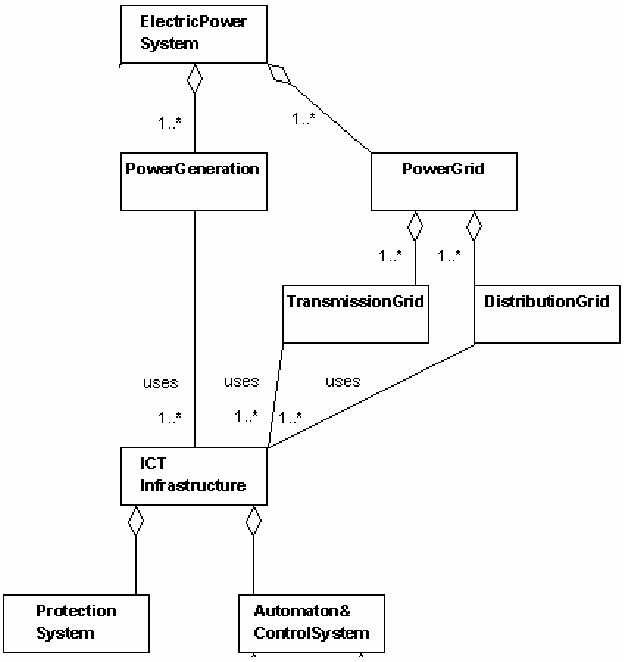


Figure 2-3: Class Diagram of the EPS completed with the ICT scheme

The major interdependencies among Electrical Power System infrastructures and ICT components are depicted in the Figure 2-4.

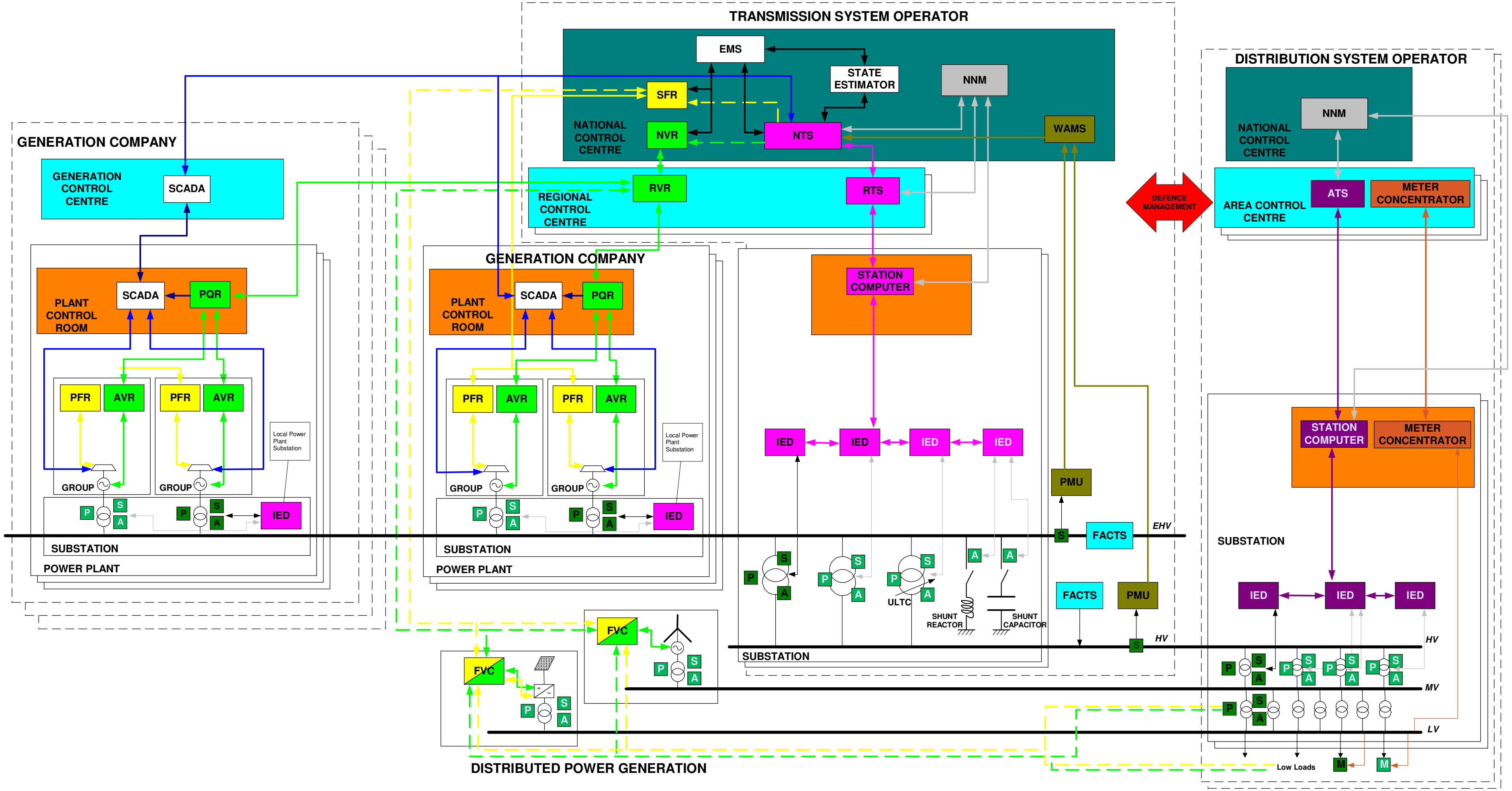


Figure 2-4: Electrical Power System interdependencies

In the following paragraphs and chapters we shall detail the single macro subsystems of the electrical system and its ICT infrastructure.

2.1 Bulk Generation

2.1.1 Bulk Generation components

The generation consists of the transformation of several types of energy present in nature into electric power. Natural energy is transformed into electric power by means of the so called *generation units*, located in power plants, which can be typically hydroelectric, thermoelectric and nuclear.

Hydroelectric plants use the potential energy of water, thermoelectric plants derive energy from combustion, while nuclear plants use atomic reactions; in all cases, the natural energy is first conveyed to turbines providing mechanical energy which is then transferred to alternators, the actual electrical generators.

The Figure 2-5 [Brand *et al.* 2003] presents a simple scheme of a steam generation system and its primary control equipment. The details of the control system are explained in the following chapters, while a brief description of the generation components are explained hereafter.

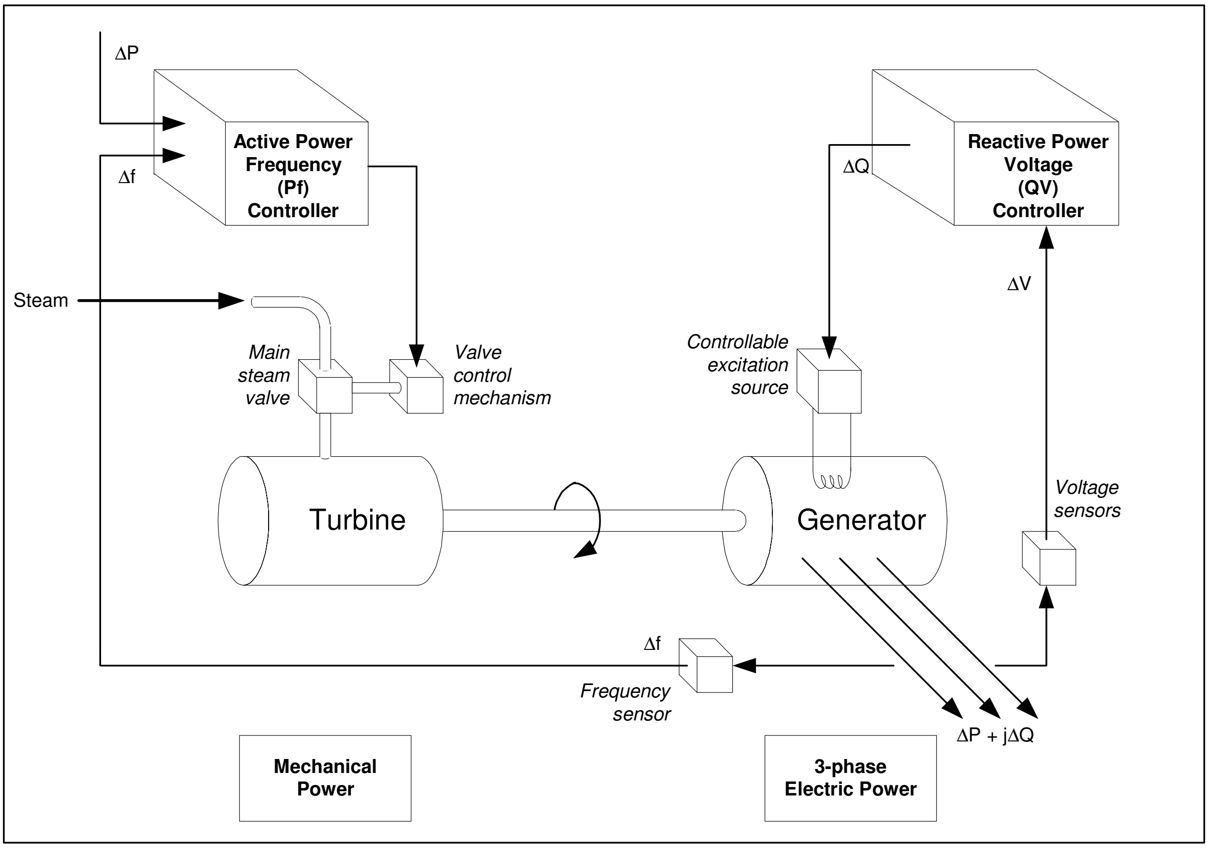


Figure 2-5: Scheme of the electric power production and its control systems [Brand *et al.* 2003]

The turbines are rotating machines that transform the potential, kinetic, or thermal energy associated to a fluid into mechanical energy. Depending on the nature of the operating fluid three types of turbines can be distinguished: hydraulic, gas, and steam.

The alternators are electrical components that convert the mechanical energy produced by the turbines in electric power. The electric power is generated in sinusoidal waveform to the rated frequency. In Italy and Europe the rated frequency is set to 50Hz.

Alternators consist of a fixed part, called stator, and of a mobile part, called rotor. On both parts there are electrical conductors connected among them so as to form two circuits. One circuit has the function to create the magnetic field and the other to induce the electromagnetic force.

The operation of a generation unit can be synthesised in the following way. The first motor (in many cases a turbine) supplies the mechanical energy used to keep in rotation a shaft, whose rotation generates (according to the law of the electromagnetic induction) electromagnetic force in the stator's windings. The resulting current flow produces the electric energy transported by the power grid according to the load demand.

The generators can also work in the reverse mode, transforming the electric power absorbed from the grid in mechanical energy. This function is used for example in pumped hydroelectric power plants where during the night hours, when the power demand is lower, the water is pumped into the upper reservoir to be again available in peak periods of power demand.

2.1.2 Automation and control of the generation system

As evidenced by the Figure 2-5 power generation systems comprise not only the power production units but also a number of components able to interact with the primary components and used to monitor their state. These components constitute the system of automation and process control of electric power production.

The *regulation* of the electrical system is the process that adapts the production of electrical power to the required loads. Regulation requirements are "communicated" by the EMS and then carried out inside each power plant and inside each unit of generation.

Both the generator and its turbine (or engine) are subject to the regulation process, which consists mainly in the control of the couple distributed by the turbine (intensity of the exit current from the generator), the control of the spin speed of the turbine and of the generator (and therefore of the power grid frequency) and the control of the excitation of the alternator (amplitude of the exit voltage).

It is important to notice that the regulations previously mentioned apply to one single generation unit, unaware of the presence of other units of generation. The presence of multiple generation units introduces another type of regulation: the control of the phase, that is the control of the angle of phase-difference between the phasors representing the voltage exiting from the generators. In particular, it is not important that this angle is null, but that the angle does not vary in time. In fact, the variation in time of the angle generates the occurrence of an oscillating phenomenon inside power grids of great extensions (more than 1000 km).

A particularly important issue is the regulation of the power grid frequency nominally of 50 Hz. As mentioned before, there is a precise dependency between the frequency and the speed of generator spin; however, this relation is influenced by the loss of balance between the generated power and the consumed power. Mathematically the dependency is expressed by the following relation:

$$\frac{df}{dt} = \frac{f_0}{T_m} \frac{\Delta p}{P_m}$$

where Δp is the difference between the generated power and the power absorbed by the load, f_0 is the medium frequency on the power grid before the occurrence of the imbalance and P_m and T_m are positive constants that depend on the structure of the power grid.

This relation means that when the absorbed power is greater of the generated power, the power grid frequency decreases because Δp assumes a negative value. Vice-versa if the generated power is greater than the consumed power, the power grid frequency increases. These assumptions stress the importance of maintaining a balance between energy production and the effective consumption. In fact, when energy consumption is too high compared to energy production, the frequency on the grid decreases because the generators, not able to supply sufficient power, use part of their kinetic energy to satisfy the demand, diminishing their speed of spin. Beyond the acceptable range, fixed in Italy between 47.5 Hz and 52.5 Hz, the generators are disconnected from the power grid in order to avoid possible breakdowns.

It's evident that the control of the generation is a complex problem. The related control systems have to provide three orders of functions: specific procedures for the control of the behaviour of each single generation unit; synchronisation of multiple generation units; control of the interaction between the generation and transmission systems and the connected loads.

2.2 Transmission and Distribution

The electric power produced by generation plants is made available to the final customers through the transmission and distribution power grids.

The electric power grid infrastructure consists of power lines (in air or earth), substations of transformation (or interconnection) and protection and control systems.

The management of the transmission/distribution power grid is under the responsibility of the grid operators (Transmission System Operator, i.e., TSO, and Distribution System Operator, i.e., DSO), who have the task to control all the power flowing through the electric power lines with the aim to guarantee the quality and the continuity of the service.

The main differences between the transmission and the distribution grid are the voltage levels and the infrastructure topology.

Based on the voltage level, power lines can be classified in three categories:

- Extra-high and high voltage lines (EHV-HV): voltage values equal to 380 – 220 (EHV) - 132 (HV) kV
- Medium voltage lines (MV): voltage values equal to 60 - 10 kV
- Low voltage lines (LV): voltage values equal to 380 - 220 V

The transmission power grid is operated in extra-high voltage levels (220 kV and 380 kV) and constitutes the backbone of the electrical system. The interconnection grid, which is operated on 132kV, is connected to transmission level and constitutes the link between transmission and distribution level. The substations in the distribution grid transform the high voltage levels into medium and low voltage levels for the final customers.

It is important to note that, while the transmission grid is easily identifiable, the distribution and interconnection grids are not clearly distinguishable. To avoid confusion, it is necessary to explicitly delimit the border between transmission and distribution grids or, in other words, to identify which are the voltage levels under the control of the different operators.

From a topological point of view, the transmission grid is similar to a meshed graph. A meshed graph is a graph in which every node is reachable through more than one line path. The nodes of the graph represent the substations, while the arcs represent the transmission lines that connect the several substations. The reason for which the power plant and loads are connected through a meshed net is because this topology increases the robustness of the entire system. We have to remind that the loss of single generators or lines must not cause dangerous consequences for the final customers.

For what concerns the connection grid (132 kV) it has been agreed to adopt a partially meshed operation; in this case the term “operation in island” is used, meaning that the grid operates in a stable state in self-sufficient zones from the point of view of the generation-load balance.

The distribution grid is instead mainly operated in a radial topology: the loads are connected to their substations in a star or in a ring with the aim of reducing service interruptions as a result of a major fault. Its nodes of interconnection are Primary Substations (PS), connected to HV lines, which transform and distribute energy to Secondary Substations (SS) and to MV customers, and Secondary Substations (SS), which transform and distribute energy to LV customers.

In the following Figure 2-6 a schematic diagram of the power grid is given. Some of the very high voltage substations are directly connected to the generation plants by means of set-up transformers that raise the voltage from 20 kV (voltage value at the generator terminal) to 220 kV or 380 kV (operation voltage of EHV lines): in this way the transmission losses are reduced. Other transformers, situated in the transformation or interconnection substations physically connect two grids with different voltage levels. Another important aspect is that not all the loads are connected to the distribution grid; some, typically the large industrial poles, are directly connected to the transmission grid, specially to the low level 132 KV.

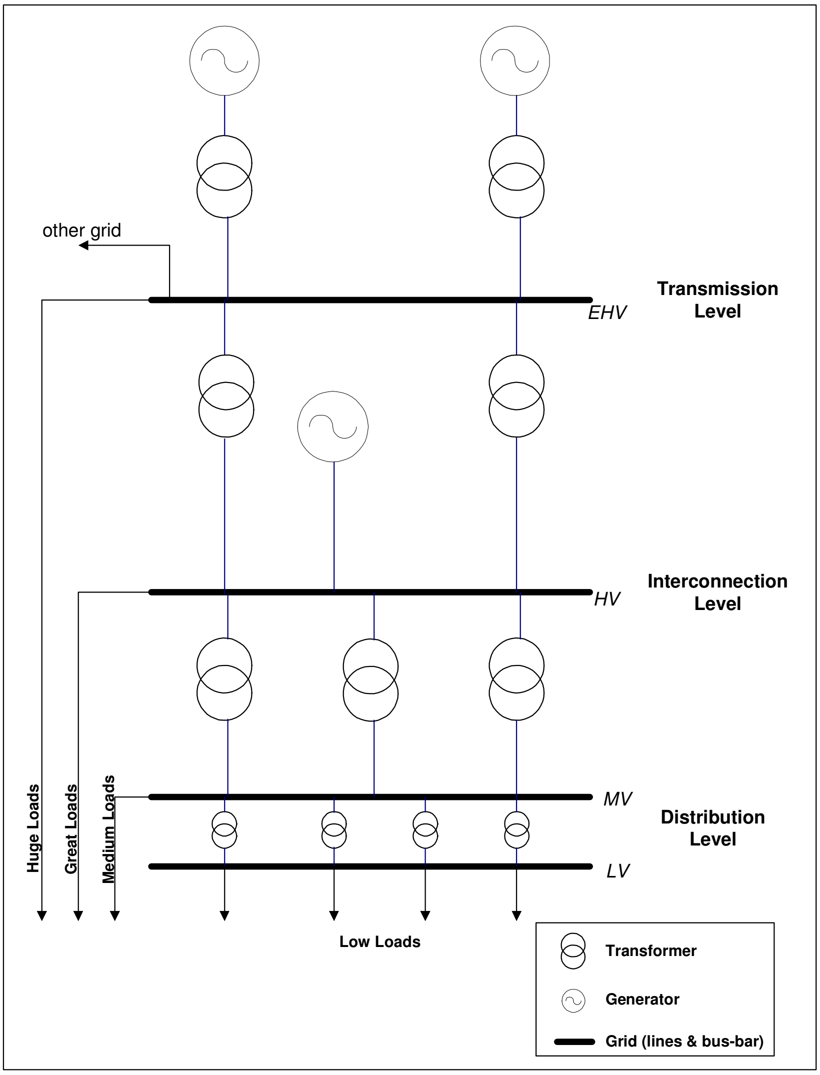


Figure 2-6: Scheme of the power grid

2.2.1 Power Grid components

The main elements that constitute the power grid are the following:

- *Power lines*: (*lines* in the following) they are components which physically connect the substations with the power plant and the final users
- *Substations*: they are structured components in which the electric power is transformed and split over several lines. In the substations there are transformers and several kinds of connection components (bus-bars, bays, switches and breakers)

2.2.1.1 Lines

The connection between the lines and the power plants or between lines and end users is implemented by means of bars, i.e., a set of components that make it possible to perform the grid operation in a dynamic and safe way. The length of a line can range from few kilometres to some hundred kilometres, and lines can be underground cables or aerial ones. The underground cables have the conductors covered by an insulating layer. The aerial (or overhead) lines are those supported by towers. The length of the underground lines is remarkably shorter than aerial lines. The aerial power lines are essentially made up of conductors which physically transport the energy. Every transmission line is composed by three conductors. This configuration is typical of a three-phase system allowing a more efficient transmission of the energy in a sinusoidal regime.

The pylons (also known as transmission towers or masts) are tall steel lattice structures used to support overhead electricity conductors for power transmission. They are approximately 50-60 meters high, they support the lines and hold them far away from the ground and the persons. Aerial power lines are often equipped with a ground conductor, or a shield wire. A ground conductor is a conductor fastened to the top of the towers, which protects the line against lightning strikes.

The insulators are the elements supporting the conductors on the pylons and at the same time isolating them electrically.

2.2.1.2 Substations

Logically every substation is subdivided into different sections: every section is characterised by a different voltage level and two sections are connected by means of transformers. Each section consists of a bus-bar and a group of bays, used to dis/connect a group of generators, a line or a transformer, a bus-bar or a portion of a same bus-bar from/to a given bus-bar. In following Figure 2-7 a simple outline of a substation is represented.

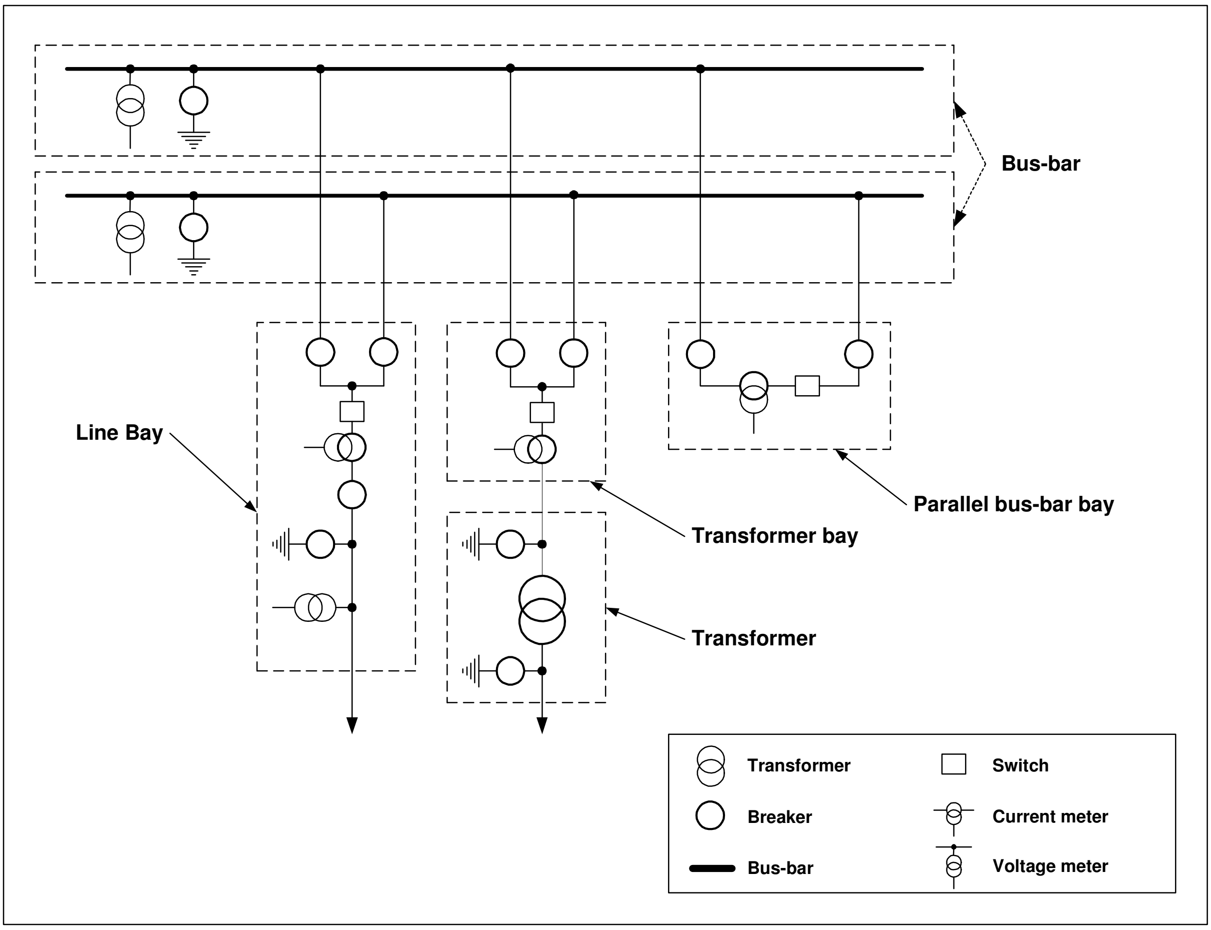


Figure 2-7: Scheme of the substation

2.2.1.2.1 Transformers

A transformer is an electrical machine that changes the voltage and current values maintaining the instantaneous power, i.e., their product, unchanged. The electrical model of the transformer (see Figure 2-8) is a double dipole, where *K* takes the name of transformation relationship.

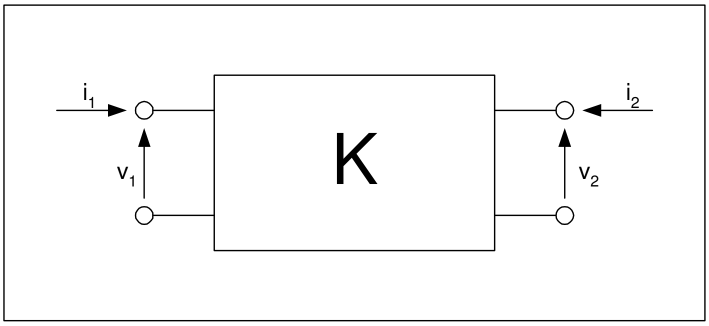


Figure 2-8: Electrical model of the transformer

According to the following equations:

$$v_1 i_1 + v_2 i_2 = 0 \qquad \frac{v_1}{v_2} = K = -\frac{i_2}{i_1}$$

the energy may be always available at the convenient voltage level, that is, the lowest voltage for the final user, and the highest voltage when it is necessary to transfer it over a long distance. Naturally, the above relations are true in the ideal case, because they do not take into account the transformer losses.

On some type of transformers it is possible to change the number of turns in order to perform the voltage regulation of the secondary side. The transformer tap is the connection point along a transformer winding that allows the number of turns to be selected. Selection of the tap in use is made via a tap changer mechanism.

2.2.1.2.2 Breakers

The breakers are components used to interrupt the current flow by opening the electrical circuit. They have short closing and opening times (of the order of the milliseconds) and they work also in presence of a current flow.

A breaker is constituted by two electrodes connecting the two ends of the breaker. Normally the two electrodes are in contact and the breaker is closed: to open the breaker the electrodes have to be separated. During this separation a voltaic arc between the two electrodes can be established causing energy dispersion and a current flow. This is normally avoided injecting a high pressure gas, the SF_6, between the two electrodes while they are being separated. This particular gas has a dielectric function and inhibits the occurrence of the arc.

The breakers are commanded by protections and control orders, but they can be controlled also for operation and maintenance purposes.

2.2.1.2.3 Switches

The switches, like breakers, are devices used to physically separate the connected grid elements. Differently from breakers, they cannot work in presence of a current flow because they are not able to tolerate the electrical arches established between the two extremities of the switch. Their manoeuvring times are longer than that of the breakers (some seconds). Consequently they are only used after that the current flow has been interrupted by means of the breakers. The combined action of breakers and switches guarantees the complete physical and galvanic isolation of the elements they connect.

2.2.1.2.4 Bus-bars

The bus-bars are the connection components of the substations to which all the other components are physically connected. The substations are the nodes of the grid from the topological point of view, the bus-bars are the nodes from the electrical point of view. In Figure 2-7 the bus-bars are represented by two horizontal lines. Physically they are constituted by three aluminium bars, one for each phase, allowing the transfer of the electrical power between the different elements of the substation. They can be single or double (also triple sometimes) depending on the requirements of the specific substation (in Figure 2-7 a substation configuration adopting a double bus-bar is given).

2.2.1.2.5 Bays

The International Standard 61850 [IEC 61850-5 2003-07] defines a bay as a meaningful substructure of a substation with some common functionality. Bays are usually constituted by a set of breakers and switches used to establish the electrical connections between the apparatus of the substation and the transmission lines. They are the elements thanks to which it is physically possible to modify the configuration of a substation and to adapt, within given limits, the topology of the grid to the requirements stated by the load. The main types of bay in the substation are the bus-bar bay, line bay and transformer bay. Bus-bar bays are used to dis/connect two or more bus-bars, or also to merge/separate two parts of a same bus-bar. Line and transformer bays are used to dis/connect a line or a transformer to/from a bus-bar or to change the bus-bar to which they are connected.

2.2.1.2.6 Voltage and current meters

Meters are fundamental grid components used to measure voltage and current of the substation components. They play an essential role in monitoring the grid's electrical state.

2.2.2 Grid management

The management of national electric power system highly depends on the strategic organisational model adopted by each country policy.

Up to the early 90s, the entire Italian electric system used to be managed by ENEL (the governative power system management operator) on a monopolistic basis, using a three level, hierarchical control structure. The subdivision had been made with the aim to simplify and to improve the monitoring and the management of the power grid.

The three levels were the following (see Figure 2-9):

- *Low level*: constituted by local area control centres (ACC - Area Control Centres). Each ACC controlled from 10 to 20 extra-high and high voltage (EHV - HV) substations and had the following objectives:
  - Guarantee the correct operation of substation equipments
  - Reconfigure the substations in case of breakdown of some apparatus

  The reconfiguration of a substation was (and still is) carried out by means of commands sent by the remote centre to the substations automation system.
- *Middle level*: constituted of regional control centres (RCC - Regional Control Centres). Every RCC controlled, through the monitoring of two or three ACCs, a large portion of the power grid, the whole Italian territory was subdivided in three regions. The main tasks of the RCC were:
  - Monitor their portion of the grid in order to diagnose faults on the power lines
  - In case of breakdowns, choose the more suitable corrective actions to restore the functionality of the grid

  Since the RCC were not directly connected to the substations, the corrective actions to adopt were communicated to the ACC of reference.
- *High level*: this was the national control centre (NCC - National Control Centre) having the main function of supervising the entire grid and handling the planning of medium and long term operations. Another function of the NCC was to assist the RCCs to localise breakdowns on the power lines situated between two regions.

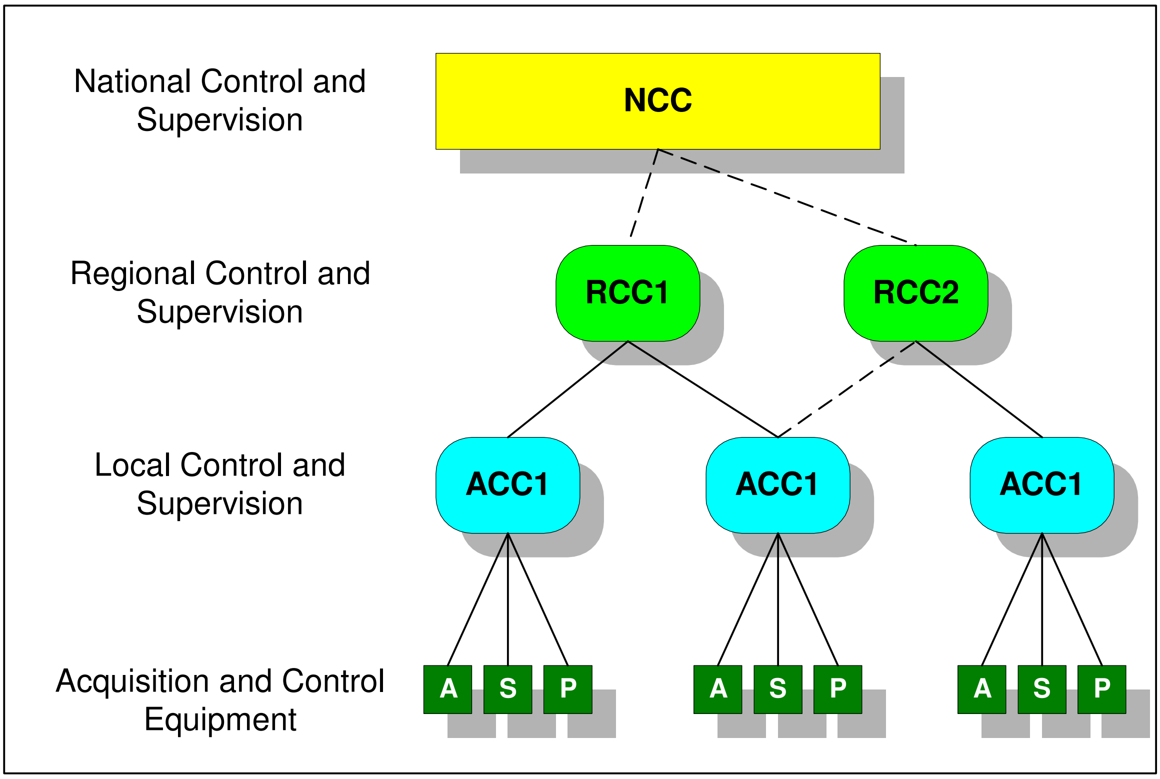

National Control and Supervision
NCC
Regional Control and Supervision
RCC1
RCC2
Local Control and Supervision
ACC1
ACC1
ACC1
Acquisition and Control Equipment
A
S
P
A
S
P
A
S
P

Figure 2-9: Hierarchical control system

Figure 2-10 shows the CD of the control centres that build up the control structure of the EPS. Each control centre is located in a site, and sites exchange information according to the associations among classes.

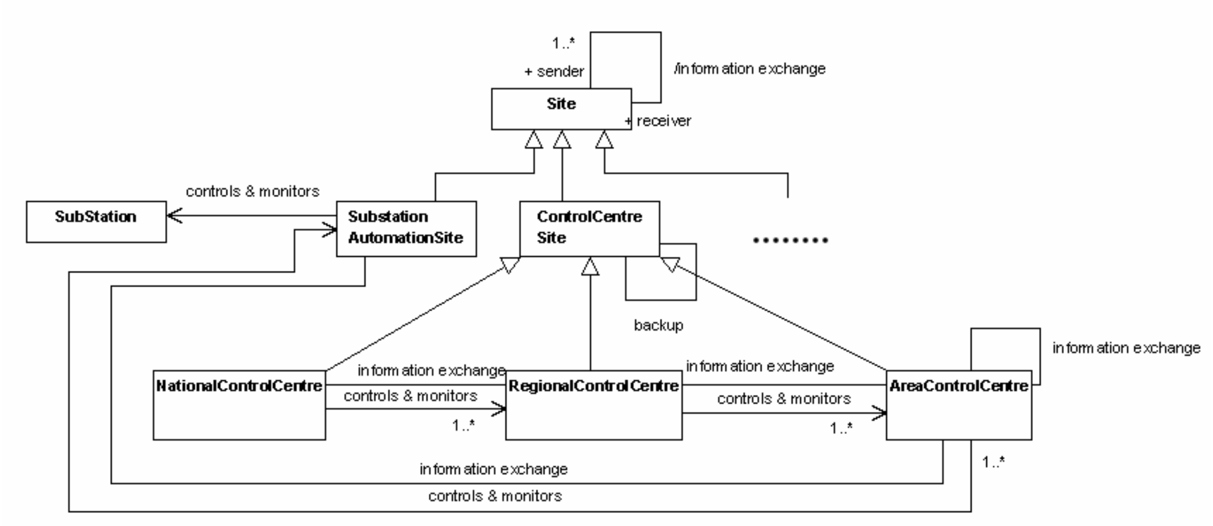


Figure 2-10: Organization of Control Sites

Today, also Italy entered into an open power market regime where the service is provided by different companies, producing energy on their own or acquiring it from other producers and traders. In this new scenario many aspects of the electrical system have changed. Although the power grid infrastructure remains substantially the same its management has undergone deep modifications, and the hierarchical structure introduced previously has lost most of its validity.

From the functional point of view the power system is still divided in homogeneous areas and regions but, in absence of a monopolist, these portions are not managed by the same actor.

Different areas of the power grid are used by different generation companies that must act in a coordinated way, in order to guarantee the continuity of the service.

In order to coordinate their actions, all the generation companies involved in the power market refer to a TSO (Transmission System Operator, Manager of the National Transmission Grid) who:

a) publishes the regulation for connecting the power production systems to the EHV-HV grid
b) defines the plans of development of the power grid
c) manages the energy stock exchange
d) handles the interactions with foreign countries through collaboration relationships with the electric power managers of bordering countries.

The role that the various actors (stakeholders) play in the management and ownership of the EPS can be nicely described through the CD of Figure 2-11.

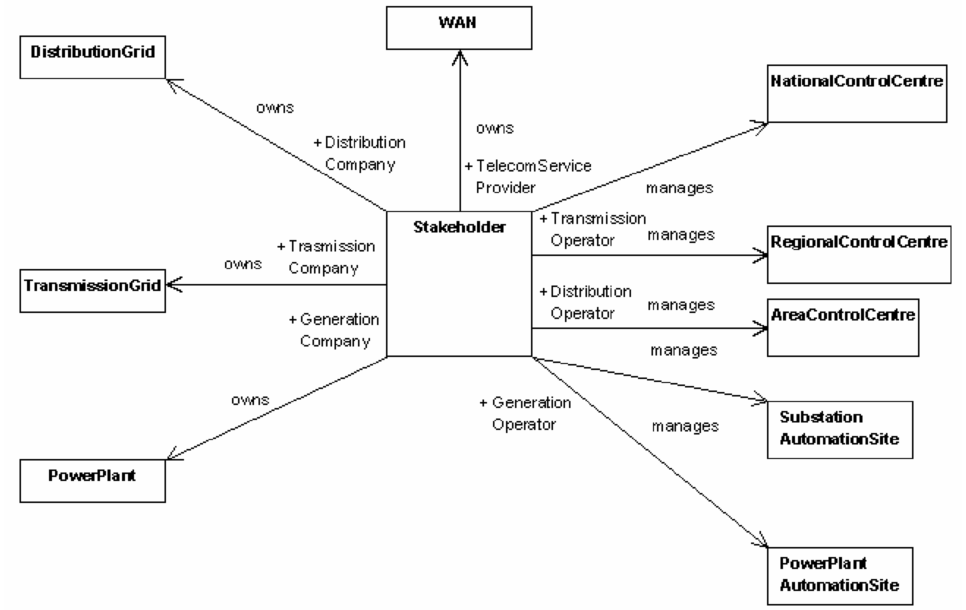


Figure 2-11: Roles of stakeholders in the EPS

From a functional point of view, we still have a hierarchical control structure but there have been major changes in its management. At the highest level there is the TSO, who coordinates the actions of all the companies involved in the energy market while these actors constitute the intermediate and lowest levels of the hierarchy.

2.2.3 Grid Automation and Control

The main purposes of the power grid control system are:

- Remote control of the installed equipment: receive alarms and send commands
- Grant availability of service by reducing out service time of lines and substations
- Grant reliability of service by optimising substation management
- Enhance quality of service through real-time monitoring of electrical power system parameters as frequency, voltage etc.
- Collect system statistics
- Coordinate maintenance: planning the interventions on the lines and substations.

- Reduce operation and maintenance costs

This is realized by a set of automation functions, whose classification is given in Figure 2-12.

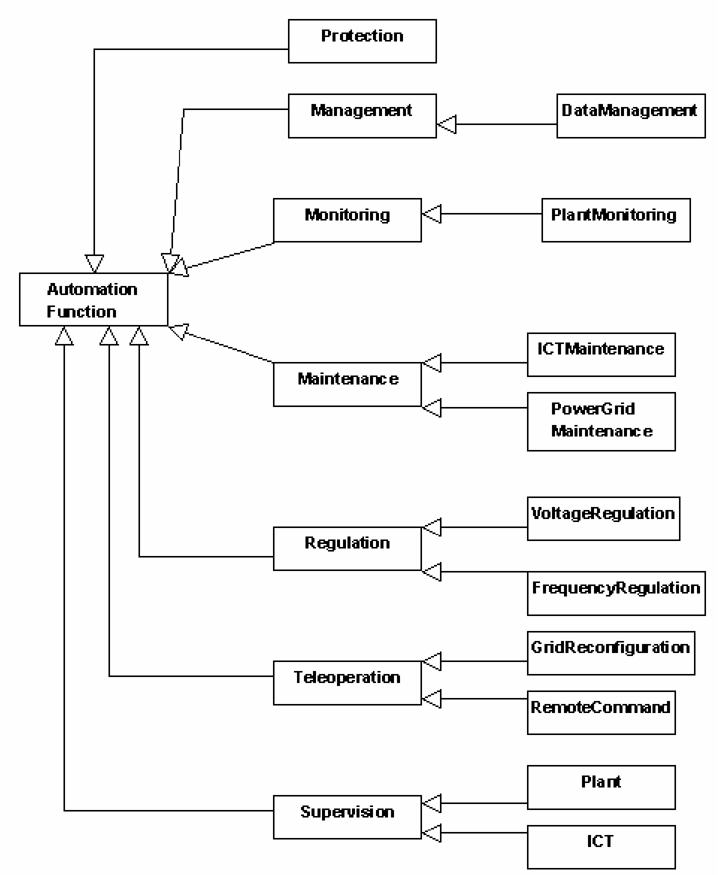


Figure 2-12: The automation functions of the EPS

Essential parts of the power grid control system are the Substation Control Systems and the communication network that supports the necessary information exchange.

2.2.3.1 Communication networks

The prerequisite for the provision of timely information to the actors involved in the operation of the power system is an efficient and reliable communication network.

This must be able to support both remote control from grid control centres and retrieval of data on loads, interruptions, voltage disturbances, and other electrical events from all substations for operation, maintenance and planning departments.

There are basically two kinds of communication over the communication network:

- Real-time communication between grid control centres for supervisory control and data acquisition (SCADA) and energy management systems (EMS) as well as between the various substations for control devices
- Non real-time communications to transmit data to the back office departments for protection engineering and maintenance as well as for planning and asset management (e.g. statistics, trends, condition related data)

Consequently, the communication system itself should consist of two partial networks, one for the exchange of real-time information and one for non time-critical data flow, with different performance requirements (see Figure 2-13).

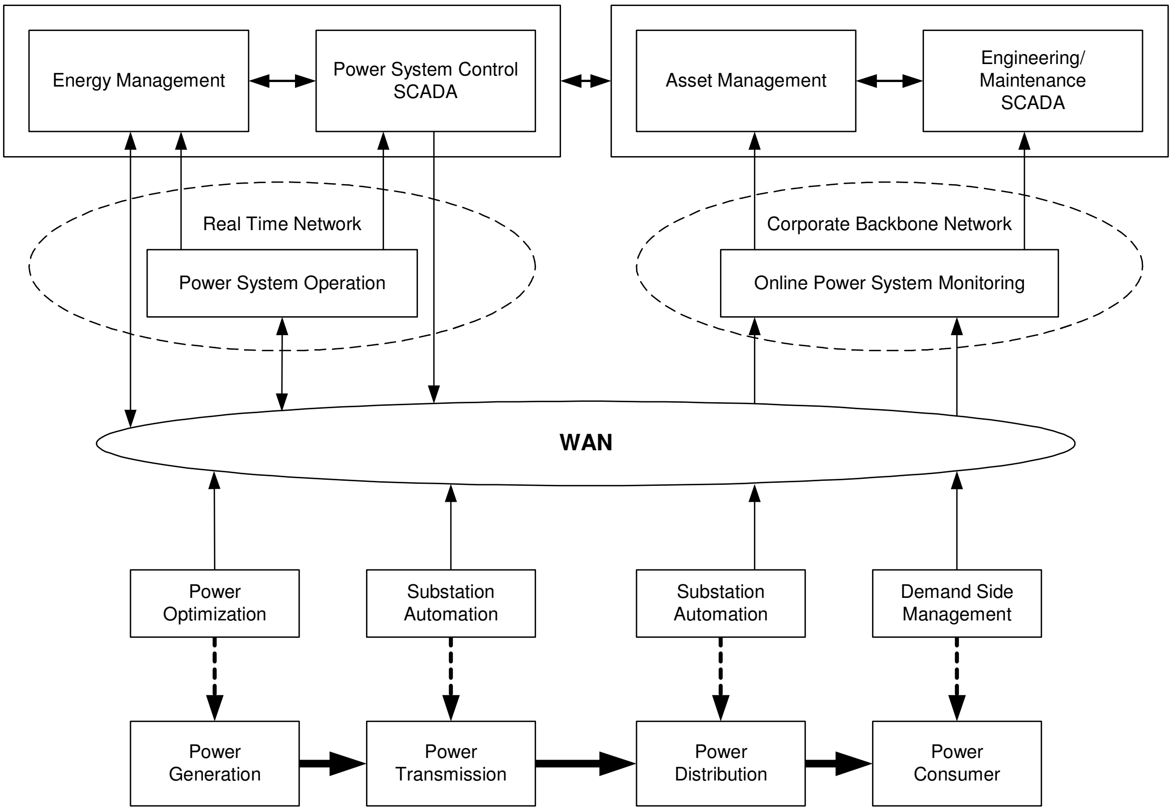


Figure 2-13: Communication System Overview

2.2.3.2 Substation Control Systems

The main functions of a Substation Control System are:

- Real-time data acquisition
- Automatic control of substation equipments
- Monitoring of power grid components with real-time alarm and anomaly handling
- Human Machine Interface: generation and upgrade of operator synoptic
- Data collection and storage in databases
- Generation of statistical reports
- Data transfer to other systems

The core of the Substation Control System is the Substation Automation Systems (SAS). A Substation Automation System (also called secondary system) is an interaction set of co-operating Intelligent Electronic Devices (IEDs), connected by a communication system, performing all the functions which are necessary to operate, protect and monitor the substation's equipment and switchgear (also called the primary system). The UML object model of a power substation reported in the standard IEC 61850-6 [IEC 61850-6 2004] is depicted in Figure 2-14.

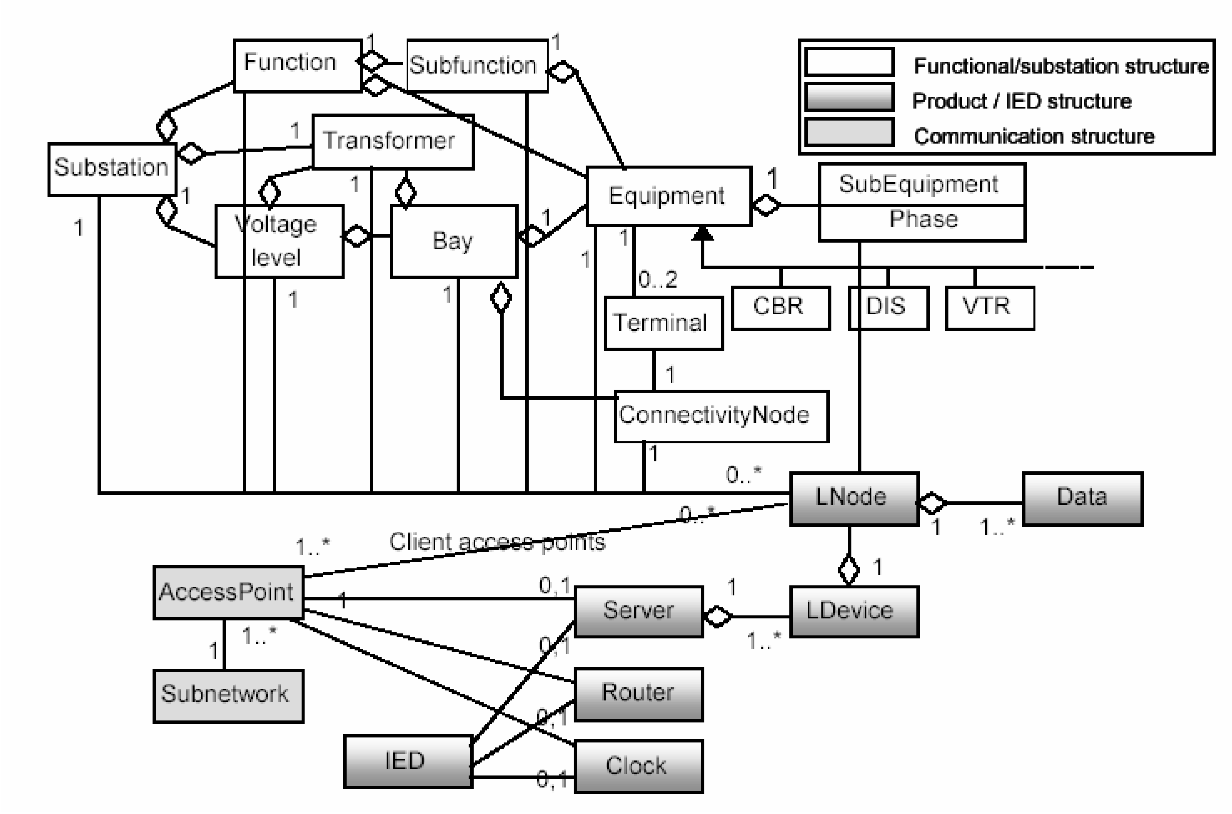


Figure 2-14: Substation object model in the IEC 61850-6

As previously mentioned the SAS constitutes the interface between the substation components and the ACC (or RCC). The automation system's main objective is to allow ACC (or RCC) operators to modify the configuration of a substations, acting on the bay level, without having to specify sequences of low level commands; for instance the operator can cause the detachment of a power line by emitting a single command and let the automation system perform the necessary sequence of elementary steps. Moreover, knowing the topology of the substation and the circulating currents, the automation system is able to evaluate the feasibility of the operator's commands and, eventually, provide an error message to the operator. Another role of the substation automation system consists in recognising breakdowns or anomalies of the components of the substation. If during operation an apparatus assumes a state that is different from what was expected, the automation system sends an alarm message to the reference ACC (or RCC). Moreover the automation system supports the continuous monitoring of the substation by collecting data which allows to diagnose undesired behaviours.

The functions being performed by a Substation Automation System have been identified and thoroughly analyzed in IEC 61850-5 [IEC 61850-5 2003-07], and attributed to three logical levels:

- Process level functions
- Bay level functions
- Station level functions

At the process level (which is close to or even integrated into the switchgear) there are the functions interfacing the process i.e., basically binary and analogue I/O functions, such as data acquisition and issuing of commands. Process level functions are normally related to a single component that is connected to a single switchyard object. They provide the interface between the SAS and the switchgear.

Bay level functions use mainly the data related to one bay and act mainly on the primary equipment of one bay. A bay is a meaningful substructure of the primary substation, i.e., a set of closely connected subparts with some common functionality [IEC 61850-5 2003-07], which requires some local, autonomous functionality in the secondary system. The control of the switchgear in such a subpart has some common restrictions like mutual interlocking and well-defined operation sequences and bay level functions handle the related local automation aspects (for example line protection or bay control). Devices performing bay level functions are referred to with the generic terms “bay controller” and “bay protection”.

Station level functions refer to the substation as a whole. There are two classes of station level functions: process related and interface related station level functions.

Process related station level functions use the data of more than one bay or, eventually, of the complete substation and act on the primary equipment of more than one bay (or of the whole substation). Examples of process related station level functions can be station wide interlocking or bus-bar protection functions.

Interface related station level functions represent the interface of the SAS to the outside world i.e., the local station operator HMI, to a remote control centre TCI (Telecontrol Interface) or to the remote engineering workplace for monitoring and maintenance TMI (Telemonitoring Interface).

Station level devices comprehend for instance, the station computer, the operator’s workplace, and interfaces for remote communication.

The logical classification of the substation control functions is not necessarily reflected in the secondary system’s physical architecture: despite the similarity of the logical and physical levels there is a definite distinction between logical structure and physical implementation. The mapping between the two depends on a variety of factors like availability, performance and cost requirements and the allocation of logical functions to physical devices is not constrained. Process and bay level functions may be integrated into a single device without physical separation and bay level functions may be implemented without the need of a physical bay controller device. Station level functions may reside in a single station computer but may be completely distributed over bay level devices.

The free allocation of automation functions to devices in a distributed automation system has to be supported by an appropriate communication system.

A more conventional classification of the substation’s control functions is based on the task performed by the function. From this applicative point of view functions may be classified in the following categories:

- Process interface functions, used to interact with the process
- Operative functions consisting of monitoring and supervision functions (used to show the state of the process, inform about possibly critical events and archive data for later elaboration) and control functions used for normal day to day operation of the substation
- System configuration and maintenance functions
- System support functions:
    - Network management
    - Time synchronization
    - Physical device checking

A substation automation application combining protection, supervision & control, and monitoring capabilities relies on secure and fast communication and is a good representative for most dependability requirements in terms of system integrity, security and availability.

In particular, the following security aspects have to be considered:

- Authentication of message origin
- Protection against Denial of Service caused by "hostile" components in the Process Control Network
- User identification and authentication, access control, data protection, accountability and tracing to ensure data integrity and confidentiality

2.3 Distributed Generation and Microgrids

2.3.1 Introduction to Distributed Generation

Distributed Generation (also known as *embedded generation* or *dispersed generation*) is the deployment of small generators on medium voltage or low voltage distribution level, near to the consumers. The exact definition however is a point of debate in the power community [Ackermann *et al.* 2001][CIRED WG04 1999][Dondi *et al.* 2002][IEA 2002]. Some define DG in terms of generation capacity (e.g. < 100MW), while others simply look at DG in terms of connection (e.g. to the distribution grid); mostly however, some combination of these is used.

The increasing use of distributed generation radically changes the traditional hierarchical generation and transmission topology. A comparison between the traditional grid topology and the emerging topology, and the power flows in both topologies is made in Figure 2-15. In the traditional topology power flows exclusively in a single direction from the generation plants, via the transmission grid, to the loads in the distribution nets. In the emerging topology however, power flow may reverse within the radial distribution grids where DG is installed, and ultimately distribution grids may even inject power into the transmission grid.

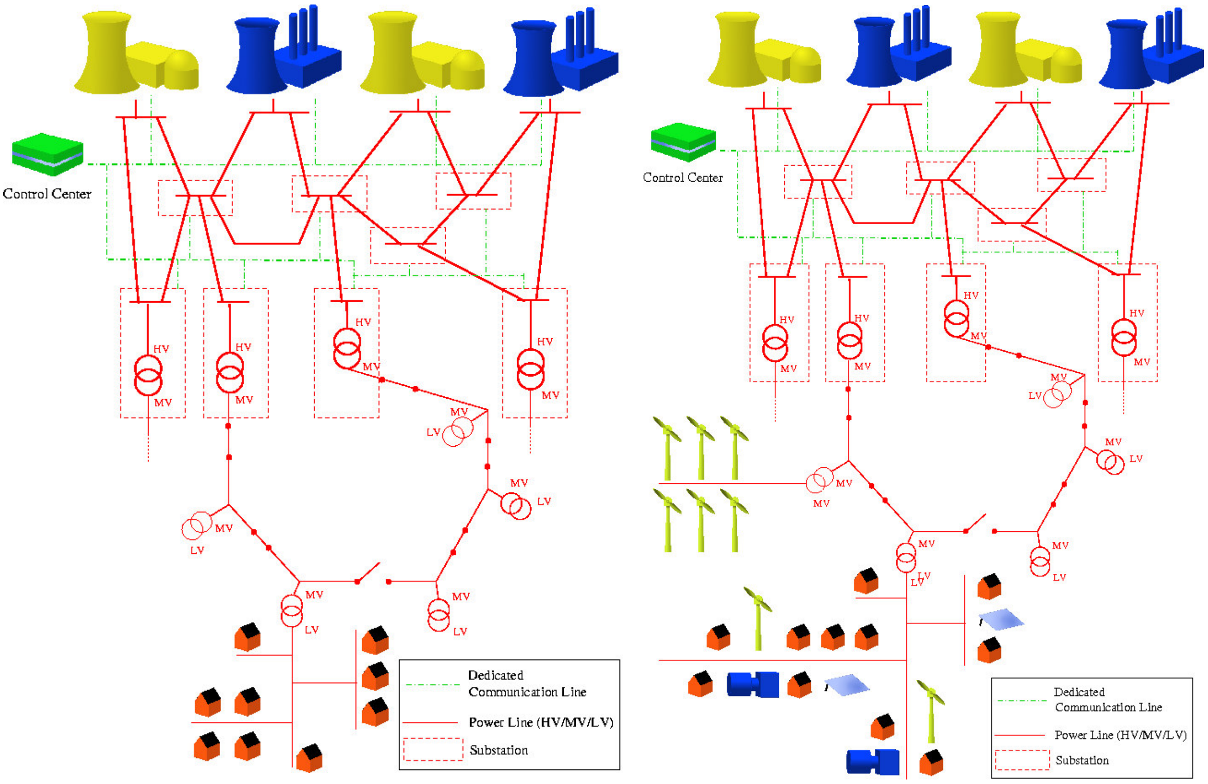


Figure 2-15: Traditional power grid layout vs. grid with distributed generation

Figure 2-16 depicts the portion of the EPS class diagram that is added to account for the presence of distributed generators in the Grid.

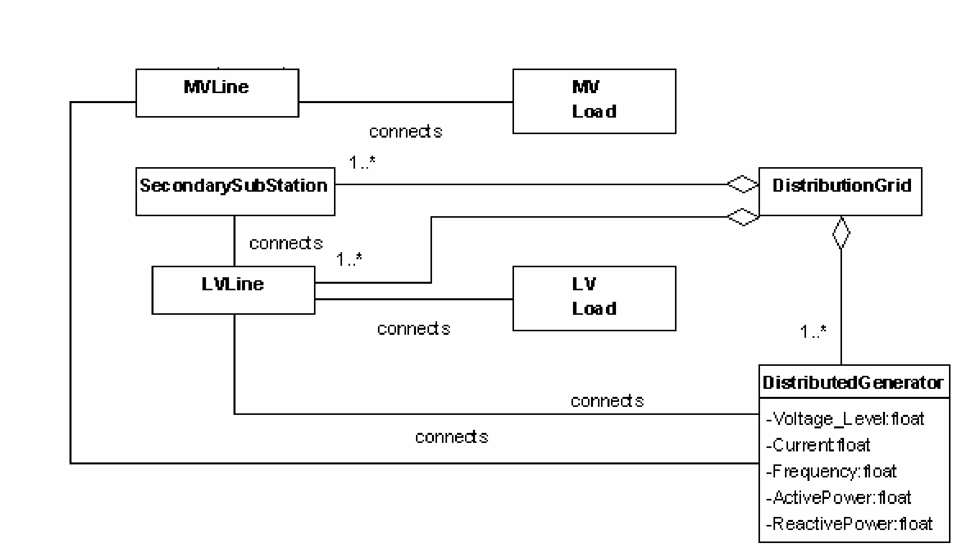


Figure 2-16: Class diagram of the distributed generation

2.3.1.1 Typical DG Technologies

Distributed generators are mainly devices that are used for harvesting renewable energy sources (wind, sun, biodiesel), improving energy efficiency (Combined Heat and Power or cogeneration or CHP), or providing some local services such as increasing availability of supply or providing peak power. The most notable examples of DG are presented next, some of which are already used extensively, while others are promising but still quite experimental.

- *Reciprocating engines* fuelled by diesel, oil, biodiesel for emergency services (e.g., UPS system) or gas (also for CHP).
- *Gas turbines* fuelled by gas used for CHP and peak power supply.
- *Microturbines* fuelled by gas, possibly with CHP (e.g., in house water boiler).
- *Fuel cells* fuelled by hydrogen, natural gas or methanol.
- *Photovoltaic cells* get their power directly from the sun. Renewable but unpredictable energy source. High price per kW installed power, only low power application.
- *Wind turbines* harvest wind power. Renewable but unpredictable energy source. Relatively expensive per kW installed power, but is starting to become profitable. Also large power applications, possibly combinations of multiple turbines in wind parks.

2.3.1.2 Reasons for DG Deployment

Of course, DG installations did not appear out of the blue. Recent years we have seen several incentives that lead to the increasing use of these technologies. We sum some of the most important reasons for the deployment of DG.

- *Liberalization of power markets* allow for small producers to enter the generation market without an all too big initial investment.
- Increased *environmental concerns* lead to the use of renewable energy sources, such as wind and solar power, which are intrinsically distributed power sources. CHP devices are also used as to improve the efficiency of primary energy resources.
- A good DG installation can *defer investments in the power grid infrastructure*, by for example giving voltage support near a large consumer or injection of power in a distribution grid with a nearly overloaded supply.
- Dispatchable DG units may provide several *ancillary services*, such as voltage support or provision of balancing reserves. These DG services can contribute to grid

stability. For this, however, the DG must be directly or indirectly controllable by some regulator, possibly the TSO or DSO.

- Bringing generation close to consumption may *decrease transmission losses*, if DG installation point are chosen properly. This has to be weighted however against the relatively lower energy efficiency of small generators in comparison to centralized large generation facilities (except for renewable sources and some CHP).
- A high degree of DG penetration may lead to the point where distribution grids are able to form *energy islands* or *microgrids* disconnected from the main grid in case of severe grid problems or blackouts. This kind of technology would of course increase local electrical security in terms of a higher grid reliability and availability. Yet many technical problems (automated frequency and voltage support, system inertia concerns, load shedding ability…) have to be overcome before these microgrids are operational in the real power grid.

2.3.1.3 Problems Concerning DG Installations

Next to the presented -sometimes theoretical- advantages, several problems come with the practical installation of distributed generators. The most notable, both economical and technical, are presented next.

- The *economic efficiency* of most DG systems is quite low, leading to a high cost per kWh produced, compared to large generation facilities. This is mainly due to economy of scale for power generation based on fossil fuels, or large capital investment and maintenance costs for renewable energy sources.
- *Availability of supply* may be endangered due to less fuel diversification, because most fuelled DG use gas, which increases the dependency of the power market on this single commodity.
- The influence a large amount of small scale distribution will have on *power system frequency and power system stability* is unknown. Especially when the TSO has no means of controlling DG output directly or indirectly.
- DG is seen as a means of postponing investments in distribution nets. Yet, injecting power in a distribution net may disturb local voltage levels seriously, especially when the grid is relatively weak. Many installations of DG lead nowadays to *extra investments* to reinforce the distribution grid, instead of postponing them.
- Distribution grid *protection systems* are based on a power flow in a single direction, which is not always true with large DG penetration. This may lead to both spurious tripping in case of short circuits in a nearby distribution grid and failure to trip in case of short circuits in the distribution grid itself. Protection systems have to be adjusted to allow large DG penetration in distribution grids.
- Most traditional generators have rotating elements, which have a considerable inertia. This inertia serves as a buffer when power consumption suddenly increases or decreases. The kinetic energy stored within these rotating masses will serve as an immediate power source when production is lower than consumption. This decreasing rotation speed and thus system frequency will be detected and production will be increased (primary control). Many DG are connected to the grid through power electronic converters, which have virtually no inertia. This means a power grid with lots of DG does not have this buffer (or a much smaller buffer) and could become unstable due to minor grid faults or unbalances.
- Unpredictable generation

2.3.2 Control of Distributed Generators

2.3.2.1 Traditional Control Paradigm Issues

The shift in the power generation topology also imposes a change in the control infrastructures of the distribution grid. The amount of small scale generators increases almost exponentially, where in the traditional system only a limited number of power plants and substations had to be accounted for. Centralized control becomes infeasible in the new scenario, due to the enormous processing power and high communication bandwidth requirements for the large amount of DG components. Also, the cost of using the dedicated communication lines for supervising and controlling these distributed generators would be way too high. Therefore, new solutions are needed.

Nowadays, most DGs are installed and controlled locally as passive elements, merely providing active power to the net, for which they receive a fixed price per generated kWh. When the transmission grid which they are connected to fails or large voltage dips occur these devices just disconnect themselves from the grid (possibly worsening the voltage dip even more, leading to cascading failures). However, DG could provide services to improve system service quality, reliability and availability. Extra functionality and flexibility in their control could make them able to function without a connection to a strong grid providing voltage and frequency stability, or let them ride through short voltage dips. Also, using power electronic equipment, most distributed generators can be used as VAr (reactive power) compensators for local voltage support.

2.3.2.2 Emerging Control Paradigms

More and more research in power grid control focuses on new control paradigms [Amin & Wollenberg 2005][Lund *et al.* 2006][Kato *et al.* 2005][Huang *et al.* 2002], to step away from the traditional centralized control paradigms to a more distributed supervisory control system. This applies especially to distributed generators, or more generally, distributed resources (which also incorporate manageable loads, such as air-conditioning or household devices like washing machines). Various schemes are proposed to manage distributed resources based on for example a power market connection [Tsikalakis *et al.* 2006][Kok *et al.* 2005].

These distributed control schemes are often based on the autonomy of a single user, who is trying to fulfil some goal, for example economical profit. This is probably the reason why the multi-agent paradigm is applied in many of these new control schemes [Dimeas & Hatziagryriou 2005][Vanthournout *et al.* 2005][Kok *et al.* 2005][Kato *et al.* 2005]. An agent is in fact an autonomous entity, possibly in software and/or hardware, which gets inputs from this environment and from other agents in the same environment, and acts on its environment as to pursue his own goals in the most optimal way.

The control system for distributed generators forming an *Autonomous Electricity Grid* (AEG) or *microgrid* which is studied in the CRUTIAL project is also based on this agent based paradigm, in which agents controlling DG output cooperate as to optimize voltage levels, frequency and production costs both during grid connected and islanded operation.

3 POWER SYSTEM MODEL AND DEFENCE PLAN

3.1 Modelling the operational states of the Power System

In order to allow a better understanding of the cascading effects in the Control System scenarios described in the following chapters, an operative states model of the Power System is provided [Fink & Carlsen 1978].

In this model a state is an operative asset of the Power System. It is characterised by attributes which are related to the following adequacy constraints:

- ***Equalities*** of the system (**E**): when the integrity of the system is respected:
    - *structure*: all the grid connected, without separate islands (an island represents a portion of a power system that is electrically separated from the main interconnected system);
    - *loads*: all loads are supplied (loads should not be confused with demand, which is the measure of power that a load receives or requires).

  Example of equalities are:
    - **P = Loads** (balance between Total Active Power and Total Active Loads)
    - **Q = Reactive Loads** (balance between Total Reactive Power and Total Reactive Loads)
- ***Inequalities*** of the system (**I**): the limits of some system variables must not exceed maximum and minimum levels representing the limitations of physical equipment:
    - ***Voltage***: all voltages ($\mathbf{V_{ni}}$ and $\mathbf{V_{gi}}$) in each grid node and eacg generator are within the controlled range,

      e.g., $\mathbf{350\ KV \leq V_{ni} \leq 450\ KV}$

      $\mathbf{0.9\ pu \leq V_{gi} \leq 1.1\ pu}$
    - ***Frequency***: unique grid frequency (**f**) is within the controlled range,

      e.g., $\mathbf{49.5\ Hz \leq f \leq 50.5\ Hz}$
    - ***Current***: all currents ($\mathbf{I_{lk}}$) in each connection line are within controlled range,

      e.g., $\mathbf{I_{lk} \leq 500\ A}$
    - ***Angle***: all generator angles (δ_i) are within the stability range,

      e.g., $\alpha \leq \delta_i \leq \beta$

Any adequacy constraint violation is represented with a not symbol (¬**E** or ¬**I**).

The **electrical security criterion N-1** means that, under all operating conditions, the loss of any given element (line, transformer, generation unit, compensation facility etc.) will not lead to abnormal operating constraints in adjoining operating zones (as results of limit values being exceeded for current, voltage, stability, etc.) and will not cause interruption in supply. Although under these conditions it will not be necessary to interrupt the grid operation as a result of the loss of one element, the structure of the system concerned will need to be reorganised in order to comply with the “N-1” criterion within the shortest possible time. In the intervening time, the loss of a further element might indeed jeopardise continuity of operation [UCTE Handbook].

According to the attribute values the Power System operative states are classified into five meta-level states [Fink & Carlsen 1978]:

- **NORMAL** (**E**, **I**): Situations in which all constraints are satisfied. All load requests are satisfied (Equality), there are no limits violations (Inequalities) and the electrical security criterion N-1 is satisfied. This state indicates that the generation is adequate to supply the current total load demand, and no equipment is being overloaded.
- **ALERT** (**E**, **I**): Situations in which all load requests are satisfied (Equality), there are no limits violations (Inequalities) but some electrical security criteria are not satisfied (Insecure) for instance the N-1 security criterion is not satisfied.
- **EMERGENCY** (**E**, ¬**I**): Situations in which all load requests are satisfied (Equality), but at least one limit is not satisfied (¬ Inequalities) (A-secure).
- **IN EXTREMIS** (¬**E**, ¬**I**): Situations in which not all load requests are satisfied (¬ Equality) and some limits are not satisfied (¬ Inequalities).
- **RESTORATIVE** (¬**E**, **I**): Situations in which after load shedding the restorative procedures are executed to re-satisfy the load requests (¬ Equality) and limits are satisfied (Inequalities). Formally this situation is a “Black-out” restoration.

The operating states are also classified on the basis of their accomplishment level:

- ***Secure***: if an electrical contingency happens in the *Normal State*, the system remains in this state. The reserve margins (for transmission as well as for generation) are sufficient to provide an adequate level of electrical security with respect to the stresses to which the system may be subjected. This attribute is verified statically.
- ***Insecure***: if the electrical security level falls below some thresholds of adequacy, or if the probability of disturbances increases, then the system enters in the *Alert State.* All constraints would still be satisfied, but existing reserve margins would be such that some disturbance could result in a violation of some inequality constraints (e.g. overloads). In this state, preventive actions can be taken to restore the system to the normal state.
- ***A-secure***: if a sufficiently severe disturbance takes place before preventive actions, the system enters the *Emergency State*. The system, however, would still be intact, and emergency control action (corrective) could be initiated in order to restore the system at least to the *Alert State.* If these measures are not taken in time, or are ineffective, and if the initial disturbance or a subsequent one is severe enough to overstress the system, the system then starts to disintegrate and move to the *In Extremis State*.

In the Figure 3-1 the finite-state diagram of the Power System is depicted.

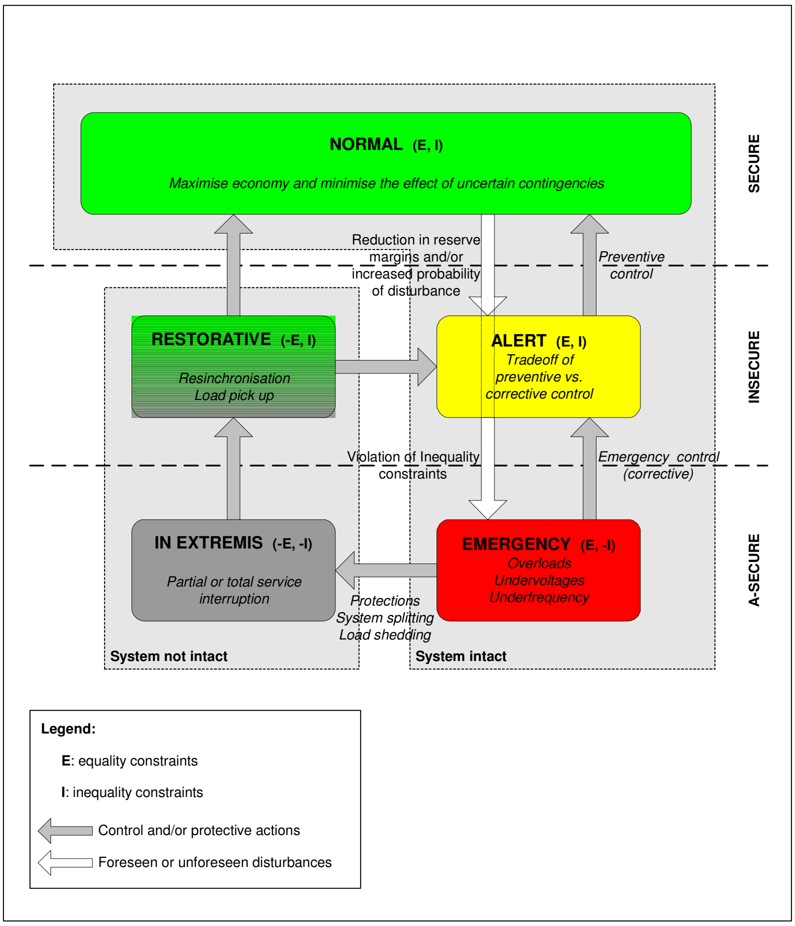

NORMAL (E, I)
Maximise economy and minimise the effect of uncertain contingencies
SECURE
Reduction in reserve margins and/or increased probability of disturbance
Preventive control
RESTORATIVE (-E, I)
Resinchronisation
Load pick up
ALERT (E, I)
Tradeoff of preventive vs. corrective control
INSECURE
Violation of Inequality constraints
Emergency control (corrective)
IN EXTREMIS (-E, -I)
Partial or total service interruption
EMERGENCY (E, -I)
Overloads
Undervoltages
Underfrequency
A-SECURE
Protections
System splitting
Load shedding
System not intact
System intact
Legend:
E: equality constraints
I: inequality constraints
Control and/or protective actions
Foreseen or unforeseen disturbances

Figure 3-1: Power System finite-state model [Fink & Carlsen 1978]

A **contingency** is the unexpected failure or outage of a system component, such as a generator, transmission line, circuit breaker, switch, or other electrical component. A contingency also may involve multiple components, which are related to situations leading to simultaneous component outages [UCTE Handbook].

A **disturbance** is an unplanned event that produces an abnormal system condition [UCTE Handbook].

The main electrical disturbances or contingencies could be summarized in:

- Unexpected increase of demand
- Tripping of large generation groups
- Transient or permanent overloads of lines or transformers
- Low dumped or unstable inter-area oscillation
- Low dumped or unstable electromechanical oscillation
- Instability or voltage collapse
- Important cascading (EHV) line tripping with consequent grid separation

One of the objectives of the identification of control system scenarios is the extension of such power system model by considering, in addition to power contingencies, also the possibility of ICT threats and control actions that may happen when the power system is in a normal state or during the management of a power contingency.

Such extension can exploit the state model proposed in [Laprie *et al.* 2006] also reported in Figure 3-2, Figure 3-3 and detailed in deliverable D3 produced in the contest of WP2 [Kaâniche *et al.* 2007].

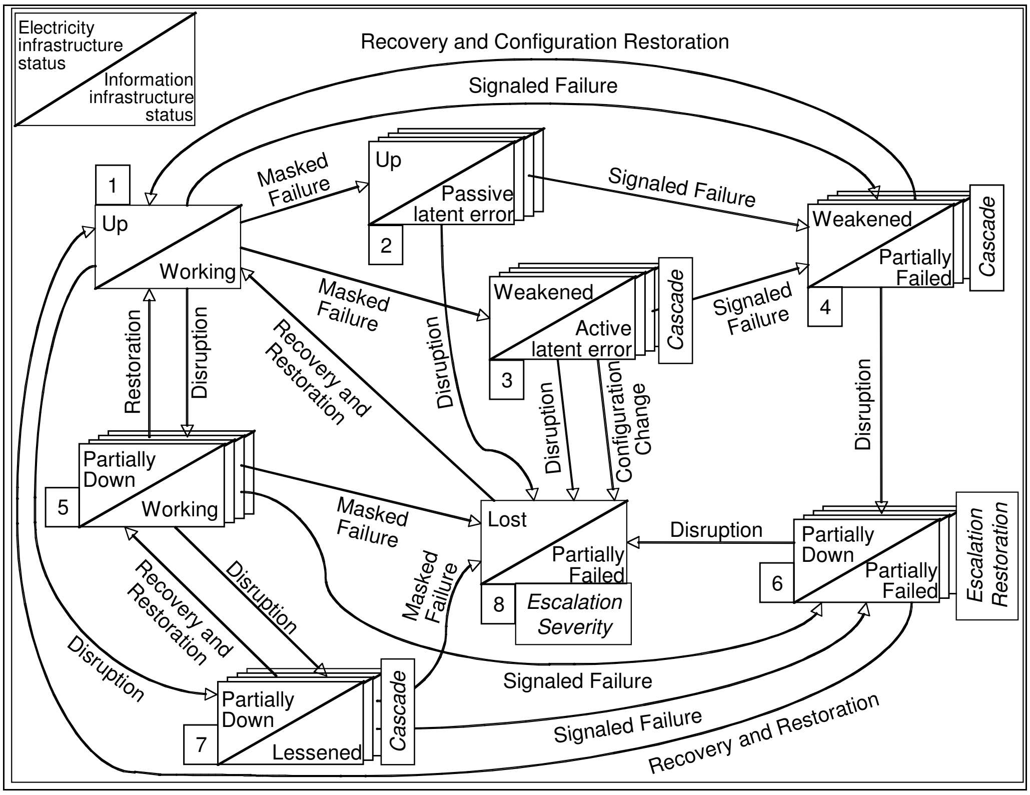


Figure 3-2: EPS State Model when considering accidental failures [Laprie *et al.* 2006]

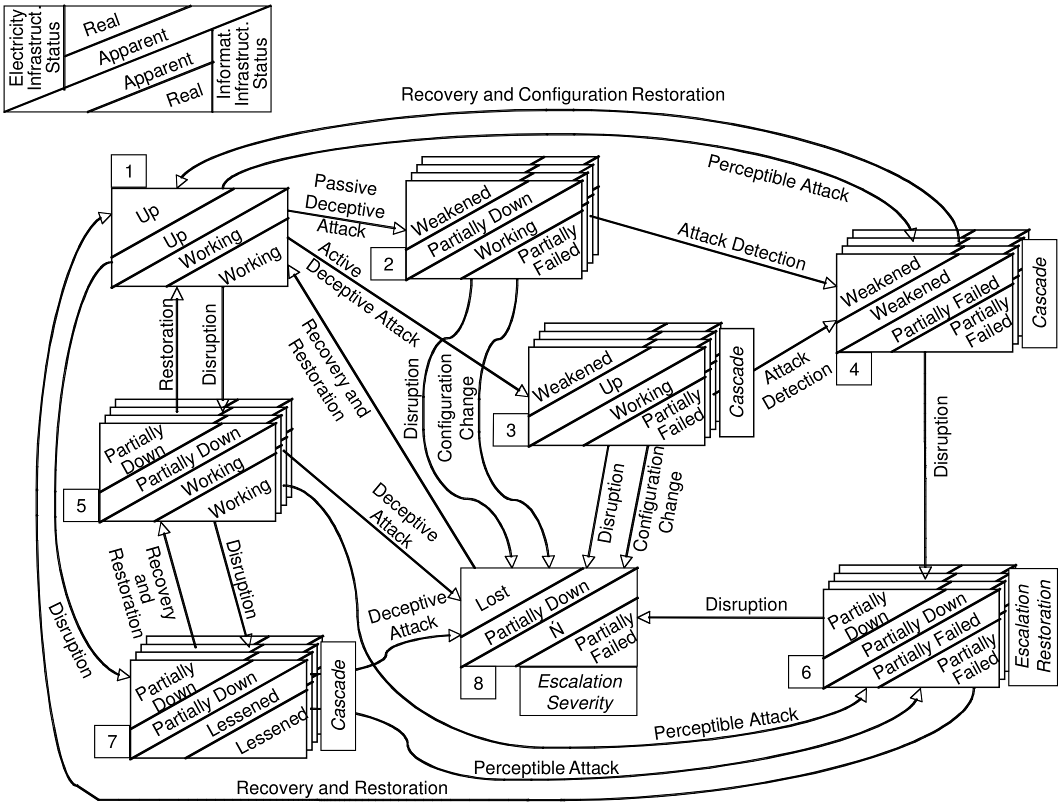


Figure 3-3: EPS State Model when considering malicious attacks [Laprie *et al.* 2006]

According to this model an a EPS state is an aggregate concept described in terms of EI and ICT characteristics. A global view of an aggregate EI/ICT state is given in Figure 3-4.

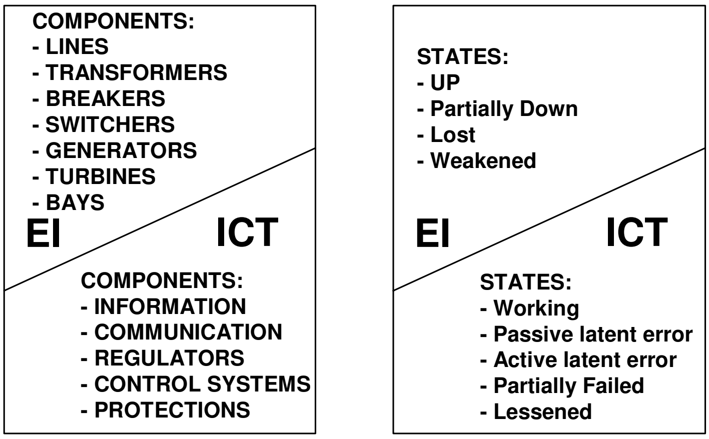


Figure 3-4: Detailed EPS State Model: a-components, b-states

The definitions of the states are as follows see Table 3-1:

EI states	ICT states
Up: Service ensured in normal condition	**Working**: ensure normal control of EI
Partially Down: Due to disruption, service in degraded conditions	**Passive latent error**: Part of ICT infrastructure is failed, which prevents monitoring of the electric infrastructure: disruptions may remain unnoticed
Lost: Service interruption, partial black-out	**Active latent error**: Part of ICT infrastructure is failed, that may lead to unnecessary, and unnoticed configuration changes
Weakened: Failure of ICT component influence the service	**Partially Failed**: Part of ICT infrastructure are knowingly failed
	Lessened: Part of ICT infrastructure can no longer implement their functions

Table 3-1: EPS State Definitions

This representation does not take into account explicitly the quantitative relationships of equality and inequality of EPS state model of Figure 3-1.

A possible mapping between the abstract model presented in [Kaâniche *et al.* 2006] and the detailed EPS model which takes in to account all the main Equalities and Inequalities is summarized in the following Figure 3-5.

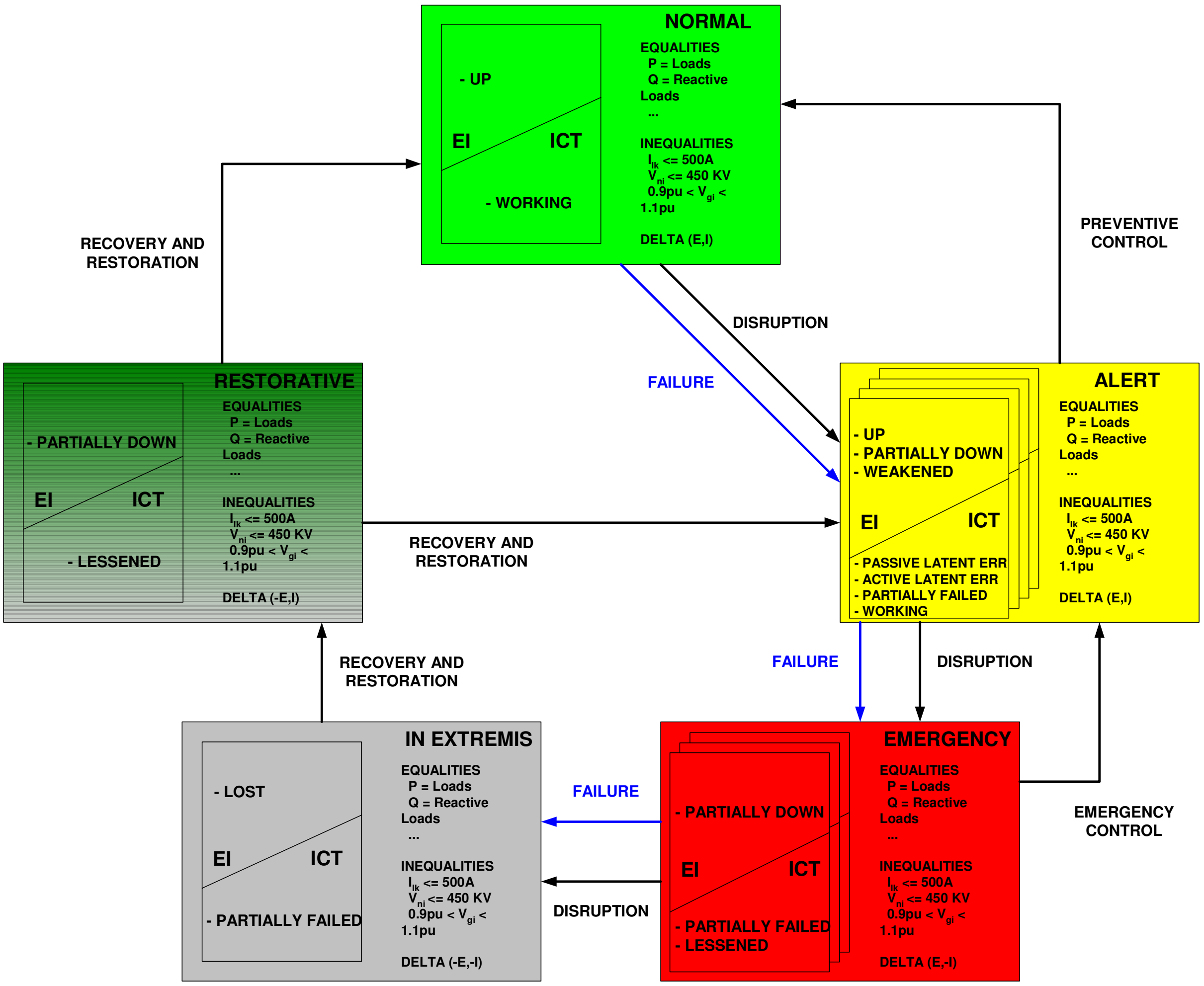


Figure 3-5: Extended EPS State Model

It may be noted that in the extended model each state is also characterised by Δ(E,I) which expresses a global electrical security margin one for each Equality/Inequality constraint.

In the propose mapping there are both alert and emergency states in which the EI assumes the Partially Down state value, i.e. the power service is degraded due to some disruptions. However, as the degradation is very different in the two cases taking in to account the composed states of the electricity and ICT infrastructures. Further investigations are needed to refine this model.

3.2 Defence plan and defence line concepts

A **defence plan** summarises all technical and organisational measures taken to prevent the propagation of incidents or the deterioration of a power system state of service in order to avoid a collapse of the Transmission Grid.

Hereafter a typical four level defence plan is shown. Its defence strategy is implemented using procedures, equipments and systems that are installed on the Transmission and Distribution grids.

- The *first line of defense* is made up of the regulation systems, which try to keep the Normal state of the Power System (electrical security criterion N-1) by voltage and frequency regulation systems and other control systems. 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.

- The *second line of defence* is represented by the protections which quickly exclude any grid element out of order (line, transformer, generation unit, compensation facility etc.).
- The *third line of defence* is performed by the systems that ensure the preventive and corrective control of the interconnected grid in order to avoid the grid separation. Among these systems there are the Anti-oscillations devices for line protection damper and the manual load shedding.
- The *fourth line of defence* acts in situation of islanding (system not intact or not interconnected). It is made by all the automatisms that guarantee the balance among demand and generation in the disconnected grid.

The systems used to implement the defence plan are called defence systems. They may be classified depending on the State of the Power Grid (see Figure 3-1):

- Defence Systems used when the Power System is intact, that is when the Power Grid is meshed:
  - Control of critical sections of the Grid
  - Generator trips through telecontrol commands
  - Automatic load shedding for minimum frequency
  - Automatic load shedding for minimum voltage
  - Manual load shedding
  - Manual set-point of tap changer transformer
  - Manual activation of shunt reactance
  - Anti-oscillation damper
- Used in case the Power System is not intact, that is when the Power Grid is in islanding
  - Under-frequency load shedding
  - Automatic Grid separator

Depending on the response time to the contingencies the defence systems may also be classified in:

- Based on automatic actions
  - Control of critical sections of Grid
  - Under-frequency load shedding
  - Automatic load shedding for minimum voltage
  - Generator trips through telecontrol commands
  - Anti-oscillation damper
  - Automatic Grid separation
- Based on manual actions
  - Manual activation of shunt reactance
  - Manual load shedding, of selected users
  - Emergency manual load shedding (distribution areas)
- Based on programmed actions
  - Manual set-point of tap changer transformer (ULTC)

- Planned load shedding

The direct measures for emergency conditions are based on a certain extent on the philosophy that in the event of major disruption (short-term and where possible) selective restrictions in the energy supply (load shedding) are more acceptable than the consequences of an extended grid breakdown resulting in a power cut lasting for several hours [UCTE Handbook].

When the situation reaches the island operation state (disconnection of part of the grid) the procedure is [UCTE Report 2003]:

- Stopping the pumps (reserve hydroelectric generation)
- Shedding part of the load (corresponding with the balance of lost import) on medium voltage level
- Keeping all running generation capacity in service.

In the following sections we will enter into details about defence systems belonging to levels one and three.

3.3 The main regulations of the Electrical Power System

The electrical power system needs a lot of different regulations and control systems. The main regulated variables are frequency, voltage, reactive and active power, etc.. These systems act in all the possible operation conditions that the process under control must cope with.

The main controls used in the electrical system are briefly described hereafter.

3.3.1 The primary and secondary frequency regulations

The primary frequency regulation has the goal to regulate the frequency of the single generators. The secondary frequency regulation has the goal to regulate the frequency of the transmission grid.

3.3.1.1 The primary frequency regulation

The general scheme of the primary frequency regulation of a thermal plant is shown in Figure 3-6, in which different types of turbines are represented, namely:

- **LP** low pressure turbine
- **MP** medium pressure turbine
- **HP** high pressure turbine

with the other fundamental apparatus of a thermal power unit, that is the condenser, the feed pump, the evaporator, the SH Super-Heater and the RH Re-Heater.

The mechanical power supplied by all the turbines to the generator shaft gives energy to the alternator, which in turn transforms the mechanical energy in electrical energy to be sent to the transmission grid.

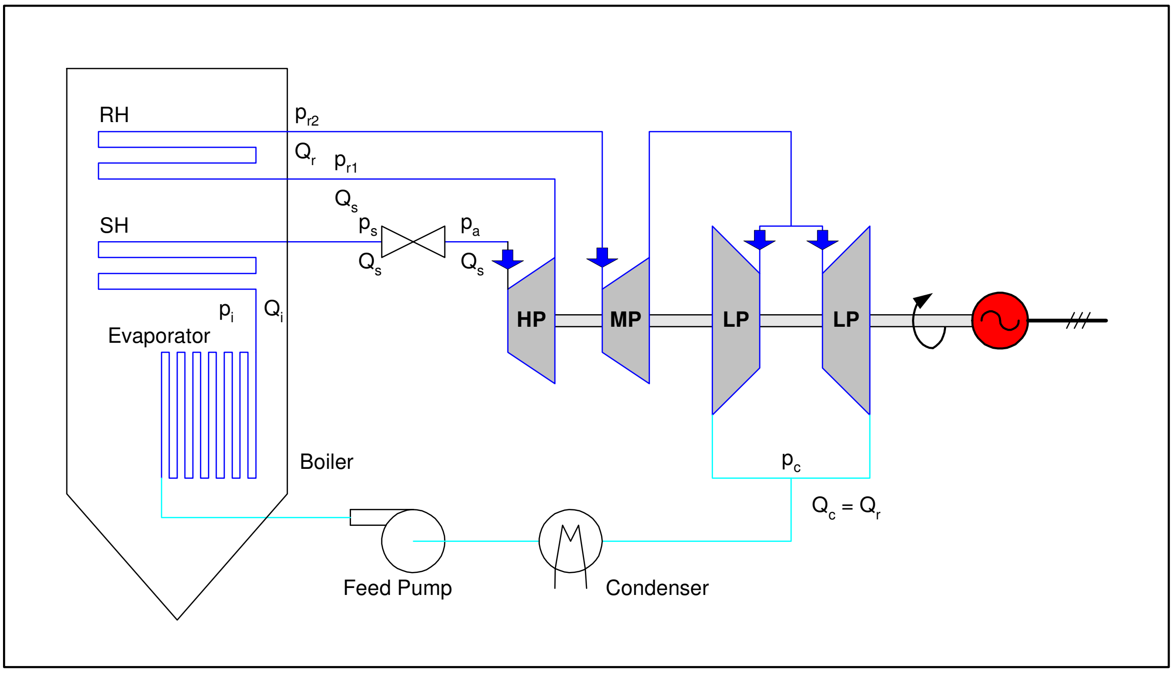


Figure 3-6: Frequency-power regulation of a steam thermal plant

The following symbols have been adopted for the various quantities of Figure 3-6:

p_i = internal pressure of the boiler

Q_i = mass steam flow at the input of super-heater (SH)

p_s = pressure at the regulation valve

Q_s = steam flow in the HP high pressure body of the turbine

p_a = pressure downstream of the regulation valve (input of the first HP stage)

p_{r1} = pressure at the input of the re-heater (RH)

p_{r2} = pressure at the output of the RH

Q_r = steam flow at the output of RH

p_c = pressure at the output of the turbine and input of condenser

Q_c = steam flow at the output of the turbine

In Figure 3-7 there is a schematisation of primary frequency regulation in closed loop; in this diagram, the meaning of the variables is:

f_{ref} = frequency of reference

f = frequency of the group

P_m = total mechanical power

P_e = electrical power

ε_f = frequency error

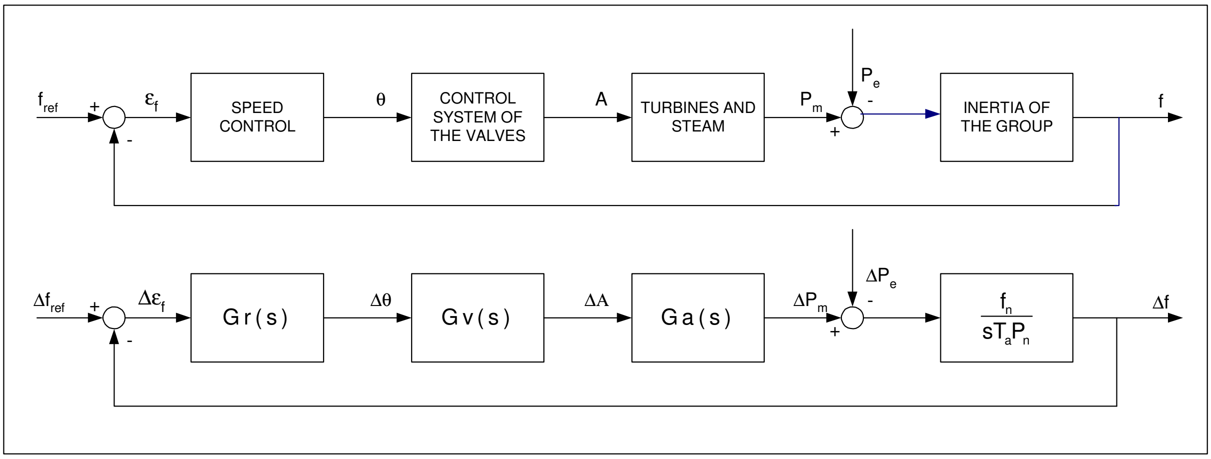


Figure 3-7: Schematisation of the primary frequency closed loop control and its linearization

The second scheme shown in Figure 3-7 represents the linearization of the controlled system. Here each block represent a linear transfer function and the variables are the variations in respect to the values around which the linearization was made.

3.3.1.2 The secondary frequency regulations

The secondary frequency regulation has the goal to control the frequency of an interconnected power system. In Europe the national power systems are coordinated by the UCTE. This coordination is obtained keeping the exchanges of energy among neighbouring countries to prefixed values.

Each member of UCTE 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, as shown in Figure 3-8, is subdivided in one actual control area and other two virtual areas, which are organised inside a decentralised adaptive scheme. This solution allows to employ 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.

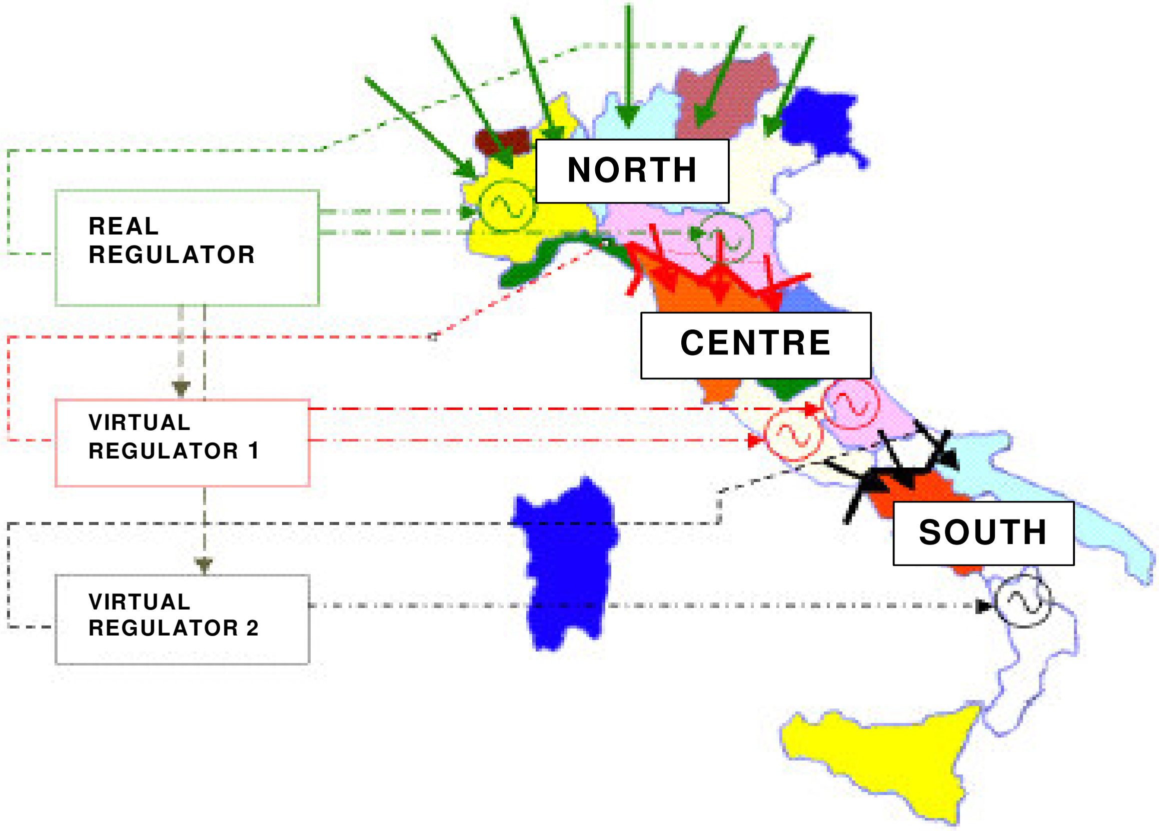


Figure 3-8: General scheme of the secondary frequency regulation

The secondary frequency control has been implemented by a secondary frequency regulator (called network regulator in the Figure 3-9), which decides the reference frequency value (f_{ref}) to be sent to all the primary frequency controllers of those generators under the secondary frequency regulation. This is done in order to guarantee a right division of the load among the generators. This function which is described in the Figure 3-9 through the primary frequency regulators, changes the mechanical power for each generator in order to guarantee a good value of the grid frequency. In the Figure 3-9 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 submitted to this secondary frequency regulation. 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.

The secondary regulator is installed in a (national or regional) control centre.

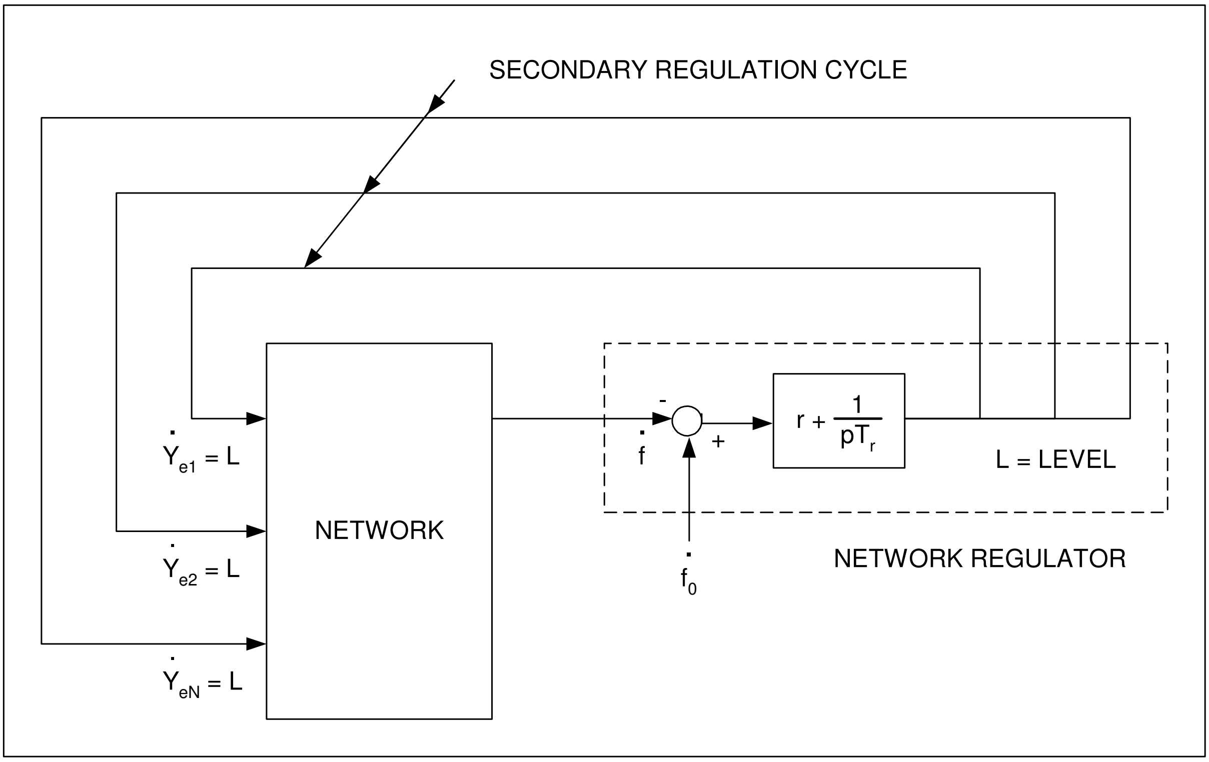


Figure 3-9: The secondary frequency regulation system

3.3.2 The hierarchical voltage regulation system for a national transmission grid

The electrical power supply grid is a complex structure of significant strategic importance to modern society. To meet the quality of supply and voltage regulation objectives a hierarchical control structure has been developed and this is shortly presented hereafter.

Three voltage control levels: primary, secondary and tertiary are used to regulate voltages of the transmission grid in order to supply to the customers (privates, publics institutions and companies) a voltage with good quality without interruptions.

Figure 3-10 shows the Use Case diagram (UC) of the Voltage regulation system. The diagram emphasizes the different players and how secondary and tertiary control requires communication, while the primary control is local and does not require communication.

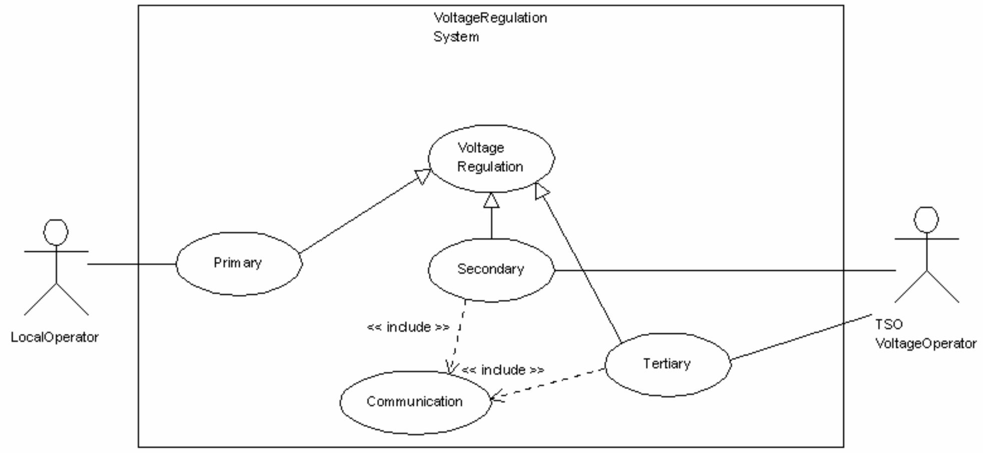


Figure 3-10: The Use Case Diagram of the Voltage regulation system

This hierarchical control system is widespread along the nation, with the different components placed in different facilities: the power stations, the regional control centres and the national one.

The global idea of the hierarchical control system is shown in Figure 3-11, in which the main components are the following:

- **AVR** – it is the Automatic Voltage Regulator which has the goal to make the primary voltage control, at the level of the single generator
- **PQR** – it is the reactive Power (Q) Regulator of a single power plant, and it is 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 which are the voltages to be achieved for each controlled node of the grid.

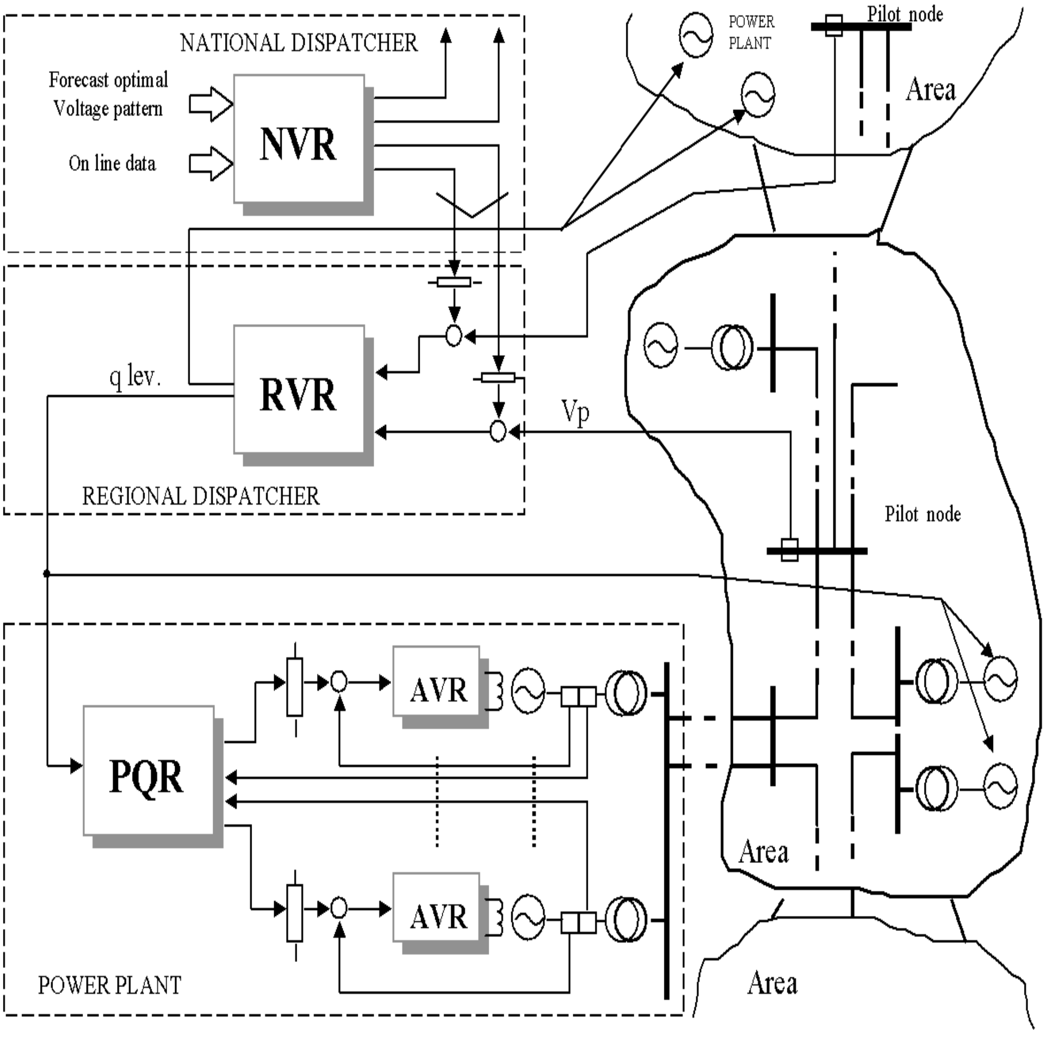


Figure 3-11: The scheme of the hierarchical voltages control of a National Transmission Grid

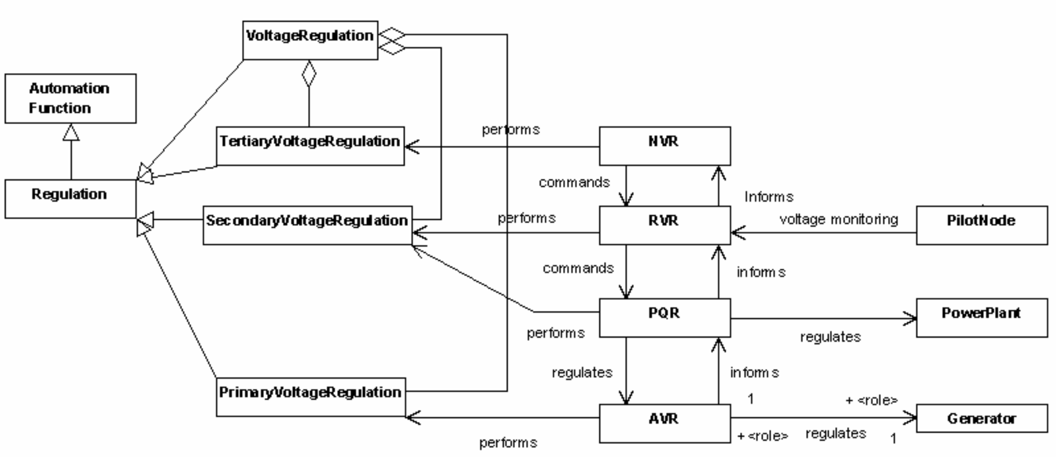


Figure 3-12 Class Diagram of the elements involved in the Voltage Regulation

Figure 3-12 depicts the CD of the elements involved in the Voltage Regulation, making explicit the links between the elements of the Power Generation and the Power Grid (Pilot Node, Power Plant and Generator) and the voltage regulation automation function. 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 the appendix Figure 8-12.

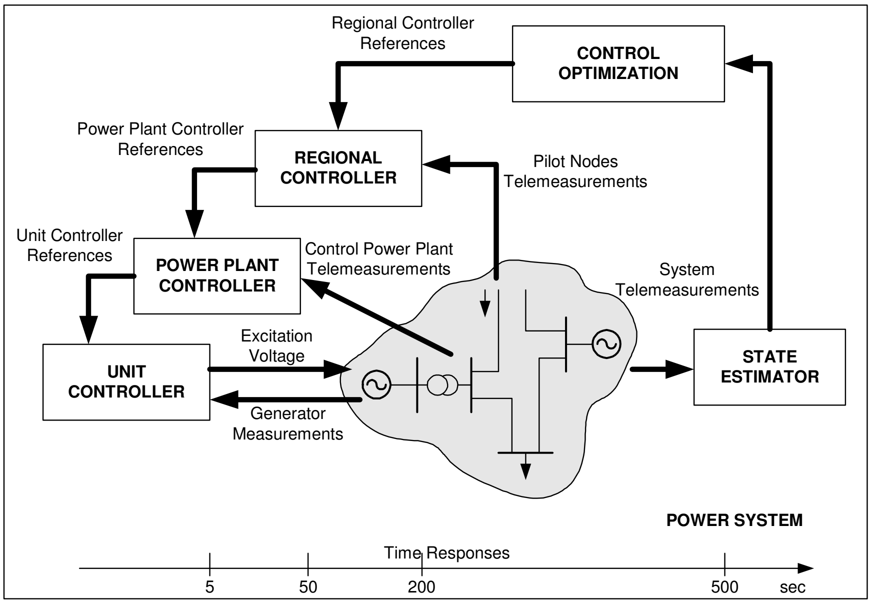


Figure 3-13: Summary diagram regarding the time responses and the flows of measurements for voltage regulations

A different schematisation of the voltage control is shown in Figure 3-13, in which the following important aspects of the voltage regulations are outlined.

First of all the time responses of the entire closed loop system are:

- 2-5 seconds for the AVR (UNIT CONTROLLER in figure) placed in the power plant one for each generator
- 20-50 seconds for PQR (POWER PLANT CONTROLLER in figure)
- 100-200 seconds for the RVR (REGIONAL CONTROLLER in figure) 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.

In the Figure 3-13 the word *References* indicates voltage references or reactive power reference values determined by the upper level regulator and sent, as reference, to the lower level regulators. The reference received by a regulator is the value which must be satisfied through the regulation.

The *State Estimator* indicates an algorithm used to compute the estimation of the state of the transmission power system that is necessary for the optimisation algorithm in order to determine the optimal voltage patterns.

After the overview of the hierarchical voltage control structure, in the following each single level of the voltage control system will be detailed.

3.3.2.1 The primary voltage control

The primary voltage control regards the voltage of the single alternator and it is realised by the AVR, the Automatic Voltage Regulator, whose control loop is shown in Figure 3-14.

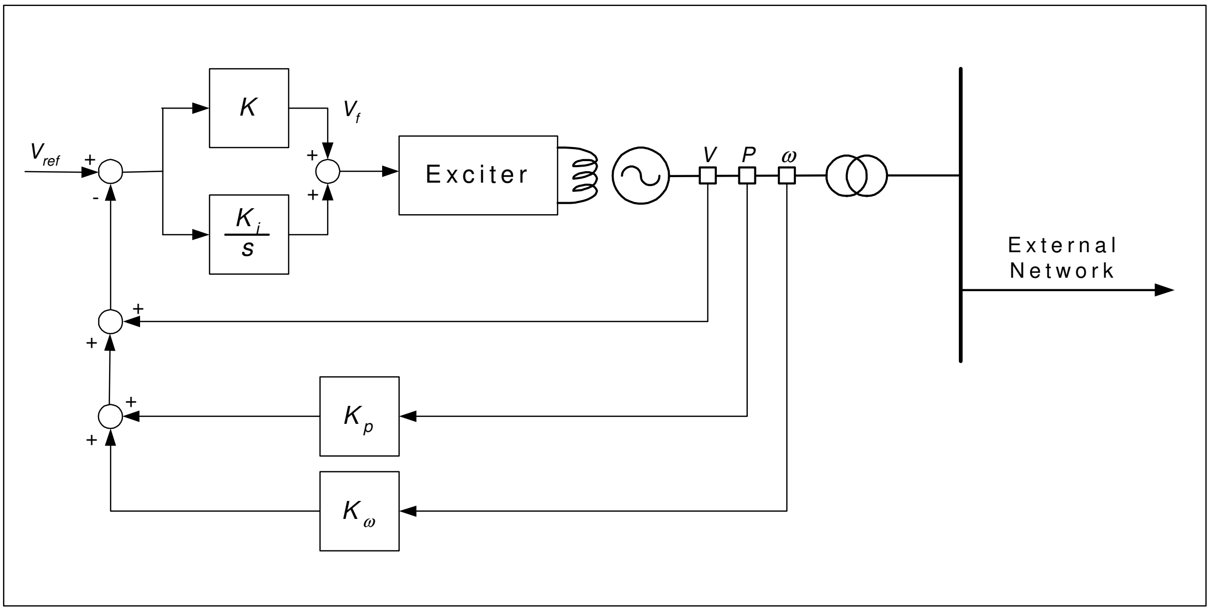


Figure 3-14: Classical AVR Controller

The following remarks must be underlined:

- The lowest and possibly the most critical level of the hierarchical voltage control of the transmission grid is the excitation control of a single alternator unit
- The main voltage loop includes a **PI** controller (that is a Proportional and Integral controller which plays two actions on the control signal, just a proportional one and an integral one) and provides a zero-steady-state-error tracking of the reference voltage
- The so called ***P**ower **S**ystem **S**tabiliser*, with the acronym **PSS,** is constituted by the *additional stabilising - feedbacks* from the variables*:* ***P*** the active power and ***ω*** the angular speed, with respective gains $\boldsymbol{K_p}$ and $\boldsymbol{K_\omega}$**.** It is used to improve the stability of the alternator-grid system
- In conclusion the complete voltage controller of a generator is a **MISO** regulator, that is a **M**ulti - **I**nput **S**ingle **O**utput controller

The Figure 3-14 outlines the main voltage loop and the additional feedback (the PSS), from active power $\mathbf{P_e}$ and rotor speed **ω** , because they are essential to guarantee the stability of the generator connected to the grid for different operation points, in presence of disturbances of different nature. Here, the terminal voltage V of a (large) power generating alternator is controlled via the strength of the magnetic field of the alternator, which is determined by the excitation voltage V_f of the exciter, that is the input variable to control the alternator.

It is also necessary, independently of the type of power plant, to introduce the limits of the capability curve with the maximum and minimum value of the active and reactive power produced and absorbed (for the capability curves defining the operation area for the generator see the Figure 3-15).

The voltage regulations of the generator verify if the generators are violating the reactive limits and if the option of the generated reactive power control is active. The values of the capability curve can be automatically modified depending on the state of each generator with the following relations:

1. **Overexcited** generator:

   for $0 \le P_G \le P = (P^2_{APP} - Q^2_{MAX})^{1/2}$ results $Q_G \le Q_{G\,MAX}$

   for $(P^2_{APP} - Q^2_{MAX})^{1/2} \le P_G \le P_{MAX}$ results $Q_G \le (P^2_{APP} - P^2_G)^{1/2}$

2. **Under-excited** generator:

   for $0 \le P_G \le P_{MAX}$ results $Q_G \ge Q_{MIN}$

where:

P_G : generated active power

Q_G : generated reactive power

P_{APP} : generator rated power

P_{MAX} , Q_{MAX} : generator maximum active and reactive power (capability curve limits)

P_{MIN} , Q_{MIN} : generator minimum active and reactive power (capability curve limits)

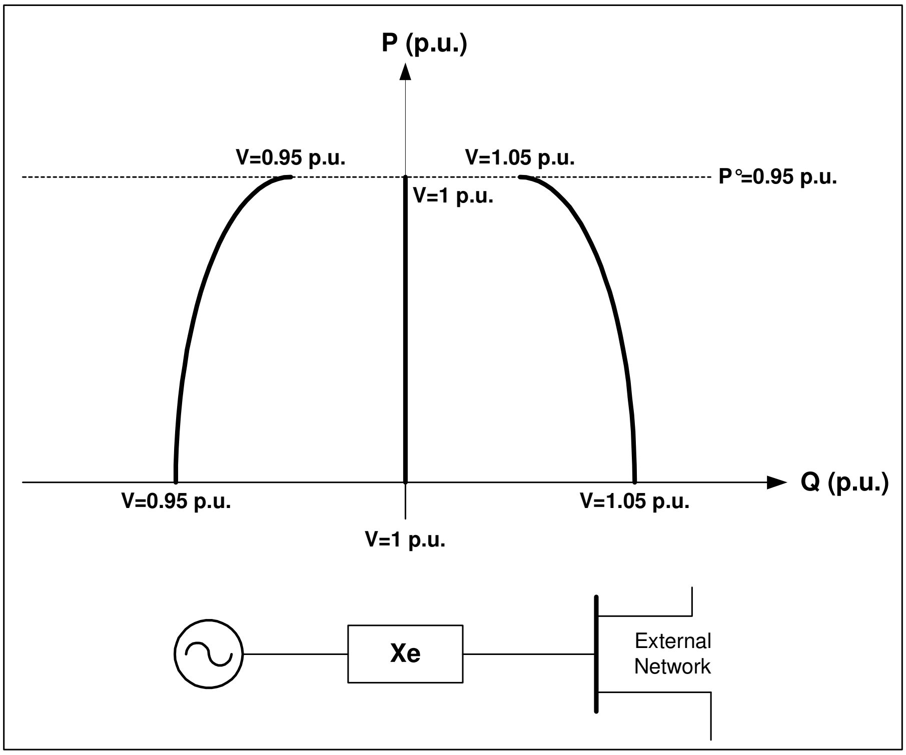


Figure 3-15: Machine operating range in parallel with the grid

The alternator operating conditions change during normal operation, for example from day to night and vice versa, due to various reasons, for instance:

- The external reactance Xe varies with the configuration of the grid and with the location of the power station, normally its value can change between 0.1 p.u. and 0.4 p.u.
- The active power P, generated by the alternator can vary between 0.9 p.u. and 0.3 p.u. (technical minimum)
- The reactive power Q, generated can change from -0.35 p.u. in under-excitation to +0.4 p.u. in over-excitation
- The voltage V, of the alternator is normally limited between 0.95 p.u. in under-excitation and 1.05 p.u. in over-excitation

All these different operation points of the electrical generator are easily recognised in the P,Q planes of the Figure 3-15. As a result of these changes in the operating conditions the system can become unstable or with a very low stability margin, so it rises the need for adaptation to guarantee stability. At present this adaptive solution is put to the test through prototypes and it will probably represent the future development in voltage regulation of the alternator, especially taking into account the liberalisation of the electric market which pushes forward operation conditions varying very quickly and frequently.

Nowadays the AVR regulator is an intelligent component with 1 or 2 CPU, a man machine interface, a LAN, etc. The human machine interface is used to set-up the regulator, to tune the parameters, etc. It is very fast and so it is not possible for the operator to interact with it to change the actions or operate to re-define the set up or the parameters. Just to give a clear idea of the time constants of this controlled system it may be considered that a response to a step variation of the voltage reference takes around 2-5 seconds and no more than 10 seconds.

3.3.2.2 The secondary voltage control

The secondary voltage control level of a transmission grid is constituted by two different kinds of regulators as shown, in a schematic way, in the Figure 3-16:

- The PQR - the Reactive power regulator - is placed in those power plants which were chosen to regulate the voltage in some defined nodes (called PILOT NODES) of the transmission grid. The PQR receives the reference value of reactive power from the RVR, the Regional Voltage Regulator, and on the basis of this consignment the PQR controls the reactive power produced by each generator
- The RVR - Regional Voltage Regulator - has the goal to define the reference values of reactive powers necessary to satisfy the constraints of PILOT NODE voltage levels. These reference values are sent to the PQRs of the power plants which are under secondary voltage control.

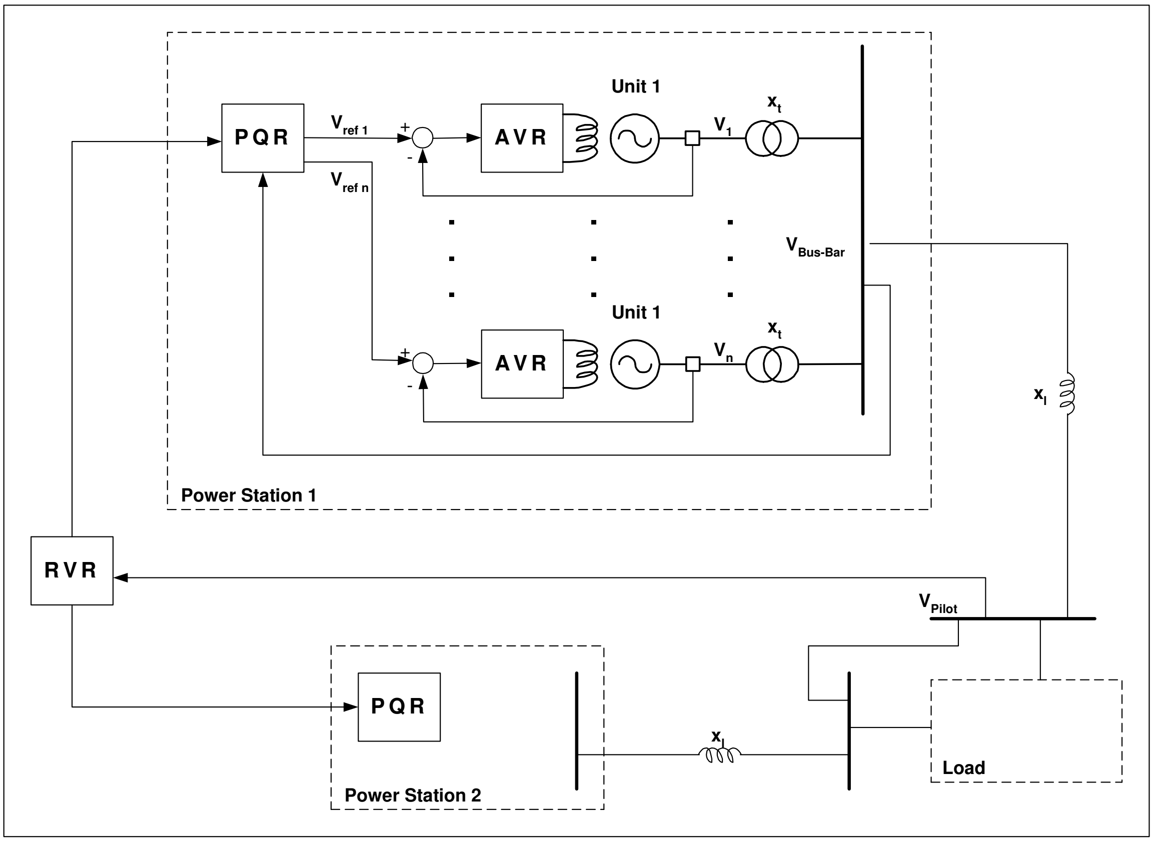


Figure 3-16: The Secondary Hierarchical Voltage Control Structure

3.3.2.3 The tertiary voltage control

The highest level in the hierarchical voltage control is the TERTIARY or NATIONAL level that has the goal to optimise the values of the voltages in the pilot nodes of the entire National grid in order to minimise the losses of energy along the transmission grid. Of course this hierarchical voltage control system that is widespread along all the national territory is quite important for the management of the system.

In Figure 3-17 there is the general schematisation of the centralised tertiary voltage control system. The regulator in charge of this regulation is the NVR (National Voltage Regulator).

In order to define the optimal voltages profiles of the pilot nodes with the objective to minimise the losses on the transmission grid, the National Voltage Regulator uses different algorithms such as a state estimator, an optimisation algorithm, etc.

This regulator has a rich man machine interface through which the operator is able to monitor the evolution of the grid and to make some actions to counteract dangerous situations with possible fatal failures.

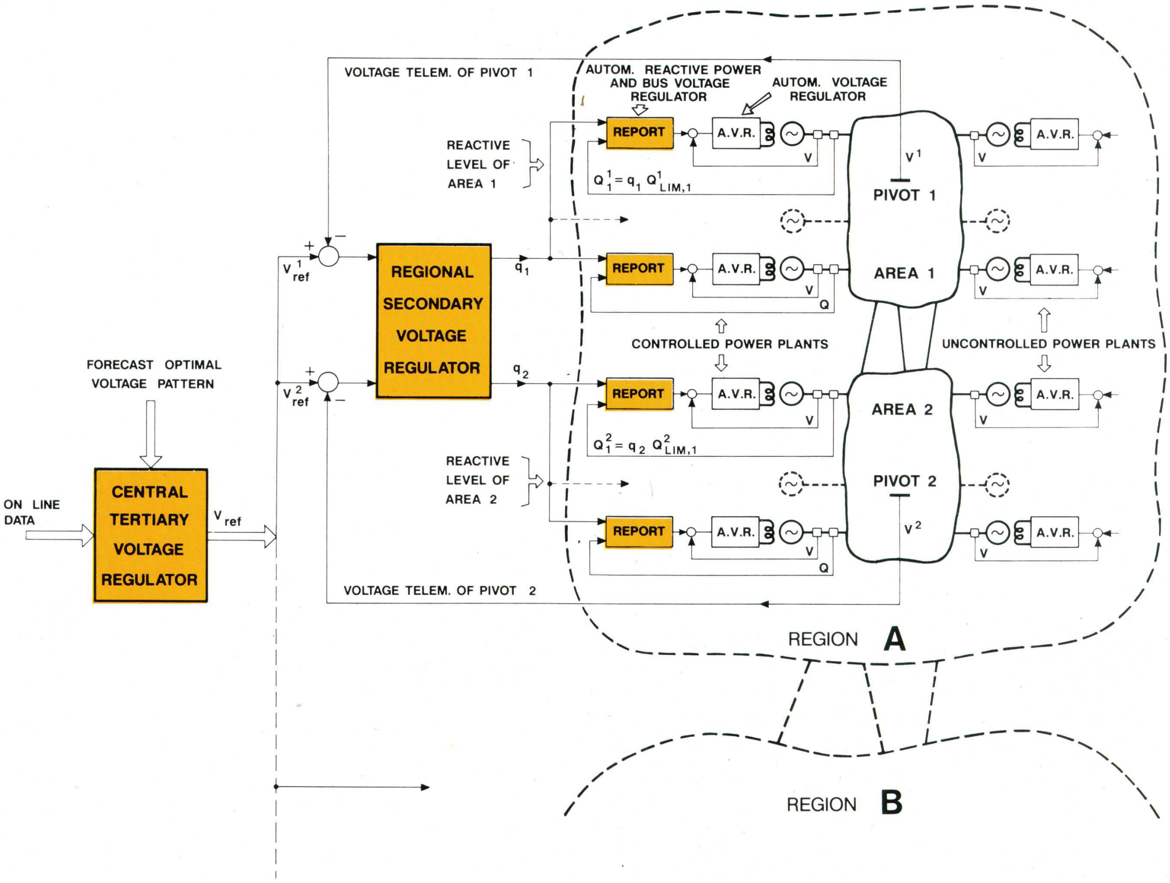

VOLTAGE TELEM. OF PIVOT 1
AUTOM. REACTIVE POWER AND BUS VOLTAGE REGULATOR
AUTOM. VOLTAGE REGULATOR
REACTIVE LEVEL OF AREA 1
REPORT
A.V.R.
V
V1
PIVOT 1
Q11 = q1 Q1LIM,1
AREA 1
Q
+
−
V1ref
REGIONAL SECONDARY VOLTAGE REGULATOR
q1
q2
V2ref
CONTROLLED POWER PLANTS
UNCONTROLLED POWER PLANTS
FORECAST OPTIMAL VOLTAGE PATTERN
AREA 2
Q21 = q2 Q2LIM,1
REACTIVE LEVEL OF AREA 2
PIVOT 2
V2
ON LINE DATA
CENTRAL TERTIARY VOLTAGE REGULATOR
Vref
VOLTAGE TELEM. OF PIVOT 2
REGION A
REGION B

Figure 3-17: The general schematisation of the hierarchical voltage control system

3.3.2.4 The system improvements achieved by the hierarchical control

The global voltage control system allows to achieve the following main improvements:

a. VOLTAGE QUALITY

- Improved voltage profiles across the whole electrical power system
- Reduced voltage variations around the decided values (set-points)
- Bus-bar voltages maintained inside the limits

b. ECONOMIC OPERATION

- Reduction of the total power system losses
- Minimization of reactive power flows through a better utilization of the reactive power resources, available at each generators under secondary voltage control

c. ELECTRICAL SECURITY

- The generators reactive power reserves made available for emergency conditions
- Increased active electric power transfer capability
- Voltage collapse prevention

3.3.2.5 The implementation of the hierarchical voltage control system in the Italian transmission grid

The implementation of the hierarchical voltage control in the Italian transmission grid is ongoing since at least ten years. Its huge structure is widespread in the whole country and it is represented in Figure 3-18.

The approximate numbers of components needed for its implementation are the following :

- Over 200 AVR - Automatic Voltage Regulators
- 70 PQR - Reactive Power Regulators
- 3 RVR - Regional Voltage Regulators
- 1 NVR - National Voltage Regulator

Of these components those already installed are:

- 50 PQR apparatus already activated and under operation
- 2 RVR Regional Dispatchers already activated and under operation in North and South of Italy
- The NVR for the National Control Centre is under operation and some updates are ongoing.

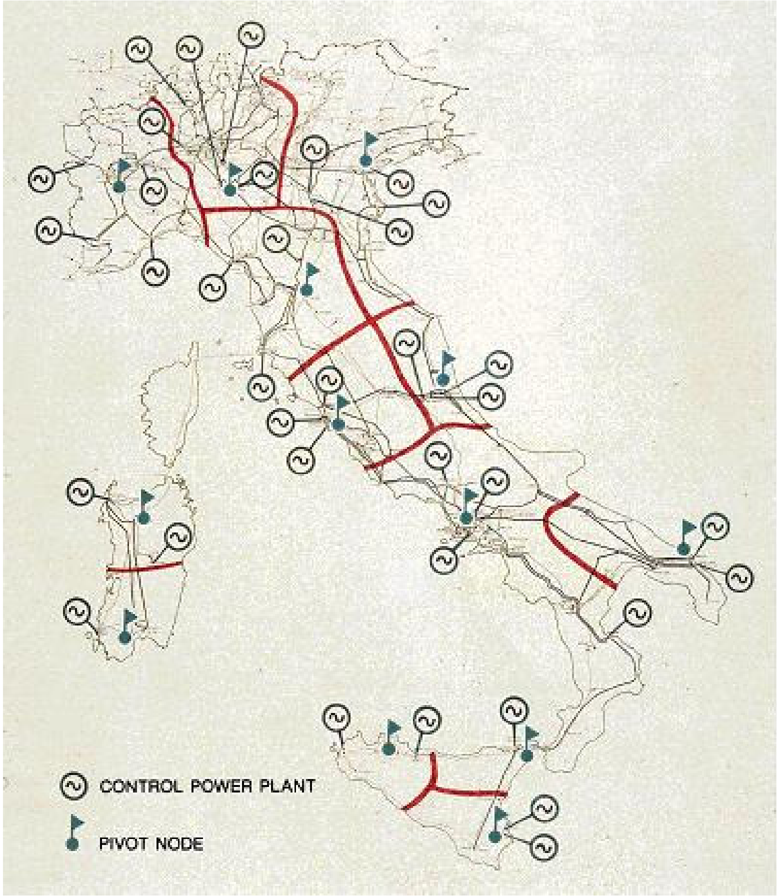


Figure 3-18: General schematisation of the Italian hierarchical voltage control system

3.4 Multi Agent Microgrid Control Systems

In this section the multi agent DG control system which is studied in the course of the CRUTIAL project is introduced. We focus on its design motivations, the physical level, the middleware level binding together a virtual agent community and the different control loops implemented by this multi agent system with different functionalities and criticality levels.

3.4.1 Control System Objectives

While designing a control strategy for Distributed Generators in a distribution net, one has to envision some important goals. First of all the control system has to be *robust*, since we are controlling physical generators injecting power into the power grid. Failures of the control system leading to a failure of the generator or even failures of a power distribution segment are mostly unwanted. Secondly, the capital investment cost and the operational cost of the control system has to be kept as low as possible, since it controls relatively small generators with relatively low financial gains.

Because of the cost limitations a fully distributed system, which does not need a centralized supervision and control system, is used. This distributed architecture has the advantage that no expensive servers and backup servers with large bandwidth requirements are needed. Also, no trusted third party is needed to provide and maintain this centralized infrastructure. The local generator controllers are designed as agents, which receive inputs from the generator (power output, voltage, frequency, production cost) and communicate with other agents in the system to optimize their behaviour. Based on the cost argument, the communication infrastructure used among agents is an open IP-network, possibly a public one such as the Internet. The Internet has the advantage that it is generally accessible and relatively cheap. A large disadvantage is the reliability of the Internet since one depends on an unknown underlying communication infrastructure and third party network providers. Also, the Internet has unpredictable communication delays and may suffer from IP-packet losses. Since the Internet is a publicly available communication infrastructure, it also may come with some security issues.

Following previous discussion, we can conclude that the agents must not rely on the communication channel for their operation. Therefore, communications are used for optimization purposes only. The control loops using communications are soft real-time (because of unpredictable network delays), and the agents are able to function in the absence of communications, be it in a less optimal way.

3.4.2 Agent Communication

The agents in the control system need some kind of middleware system which binds the agent population together. They need a way of finding other interesting agents and fixed protocols for communication and interaction among participating agents. The middleware for agent interaction presented here is designed to function in the absence of centralized coordination; it must cope with dynamic behaviour of agents and the unreliable underlying IP-network. This section presents both the use of overlay networks within this system and the communications patterns among the agents.

3.4.2.1 Structure of the Overlay Network

Agents in a power distribution net set up an overlay network (or virtual network) on an underlying network, forming peer-to-peer (P2P) connections between agents (comparable to systems such as Gnutella or Napster[1]) [Vanthournout *et al.* 2004b][Vanthournout *et al.* 2004a]. In such an overlay network, an agent has the address of a number of other agents in the network, called the neighbours of that agent. If these neighbours are chosen with a proper degree of randomness, a network will be formed where a path exist between every

[1] Although Napster is generally not seen as a pure distributed peer-to-peer system because of the centralized listing of nodes and indexing of resources (music files) on these nodes.

two agents in the system. The amount of agents passed on such a path between the agents is called the number of hops. It must be clear that the virtual connections (neighbours) are independent of the underlying physical network, which is treated as a black box.

An illustrative example of an overlay network is shown in Figure 3-19. Four computers A, B, C and D are connected by an IP-based network. Each of these computers (or at least the software agents running on these) has a limited number of neighbours as is shown with the red arrows. Although each agent only knows a few other agents, there exists a path between every two agents in the overlay network. For clarity, the overlay network is shown again in Figure 3-20, without the underlying physical connections. One can see very clearly that the overlay network topology is logically independent of the underlying physical network topology. While node A and node B are for example in the same physical LAN (on the same switch), there exists no direct path between them in the overlay network.

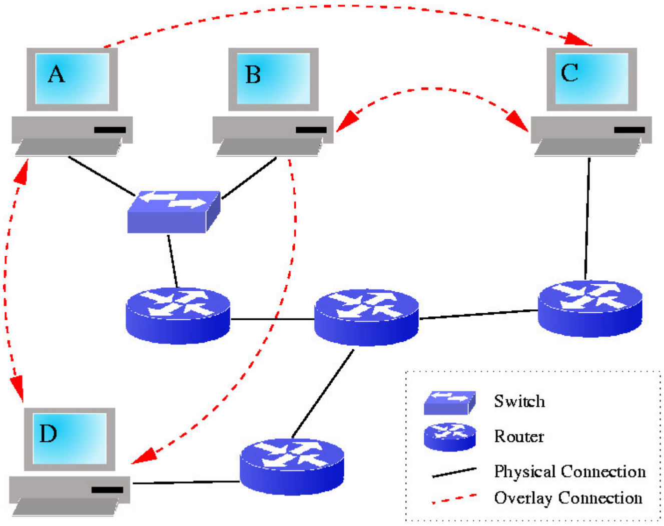


Figure 3-19: Illustrative layout of IP-network with four computer nodes attached. Both the physical connections and the virtual overlay connections are shown.

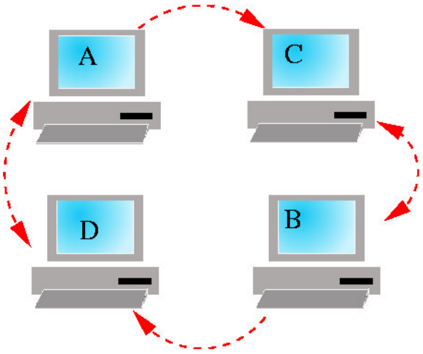


Figure 3-20: Overlay network formed in Figure 3-19.

Now we have shown what an overlay network is, but how is it constructed? This is done in a fully distributed way; no server listing of its members is needed. An agent joining the overlay network must know only one current member, which it will contact. This member will pass on other members with whom the new agent can form a limited number of peer-to-peer connections. The choice of these new neighbours is based on certain rules, which are different in different types of overlay networks. It are these rules that determine (stochastically or deterministically) the topology of an overlay network. In the overlay network used for the multi agent control system a semantic distance metric based on XML descriptions of the agents is used. The smaller this distance between the descriptions of two agents, the higher the probability that one agent will choose the other agent as a neighbour. Consequently, an agent will tend to connect to similar agents. Additionally a limited number of neighbours with a very large semantic distance are chosen, as to avoid the P2P network splitting up in clusters of similar agents and to limit the diameter of the overlay network (maximal number of hops to go from one agent to another). Finally, to improve robustness of the overlay network, an agent keeps a list of former neighbours, which can be used as access points after the agent has been disconnected from the network.

This overlay network forms an ideal structure for communication over unreliable packet switched networks; agents can join, leave and re-enter at will, there is no need for central coordination and scalability is high. The topology is random enough to avoid an accidental partitioning of the network, but also has some logical structure to allow quick resource discovery without too much communication overhead. An example of such an overlay network connecting generators in a power distribution grid is shown in Figure 3-21 and Figure 3-22.

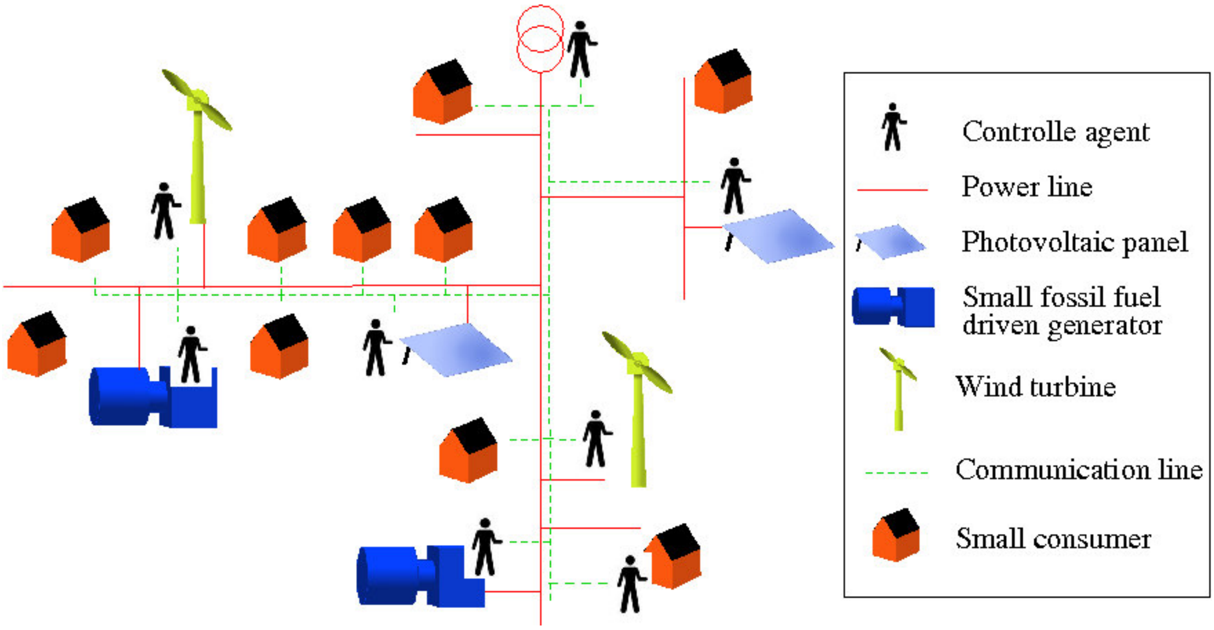


Figure 3-21: Power distribution segment with large DG penetration, and an agent deployment.

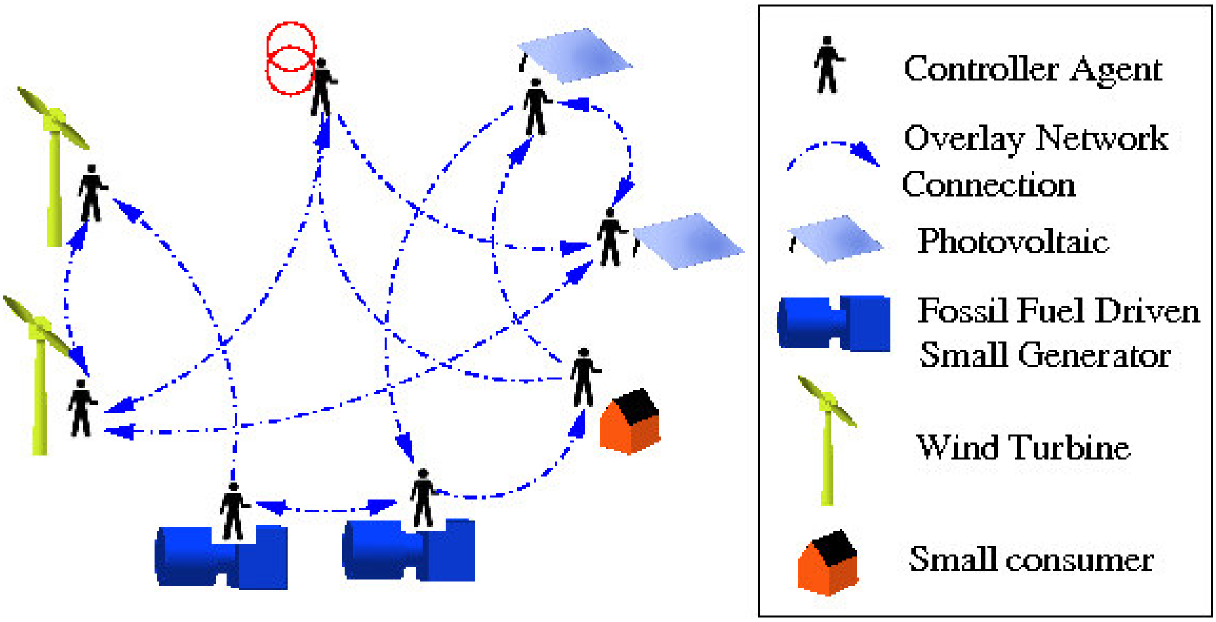

Controller Agent
Overlay Network Connection
Photovoltaic
Fossil Fuel Driven Small Generator
Wind Turbine
Small consumer

Figure 3-22: Example overlay network topology between agents controlling the autonomous electricity grid of Figure 3-21.

3.4.2.2 Gossiping Based Communication

Basic Algorithm

For the exchange of information over such an overlay network, there are multiple options. *Flooding* or *multicasting* of messages could be used. The former has quite high network demands, while the latter is not supported by most routers on the Internet. The method we use here is called *gossiping*; every agent exchanges information at fixed time intervals with one of its neighbours (chosen randomly). If that neighbour exchanges this new information with one of its neighbours (and so forth), the news spreads in the network. This also explains its name; the way information is spread is very similar to how gossips are spread in a society from person to person.

As an example of this gossiping process, have a look at Figure 3-20. Suppose agent A has some news to spread in the overlay network. Now, the following steps occur in given order on some discrete instances in time:

- A has news to be spread in the overlay network
- A does a gossiping step, randomly choosing neighbour C as gossiping partner. C learns the news.
- D does a gossiping step, randomly choosing neighbour A as gossiping partner. D learns the news
- C does a gossiping step, randomly choosing neighbour B as gossiping partner. B learns the news

This way, every agent has learned the news. Notice there are many other possibilities in which the news could have spread in this network.

Distributed Averaging Using Gossiping

Using this basic communication paradigm, some basic functions can be implemented over overlay networks. One of these basic functions using gossiping based communication is distributed averaging. In this, every node has a certain value (any real number) and using only gossiping, an overlay network wide average can be calculated. Since this distributed averaging algorithm is used in the control scheme, we explain the algorithm here.

To understand why, we should have a look at the algorithm which is used for secondary control, namely gossiping based averaging. During such a gossiping step the following happens:

DG Controller C_1	DG Controller C_2
send current average $\text{Average}_1 \rightarrow$ C2	**send current average $\text{Average}_2 \rightarrow$ C1**
receive average Average_2	**receive average Average_1**
calculate and set new average **$\text{Average}_1 \rightarrow (\text{Average}_1 + \text{Average}_2)/2$**	**calculate and set new average** **$\text{Average}_2 \rightarrow (\text{Average}_2 + \text{Average}_1)/2$**

One can think of this algorithm as a certain amount of money which is divided among a fixed group of people. If all people in a group randomly exchange money between one another according to above-mentioned scheme, they will all have an equal amount of money after a certain time. The total amount of money in the group however stays the same, since they are only exchanging money within this fixed group. This leads to the conclusion that the amount of money each one has at the end is the average. A graphical illustration of the distributed averaging scheme is shown in Figure 3-23.

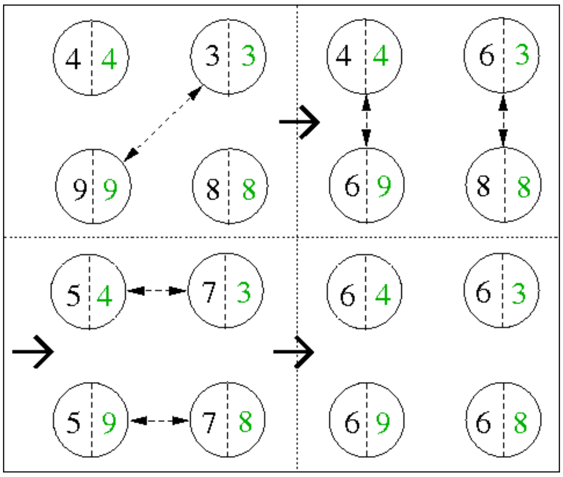


Figure 3-23: Illustration of the distributed averaging algorithm between four nodes using gossiping. After four steps convergence is seen in the algorithm on the exact average of '6'.

3.4.3 Controlling Distributed Generators in a Microgrid

The goal of the distributed control system is the coordinated control of small generators in a single distribution grid. The basic control loops which are implemented in a microgrid are quite similar to the control loops that are found in large generation facilities on transmission level, namely:

- *Primary control* or *droop control*, which ensures *energy balance* for both active power P and reactive power Q. Based on local measures voltage and frequency primary control will adjust power output as to limit divergence from rated voltage and frequency levels.
- *Secondary control*, which keeps voltage and frequency within certain bounds of their rated values, if possible. Where primary control only *limits divergence* from rated voltage and frequency values, secondary control brings voltage and frequency back to the rated values after a divergence.
- *Tertiary control* optimizes power production for economical concerns. Power production is redistributed among participating generators as to minimize production costs. This control loop may also be used to implement a market based mechanism.

Furthermore, the multi agent system may also aggregate the distribution grid within a single agent located on the feeding transformer. This aggregating agent may connect to the high level SCADA system as a single logical consumer or producer for supervision or control purposes. This might allow a limited level of control over DG and smart loads by the TSO or DSO. The connection on ICT level between the microgrid and transmission level can also be used as the link between the power spot market price and the price within the distribution net. Another function for this aggregating agent could be the (re)synchronization of the microgrid with the transmission grid to allow reconnection after an islanding of the microgrid.

3.4.3.1 Primary Control

Primary control thus only needs local measurements, namely local voltage and frequency, to control the generator's active and reactive power outputs [Marwali *et al.* 2004][De Brabandere *et al.* 2004]. In resistive power grids, such as low or medium voltage distribution grids, voltage is dependent on active power, and frequency on reactive power. Figure 3-24 shows how active power output is adjusted using a proportional controller with local voltage as its input. A similar controller is used for the control of reactive power vs. frequency, further we only look at active power output. In active power control, P_0 is the setting for the desired active power output when voltage is at its rated value *U_0*. *P* is the actual power output at the current (divergent) voltage and *ΔP* is the difference between these two.

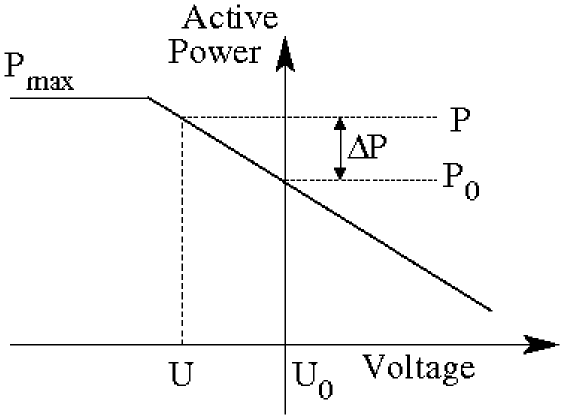


Figure 3-24: Droop graph controlling active power output vs. locally measured voltage.

The primary control loop can maintain power balances and react quickly to changes in the distribution grid, without need for communications. When the distribution segment is connected to the transmission grid, distributed generators equipped with this fast reacting droop control can give support to the power grid in case of severe faults, such as quickly decaying frequency or voltage collapses. When the distribution segment is disconnected from the power grid and keeps operating in islanded mode, primary control is indispensable for controlling frequency and voltage in the distribution grid, since these are no longer externally controlled by the large transmission grid. Maintaining frequency and voltage in an islanded distribution segments essentially means maintaining power balance in the segment (= equalize consumption to production).

Many installations of DG nowadays are not equipped with droop control or automatic voltage regulators, so they merely provide a fixed or stochastically varying (wind, solar or CHP) amount of active power. This lack of primary control poses no problem as long as DG comprise only a small amount of the power generation in a power grid, and the DG units are installed in a strong portion of a distribution grid (e.g. cabling with sufficiently high power flow capacity). The first condition means large power plants can maintain frequency and voltage stability, the second ensures voltage drop/rise along a distribution grid does not reach unacceptable limits due to increased current flows caused by local power production.

Although primary control as implemented in our scheme counters large voltage or frequency variations as to minimize divergence from their rated values, the proportional controller alone can't maintain rated values. For this we need a proportional-integral controller (PI). Unfortunately, implementing a local PI-controller in all DG units may lead to unwanted and possibly dangerous oscillations. That is why there is a need for a secondary control loop using communications for coordination between DG controllers.

The primary control implemented in our AEG has been adjusted a little to allow economical optimization. A dead zone is defined in which power output is not adjusted although voltage and frequency may diverge from rated values. This primary control curve looks like the one in Figure 3-25.

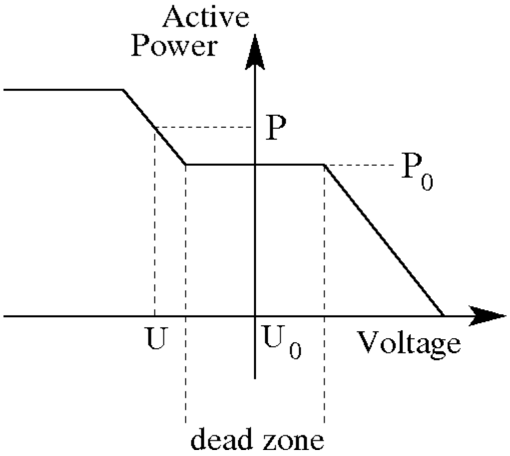


Figure 3-25: Droop graph with dead zone to allow for economical optimization.

3.4.3.2 Secondary Control

In this control scheme, secondary control controls both voltage and frequency. It is used to maintain rated voltage and frequency levels. When the microgrid is connected to the power grid, the frequency is controlled by this external grid. The most important factor to control locally is the voltage level. For this, the DSO draws up a voltage planning for the classic radial power distribution grids. In a traditional low voltage distribution segment, there are only passive elements. At the feed in point there is a single transformer that keeps the voltage around a certain value. Along the radial low voltage distribution line there is a voltage drop which is dependent on the fixed line impedance and the variable power consumption. The voltage at the feed in point is determined in function of this minimal and maximal voltage drop as to keep the voltage within a certain range of the rated voltage. All this is illustrated in Figure 3-26.

If a DG unit is installed in such a distribution segment, the voltage level is raised near the generator due to the extra active power fed into the line (see Figure 3-27). In current applications of DG the voltage near the DG should stay within small bounds of the locally rated voltage as to minimize the influence on the voltage profile along the line, if this is not possible, power line reinforcements or an automated voltage regulator (AVR) are needed.

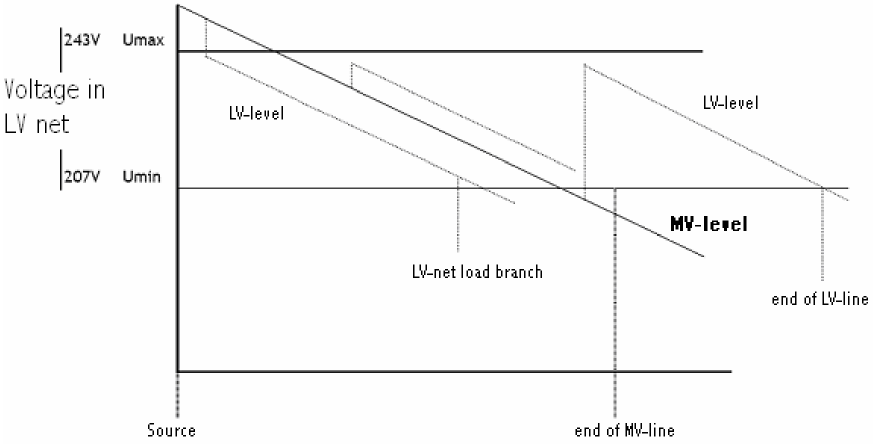


Figure 3-26: Voltage profile along a low voltage (LV) and medium voltage (MV) distribution line

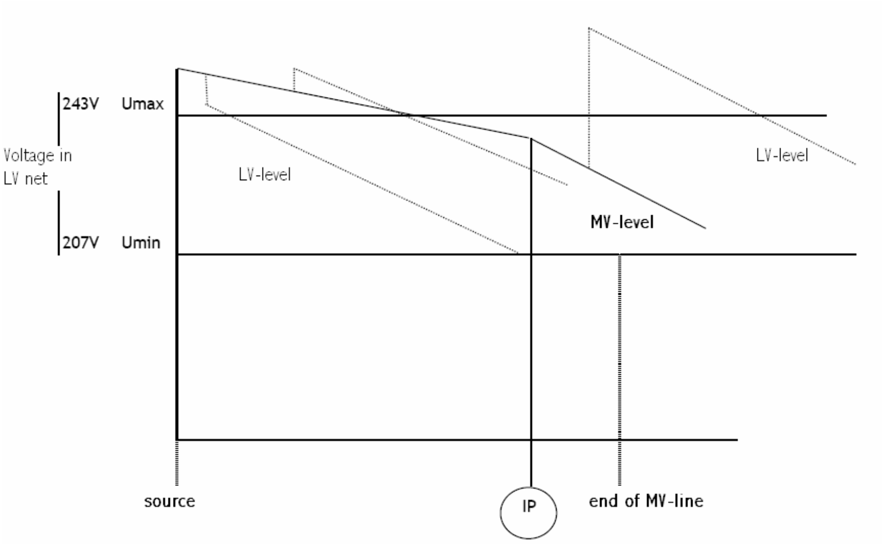


Figure 3-27: Local voltage boost near DG unit (IP) raises voltage level above allowable limits in certain parts of the distribution grid

The voltage control scheme implemented in the microgrid application presented, does not simply try to keep rated local voltages, but instead tries to optimize global divergence over the whole distribution grid. As mentioned in previous paragraph, one needs the functionality of a PI-controller to maintain these rated voltage and frequency levels with some coordination among the DG units in the distribution net to avoid oscillations, or sub-optimal solutions. For this, the average divergence from power output setpoints P_0 and Q_0 are calculated system-wide, which are an indication for the divergence from rated voltage and frequency. Adjusting the active and reactive power outputs as to regulate this average system-wide divergence to zero, should optimize the distribution system voltage and, to a lesser degree when the system is grid connected, its frequency. So, using the distributed averaging algorithm as presented in section 3.4.2.2, we calculate the system-wide average ΔP_k (and similarly ΔQ_k) for all generators k in the distribution net:

$$\overline{\Delta P} = (\sum_{i=1}^{n} \Delta P_i) / n$$

And then, when this value calculated locally in generator k converges, the setting $P_{0,k}$ for generator k is adjusted (and so for each generator in the system):

$$P_{0,k} = P_{0,k} + \overline{\Delta P}$$

This way, divergence from rated values is not necessarily eliminated near each DG unit, but at least the divergence is minimized and equally spread along the distribution grid.

3.4.3.3 Tertiary Control

Tertiary control optimizes generator output for economic criteria. Traditionally, a central controller knows the marginal production costs of all generators and aggregates these[2]. Based on these curves and the total power demand, power output settings for all generators are calculated so as to minimize costs, and dispatched to the generators in the field.

In our control scheme however, tertiary control is performed in a distributed way. Agents controlling generators communicate only with their direct neighbours (see section 3.4.2.2),

[2] Nowadays, this kind of centralized tertiary control is abolished and replaced by power market mechanisms. It is however still used internally by large generation companies to optimize their production.

exchanging their marginal cost (MC) curves. Next, the two gossiping generators adjust their power output as to make their MCs equal, while the total power production remains constant. Continuing this gossiping process ultimately leads to the point where all generators in the distribution grid produce at the same marginal cost, which is the theoretical economical optimum. Figure 3-28 shows the marginal cost curves of two generators, their production setting before a gossiping step, and the resulting power output of both generators after the gossiping step.

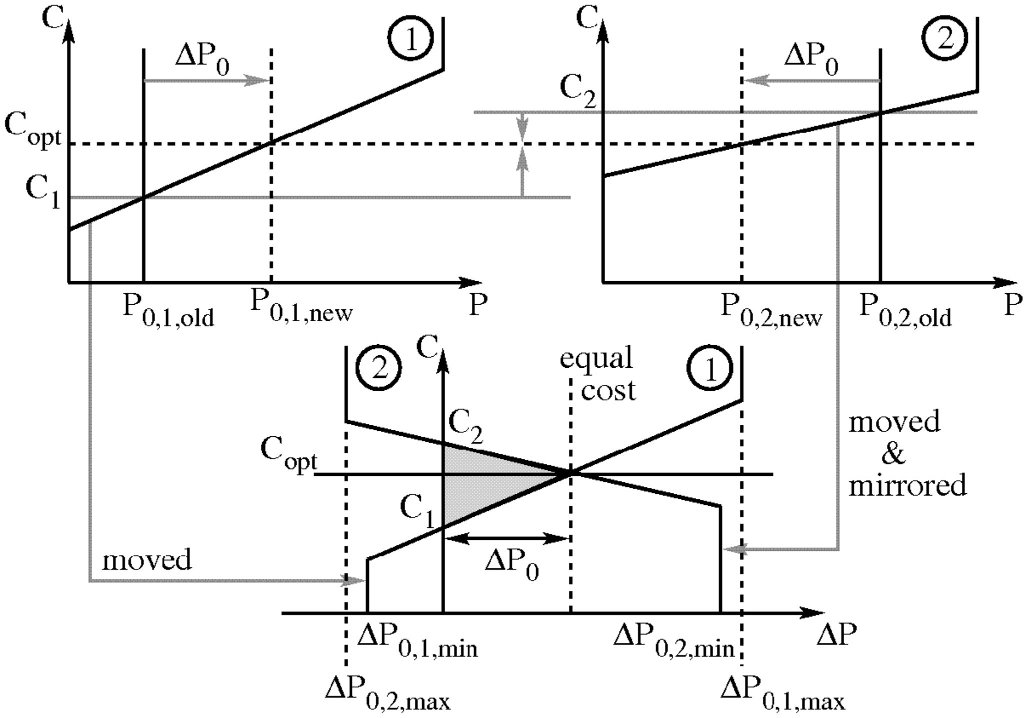


Figure 3-28: Marginal cost curves of two generators (1, 2) and an illustration of the algorithm used to equalize their marginal production costs while keeping the total production constant (3).

The voltage regulation in the distributed generation system is represented by the class diagram in Figure 3-29. In such diagram, the class representing the general voltage regulation (or control) is *DGVoltageControl*. This class specializes the class *Regulation* representing the generic function of regulation (or control). The class *DGVoltageControl* is the aggregation of three classes: *DGPrimaryVoltageControl*, *DGSecondaryVoltageControl*, *DGTertiaryVoltageControl*; these classes represent the primary, the secondary and the tertiary voltage regulation respectively, and they are specializations of the class *Function* representing the generic function.

The class *OverlayNetwork* represents the network composed by the agents exploited in the distributed generation system in order to perform the secondary and tertiary voltage regulation. For this reason the class *OverlayNetwork* is the aggregation of instances of the class *Agents*. Agents exchange information so the class *Agents* is associated with itself.

The class *OverlayNetwork* is associated with the class *DGSecondaryVoltageControl* and with the class *DGTertiaryVoltageControl* because the overlay network performs the secondary and tertiary voltage regulation.

An agent can be hosted on a regulation component; therefore, the class *Regulation&ControlComponent* is associated with the class *Agents*. Moreover, a regulation component may regulate a distributed generator present in the distributed generation system; so, the class *Regulation&ControlComponent* is associated with the class *DistributedGenerator*. A regulation component may also perform the primary voltage regulation; this is represented by associating the class *Regulation&ControlComponent* with the class *DGPrimaryVoltageControl.*

A distributed generator is an element of the distribution grid; this aspect is represented by connecting the class *DistributionGrid* with the class *DistributionGenerator* by means of an aggregation arc.

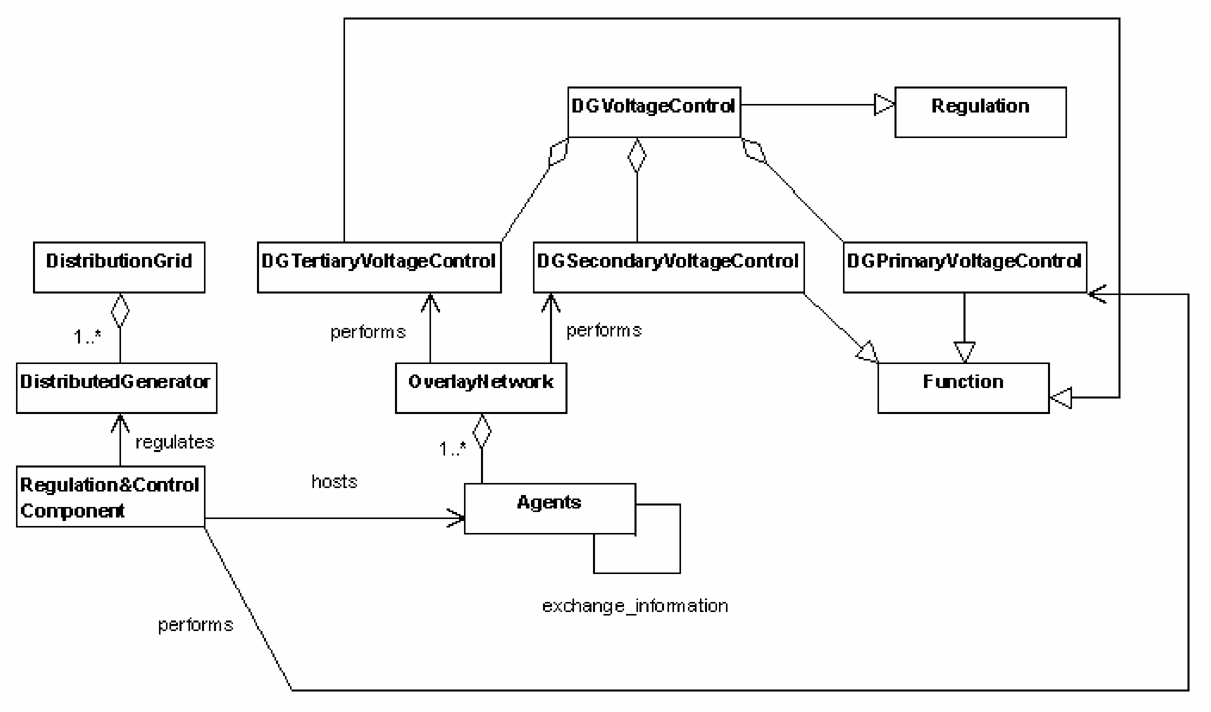


Figure 3-29: Voltage regulation in the distributed generation system.

The state diagram in Figure 3-30 shows the possible states of a non malicious agent. In such diagram, the agent is initially in the state *Created*, then it turns to the state *UnderRegistration*; in this state, the agent has been recently created and its neighbours are being informed of its presence. At the end of this process, the agent turns to the *Active* state; in such state, the agent is known by all its neighbours and is performing its activity. If the agent decides to leave the overlay network, then the agent turns from the *Active* state to the *RemoveRegistration* state; during such state the agent is removed by the overlay network by informing the neighbours of the agent about the fact that the agent is being excluded from the network. At the end of the removing activity, the agent turns to the final state *Removed*.

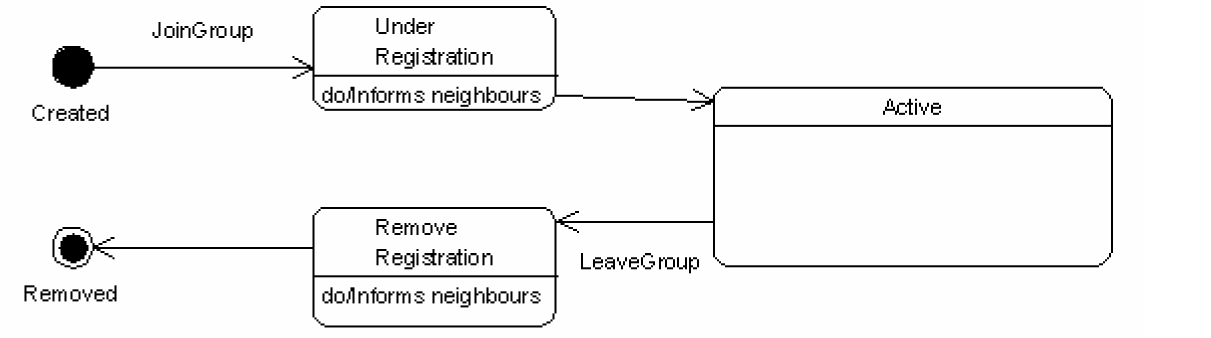


Figure 3-30: State diagram of a non malicious agent

3.4.3.4 Timing Constraints for Control Loops

The primary control loop controls in real-time the power output of the generator, based on local real-time measurements of voltage and frequency. This control loop has hard-real-time requirements, which can be guaranteed since no external communication channels are needed, all measurements are done close to the generator. We will not go any deeper into this embedded local control system, since timing parameters and system parameters are case specific and variable for different kinds of measurement devices, embedded controllers, generators, or inverters connecting the generator to the power grid.

Given both secondary and tertiary control loops are merely meant for optimization, and the functionality of the critical primary control loop is independent of their functionality, there are no timing requirements for secondary or tertiary control loops in the sense that a generator may exhibit faulty behaviour when messages between generator controllers are delayed or communication is down totally. Yet when communications are slow or totally down power generation may be suboptimal, which may have an impact on power quality or production costs. Given some form of timely behaviour is expected from the secondary and tertiary control loops, but failure to stay within these limits has no severe consequences, these may be considered soft-real-time systems.

3.5 Emerging ICT system architecture for the Power System

A possible architecture of the ICT systems involved in Power System infrastructures is depicted in the Figure 3-31 that shows the Stakeholders (GENCO, TSO, DSO, TSP), and their interconnections.

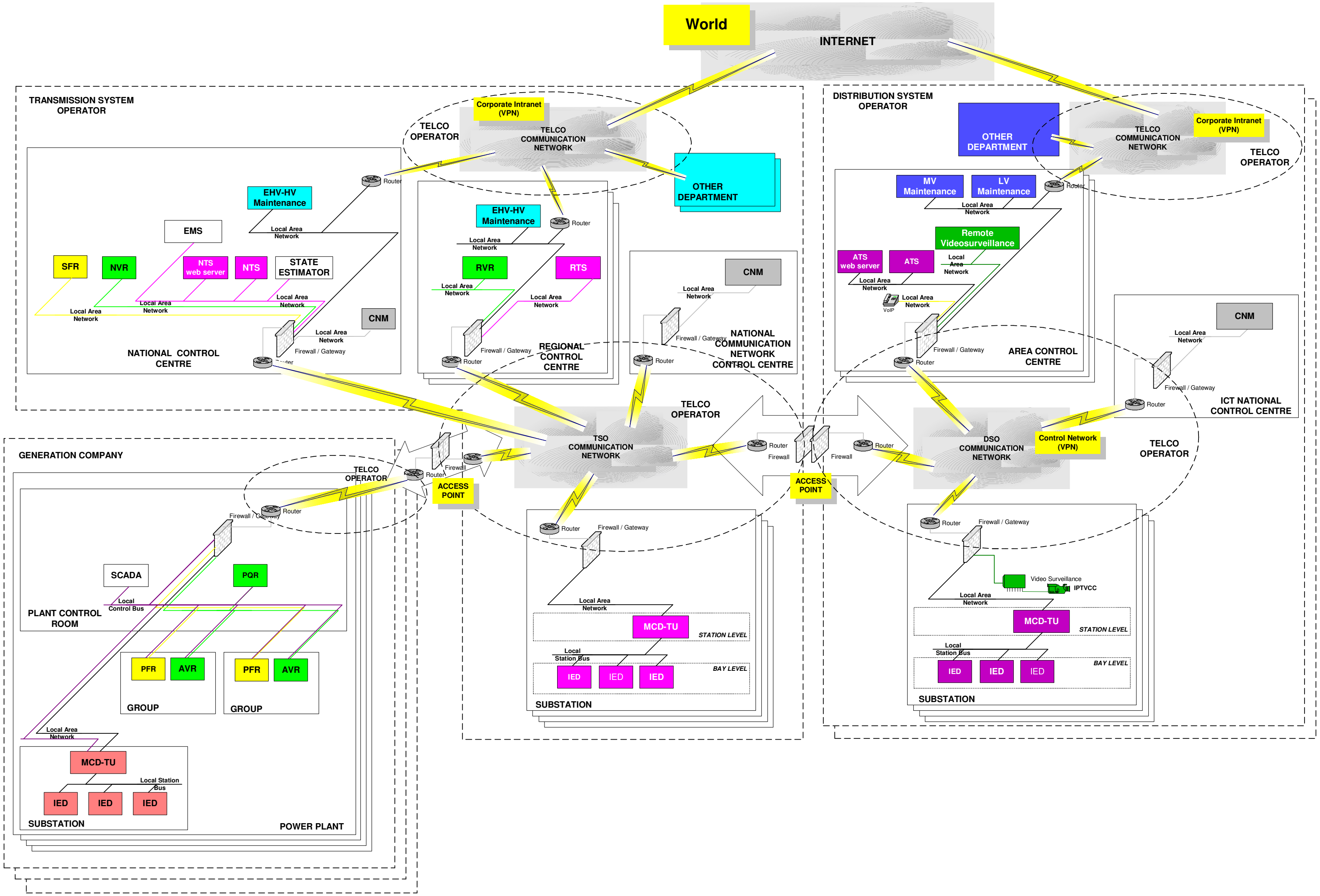


Figure 3-31: ICT infrastructure in the Power Systems

In the following paragraphs a description of the ICT infrastructures adopted by the major Stakeholders is summarised. As a reminder of the points interfacing the ICT and the power components the reader may keep an eye on the Figure 2-4.
The main characteristics of all these infrastructures are summarised hereafter:

- Use of standard communication protocols (IEC-60870-5-104, RPC) between centres and Terminal Units
- Use of IP Networks for the regulation and teleoperation functions, owned and operated by Telecommunication Service Providers (TSP)
- Presence of different logical networks on the same physical support
- SCADA system based on Commercial Off-the Shelf hardware or software components (COTS)
- Centralised ICT monitoring, control and maintenance functions for the whole ICT infrastructure (communication devices, IEDs-Intelligent Electronic Devices, etc.)
- Interaction between TSO/DSO, GENCO/TSO, DGSO/TSO ICT infrastructures to carry out emergency actions
- Integration of Process and Corporate networks.

Different study scenarios will be identified involving several stakeholder infrastructures.

ITC for Distribution System Operator - DSO

The main UML class diagrams that accounts for the ICT infrastructure of the DSO are the description of the ACC and of the substation automation site given in Figure 3-32.

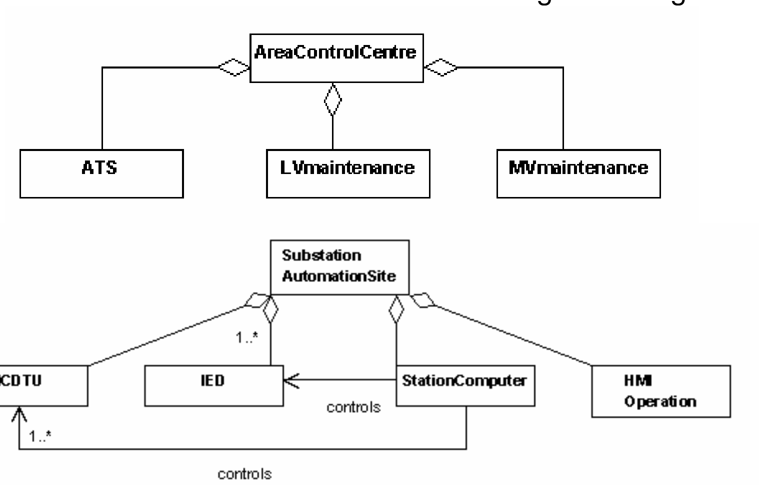


Figure 3-32: UML Class Diagram of ACC and Substation Automation Site

ICT for Generation Company - GENCO

The CD of control aspects of a power plant are summarized in the CD of Figure 3-33.

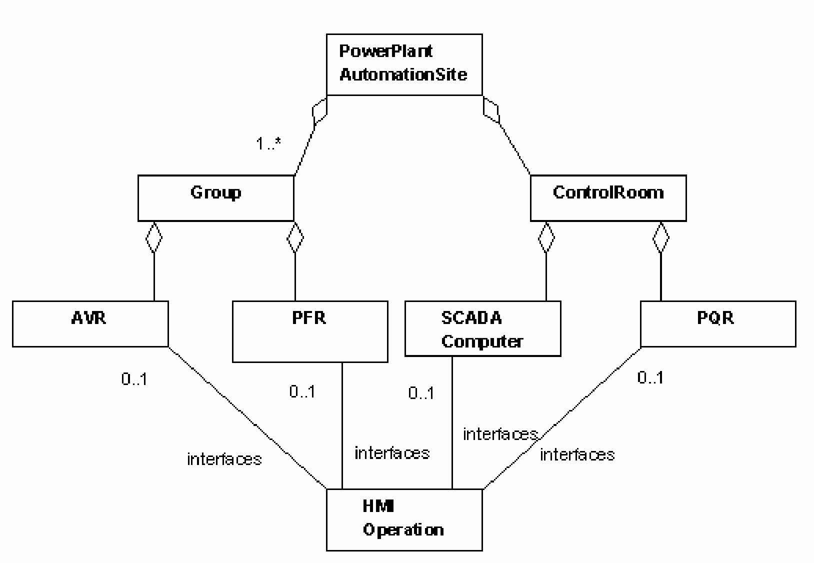


Figure 3-33: The automation aspects of a Power Plant

ICT of Transmission System Operator - TSO

The CD of the control aspects of TSO are summarized in the CD of Figure 3-34.

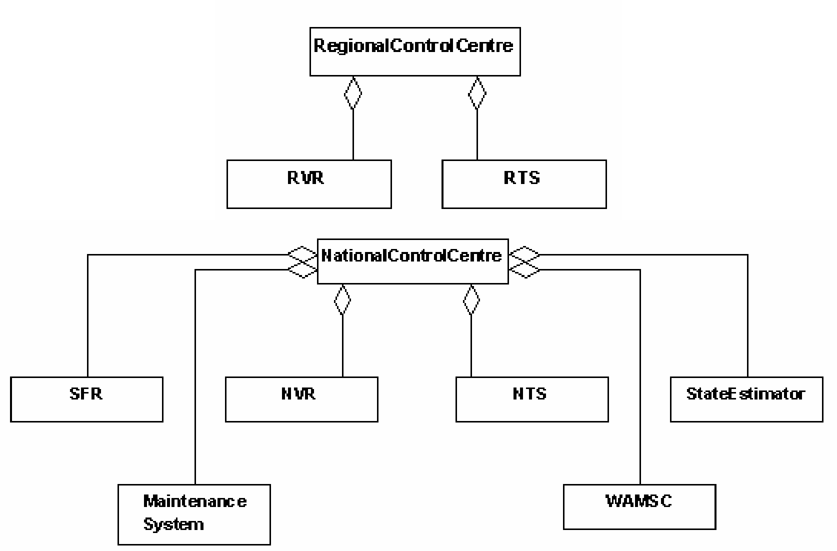


Figure 3-34: The automation aspects of TSO

3.5.1 Security issues

The descriptions of the vulnerabilities and the threats incurred by the system are the two pillars of any security analysis [Dondossola & Lamquet 2006], [Dondossola *et al.* 2006b].

Vulnerabilities are flaws or weaknesses in a component or in the system's design, implementation, or operation and management, which could be exploited to violate the system's security policy.

The vulnerabilities under consideration are selected with reference to their relevancy or priority, in order to identify which are likely and which not. Relevancy means not only the likelihood aspect but also the severity one. Combining the two indexes of severity and likelihood, it should be possible to evaluate the relevancy of each vulnerability for the whole subsystem.

Threats act at a higher level than vulnerabilities and represent menaces to the system or subsystem services. A threat is any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals. In case of malicious threats if acts through an information system via unauthorised access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability. [CNSS I4009 2006], [FIPS 200 2006]

Each threat is characterised by the type of agent (human, environmental, etc.), the objective, the motivation (malicious, accidental), etc.

The combination of two threat indexes of likelihood and severity provides an evaluation of the relevancy of each threat for the whole system.

In principle the choice of a set of threat hypotheses to investigate on a given control scenario should be based on the results of a risk assessment activity. As an initial proposal the following classes of malicious faults will be used:

- ***DoS*** attacks e.g. those towards the teleoperation communications, generated by enemies located on the Telecom IP backbone (e.g. connection requests on the port used by the IEC protocol)
- ***Intrusions*** like those into the Centre/Substation communication flow followed by authentication violation or the execution of faked commands
- ***Malicious logics*** faults (viruses, worms, Trojan horses, ..) e.g., by hostile use of maintenance activities by means of a portable PC in the Substation Networks.

4 CONTROL SYSTEM SCENARIOS

4.1 Summary of the features addressed

With the advent of the liberalised markets an increasing number of different actors (TSOs, DSOs, GENCOs, DGSO, Power Exchange, Energy Authority, etc.) are involved in the electrical system's management and there can be a necessity to exchange power system status information and control data over public and shared networks (see Figure 4-1) [Brand *et al.* 2003].

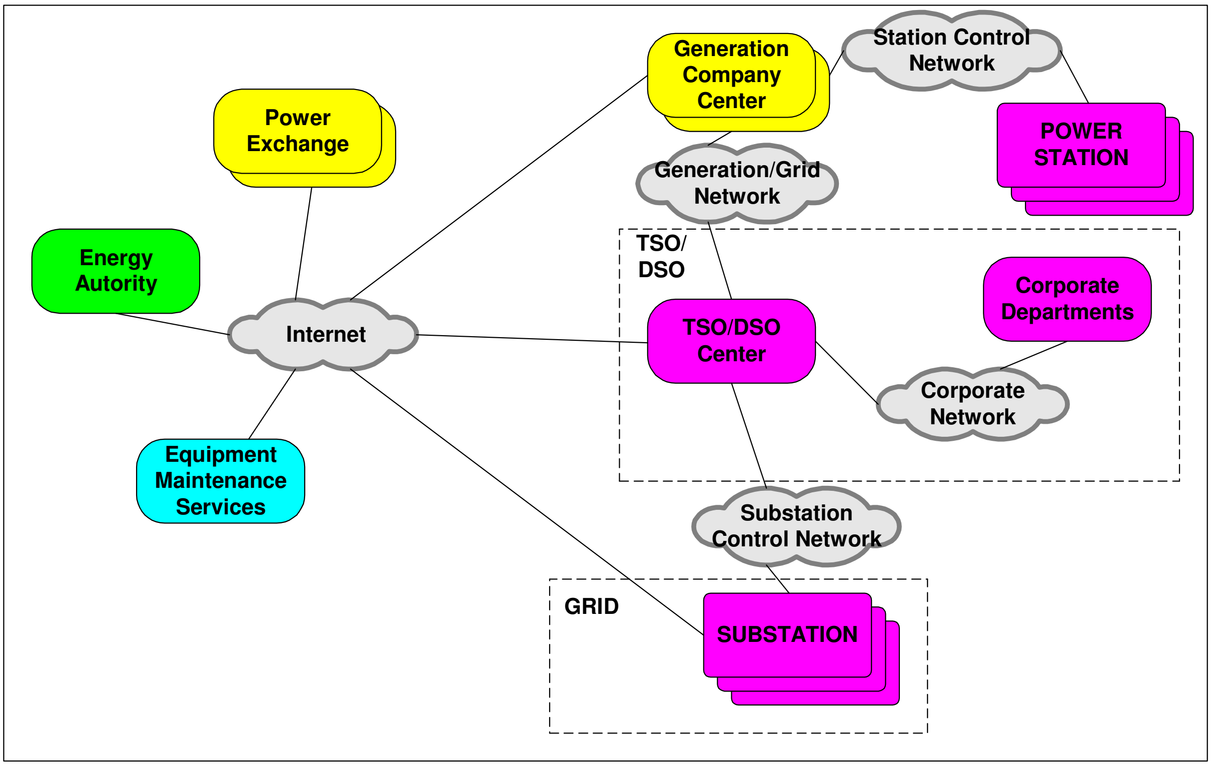


Figure 4-1: Communications between Electrical System actors

In order to maintain their infrastructures the stakeholders use to buy maintenance services from external providers [Schainker *et al.* 2006]. These providers mostly use public communication networks to receive up to date status information about the equipment to be maintained.

In the evolving context depicted above the following technical issues have been identified to finalize the analysis:

- How to guarantee availability and information security requirements for the remote control adopting third party communication channels?
- How to support the development of highly resilient corrective control actions for emergency management?
- How to protect ICT networks including SCADA-operational functions and corporate-maintenance functions, characterized by different levels of security and risk?
- How to support flexible operation of the power grid and remote configuration of its substation automation systems?
- How to prevent ICT threats provoking cascading phenomena due to interdependencies between power and ICT infrastructures?

The set of control system scenarios has been conceived in view of the development of a global national defence plan involving all operation and control infrastructures of the different stakeholders at generation, transmission and distribution levels.

The scenarios focus on threat hypotheses, having either external or internal sources, such as:

- Denial of Service (DoS) attacks on control systems by enemies located on the Telecom IP backbone.
- Intrusions into Centre-Substation communication flow and execution of faked commands (spoofing attacks/man-in-the-middle attacks).
- Exploitation of standard application layer protocols' vulnerabilities.
- Accidental or malicious infections by worms or viruses in the Substation or Centre Networks caused by maintenance (e.g. an infected lap-top connected to the network) or non allowed activities of control personnel (e.g. unanticipated direct Internet link between PC used for control system supervision).
- Intrusions and viral infections through ICT devices for the Primary, Secondary and Tertiary voltage and frequency regulations of generation power plants.

4.2 Overview of scenarios

The identified scenarios are divided in two groups:

- a first group of scenarios is related to hierarchical regulation and teleoperation system
- a second group of scenarios deals with distributed generation applications or microgrids.

The list of scenarios with their main characteristics are summarised in Table 4-2:

- **Identifier**: short description of the scenario composed by: the Power System Infrastructural identifier (G = Generation, T = Transmission, D = Distribution), the ICT identifier (ICT) and an increasing index.
- **Stakeholders**: the owners of services involved (GENCO = Generation Company, DSO = Distribution System Operator, TSO = Transmission System Operator, TSP = Telecommunication Service Provider, DMO = Distribution Maintenance Operator, ICTM = ICT Maintainer).
- **Information Control Systems**: the control systems and applications that are involved in the scenario.
- **Power Contingencies**: the initial electrical event that changes the status of the Power System. In most cases this event is managed by Defence Systems and Procedures.
- **ICT Threats**: ICT threat sequence which, if successfully carried out, may compromise the control function and provoke cascading or escalating effects.
- **Cascading Effects**: list of possible worst cascading effects depending on the escalation of situation.

Table 4-2: Control System Scenarios

Scenario description						
Case	**Identifier**	**Stake holders**	**Information Control Systems**	**Power Contingencies**	**ICT Threats**	**Cascading Effects**
Scenario 1 – DSO Teleoperation						
1	**D-ICT-1**	DSO TSP1	MCD-TU (DSO) ATS (DSO)	Load shedding plan Insufficient production Generation trip HV line unavailability	DoS Intrusion Viral infection Authentication violation	Lack of measurements Lack of signals Loss of automatic local control Loss of remote monitoring Loss of remote control Discrepancies with other monitoring functions Lack of operator awareness Lack of operator actions Substation level protection trip
Scenario 2 – Interaction between TSO and DSO in emergency conditions						
2	**TD-ICT-1**	TSO TSP2 DSO TSP1	MCD-TU (TSO) NTS (TSO) ATS (DSO) MCD-TU (DSO)	High voltages on the transmission grid	DoS Intrusion	Loss of Circuit Breakers arming/unarming requests Loss of commands
Scenario 3 – Integration of DSO Operation and Maintenance functions						
3	**D-ICT-3**	DSO TSP1 TSP3 DMO	MCD-TU (DSO) ATS (DSO) Web Server (Corporate) Data Archive (Corporate)		Viral infection Intrusion	Loss of process data Decreasing of maintenance response time
Scenario 4 – Maintenance of ICT components of DSO						
4	**D-ICT-4**	DSO TSP1	All DSO systems		ICT failures	Loss of remote maintenance functionality

Scenario description						
Case	**Identifier**	**Stake holders**	**Information Control Systems**	**Power Contingencies**	**ICT Threats**	**Cascading Effects**
		TSP3 ICTM				
Scenario 5 – Transmission Grid Voltage and Frequency Regulations						
Case 5.1 – TSO and GENCO interactions						
5.1	**TG-ICT-6**	GENCO TSP4 TSO TSP2	NVR, RVR, PQR, AVR PFR, SFR SCADA NTS, RTS		Viral infection DoS Intrusion	Loss of remote monitoring Loss of remote control Lack of operator awareness Lack of operator's actions
Case 5.2 – Erroneous measurements						
5.2	**TG-ICT-5**	GENCO TSP4 TSO TSP2	AVR, PQR SCADA PFR, SFR	Erroneous measurements, of frequency or/and voltages	DoS Intrusion	Generators trip (Loss of electrical security N-1)
Scenario 6 – Instability of Electromechanical Mode of Power Plant-Transmission Grid Systems						
Case 6.1 – Instability of Electromechanical Mode management						
6.1	**G-ICT-1**	GENCO TSO DSO	AVR, PQR PFR, SFR SCADA MCD-TU RTS, NTS	Instability of Electromechanical mode	Viral infection Intrusion DoS	Change of grid configuration (Case a) Failure of PSS (Case b) Generators trip (Loss of electrical security N-1) Spinning reserve power Decrement of frequency Over-voltage Grid Separation (Partial or total Blackout)
Case 6.2 – Supervision and Control functions of GENCO						
6.2	**G-ICT-2**	GENCO TSO	AVR, PQR PFR, SFR SCADA		Viral infection Intrusion DoS	Loss of regulation functions Lack of supervision and control functions Lack of automatic load shedding

Scenario description						
Case	Identifier	Stake holders	Information Control Systems	Power Contingencies	ICT Threats	Cascading Effects
			MCD-TU RTS, NTS			Lack of manual load shedding Lack of activation of shunt reactance Loss of confidentiality Spurious activation of shunt reactance Spurious manual load shedding
Scenario 7 – Low damped or unstable inter-area oscillations						
7	**TG-ICT-1**	GENCO TSP4 TSO TSP2	AVR, PQR PFR, SFR PSS SCADA RTS, NTS	Unstable inter-area oscillations	Viral infection Intrusion DoS	Inter-area oscillations Line Trip (Loss of electrical security N-1) Area A: Decrement of frequency Over-voltage Area B: Teleoperation trip of generators Over-voltage / Over-frequency Grid Separation (Partial or total Blackout)
Scenario 8 – Transmission Grid Short Circuit with loss of Synchronism						
8	**TG-ICT-2**	GENCO TSP4 TSO TSP2	AVR, PQR, RVR, NVR PFR, SFR SCADA	Short circuit with loss of synchronism	DoS Viral infection	Short Circuit Loss of synchronism (Loss of electrical security N-1) Grid Separation (Partial or total Blackout)
Scenario 9 – Transmission Grid Voltage instability						
9	**TG-ICT-3**	GENCO TSP4 TSO TSP2	AVR, PQR, RVR, NVR PFR, SFR SCADA	Voltage Instability cases Voltage Collapse	DoS Viral infection	Voltage drop Line tripping (Loss of electrical security N-1) Grid Separation (Partial or total Blackout)
Scenario 10 – DG Network Latency						

Scenario description						
Case	**Identifier**	**Stake holders**	**Information Control Systems**	**Power Contingencies**	**ICT Threats**	**Cascading Effects**
10	**DG-ICT-1**	DG DSO Loads TSO	Local Control Systems Controllers Agents Communication Systems		Packet loss	Loss of regulation
Scenario 11 – DG IP-Packet Losses						
11	**DG-ICT-2**	DG DSO Loads TSO	Local Control Systems Controllers Agents Communication Systems		Packet loss	Loss of regulation
Scenario 12 – DG Agent Control System (or Network) Unavailable						
12	**DG-ICT-3**	DG DSO Loads TSO	Local Control Systems Controllers Agents Communication Systems			Loss of regulation
Scenario 13 – DG Critical Control System Failure						
13	**DG-ICT-4**	DG DSO Loads TSO	Local Control Systems Controllers Agents Communication Systems		Control System Failure	Loss of local control
Scenario 14 – DG Denial of Service Attacks on IP-Network						
14	**DG-ICT-5**	DG DSO Loads TSO	Local Control Systems Controllers Agents Communication Systems		DoS	Communication delay
Scenario 15 – DG Attack on Overlay Network Topology						

Scenario description						
Case	**Identifier**	**Stake holders**	**Information Control Systems**	**Power Contingencies**	**ICT Threats**	**Cascading Effects**
15	**DG-ICT-6**	DG DSO Loads TSO	Local Control Systems Controllers Agents Communication Systems		Intrusion	Loss of confidentiality
Scenario 16 – DG Overlay Network Partitioning						
16	**DG-ICT-7**	DG DSO Loads	Local Control Systems		Intrusion	Marginal Costs variation
Scenario 17 – DG Economical Tampering Attack						
17	**DG-ICT-8**	DG DSO Loads	Local Control Systems Controllers Agents Communication Systems		Intrusion	Market Price variation
Scenario 18 – DG Voltage Level Attack						
18	**DG-ICT-9**	DG DSO Loads TSO	Local Control Systems Controllers Agents Communication Systems		Intrusion	Over-Voltage Grid separation Local black-out
Scenario 19 – DG Alternative Approach, Centralized Control Architecture						
19	**DG-ICT-10**	Servers DSO Loads TSO	SFR Local Control Systems Controllers Agents Communication Systems		DoS	Loss of communication

4.3 Emerging issues in ICT system for Power System

A first group of scenarios have been identified starting from the actual situation which does not consider DG.

The main purposes of these scenarios are to assess:

- the capability of the communication architecture of tolerating the threat hypotheses
- the security of the communications between operators to evaluate the impact of attacks in emergency conditions
- breaches caused by interactions between the corporate and the process network and on innovative functions related to the ICT system's remote maintenance

Scenario 1: DSO Teleoperation

This scenario considers the possible cascading effects of ICT threats to the DSO communication channel among Area Control Centres and their supervised Substations in presence of Power Contingencies (insufficient production, generation trip or HV line unavailability).

Scenario 2: Interaction between TSO and DSO in emergency conditions

This scenario considers the possible cascading effects due to ICT threats to the communication channel among TSO and DSO Control Centres and MCD-TUs in emergency conditions (under-frequency or voltage instability).

Scenario 3: Integration of DSO Operation and Maintenance functions

This scenario explores the integration of process control and corporate networks in a DSO Control Centre, evaluating the possible cascading effects of cyber attacks on the integrated architecture.

Scenario 4: Maintenance of ICT components of DSO

This scenario considers the use of a centralized ICT maintenance service assuming the presence of a central Control Centre for the monitoring and control of the components of all the ICT assets in the DSO process network.

Scenario 5: Voltage and frequency regulations

This scenario considers the possible cascading effects due to :

- ICT threats to the communication channel among TSO Control Centres and GENCOs and to Control Systems used for voltage and frequency regulations
- Measurement failures of TSO and GENCO voltage and frequency regulation systems

Scenario 6: Instability of electromechanical mode of Power Plant-Transmission Grid Systems

This scenario considers the possible cascading effects due to :

- Specific abnormal operating conditions of the system constituted by a Power Plant and the transmission grid, which is related to the electromechanical oscillation mode
- ICT threats to GENCO Control Systems used for voltage and frequency regulations.

Scenario 7: Low damped or unstable inter-area oscillation

This scenario takes into account the phenomenon of low damped or unstable inter-area oscillation.

Scenario 8. Short Circuit with loss of Synchronism

This scenario considers the loss of Synchronism caused by a Short Circuit.

Scenario 9: Voltage instability

This scenario explores the Voltage collapse due to voltage regulation by ULTC – Under Load Tap Changer.

4.4 New control scheme for microgrids

In order to study the behaviour of the microgrid control scheme under certain fault scenarios, a series of control system scenarios have been sketched and discussed. Most of these scenarios have been simulated on a platform incorporating both ICT behaviour (controller agents, communication channels, overlay network) and electrical behaviour (static power flows and droop control schemes of DG units) within the microgrid.

Reference scenario 1: Primary control only
This scenario is inserted to show how the system behaves in the absence of communications, and illustrates how only serve optimization purposes.

Reference scenario 2: Normal behaviour, all control loops available
This scenario illustrates the normal functionality of the microgrid when all control loops are available. It can be seen as a benchmark for the other scenarios.

Reference scenario 3: Secondary control only
This scenario illustrates the functionality of secondary control (compared with first reference scenario), or similarly, the impact of the lack of tertiary control (compared with the second reference scenario).

Reference scenario 4: Tertiary control only
This scenario illustrates the functionality of tertiary control (compared with first reference scenario), or similarly, the impact of the lack of secondary control (compared with the second reference scenario).

Scenario 10: Network latencies
This scenario discusses the influence of unpredictable communication latencies over typical public IP-networks (or the Internet).

Scenario 11: IP-packet losses
This scenario discusses the influence of packet losses over typical public IP-networks (or the Internet).

Scenario 12: Agent control system or network unavailable
This scenario discusses the influence of isolated agent control system failures (e.g. crash of computer or agent software) or the isolation of a small number of agent controllers by a communication network failure.

Scenario 13: Critical control system failure
This scenario deals with isolated failures of primary control systems, which directly control generator outputs (or similarly the inverter outputs).

Scenario 14: Denial of Service attacks on public IP-network
This scenario discusses the influence of Denial of Service attacks on public IP-networks over which the agents communicate.

Scenario 15: Attack on overlay topology
This scenario sketches a typical attack on the middleware level which enables agent communication, namely the overlay network. This attack can be a means to achieve a higher goals, next to simply change or disturb overlay topology, for example an attack on the economical optimization system or distribution net voltage level.

Scenario 16: Overlay network partitioning
A dreaded fault in all overlay network types is the partitioning of the overlay network, by which nodes are split up in two or more independent groups unable to communicate to one

another. It is very hard to detect this kind of faults, but they can have a tremendous impact on overlay network functionality, and consequently the application implemented on these overlays.

Scenario 17: Economical tampering attack
Personal, economical profit is probably the strongest motive for human misbehavior. Therefore we can anticipate attacks on the economical control loop by parties hoping to sell power at higher prices, or buy at lower prices, or simply trying to harm a competing party by disturbing their economical optimization.

Scenario 18: Voltage level attack
The single most important aspect locally controllable by distributed generators is the voltage level in a distribution grid. Trying to convince a large amount of DG to increase their production may lead to over-voltages in the distribution grid, and consequently damage to equipment or disconnections.

Scenario 19: Alternative approach, centralized control architecture
This scenario discusses what would be the influence on the control system if one would use a more traditional centralized control system, implemented by a central server controlling active/reactive power output of each single DG unit in the distribution grid?

5 CONTROL SYSTEM SCENARIOS: HIERARCHICAL ELECTRICAL INFRASTRUCTURES

This chapter provides a detailed description of the scenarios summarised in Table 4-2, introducing their common features.

Network architecture

The information exchange among ICT automation and control levels is based on IP protocols compliant with the standard protocol stacks (Figure 5-1): the OSI (Open System Architecture) and the TCP/IP (Internet Protocol Suite) which is the "de-facto" international standard.

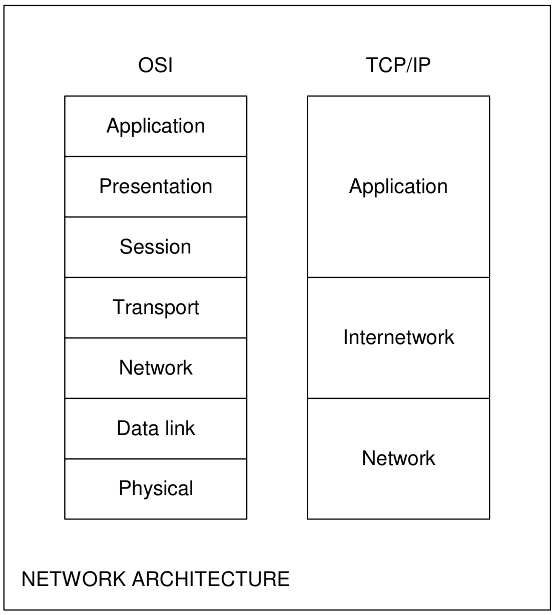


Figure 5-1: Standard information exchange protocol stacks

Application layer protocols

Data is exchanged among Centres and Substations using standard application layer protocols (Figure 5-2) based on a IP Network:

- IEC 60870-5-104 and IEC 60870-6 (ICCP/TASE-2) protocols, whose access port numbers are officially declared in the reference documents [IEC 60870-5 2006] [IEC 60870-6 2002]
- ftp
- http

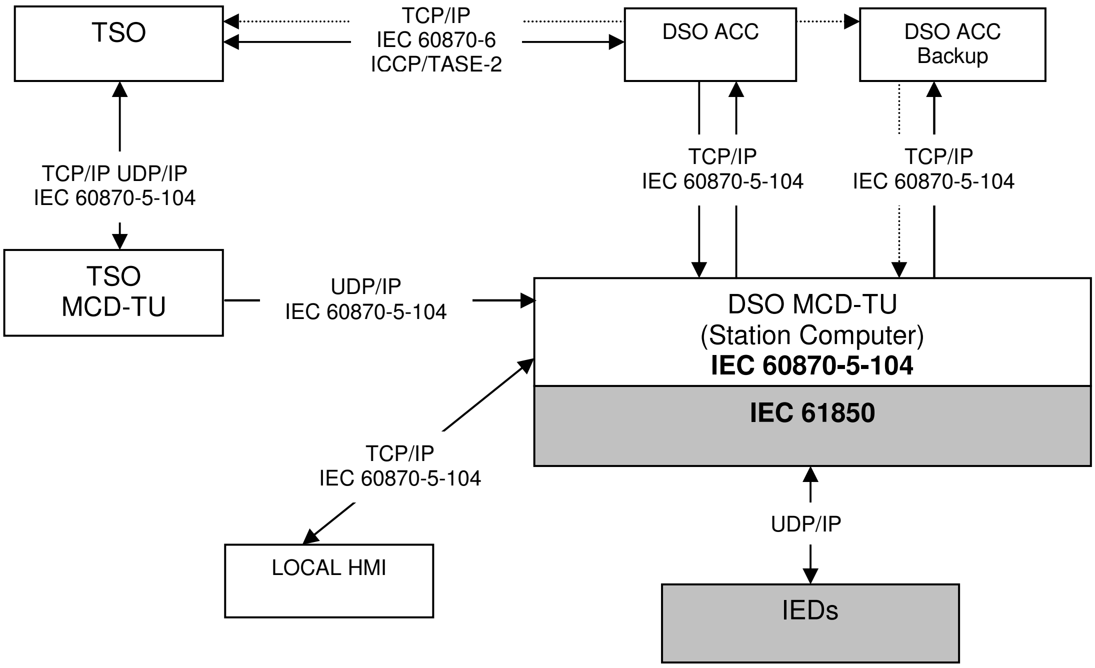


Figure 5-2: Control Centres and Substation exchange protocol definitions

No encryption mechanisms are used for authentication and message security.

5.1 DSO Teleoperation (Scenario 1)

This scenario considers the possible cascading effects of ICT threats to the DSO communication channel among Area Control Centres and their supervised Substations in presence of Power Contingencies (insufficient production, generation trip or HV line unavailability).

This scenario considers the information flow between DSO-Control Centres (Area and National) and their supervised MV/LV Substations, in NORMAL Distribution Grid operating condition. The information flow is supported by standard Telecom IP backbones owned and operated by an external provider who supplies a virtual, dedicated channel over a communication link shared with other customers. The inter-site communication infrastructure may be assimilated to a public WAN.

The communication requirements for the teleoperation traffic are expressed as follows:

- Bandwidth throughput of 64kbps
- Network availability 0.99999, i.e., unavailability[3] 10^{-5}.

Due to the strong availability requirements on the communication system, it is supposed that redundant communication paths are used, implemented over physically independent carrier lines, eventually owned by distinct Telecommunication providers (see Figure 5-3).

[3] The availability attribute is sensitive to both accidental and malicious threats, which may have an external or internal source. Therefore it is also affected by all those cyber threats which provoke an interruption of the communication service as a whole. No other security requirements are imposed to the Telecom provider.

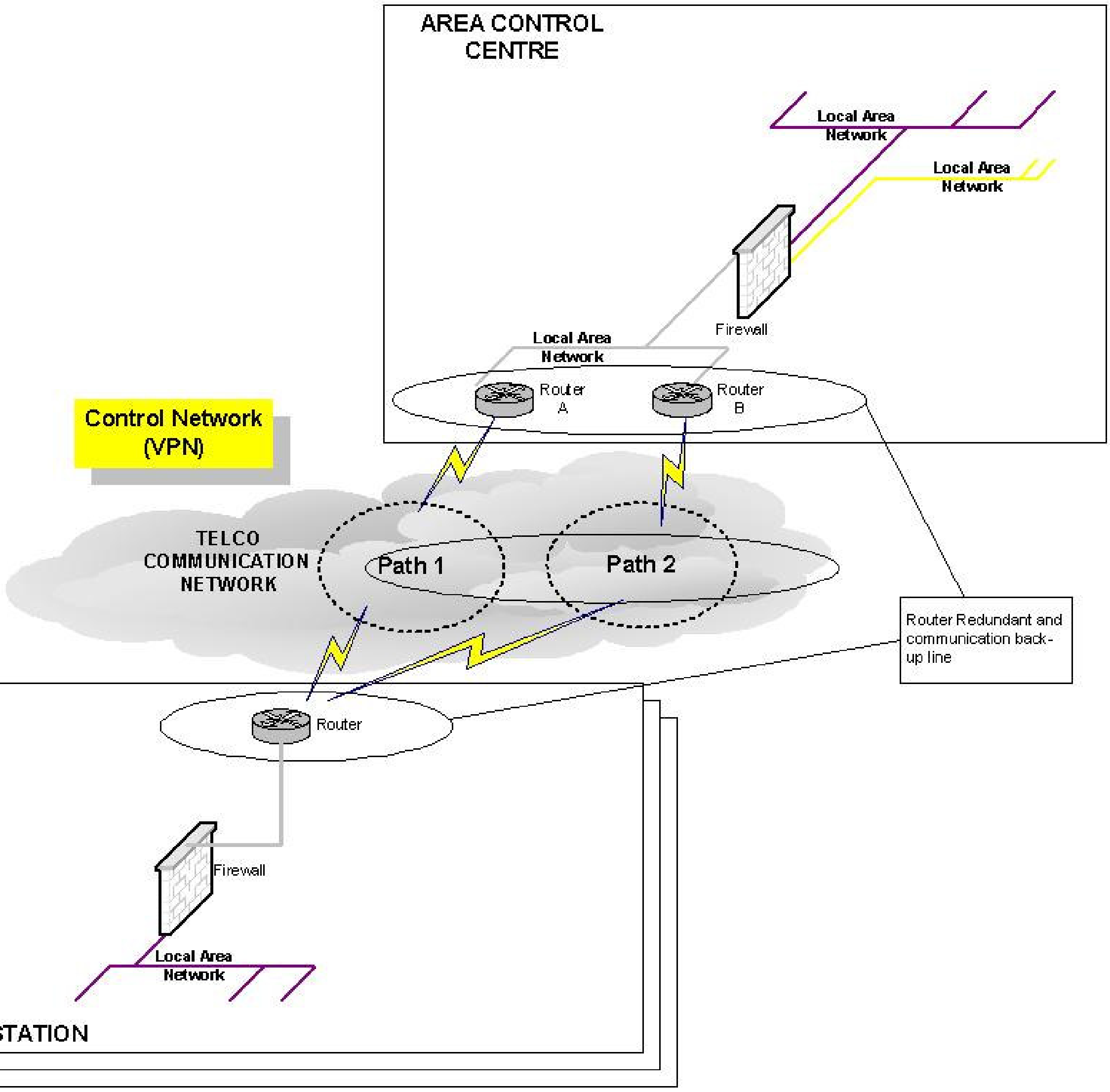


Figure 5-3: DSO Supervision and Teleoperation communications

The scenario explores the effects of ICT threats in case of:

- load shedding due to insufficient production/generation trip/HV line unavailability (eventually originated by the Operator of the Transmission Grid)
- programmed load shedding plan.

Stakeholders involved:

- DSO
- TSP of DSO

Information Control System involved:

The scenario involves a DSO Area Control Centre, its back-up and its n-controlled Substations (see Figure 5-4):

- ATS (DSO Area Control Centre): SCADA for grid management
- MCD-TU (DSO Substation): substation management

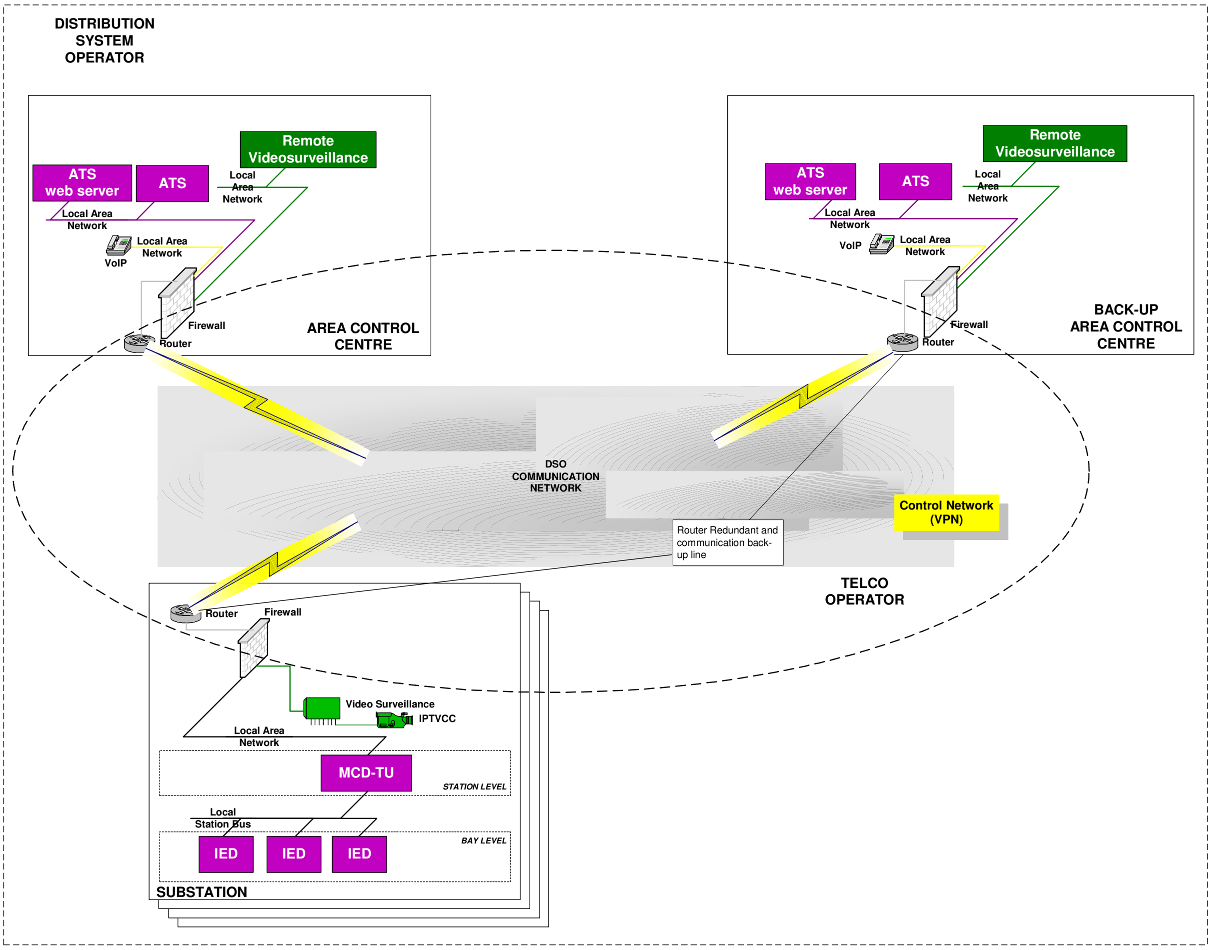


Figure 5-4: DSO-ICT systems involved in Supervision and Control

Information Flow:

The information flow among Substations, MCD-TU and Control Centres is classified as follows:

- Measurements: of P, Q, V and breakers positions from Substations towards Control Centres
- Signals: alarms and status variations from Substations towards Control Centres
- Commands: from Control Centres or MCD-TU towards Substations
- ICT Configuration Commands: specialised configuration commands of ICT components (IEDs, Firewalls, …)
- Information among Control Centres: data exchange in order to align the databases and the operation capabilities

Real-time requirements:

- Measure update 4 sec.: the refresh time of the measurement on the control system HMI
- Signals update 1 sec: the refresh time for alarm signalling and switchgear status variations
- Commands delivery time 2 sec.: teleoperation requests from Centres to Substations
- Defence commands delivery time:

- Low priority commands delivery time 500 msec
- High priority commands delivery time 200 msec.: (automatic load shedding) necessary to dispatch the load shedding command from Access Point to MCD-TU.

Power Contingencies:

This scenario explores power contingencies causing load shedding.

Goals:

The main purpose of the Scenario 1 consists in the assessment of the security of the ICT components involved in the Teleoperation activities i.e.:

- assess the capability of the redundant communication architecture to tolerate the threat hypotheses and evaluate the possible cascading effects in presence of power contingencies
- assess the vulnerabilities of the activities based on standard protocols (e.g. IEC 60870-4-104, IEC 60870-6 (ICCP), http, ftp)
- assess the sharing of the same channel for real-time and not real-time activities.

ICT Threats:

The most plausible ICT threats are:

- ***DoS*** attacks to the teleoperation communications, generated by enemies located on the Telecom IP backbone (e.g. connection requests on the port used by the IEC protocol)
- ***Intrusion*** into the Centre/Substation communication flow followed eventually by the execution of faked commands
- ***Viral infections*** of a Substation component caused by maintenance activities (e.g. by means of a portable PC)
- ***Authentication violation*** of a Substation Control System through hostile use of maintenance activities (e.g. by means of a portable PC, insider attack)

Cascading Effects and possible countermeasures:

In the following we discuss the consequences of the considered threats in function of the ICT components involved.

- **DoS attack to the VPN connection a Substation to the ATS (ICT-T1)**

  This attack reduces the communication bandwidth causing delay or failure in the delivery of status information to the ATS and in the reception of commands from ATS with consequent partial or complete **loss of remote control functions (ICT-C1)**, the loss of N-1 criterion electrical security and the wrong perception of the system's status at the control level (see Figure 5-5). The local control functions are not affected.

  Possible **ITC countermeasures (ICT-A1)**:

  - Firewalling
  - Monitoring of anomalous traffic (increasing amount of packets and proactive verification of their contents)
  - Redundancy of communication channel

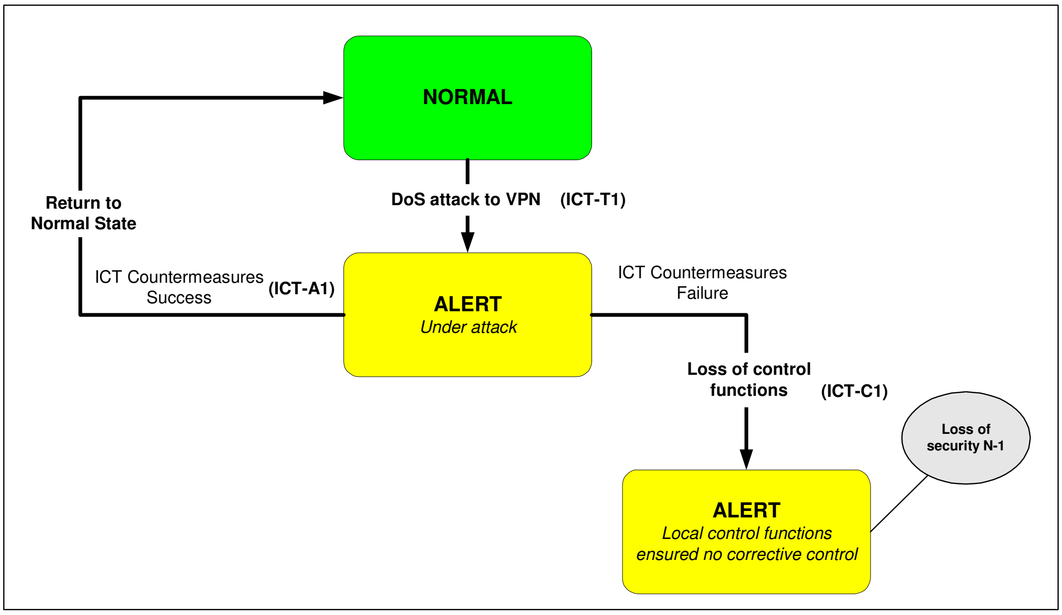

NORMAL
DoS attack to VPN (ICT-T1)
Return to Normal State
ICT Countermeasures Success
(ICT-A1)
ALERT
Under attack
ICT Countermeasures Failure
Loss of control functions
(ICT-C1)
Loss of security N-1
ALERT
Local control functions ensured no corrective control

Figure 5-5: DoS attack to VPN - Sequence of Cascading Effects

- **Intrusion into the Centre/Substation communication network (ICT-T2)**

  This kind of attack may have far reaching consequences as for instance the **execution of faked commands on MV/LV Substations (ICT-C2)** (see Figure 5-6). The local control functions are not affected.

  Possible **ITC countermeasures (ICT-A2)**:

  - Cryptation
  - Authentication

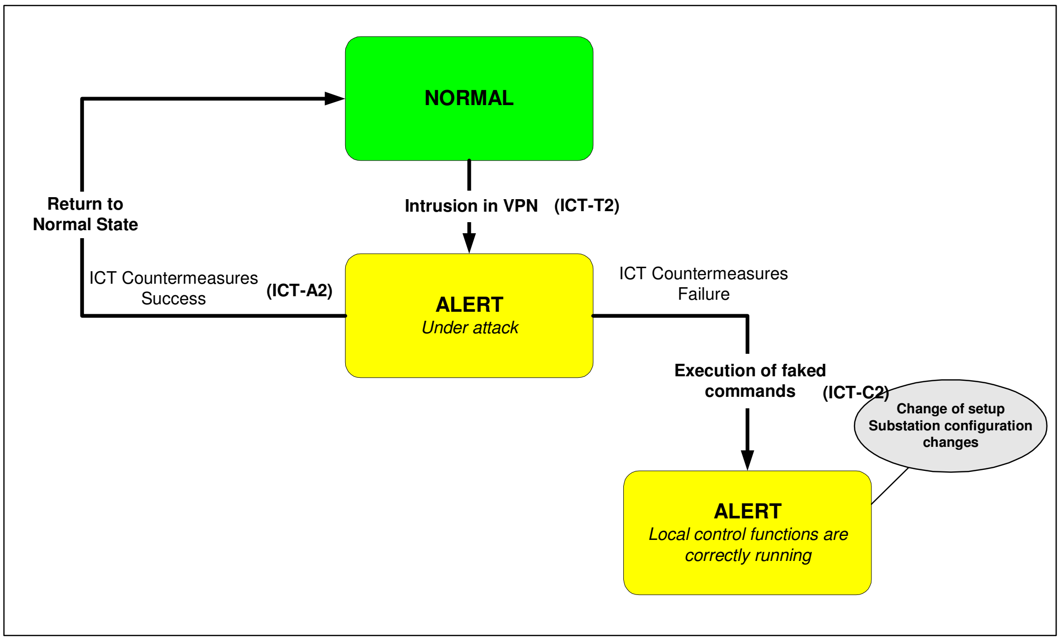

NORMAL
Intrusion in VPN (ICT-T2)
Return to Normal State
ICT Countermeasures Success
(ICT-A2)
ALERT
Under attack
ICT Countermeasures Failure
Execution of faked commands
(ICT-C2)
Change of setup Substation configuration changes
ALERT
Local control functions are correctly running

Figure 5-6: Intrusion on Centre/Substation communication network - Sequence of possible Cascading Effects

- **Viral infection of Substation ICT components (ICT-T3)**

Viral infections may cause the total or partial **loss of control and monitoring functions (ICT-C3)** (see Figure 5-7). This kind of attack affects the local control system; no information or inconsistent information shall be delivered to the ATS.

Possible **ITC countermeasures (ICT-A3)**:

- Antivirus
- Authentication mechanisms on the firewall

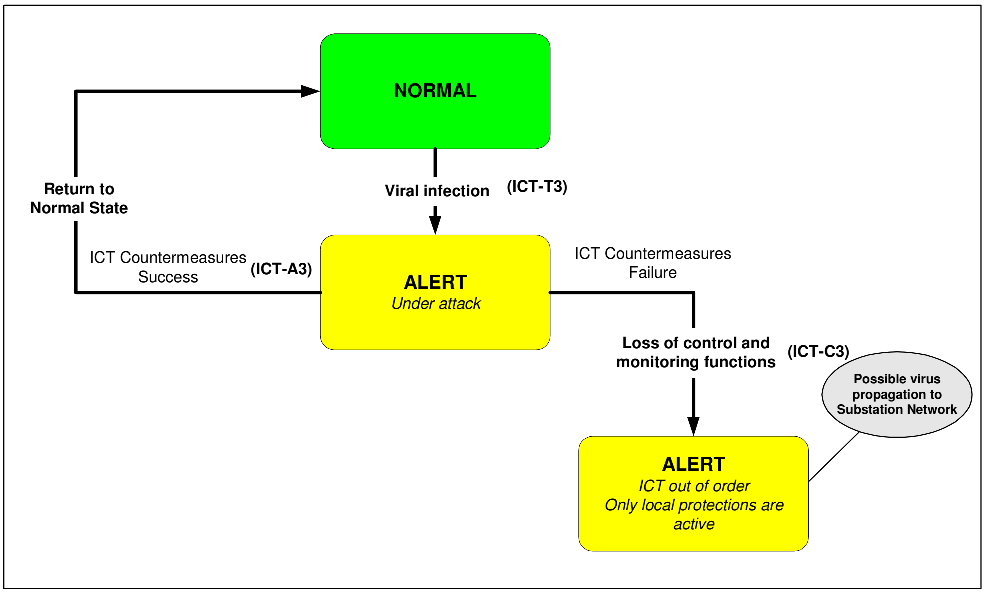

NORMAL
Viral infection
(ICT-T3)
Return to Normal State
ICT Countermeasures Success
(ICT-A3)
ALERT
Under attack
ICT Countermeasures Failure
Loss of control and monitoring functions
(ICT-C3)
Possible virus propagation to Substation Network
ALERT
ICT out of order
Only local protections are active

Figure 5-7: Viral infection of Substation network - Sequence of possible Cascading Effects

- **Authentication violation of the Substation control system (ICT-T4)**

Unauthorised access to the Substation firewall causes **loss of confidentiality of the Substation (ICT-C4)** and opens the way to uncontrolled changes of the set-up parameters (ICT-C3) (see Figure 5-8). The local control functions are not affected.

Automatic application of **ITC countermeasures (ICT-A4)**:

- Enhanced firewall maintenance authentication mechanisms

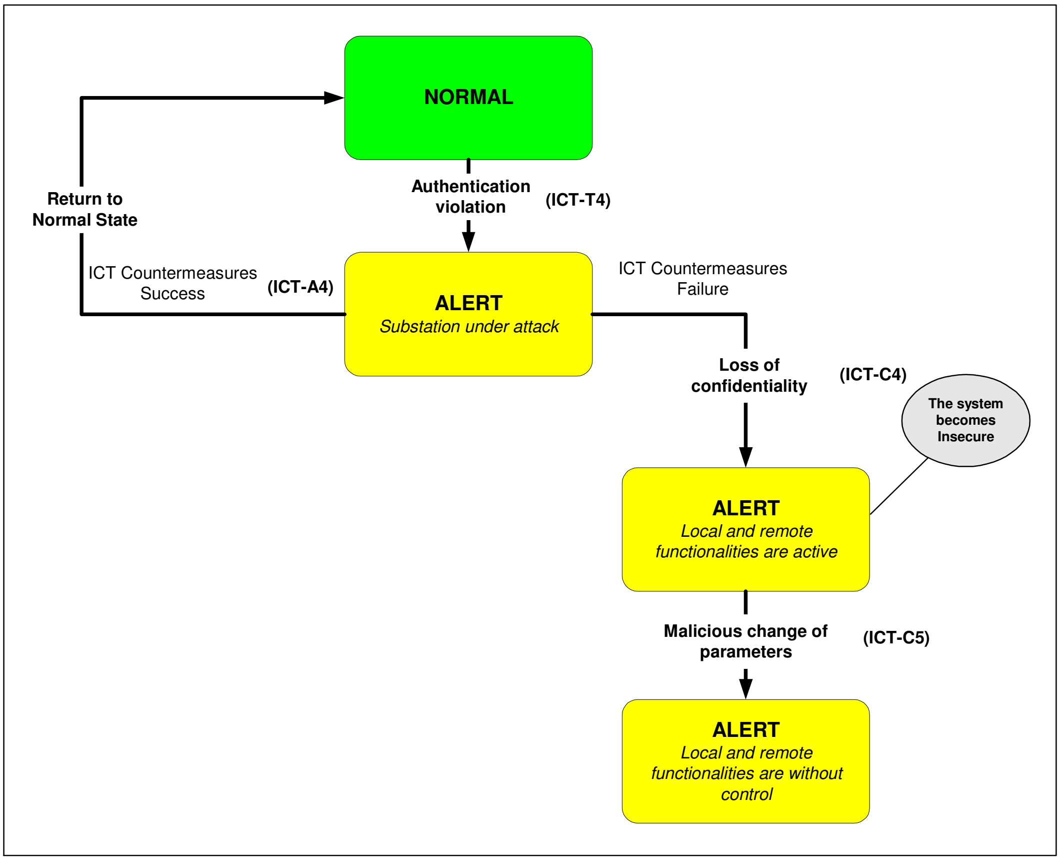

NORMAL
Authentication violation
(ICT-T4)
Return to Normal State
ICT Countermeasures Success
(ICT-A4)
ALERT
Substation under attack
ICT Countermeasures Failure
Loss of confidentiality
(ICT-C4)
The system becomes Insecure
ALERT
Local and remote functionalities are active
Malicious change of parameters
(ICT-C5)
ALERT
Local and remote functionalities are without control

Figure 5-8: Authentication violation of Substation network - Sequence of possible Cascading Effects

The effects on the Power System of the considered ICT attacks depend on the number of Substations involved.

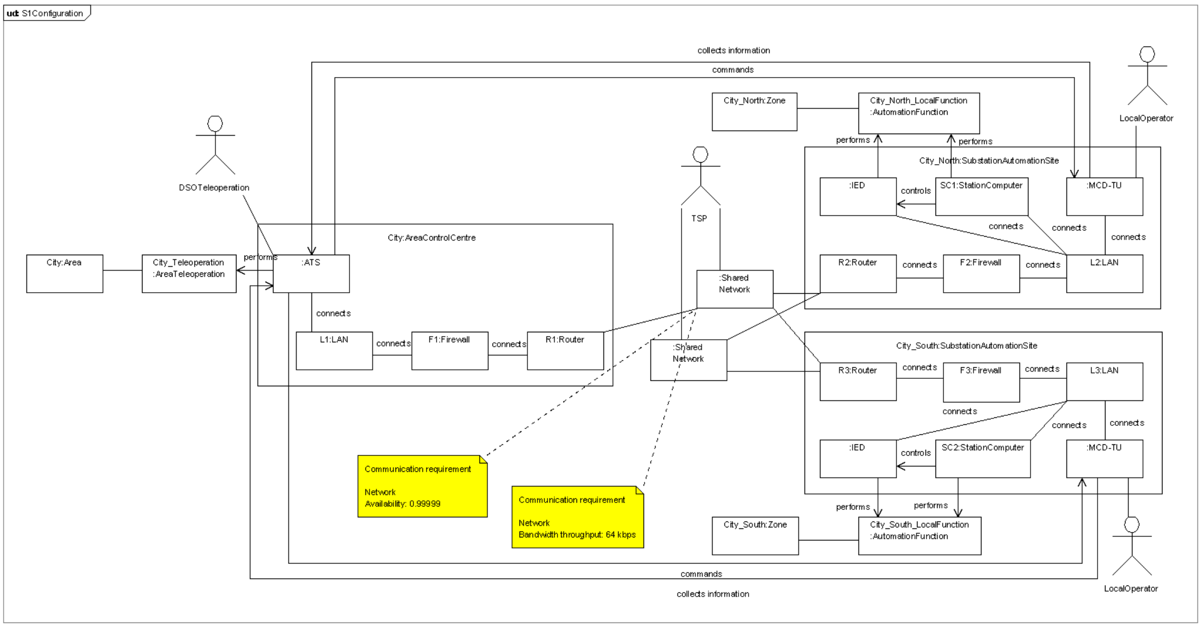
In NORMAL operating condition, an attack to a single Substation will probably not lead to a loss of electrical security N-1 criterion because the control system is intrinsically redundant.

If the attack is aimed at a group of Substations, operating in a specific area, the effects could be the impossibility to withstand the occurrence of an electrical contingency (e.g., line overloads).

5.1.1 Representation of the Scenario by means of UML diagrams

In this section, we propose our approach for the UML representation of control system scenarios. Scenarios were initially textually described; their representation in form of UML diagrams aims to support the textual description by providing a formal graphical notation describing the key aspects of the scenario. The textual description of a scenario puts in evidence the following aspects: control systems, information flow, time requirements, stakeholders, power contingencies, goals, ICT threats, cascading effects.
In our approach, we use several kinds of UML diagram, and we focus on the scenario aspects whose textual description can be enriched by the corresponding UML representation. Each of these aspects is represented by the most suitable form of UML diagram: we resort to object diagrams to represent control systems and information flows; time requirements are indicated by means of comments inside the object diagrams. At the moment, threats are represented as class diagrams. Cascading effects are represented in form of state diagrams.

5.1.1.1 Configuration



Created with Poseidon for UML Community Edition. Not for Commercial Use.

Figure 5-9: Context Diagram

The object diagram in Figure 5-9 shows the elements of the power grid infrastructure involved in the Scenario 1. Such scenario deals with a case of teleoperation between an area control centre and a couple of substation automation sites; the teleoperation activity is performed through the exchange of commands and measures between the area control centre and the substation automation sites.

In Figure 5-9, we have three main objects: *City* of class *AreaControlCenter*, *City_North* and *City_South* of class *SubstationAutomationSite*. Such objects represent a specific area control centre whose area of competence is a certain city, and two substation automation sites concerning the northern zone of the city and the southern zone of the city respectively. The area control centre monitors and controls the substation automation sites.

Two objects of class *SharedNetwork* represent the redundant communication lines realizing the communication between the area control centre and the substations automation sites.

The object *City* of class *AreaControlCentre* (*City:AreaControlCentre*) is composed by several objects: an object of class *ATS* represents the component dedicated to the teleoperation in the area control centre; for this reason, such object is associated with the object *City_Teleoperation:AreaTeleoperation* which is in turn associated with the object *City:Area* in order to indicate that the area control center is involved in the teleoperation activity concerning the city area.

Still inside the object *City*, the object *L1:LAN* represents the local network for the communication inside the area control centre; such object is associated with the object *F1:Firewall* which is in turn associated with the object *R1:Router* in order to represent that the access to the local network of the area control centre is ruled by the router and the firewall of the centre. The object *R1:Router* is associated with the object of class *SharedNetwork* to indicate that the router of the area control centre is the point of connection with the external network.

In a similar way, the object *City_North* is composed by several objects; in particular, the object of class *IED* represents the component dedicated to the teleoperation activities in the substation automation site. The object *SC1:StationComputer* represents the computer dedicated to the control of the IED. Finally, the object of class *MCDTU* represents the MCDTU component inside the substation automation site.

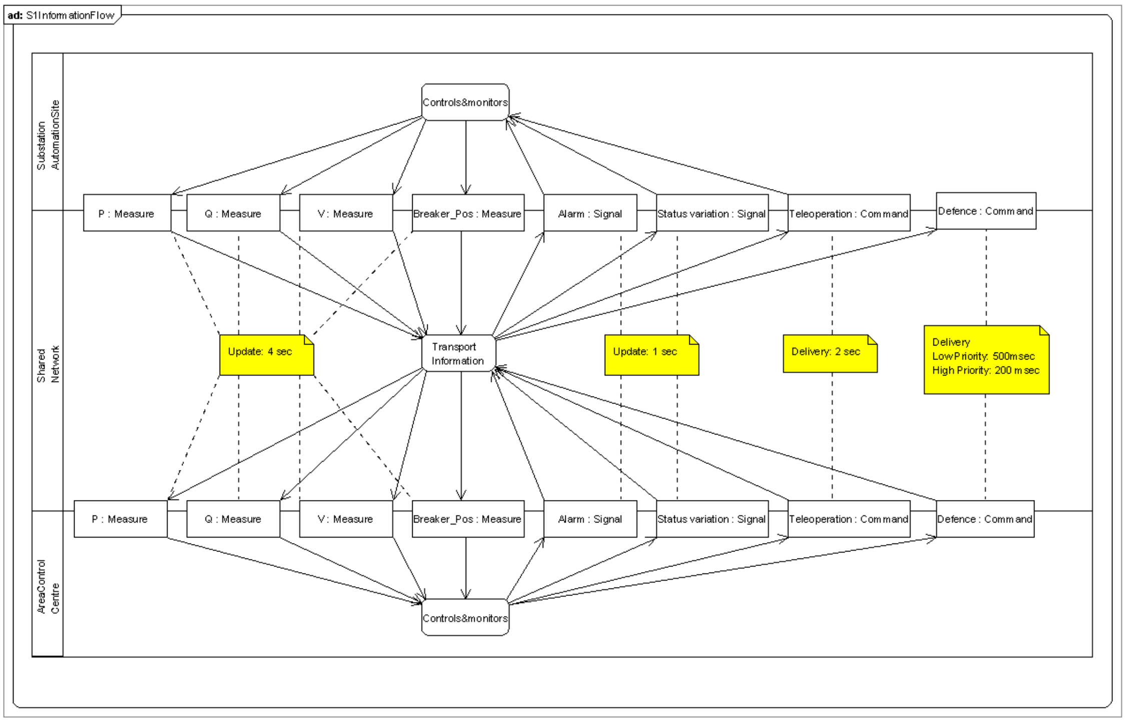
The composition of the object *City_South* reflects the composition of the object *City_North*.

The object of class *ATS* inside the object *City:AreaControlCentre* is associated with the objects of class *MCDTU* inside *City_North:SubstationAutomationSite* and *City_South:SubstationAutomationSite* respectively. This association is due to the fact that the ATS in the area control centre sends commands to the MCDTU components located in the substation automation sites. Another association links the same objects; in this case we represent that the ATS collects information from the MCDTU components.

In the object diagram in Figure 5-9, we also show the operators acting on the teleoperation components located in the area control centre and in the substation automation sites. The operators are represented in form of actors (sticked figures) associated with the objects representing the components influenced by the operators. In particular, in Figure 5-9, the actor *DSOTeleoperator* represents the operator acting on the ATS component in the area control centre, while the actor *LocalOperator* identifies the operators acting on the MCDTU component placed inside the substation automation sites. The communication provider is represented by the actor *TSP* associated with the object of class *SharedNetwork*.

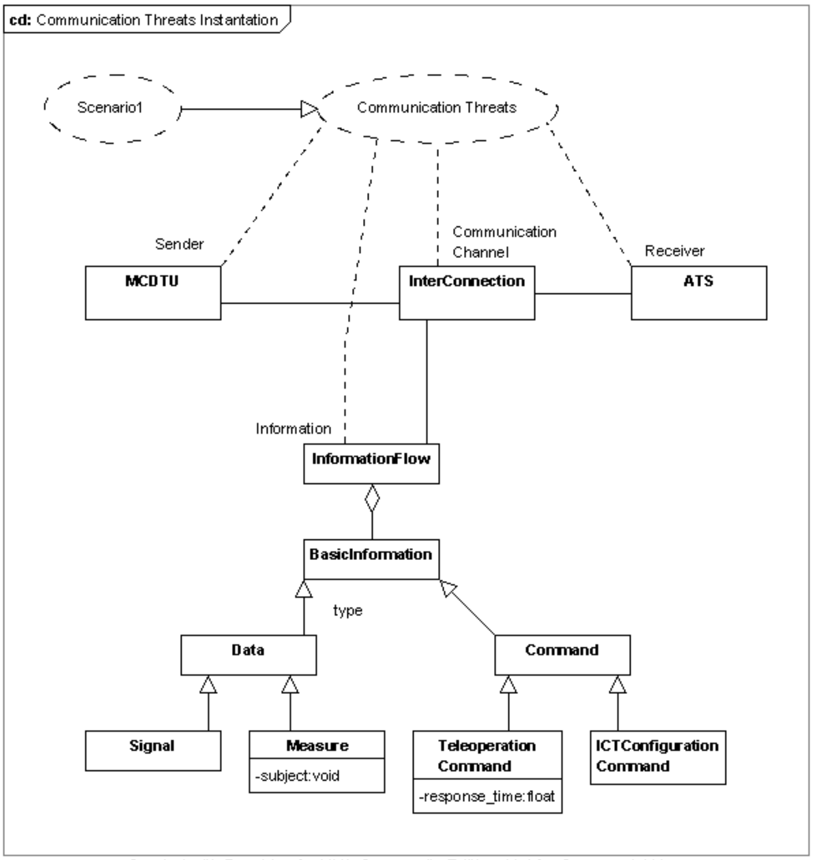
Finally, the comments in the object diagram in Figure 5-9 indicates the communication requirements that the shared network must satisfy (availability and bandwidth throughput).

5.1.1.2 Information Flow



Created with Poseidon for UML Community Edition. Not for Commercial Use.

Figure 5-10: Activity diagram of the information flow in the Scenario 1



Created with Poseidon for UML Community Edition. Not for Commercial Use.

Figure 5-11: Threats instantiation

In Figure 5-11, the scenario 1 is considered as an instantation of the collaboration in Figure 8-18. In Figure 5-11, the classes *MCDTU*, *InterConnection*, *ATS* and *InformationFlow* have the role of *Sender*, *Communication*, *Receiver* and *Information* respectively. The sequence diagrams in the appendix can be referred to this scenario according to such roles. The object *MCDTU* corresponds to the object *Sender* in the sequence diagrams, the object *ATS* corresponds to the object *Receiver* in the sequence diagrams, and so on. The InformationFlow is composed by basic information instances which can be data or commands.

5.1.1.3 Viral Infection

In this section, we represent by means of UML state diagrams, the effects of a denial of service attack influencing the communication inside the teleoperation activity, as described in the Scenario1. The other forms of attack described in the Scenario 1 are represented in section 8.2.7 (appendix).

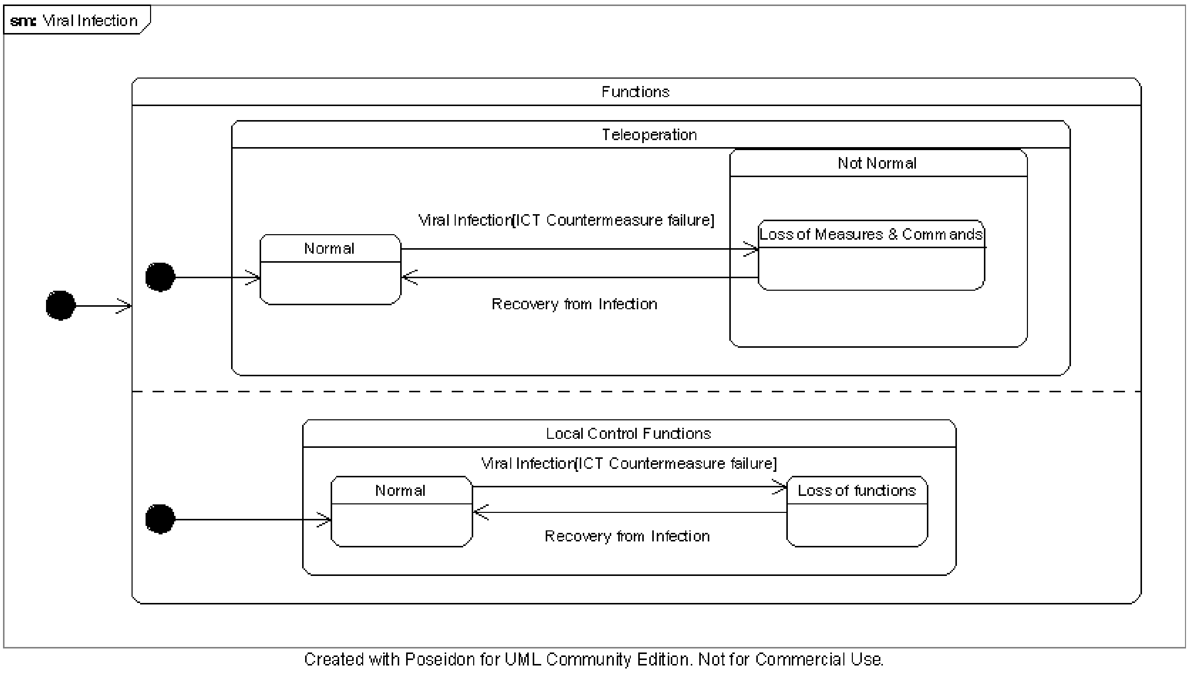

sm: Viral Infection
Functions
Teleoperation
Not Normal
Viral Infection[ICT Countermeasure failure]
Normal
Loss of Measures & Commands
Recovery from Infection
Local Control Functions
Viral Infection[ICT Countermeasure failure]
Normal
Loss of functions
Recovery from Infection
Created with Poseidon for UML Community Edition. Not for Commercial Use.

Figure 5-12: States of the Teleoperation and of the Substation local control functions, in case of viral infection

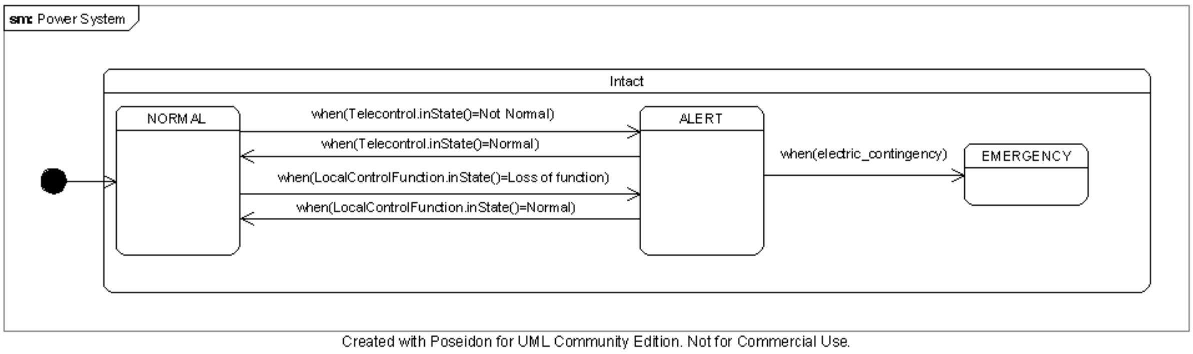

sm: Power System
Intact
NORMAL
when(Telecontrol.inState()=Not Normal)
when(Telecontrol.inState()=Normal)
when(LocalControlFunction.inState()=Loss of function)
when(LocalControlFunction.inState()=Normal)
ALERT
when(electric_contingency)
EMERGENCY
Created with Poseidon for UML Community Edition. Not for Commercial Use.

Figure 5-13: States of the Electric Power System in case of viral infection

The state machine in Figure 5-12 shows the possible states of the Teleoperation and of the local control functions in case of viral infection according to the scenario 1. A viral infection and the failure of the corresponding countermeasure cause the state transition by the Teleoperation, from the state *Normal* to the state *Loss of Measure & Commands*; such state belongs to the global state *NotNormal* of the Teleoperation. The inverse state transition is caused by a recovery action.

The viral infection influences also the state of the local control functions; their transition from *Normal* to *Loss of Functions* is determined by the viral infection combined with the failure of the corresponding countermeasure. A recovery action enables the inverse state transition.

The state transitions in the state machine in Figure 5-13 depend on the state machine in Figure 5-12. In Figure 5-13, the electric power system turns from the state *NORMAL* to the state *ALERT* if the Teleoperation is in state *NotNormal* or if the local control functions are in the state *Loss of Functions* (see Figure 5-12). The transition by the electric power system from *ALERT* to *NORMAL*, occurs in two cases: the state *Normal* of the Teleoperation, or the state *Normal* of the local control functions.

The state transition by the electric power system, from *ALERT* to *EMERGENCY*, occurs in case of electric contingency.

The states *NORMAL*, *ALERT* and *EMERGENCY* compose the global state *Intact* of the electric power system.

5.2 Interaction between TSO and DSO operators in emergency conditions (Scenario 2)

This scenario considers the possible cascading effects due to ICT threats to the communication channel among TSO and DSO Control Centres and MCD-TUs in emergency conditions (under-frequency or voltage instability).

This scenario explores the security of the communications between the Transmission and Distribution System Operators under emergency operating conditions.

It is assumed that in emergency conditions the TSO is authorised by the DSO to activate defence plan actions consisting in the performance of load shedding activities on the Distribution Grid.

The procedure of automatic load shedding must be executed in 1 second. Some special TSO master MCD-TUs arm the DSO MCD-TUs and then automatically send the command of load shedding. The operations are monitored by the ATS and NTS.

Stakeholders involved:

- TSO
- DSO
- TSP of TSO
- TSP of DSO

Information Control Systems involved:

All the telecontrol systems of TSO and DSO are involved (see Figure 5-14):

- NTS (TSO NCC)
- MCD-TU (TSO Substation)
- ATS (DSO CC)
- MCD-TU (DSO Substation)

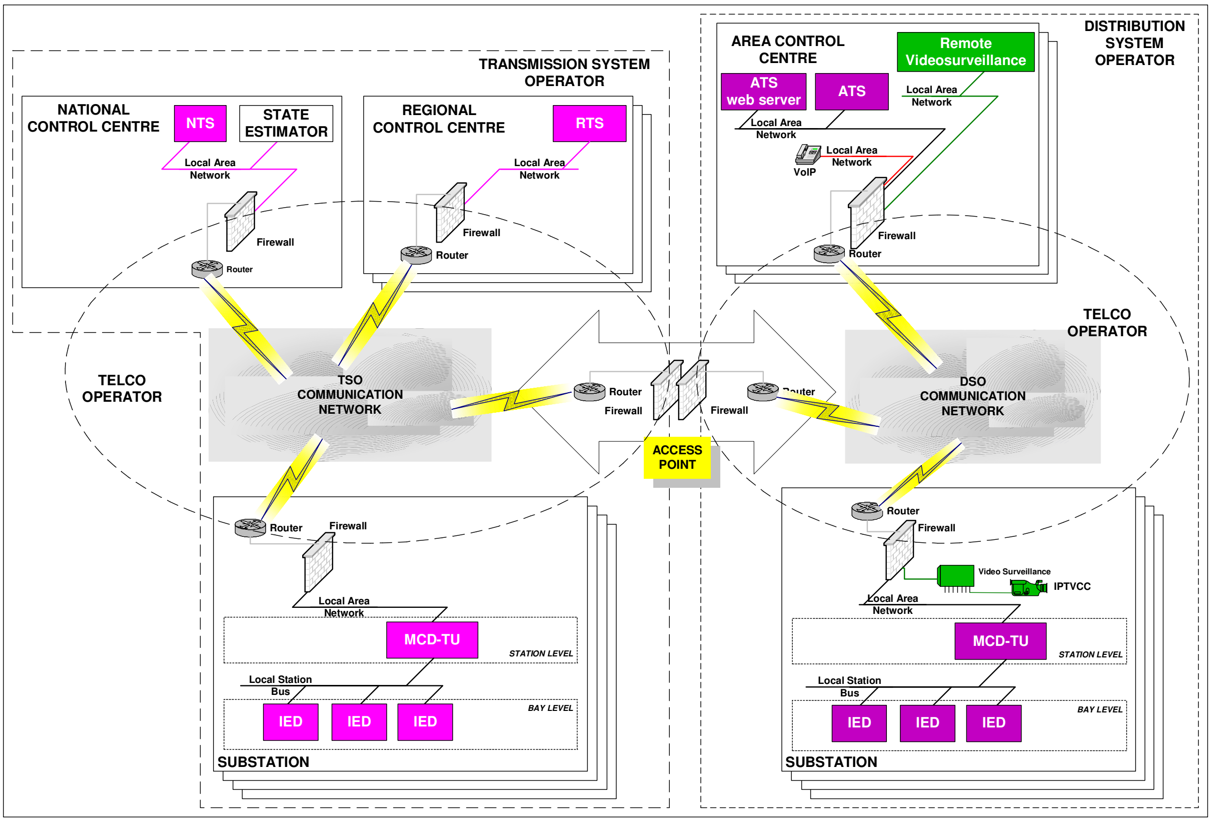


Figure 5-14: TSO and DSO telecontrol systems

Information Flow:

- Measurements from DSO CC to TSO CC
- Signals from DSO CC to TSO CC
- Commands from TSO MCD-TU to MCD-TU through DSO CC
- Arming/unarming requests: from TSO CC to DSO CC.

Real-time requirements:

Commands have a maximum response time of 1 sec. This is the reaction time to the variation of frequency detected by the MCD-TUs (TSO). It is important to notice that delivery time does not exceed 600 ms because the opening of circuit breakers (managed by MCD-TU (DSO)) needs hundred milliseconds.

Power Contingencies:

This scenario explores power contingencies causing load shedding.

Goals:

The main purpose of the Scenario 2 consists in the assessment of the security of the TSO-DSO communications

ICT Threats:

The most plausible ICT threats are:

- ***DoS*** attacks to the Substation Automation Systems, generated by enemies located on the TSO telecontrol backbone

- ***Intrusion*** into the Centre/Substation communication flow followed eventually by the execution of faked commands

Cascading Effects and possible countermeasures:

Cyber attacks carried out under emergency conditions, when defence actions have to be performed out under strict real time constraints, can cause severe damages, like inhibiting the required automatic load shedding actions.

As stated in the Scenario 1 the effects on the Power System of the considered ICT attack depend on the number of components involved.

5.3 Integration of DSO Operation and Maintenance functions (Scenario 3)

This scenario explores the integration of process control and corporate networks in a MV DSO Control Centre, evaluating the possible cascading effects of cyber attacks on the integrated architecture.

It assumes the use of a DSO corporate intranet to access data for:

- Maintenance of MV and LV grid. The maintenance manager needs to know both the status of the Grid and the availability of the maintenance personnel, in order to carry out maintenance plans
- Access to process information by other Corporate functions (administrative, management, metering, …)

Communications are filtered by a central firewall.

Stakeholders involved:

- DSO
- Distribution Maintenance Manager
- TSP of the DSO Process Network
- TSP of the DSO Corporate Network

Information Control Systems involved:

All the ICT systems of DSO are involved (see Figure 5-15):

- ATS (DSO CC)
- Web Server (Corporate)
- Data Archive (Corporate): process data, service data
- MCD-TU (DSO)
- TSP that has in charge the Process Network
- TSP that has in charge the Corporate Network

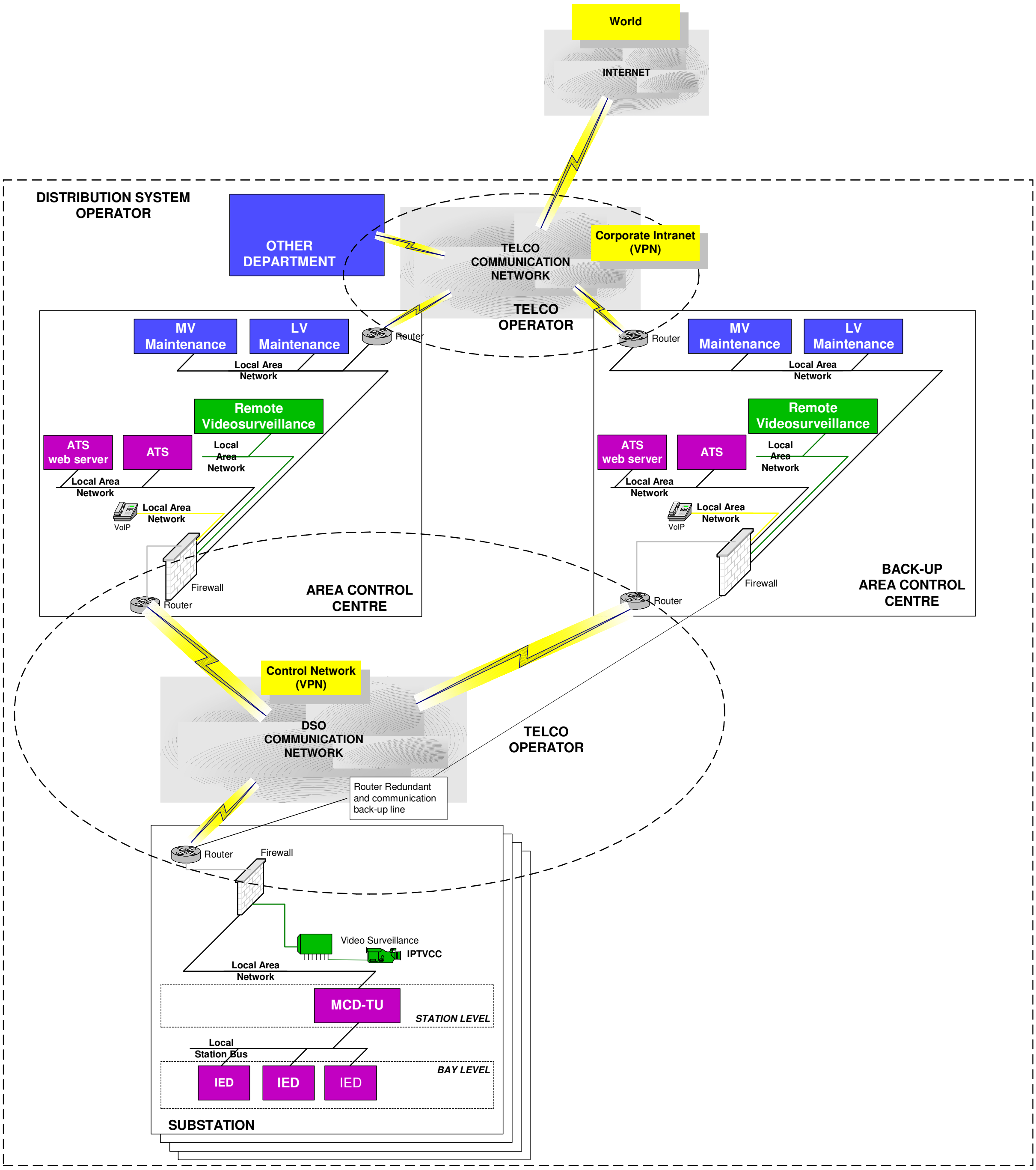


Figure 5-15: Integration of Operation and Management DSO functions

Information Flow:

The information are:

- Measurements
- Signals
- Metering data
- Information are exchanged by means of IP Network based standard protocols:
  - Web Services in case of web applications (e.g. http)
  - SQL queries to access the Data Base

  - Data Exchange protocols (e.g. ftp)

Real-time requirements:

Not relevant.

Power contingencies:

Not relevant.

Goals:

The main purposes of the Scenario 3 are:

- assess the vulnerability of the central firewall in the Control Centre
- test the resilience of the most critical control applications
- assess the possibility of compromising process data

ICT Threats:

The most plausible ICT threats are:

- ***Viral infections*** propagating from the Corporate Network to the Process Network
- ***Vulnerabilities of standard application layer protocols*** (ex. http and ftp) used for power management related communications
- ***Intrusion*** into the databases of the Area Telecontrol System, Metering systems and corruption of process data

Cascading Effects and possible countemeasures:

The occurrence of the considered ICT threats may cause the reduction of the DSO communication bandwidth with degradation in SCADA response time and possible cascading phenomena as in the first scenario and the unavailability or wrong perception of essential data with possibly severe consequences as for instance economic losses due to wrong billing.

As stated in the Scenario 1 the effects on the Power System of the considered ICT attack depend on the number of components involved.

5.4 Maintenance of ICT components of DSO (Scenario 4)

This scenario considers the use of a DSO Centralized ICT maintenance service. It assumes the presence of a central Control Centre for the monitoring and control of the components of all the ICT systems of the Power Utility providing:

- Remote ordinary maintenance activities on the ICT components
- Continuous monitoring of the ICT equipment status, including security monitoring functions
- Repair actions on ICT network and equipment configurations.

Stakeholders involved:

- DSO
- Distribution ICT Manager
- TSP that has in charge the Process Network
- TSP that has in charge the Corporate Network.

Information Control Systems involved:

All the ICT systems of DSO are involved (see Figure 5-16).

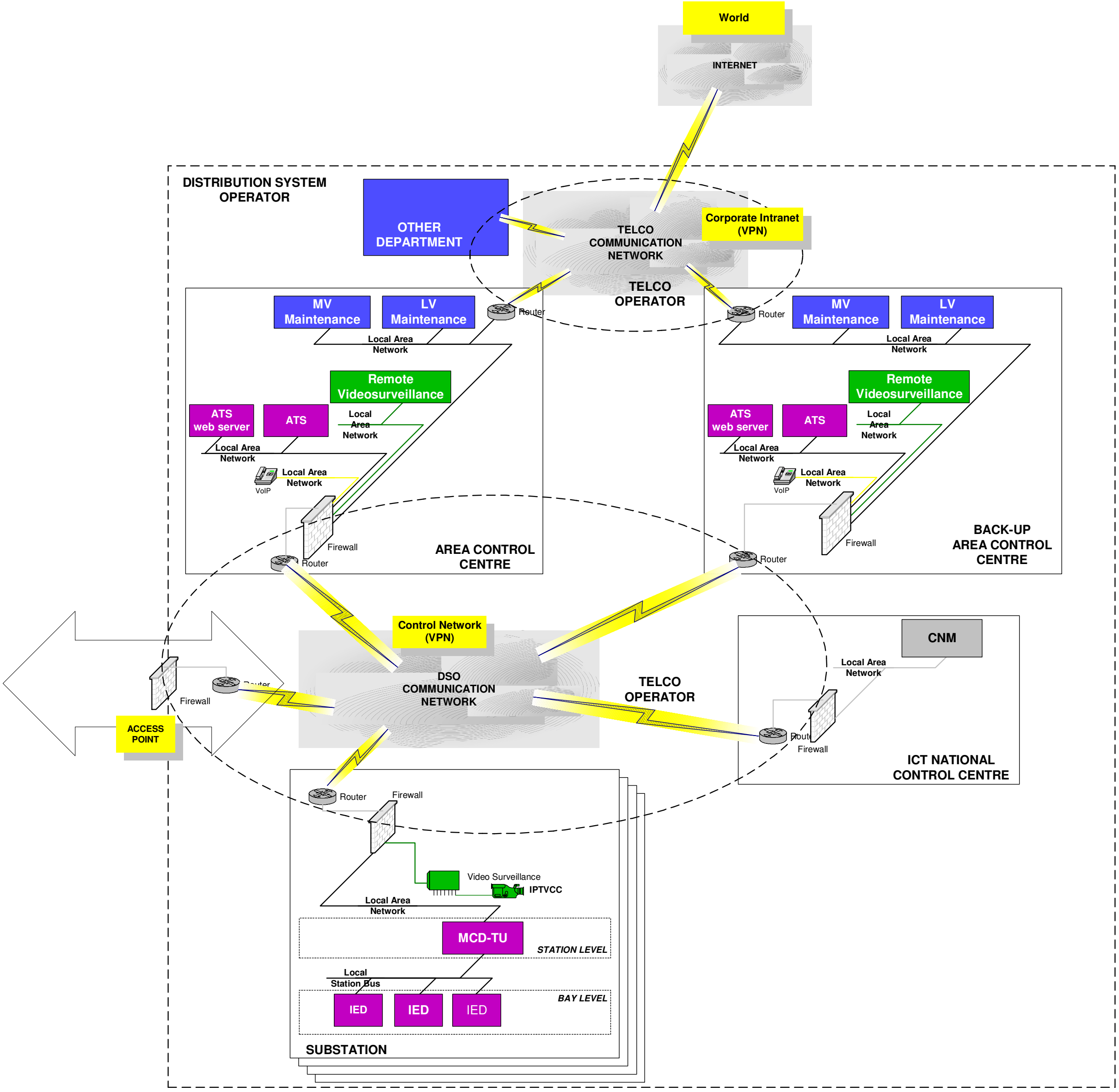


Figure 5-16: DSO Centralised ICT Maintenance

Information Flow:

The information flow interesting maintenance activities includes the transmission of status information towards the Control Centre and the delivery of commands and data related to functional testing and remote operation of ICT devices (e.g. runtime reconfiguration) from the Centre.

Real-time requirements:

Not relevant.

Power contingencies:

Not relevant.

Goals:

The main purposes of the Scenario 3 are:

- assess the remote functional testing and operations on the ICT devices
- assess the remote reconfiguration of the substation automation.

ICT Threats:

The remote maintenance system relies strongly on the internet and is exposed to all possible cyber threats affecting ICT components (e.g. IEDs, Routers, Servers, Firewalls).

Cascading Effects and countermeasures:

The severity of the damage caused by the cyber attacks depends of course on the number of components affected and on their role in the operator's services, with cascading effects having as ultimate consequence the loss of the supervision and monitoring maintenance functions.

5.5 Interaction among GENCOs and TSO for electrical contingency and ICT threats

The important points are those regarding the critical situations in which the system could operate and for which attacks or/and non malicious circumstances could lead to the instability of local systems or, in the worst case, instability of large areas and also of the whole system, as in the black-out of Italy in 2003.

1. Possible instability problems

   a- Instability of the electromechanical mode for:

   a1- PSS (Power System Stabiliser) out of order, by the operator

   a2- very critical grid configuration

   a3- mistakes in the tuning of the PSS parameters.

   b- Voltage collapse, due to too much load in comparison with the available electric power

   c- Instability of inter-area oscillations of the Electric Power System

2- Possible problems with protections

   Some problems can be due to protections as e.g.:

   a- mistakes in the tuning of protection parameters (thresholds, time constants, etc.)

   b- misbehaviour of the protection for lack of coordination or for misunderstanding among protections and the SCADA system

3- Problems due to interdependencies among the transmission grid and the information networks

   a- Communication problems among the different regulators

   b- Mistakes due to malicious attacks to the SCADA of the control room in the power plant

   c- Malicious attacks to the information links inside the Power Plants (AVR and PQR) from power plant to Regional Voltage Regulator(RVR), and the National Voltage Regulator (NVR).

5.5.1 Transmission Grid Voltage and Frequency regulations (Scenario 5)

This scenario considers the possible cascading effects due to :

- ICT threats to the communication channel among TSO Control Centres and GENCOs and to Control Systems used for voltage and frequency regulations
- Measurement failures of TSO and GENCO voltage and frequency regulation systems

5.5.1.1 Hierarchical Voltage and Frequency Regulation Systems (Scenario 5.1)

This scenario (Case 5.1) considers the information exchange among TSO Control Centres and GENCO Power Plant under voltage and frequency regulations of Power System in the NORMAL operating conditions. It ensures the regulation of the Generation Groups of the Power Plant.

The hierarchical voltage and frequency regulation systems allow the TSO to perform voltage and frequency regulations and data acquisition activities of generation groups.

Stakeholders involved:

- GENCO
- TSO
- TSP of GENCO
- TSP of TSO

Information Control Systems involved:

The Voltage and Frequency regulation systems of TSO and GENCO involved are (see Figure 5-17):

- AVR (GENCO)
- PQR (GENCO)
- RVR (TSO RCC)
- NVR (TSO NCC)
- PFR (GENCO)
- SFR (TSO NCC)

The Teleoperation systems involved are (see Figure 5-17):

- SCADA (GENCO)
- RTS (TSO RCC)
- NTS (TSO NCC)

Component involved are (see Figure 5-17):

- MCD-TU (GENCO proprietary Substation)
- MCD-TU (TSO Substation)

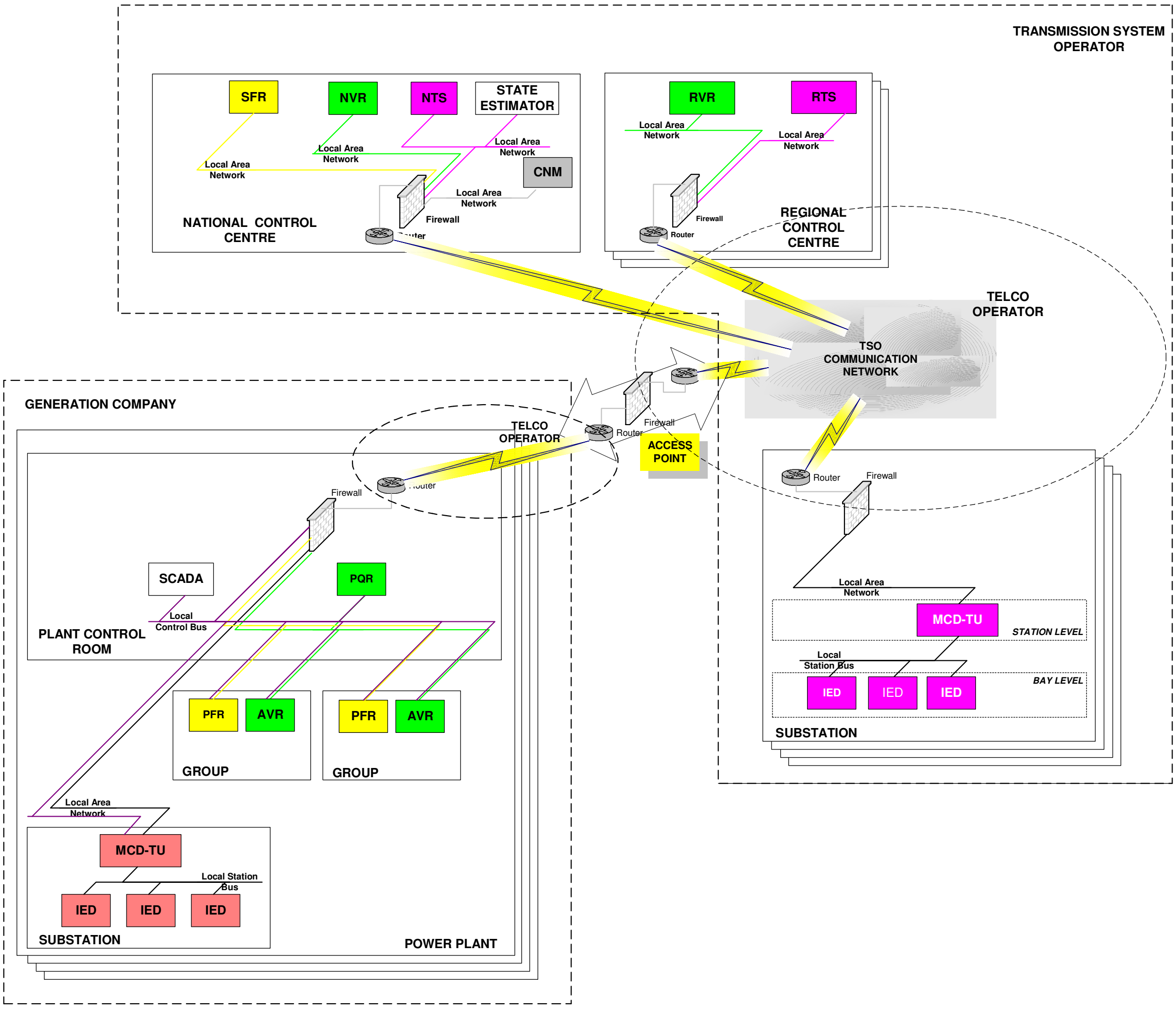


Figure 5-17: Interaction between TSO and GENCO regulation systems

Information Flow:

- Measurements: from AVR and PQR to SCADA, RVR and RTS; from PFR to SFR
- Signals:
  - regulation levels from PQR to AVRs; from AVRs and PFRs to generators
  - alarms from AVRs to PQRs; from PQRs to RVR; from RVRs to NVR; from PFRs to SFR
- Commands:
  - frequency and voltage regulation levels from TSO NVR to RVRs; from RVRs to PQRs; from PQR to AVRs; from TSO SFR to PFR
  - inclusion/exclusion of GENCO groups in TSO frequency or voltage regulations
  - variation of transformation ratio (ULTC)

Real-time requirements:

Commands have a response time within the time required by PQR, AVR, RVR and NVR and SFR and PFR.

Goals:

The main purpose of the scenario is to assess the security of the TSO-GENCO communications.

ICT Threats:

The most plausible ICT threats are:

- ***DoS*** attacks to the telecontrol communications, generated by enemies located on the Telecom IP backbone or inside the TSO (e.g. connection requests on the port used by the IEC protocol)
- ***Intrusion*** into the Regional Centre/Power Plant communication flow followed by the execution of faked commands (sending wrong set-up parameters)
- ***Intrusion*** into the Regional Centres/National Centres communication flow followed by the execution of faked commands (sending wrong set-up parameters)
- Exploitation of the ***vulnerabilities of the standard application layer protocols*** (e.g., http and ftp) used for supervision and monitoring activities
- ***Viral infections*** of System computers provoked by:
    - Voluntary diffusion/propagation during maintenance of SCADA
    - Involuntary propagation using external PC for maintenance

Cascading Effects:

Referring to the ICT components involved in the Control Systems are depicted the consequences of each threats:

- **DoS attack on the VPN that connect TSO to a GENCO (ICT-T1)**

  This attack reduces the communication bandwidth with consequent partial or complete **loss of remote voltage control functions (ICT-C1)** (due to the consumption of communication bandwidth that cause delay or black-out to delivery of measurements to RVR, NVR, SFR and ATS and to receive of commands from RVR, NVR and SFR) and transition in ALERT situation (with extreme consequence the loss of electrical security N-1) (see Figure 5-5). The local control functions are not affected, but there are:

    - Lack of measurements from AVR, SCADA, PQR, PFR to the RVR, NVR, SFR and ATS
    - Lack of receiving commands from NVR, RVR, PQR and SFR

  The targets of an attack could be:

    - a PQR: in this case the effect is the loss of remote control of some generation groups
    - a RVR: this is the worst case in which there is as possible effect the loss of remote voltage control of a large area

  Possible **ITC countermeasures (ICT-A1)**:

    - Firewalling
    - Monitoring of anomalous packets traffic (increasing amount of packets and proactive verification of their contents)
    - Redundancy of communication channel

- **DoS attack on the VPN that connect the TSO centres (ICT-T1)**

  This attack reduces the communication bandwidth with consequent partial or complete **loss of remote voltage control functions (ICT-C1)** (due to the consumption of communication bandwidth that provoke delay or black-out of delivery of measurements to RVR and NVR and of receive of commands from NVR) and transition in ALERT situation (with extreme consequence the loss of electrical security N-1) (see Figure 5-5). The local control functions are not affected, but there are:

- Lack of measurements from ATS to NTS and RVR to NVR
- Lack of receiving commands from NVR

The targets of an attack could be:

- a RVR: in this case the effect is the loss of remote voltage control of an area
- the NVR: this is the worst case in which there is as possible effect the loss of remote control of the entire nation in term of optimization of pilot node voltages.

Possible **ITC countermeasures (ICT-A1)**:

- Firewalling
- Monitoring of anomalous packets traffic (increasing amount of packets and proactive verification of their contents)
- Redundancy of communication channel

- **Intrusion into the Centre/Power Plant communication network (ICT-T2)**

  This kind of attack may have far reaching consequences as for instance the **execution of faked commands on PQR (ICT-C2)**, as receiving wrong PQR set-up parameters (see Figure 5-6) and transition in ALERT situation (with extreme consequence in case of generators tripping). The local control functions are ensured.

  Possible **ITC countermeasures (ICT-A2)**:

  - Cryptation
  - PQR/RVR authentication mechanisms

- **Intrusion into the Regional Centre/National Centre communication network (ICT-T2)**

  This kind of attack may have far reaching consequences as for instance the **execution of faked commands on RVR (ICT-C2)**, as receiving wrong RVR set-up parameters (see Figure 5-6) and transition in ALERT state (with an extreme consequence in case of generators tripping). The local control functions are ensured.

  Possible **ITC countermeasures (ICT-A2)**:

  - Cryptation
  - RVR/NVR authentication mechanisms

- **Viral infection of the ICT components (ICT-T3)**

  Viral infections may cause the total or partial **loss of control and monitoring functions (ICT-C3)** (see Figure 5-7). The local control functions are not ensured and the Power Plant risks the generation trip. There are:

  - Lack of measurements from SCADA, PQR to the RVR, NVR and ATS, from PFR to SFR
  - Lack of receiving commands from RVR, NVR and SFR
  - Lack of signals from PQR to AVRs and SFR to Generators

  Possible **ITC countermeasures (ICT-A3)**:

  - Gateway antivirus
  - Authentication mechanisms of firewall

- **Authentication violation of TSO network (ICT-T4)**

  Unauthorised access causes **loss of secure access to the GENCOs (ICT-C4)** PQR component functions (see Figure 5-8). The local control functions are ensured, but is possible an:

  - Uncontrolled changing of some PQR set-up parameters (ICT-C4)

  Automatic application of **ITC countermeasures (ICT-A4)**:

  - Firewall maintenance authentication mechanisms
  - PQR maintenance authentication mechanism

The effects on the Power System of the considered ICT attacks depend on the number of components involved.

In NORMAL operating conditions, an attack to a single PQR or SFR probably there is not lead a loss of electrical security N-1 criterion because the control system is intrinsically redundant.

If the attack is to a RVR or NVR and SFR, that manage a specific area, the effects are the loss of possibility to manage other electrical contingency (e.g., line overloads) with transition to ALERT operating state.

5.5.1.2 Protection intervention due to erroneous measurements (Scenario 5.2)

This scenario (Case 5.2) considers in the NORMAL or EMERGENCY Power System operating state the possible measurement failures of generation and transmission systems. The protection intervention ensures the second line of defence of the Power System. The protection intervention depends on measurements acquired.

The incorrect intervention of protections mechanism, due to erroneous measurements, may cause consequences similar to the electrical contingencies.

The protections are programmed with thresholds and algorithms.

The use of digital equipment to acquire measurements and elaborate them using algorithms that are tuned using PCs is now widespread.

Stakeholders involved:

- GENCO
- TSO
- TSP of GENCO
- TSP of DSO

Information Control Systems involved:

All the regulation systems of GENCO and DSO are involved (see Figure 5-17):

- AVR (GENCO)
- PQR (GENCO)
- RVR (TSO RCC)
- NVR (TSO NCC)
- PFR (GENCO)
- SFR (TSO NCC)

The Teleoperation systems involved are (see Figure 5-17):

- SCADA (GENCO)
- RTS (TSO RCC)
- NTS (TSO NCC)

Component involved are (see Figure 5-17):

- MCD-TU (GENCO proprietary Substation)
- MCD-TU (TSO Substation)

Information Flow:

- Measurements from MCD-TU to SCADA and RTS, from AVR to PQR and RVR, NVR, from PFR to SFR
- Signals from PFR and AVR to Generators
- Commands from RTS and NTS to MCD-TU, from NVR and RVR to PQR, form SFR to PFR

Real-time requirements:

Not relevant.

Power Contingencies:

The power contingencies considered for this scenario are related with the failure of protections in NORMAL and EMERGENCY conditions.

Goals:

The main purpose of the scenario is to assess the security of the Protection configuration.

ICT Threats:

The most plausible ICT threats are:

- ***DoS*** attacks on the telecontrol communications, generated by enemies located on the Telecom IP backbone or inside the TSO (e.g. connection requests on the port used by the IEC protocol)
- ***Intrusion*** into the National Centre/Power Plant communication flow followed by the execution of faked commands (send of wrong set-up parameters)

Cascading Effects and possible countemeasures:

Referring to the ICT components involved in the Control Systems are depicted the consequences of each threat:

- **DoS attack to the VPN that connect TSO to a GENCO (ICT-T1)**

  This attack reduces the communication bandwidth causing partial or complete **loss of remote control functions (ICT-C1)** (due to the consumption of communication bandwidth that provoke delay or black-out to delivery of measurements to RVR and SFR and to receive of commands from RVR and SFR) and transition in ALERT situation (with extreme consequence the loss of electrical security N-1) (see Figure 5-5). The local control functions are ensured, but there are:

  - Lack of measurements from SCADA, PQR and PFR to the NTS, RVR and SFR
  - Lack of receiving commands from SFR

The targets of an attack could be:

- a PFR: in this case the effect is the loss of frequency remote control of some generation groups
- a SFR: this is the worst case in which there is as possible effect the loss of frequency remote control of a large area
- a PQR: only one power plant is affected
- a RVR: in this case the effect is the loss of voltage remote control of an area
- the NVR: this is the worst case in which there is as possible effect the loss of optimal voltage remote control of the entire nation

Possibly **ITC countermeasures (ICT-A1)**:

- Firewalling
- Monitoring of anomalous packets traffic (increasing amount of packets and proactive verification of their contents)
- Redundancy of communication channel

- **Intrusion into the National Centre/Power Plant communication network (ICT-T2)**

  This kind of attack may have far reaching consequence as for instance the **execution of faked commands on NVR, RVR and PFR (ICT-C2)**, as receiving wrong RVR and PFR set-up parameters (see Figure 5-6) and transition in ALERT situation (with extreme consequence in case of generators tripping). The local control functions are ensured.

  Automatic application of **ITC countermeasures (ICT-A2)**:

  - Cryptation
  - NVR/RVR/PQR and /PFR/SFR authentication mechanisms

The effects depend on the number of components attacked. If we consider, in NORMAL operating state, an attack to a single PQR and PFR probably there is not a loss of electrical security N-1 because the protection system is designed intrinsically redundant. If the attack is to a RVR or SFR, that manage a specific area, the effects are the loss of possibility to manage other electrical contingency (e.g., line overloads) with transition to ALERT operating state.

The ICT threats are assumed to happen in presence of the power contingency described in the scenario. The magnified effects of ICT threats are strictly depending on the kind of attack and the instant in which is performed:

- during the manual load shedding actions (see state diagram)
- by provoking a wrong intervention of protections

5.5.2 Instability of Electromechanical Mode of Power Plant-Transmission Grid Systems (Scenario 6)

This scenario considers the possible cascading effects due to :

- Specific abnormal operating conditions of the system constituted by a Power Plant and the transmission grid, which is related to the electromechanical oscillation mode
- ICT threats to GENCO Control Systems used for voltage and frequency regulations.

5.5.2.1 Instability of Electromechanical Mode management (Scenario 6.1)

This scenario (Case 6.1) considers specific abnormal operating conditions of the system constituted by a Power Plant and the transmission grid, which is related to the electromechanical oscillation mode (see section 3.3.2).

The electromechanical oscillation mode can become unstable for:

a) very high value of the external reactance Xe as a consequence of an abnormal network configuration

b) wrong parameters of the PSS (Power System Stabiliser), that is the additional feedbacks of the excitation regulation system

Another way through which the electromechanical oscillation mode can become unstable is by ***predatory control*****,** this type of control is described in [DeMarco & Braden 2006]. This paper evidenced the possibility to destabilise a Power Plant through a special state control from another Power Plant.

Case a:

In this situation some **change in the grid configuration (C1)** could bring the electromechanical mode of power plant-transmission grid system to be unstable in some operating conditions, especially during the night when the reactive power must be absorbed by the power plants and the generators are in under-excitation.

Let us now describe some worst case evolutions of cascading effects taking into account that the propagation of the effects happens when a given defence action does not work due to some device malfunction.

Starting from the system in the operation state **NORMAL** (see **Figure** 3-1), the system pass to the **ALERT** state.

If the contingency provoking the alerting condition is removed (the **grid configuration is recovered (A1)**) the system state returns to **NORMAL**.

Otherwise the unstable condition has kept so a **disturbance on the grid** or on the ICT system leads to have electromechanical oscillations higher and higher leading to the **trip of the power plant (C2)** under consideration. So probably the **electrical security N-1 has been lost** and the system shifts to the **EMERGENCY** state.

This is a typical case in which the first line of defence (constituted by the regulation and control systems) becomes not adequate, because the values of the PSS parameters are not adequate for the new abnormal value of the external reactance to face all the variations in the operating conditions of the power plant.

From the EMERGENCY state the system may pass to the ALERT/NORMAL state by means of the intervention of the **spinning reserve power (A2)**, depending on the amount of available reserve power and on the instability removal. In parallel to the reserve management there is the activity of the Secondary Frequency Regulator (SFR).

In case the regulation performed by means of the reserve intervention and the SFR does not succeed the system may observe a **decrease in the value of the frequency (C2)**.

To react to the decrease in the frequency the TSO puts in operation the normal actions of defence that are based on **automatic load shedding (A3)** in under-frequency conditions, in order to achieve the equilibrium between energy produced and the loads.

However, from statistical data, it has been proved that 15% of the automatic load shedding devices do not work correctly once activated.

If these automatic actions are not able to regain the NORMAL/ALERT state of the system then it will be necessary to take additional emergency actions based on **manual load shedding (A4)**.

In particular load conditions, as during the night and in ferial days, the **voltage values could be too high (C4)** on the HV and EHV grid, which could damage the isolation of the components. In the meanwhile the synchronous generators are called to operate at under-excitation limits with consequently reduction of system wide transmission stability of the whole electric grid, generally speaking the stability margin is lower in correspondence of negative reactive power production.

To avoid reductions in the interconnection of the grid it is possible manually introduce some **shunt reactances (A5)**, which have the goal to absorb reactive power for:

- reduce the values of voltage
- to lead the synchronous generators in more stable operating conditions

If the situation becomes very critical it is possible to have the **reductions in the interconnection of the grid (C5)**. This situation is defined **IN EXTREMIS** state (**island operation state).**

Case b:

This case involves AVR, in particular the additional feedbacks (or **PSS**), that could receive wrong set up parameters (eventually due to some intrusion through the AVR Engineering HMI or through the PQR or the GENCO-SCADA system) and/or **generate erroneous regulation signals (C1)**.

The instability of the electromechanical mode will provoke the **group trip (C2)**. The first action to **compensate the lost power of the group (A2)** under consideration is constituted by the Primary Frequency Regulators (PFR) of the other groups of the power plant . They will try to recover by producing the lost power. In the case that this action is not sufficient the spinning **reserve power (A3)** management will come into action to return the system to the ALERT/NORMAL state. It is assumed that this last intervention is sufficient to face the power contingency, otherwise it is necessary to return to the evolution of **underfrequency (C3)** contingency described for the case a).

Stakeholders involved:

- GENCO
- TSO

Information Control Systems involved:

In case b all the GENCO telecontrol systems are involved (see Figure 5-18):

- SCADA: Power Plant supervision
- AVR: voltage regulators
- PQR: reactive power regulator and bus bar voltage regulator

In order to manage the load shedding the TSO telecontrol system is involved and also it is necessary a direct communication with DSO local Substation management units (see Figure 5-14):

- MCD-TU (TSO and DSO Substation): that manage the automatic load shedding
- RTS, NTS: that manage the manual load shedding

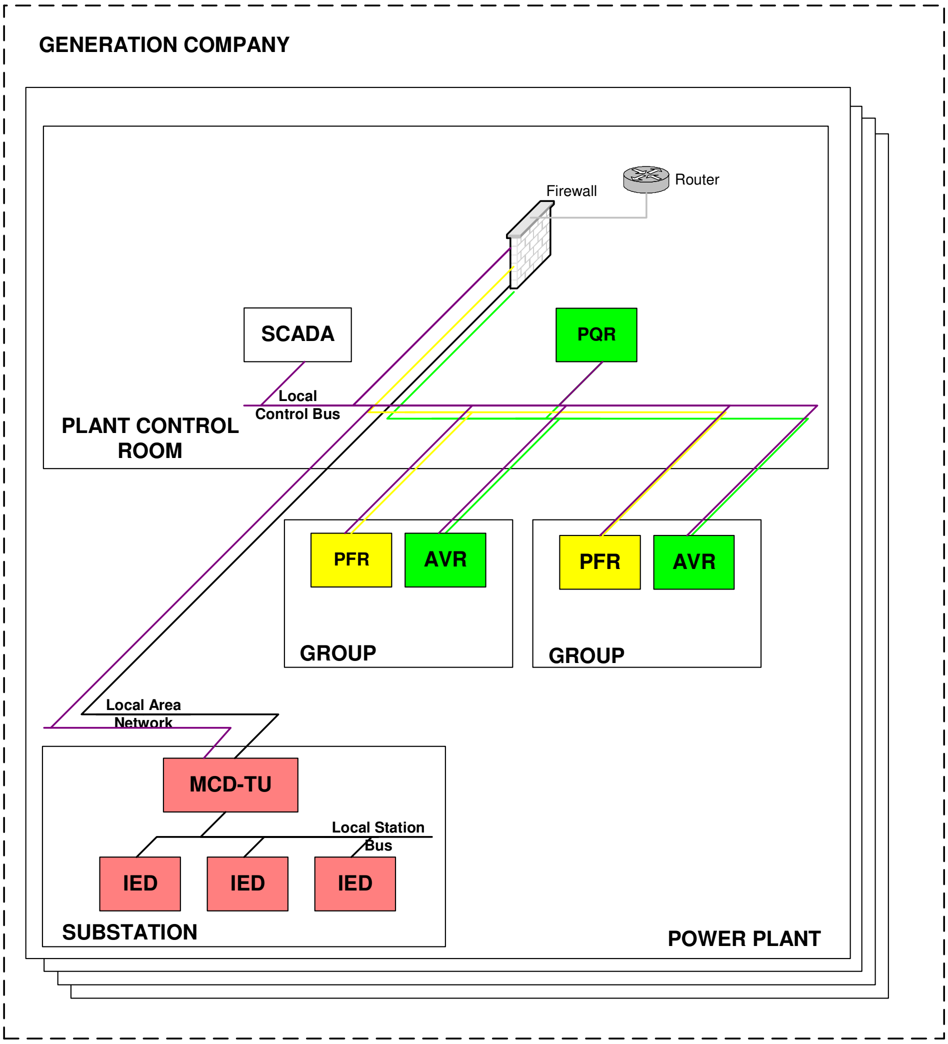


Figure 5-18: ICT systems involved in GENCO Teleoperation and Control

Information Flow:

The information flows are in:

- ***Case a:*** involves MCD-TU, RTS and NTS:
  - Measures:
    - V_i, I_i, P_i, Q_i and δ_i , with i= 1…..N groups, from the AVR of each group to PQR and SCADA
    - V_i, I_i, P_i, Q_i and δ_i, with i= 1…..N groups, from SCADA to RVR inside the RTS
    - $V_{Bus\text{-}bar}$ and V_{Pilot} from MCD-TU to RVR inside the RTS
  - Signals: alarms from MCD-TU to RTS and NTS
  - Commands:
    - from RVR to adjust the reactive power reference for the PQR
    - from NVR adjust the pilot nodes voltage reference for the RVR
    - from RTS and NTS to MCD-TU for:
    - manual load shedding

        - insertion of shunt reactances

- ***Case b***: involves AVR with PSS, PQR, PFR, SCADA, RTS and NTS:
    - Measures:
        - V_i, I_i, P_i, Q_i and δ_i, with i= 1…..N groups, from the AVR of each group to PQR and SCADA
        - V_i, I_i, P_i, Q_i and δ_i, with i= 1…..N groups, from SCADA to RVR inside the RTS
        - f_{ref} and f from each PFR to SCADA
        - $V_{Bus\text{-}bar}$ from MCD-TU to PQR and RTS
    - Signals: alarms from MCD-TU to RTS and NTS
    - Commands:
        - from PQR to adjust the reference of each AVR
        - from RVR to adjust the reactive power reference for the PQR
        - from NVR adjust the pilot nodes voltage reference for the RVR
        - from RTS and NTS to MCD-TU for:
        - manual load shedding
        - insertion of shunt reactors

Real-time requirements:

Commands have a maximum response time of 1 sec.

Power contingencies:

This scenario explores the consequences of an abnormal network configuration due to a very high value of the external reactance Xe.

Goals:

The main purpose of the scenario is to show the interdependencies among the macro-parts of the Power Infrastructure, e.g., how a power disturbance may propagate from the Grid to the Power Plant causing the generators to trip and this situation requires an intervention of TSO to avoid an under-frequency situation that could cause a disconnection of a part of the Grid.

ICT Threats:

The most plausible ICT threats are:

- ***Viral infections*** propagating from the PQR and SCADA PCs through the Local Area Network. Infection diffuses by PC used for maintenance or other PC on the network.
- ***Intrusion*** into the local Power Plant and TSO Centre/Power Plant communications flow followed by the execution of faked commands (like modify parameters settings)
- ***DoS*** attacks to the telecontrol communications, generated by enemies located on the Power Plant, Telecom IP backbone or TSO centres

The effects of threats are strictly depending on the instant in which they are performed:

- The ICT threats are assumed to happen in presence of the power contingency described in the scenario Case 6.1 a). In particular they occur during the manual load shedding actions (see state diagram).

- The ICT threats are assumed to happen in presence of the power contingency described in the scenario Case 6.1 b), by provoking a wrong intervention of the PFRs.

Cascading Effects and possible countermeasures:

In Figure 5-19 and Figure 5-20, referring to the state of the Power System (see Figure 3-1) are depicted possible sequences of the cascading effects that may collapse into an *IN EXTREMIS* situation.

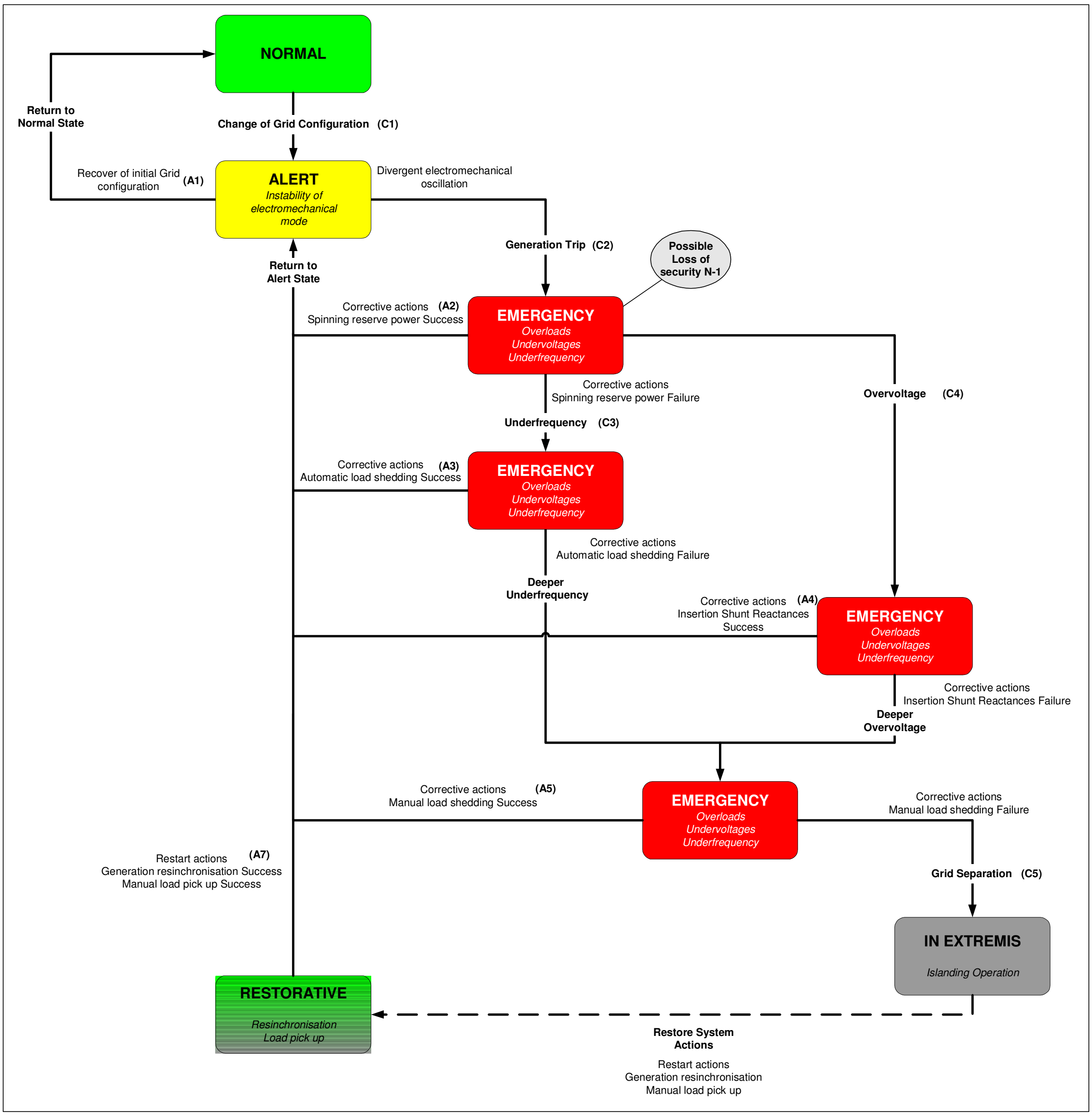


Figure 5-19: Instability of electromechanical mode Case a) - Sequence of possible Cascading Effects

Regarding this sequence (case a) the state transitions are generated by:

- **Change of grid configuration (C1)** with consequent changing of grid Xe parameter in NORMAL situation, and so the system moves to ALERT state automatic applying a set of regulation actions. If the **grid configuration is restored (A1)** the system return into NORMAL state.

- **Generators trip (C2)** with consequent possible loss of electrical security N-1 and transition from ALERT to EMERGENCY power system state. Automatic application of preventive actions:
  - **Spinning reserve power (A2)**
- **Decrement of frequency (C3)** with consequent maintaining of state of EMERGENCY situation. Automatic applying of corrective actions:
  - **Automatic load shedding (A3)**

  Manual application of corrective actions:
  - **Manual load shedding (A4)**
- **Over-voltage (C4)** with consequent maintaining of state of EMERGENCY situation. Manual applying of corrective actions:
  - **Manual activation of shunt reactance (A5)**
  - **Manual load shedding (A4)**
- **Separation of grid (C5)** with consequent formation of system islands, transition in IN-EXTREMIS situation. Automatic application of corrective actions in order to ensure the islands are:
  - Regulation of reserve back up generation
  - Automatic load shedding

In conditions where the Grid is not intact, the restoration actions start. These actions are managed by TSO.

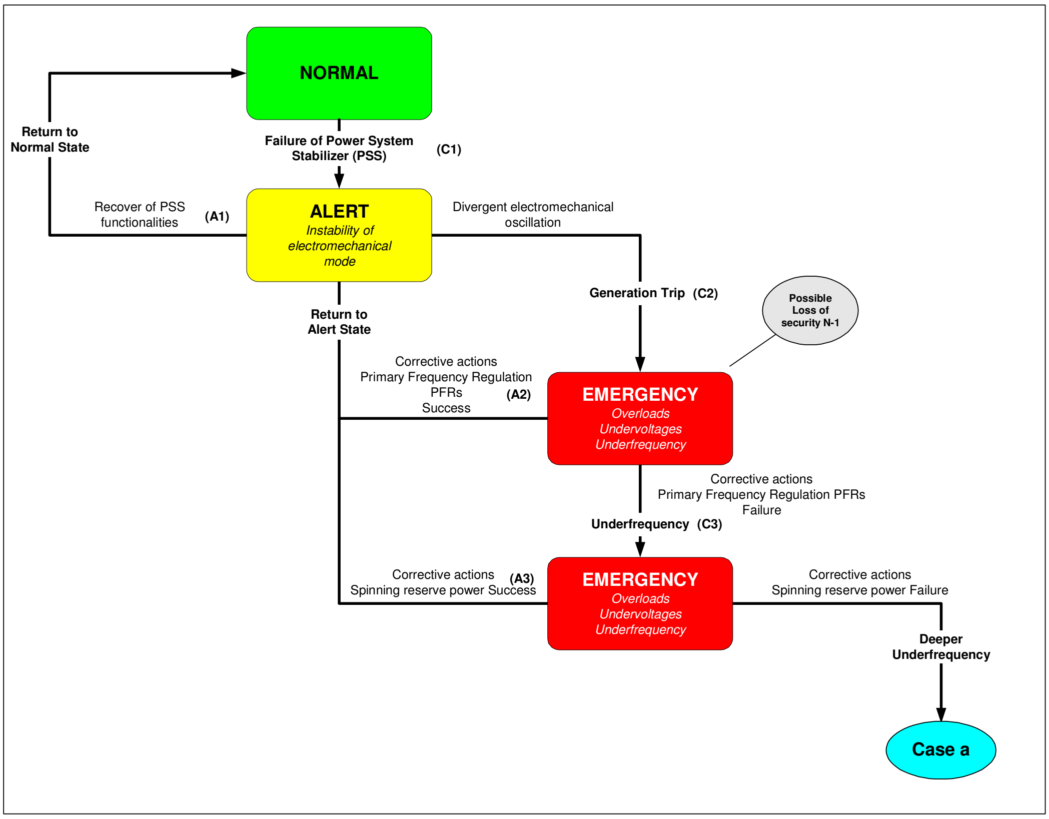


Figure 5-20: Instability of electromechanical mode Case b) - Sequence of possible Cascading Effects

Regarding this sequence (case b) the state transitions are generated by:

- **Failure of PSS (C1)** with consequent instability of the electromechanical mode of a group in NORMAL situation, and so the system pass to ALERT state automatic applying of groups regulation actions. If the **PSS functionalities are restored (A1)** the system return into NORMAL state.
- **Generators trip (C2)** with consequent possible loss of electrical security N-1 and transition from ALERT to EMERGENCY power system state. Automatic application of preventive actions:
    - **PFRs regulations (A2)**
- **Decrement of frequency (C3)** with consequent maintaining of state of EMERGENCY situation. Automatic application of corrective actions:
    - **Spinning reserve power (A2)**

If the contingency of decrement of frequency remain the cascading effects are the same that in case a):

- **Over-voltage (C4)** with consequent maintaining of state of EMERGENCY situation. Manual application of corrective actions:
    - **Manual activation of shunt reactance (A4)**
    - **Manual load shedding (A5)**
- **Separation of grid (C5)** with consequent formation of system islands, transition in IN-EXTREMIS situation. Automatic application of corrective actions in order to ensure the islands are:
    - Regulation of reserve back up generation
    - Automatic load shedding

In conditions of not intact Grid the restoration action starts. These actions are managed by TSO.

The effects presented in Case 6.1 are amplified by the ICT threats. This situation is due to the delay in execution of commands. Oscillations may degenerate in an escalation in tenths of seconds if the countermeasures are not executed in time.

5.5.2.2 Supervision and Control functions of Generation (Scenario 6.2)

This scenario (Case 6.2) considers the possible consequences of ICT anomalies on Power Plant supervision and control system not in presence of electrical contingencies.

In a Power Plant the SCADA system is linked to PQR and PFR and with the AVRs in order to collect all the data about the primary and secondary voltage regulation, statistics on production, failures, abnormal operations, etc.. On this basis different logical networks are on the same physical networks.

The supervisory systems are based on commercial operating systems.

The maintenance of systems is made using also external PCs.

Stakeholders involved:

- GENCO
- Software (SCADA, PQR, AVR, PFR) maintenance provider

Information Control Systems involved:

(see Case 6.1)

All the GENCO telecontrol systems are involved (see Figure 5-18):

- SCADA: Power Plant supervision
- AVR, PQR: voltage regulators
- PFR: frequency regulator
- MCD-TU (Substation): substation management

Information flow:

The information flow involves AVR, PQR, PFR, SCADA, RTS:

- Measures:
  - V, P, Q and ω from AVR to SCADA
  - V, P, Q and ω from SCADA to RTS
  - V, P, Q, q_{ref}, Q_{tot} and ω from AVRs to PQR
  - f_{ref} and f from PFR to SCADA
  - $V_{Bus\text{-}bar}$ from MCD-TU to PQR and RTS

Real-time requirements:

Commands have a response time within the time required by PQR, AVR and PFR.

Power Contingencies:

Not relevant.

Goals:

The main purposes of this scenario are (see also Case 6.1):

- show the interdependencies among the macro-parts of the Power Infrastructure, e.g., how an ICT problem on the telecontrol system may propagate from the single component to the other involved in the Power Plant causing an escalation.
- show the possibility that a slow down of communication could provoke unexpected fault on execution of control or delay in reaction to change of variables.
- show the vulnerability of the communication due to the use of the same channel for different real-time activities.

ICT Threats:

In principle the set of threat hypothesis to investigate on a given control scenario should be stated on the basis of the results of a risk assessment activity.

- ***Viral infections*** propagating from the PQR and SCADA PCs through the Local Area Network. Infection diffuses by PC used for maintenance or other PC on the network
- ***Intrusion*** into the local Power Plant and TSO Centre/Power Plant communications flow followed by the execution of faked commands (like modify parameters settings)
- ***DoS*** attacks to the telecontrol communications, generated by enemies located on the Power Plant, Telecom IP backbone or TSO centres

One instance of ICT threat is related to the setting of the AVR parameters, by provoking the instability of the electromechanical mode (see the Case 6.1 b)).

Cascading Effects and possible countermeasures:

In this scenario are reported consequences related to fault of ICT components related to:

- The loss of functionality of each ICT component of Telecontrol systems:

  - Lack of supervision and control (RTS/NTS)
  - Lack of automatic load shedding
  - Lack of manual load shedding
  - Lack of manual shunt reactance
- The loss of confidentiality:
  - Improper activation of shunt reactance
  - Not adequate load shedding

5.5.3 Low damped or unstable inter-area oscillations (Scenario 7)

This scenario takes into account the phenomenon of low damped or unstable inter-area oscillation. Also the UCTE (Union for Coordination for Transmission of Electricity) considers the phenomena of inter-area oscillations – like other large synchronously interconnected power systems world-wide, too. This phenomenon has an increasing meaning in extended power systems, especially if they are loaded by high power transfers. It has to be tackled in an adequate manner as otherwise the risk of instability may arise in certain system conditions with serious consequences for the electrical security of the system [UCTE Report 2002].

Inter-area oscillations involve combinations of many machines on one part of a system swinging against machines on another part of the system. The characteristic frequency of inter-area modes of oscillation is generally in the range of 0.1 to 0.6 Hz for example in the case - in UCTE/CENTREL system - two significant inter-area mode can be observed: 0.26 and 0.32 Hz.

The interconnected electric power systems under certain operating conditions, through increased efforts to transfer electric power across wide geographical and electrical distances, shown low frequency oscillations between two specific power plants located in two administratively different subsystems.

These oscillations are known as the inter area oscillations, their frequencies are low and they can be excited by any type of disturbance in the system.

These oscillations could severely restrict system operation by requiring the curtailment of electric power transfer as operational measure.

These oscillations could also lead to widespread system disturbances if cascading outages of transmission lines occur due to oscillatory power swings.

When these oscillations are unstable the situation is very critical because the trip of generators could bring us in a very critical situation: when one generator is tripped from the network, and the situation could become worse and worse.

The damping of the oscillation depends on the system loading, the load characteristics and generator/turbine control. A poor damping may lead to severe consequence for the whole system. Insufficient damping may become a problem especially for systems with such oscillation frequencies which are not damped by the generators and their standard control systems. Unfortunately, an oscillation frequency (≈ 0.26 Hz) exists in the UCTE system, which lies in this critical range of poor natural system damping. Therefore, damping had to be improved by optimising parameter settings of generator voltage control and implementation of Power System Stabilisers (PSS).

The mechanical model illustrates that the supra-regional structure of the system is the main factor regarding the basic dynamic system characteristic, whereas the regional grid design has only little influence. It is evident that the system dynamics will change significantly in case of interconnection with a further area. The new system configuration may lead to new frequencies of possible oscillations.

This aspect is presently an important issue dealt with by the UCTE Working Group on System Development. While the UCTE system has grown more or less gradually in the past, UCTE is now faced with requests to extend the synchronous area in relatively large steps through interconnection with other existing interconnected power systems. UCTE has to investigate carefully the effect on the dynamic system behaviour before synchronising an adjacent system.

To this end, UCTE uses a complete dynamic model for the synchronous area representing the 380/220 kV grid and all large generation units including their generator and turbine control systems. This model is validated by recordings from the real system. This process is also required from the extension area: modelling on the basis of dynamic data and validation by recordings collected during isolated operation. The technical requirements are defined by investigations of the whole extended synchronous area. Using modern techniques for power system analysis and control, UCTE meets its obligation to maintain the electrical security of the whole system, and enables the technical means to be optimally used for reliable parallel operation with new partners.

Stakeholders involved:

- GENCO
- TSO
- TSP (GENCO)
- TSP (TSO)

Information Control Systems involved:

Regulation systems of TSO and GENCO involved (see Figure 5-17):

- AVR-PSS (GENCO)
- PQR (GENCO)
- PFR (GENCO)
- SFR (TSO NCC)
- SCADA (GENCO)
- RTS (TSO ACC)
- NTS (TSO NCC)

Information flow:

The information flow is classified as follows:

- Measurements: from AVR, PQR, PFR and Substation to SCADA, SFR, RTS and RTS
- Signals: from AVR, PQR, PFR and Substation to SCADA, SFR, RTS and NTS
- Commands: from PQR, SFR, RTS, NTS and SCADA
- Information flow AVR, PQR, RVR, NVR, PFR, SFR, Substation and SCADA

Real-time requirements:

Commands have a response time within the time required by PQR, AVR, PFR, RVR and NVR.

Power contingencies:

The interconnected electric power systems under certain operating conditions, through increased efforts to transfer electric power across vast geographical and electrical distances, shown low frequency oscillations between two specific power plant located in two administratively different subsystems.

Goals:

The main purpose of the scenario is to show the interdependencies among the macro-parts of the Power Infrastructure, i.e., how a power disturbance may propagate from the Grid to the Power Plant causing the line trip and this situation requires an intervention of TSO to avoid an under-frequency situation that could cause cascading effects.

ICT Threats:

The most plausible ICT threats are:

- ***Viral infections*** propagating from the PQR and SCADA PCs through the Local Area Network. Infection diffuses by PC used for maintenance or other PC on the network.
- ***Intrusion*** into the local Power Plant and TSO Centre/Power Plant communications flow followed by the execution of faked commands (like modify parameters settings)
- ***DoS*** attacks to the telecontrol communications, generated by enemies located on the Power Plant, Telecom IP backbone or TSO centres

Cascading Effects and possible countermeasures:

In Figure 5-21 referring to the state of the Power System (see Figure 3-1) are depicted possible sequences of the cascading effects, that may collapse into an *IN EXTREMIS* situation.

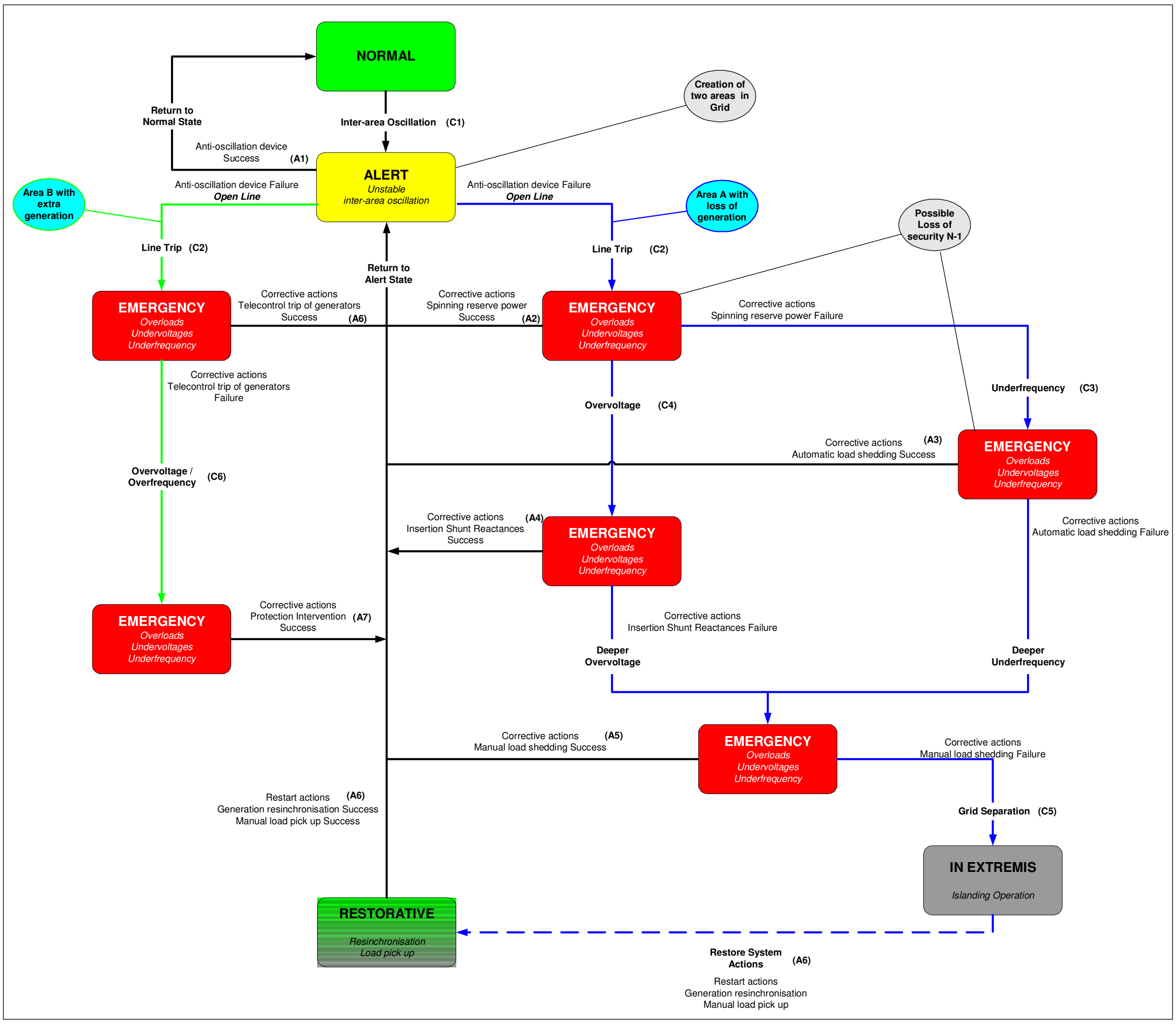


Figure 5-21: Inter-area oscillation - Sequence of possible Cascading Effects

Regarding this sequence the state transitions are generated by:

- **Inter-area oscillation (C1)** with consequent low frequency oscillation in NORMAL situation, and so the system pass to ALERT state automatic applying of anti-oscillation regulation actions. If the **oscillation is damped (A1)** the system returns into NORMAL state.
- **Line trip (C2)** among the two areas oscillating (Area A and Area B) ***through telecontrol command***. This situation provokes two different distinct contingencies in each area:
- ***Evolution of Area A*** (***blue*** path in Figure 5-21) with loss of Power Generation incoming:
    - **Line trip (C2)** with consequent loss of electrical security N-1 and transition from ALERT to EMERGENCY power system state. Automatic application of preventive actions:
        - **Spinning reserve power (A2)**
    - **Decrement of frequency (C3)** with consequent maintaining of state of EMERGENCY situation. Automatic application of corrective actions:
        - **Automatic load shedding (A3)**

      Manual application of corrective actions:

        - **Manual load shedding (A5)**
    - **Over-voltage (C4)** with consequent maintaining of state of EMERGENCY situation. Manual application of corrective actions:
        - **Manual activation of shunt reactance (A4)**
        - **Manual load shedding (A5)**
- ***Evolution of Area B*** (***green*** path in Figure 5-21) with surplus of Power Generation:
    - **Line trip (C2)** with consequent possible loss of electrical security N-1 and transition from ALERT to EMERGENCY power system state. Automatic application of preventive actions:
        - **Telecontrol trip of generators (A6)**
    - **Overvoltage/Overfrequency (C6)** with consequent maintaining of EMERGENCY situation. Automatic application of corrective actions:
        - **Intervention of protection (A7)**
- **EXTREMIS situation**. Automatic application of corrective actions in order to ensure the islands:
    - Regulation of reserve back up generation
    - Automatic load shedding (that involves substations of distribution)

In conditions where the Grid is not intact the **restoration actions (A6)** start. These actions are managed by TSO.

The effects presented in this case are amplified by the ICT threats. This situation is due to the delay in execution of commands. In particular oscillations may degenerate in an escalation of them in tenths of seconds if the countermeasures are not executed in time.

The magnified effects of ICT threats are strictly depending by the kind of attacks and the instant when they are performed.

5.5.4 Transmission Grid Short Circuit with loss of Synchronism (Scenario 8)

This scenario considers the loss of Synchronism caused by a Short Circuit. In Figure 5-22 is shown the one-line diagram of the Brindisi area. It is characterised by a strong power production and a narrow corridor through which power is transmitted. This determines a **low Critical Clearing Time (CCT)**, even if no main lines are lost following the transient. The CCT can be roughly estimated to be in between 100 ms and 125 ms.

Three cases have been considered, namely:

- stable when the fault duration is 50 ms
- limit, when fault duration is 100 ms
- unstable, when the fault duration has length of 125 ms and generators at Brindisi South power plant lost synchronism, compared with the rest of Italy - Europe generators

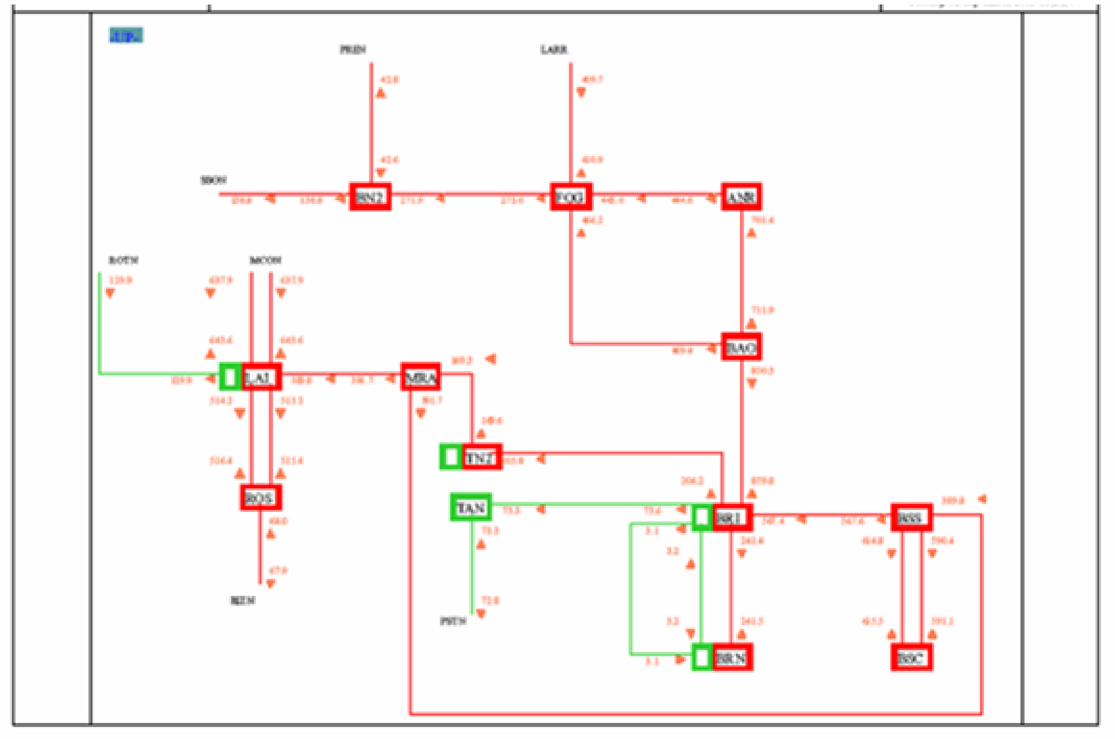


Figure 5-22: The 400/240 kV diagram of Brindisi

The angle of generators in Southern Italy can be compared with the angle of "LA CASELLA" power plant, located in Northern Italy, that moves in accordance with the rest of the unperturbed network. In the Figure 5-23 are shown the generators subdivided in two clusters:

- the stable cluster in which there are the generators which are in stable situation
- the unstable cluster in which are the generators which could be unstable in consequence of short circuit

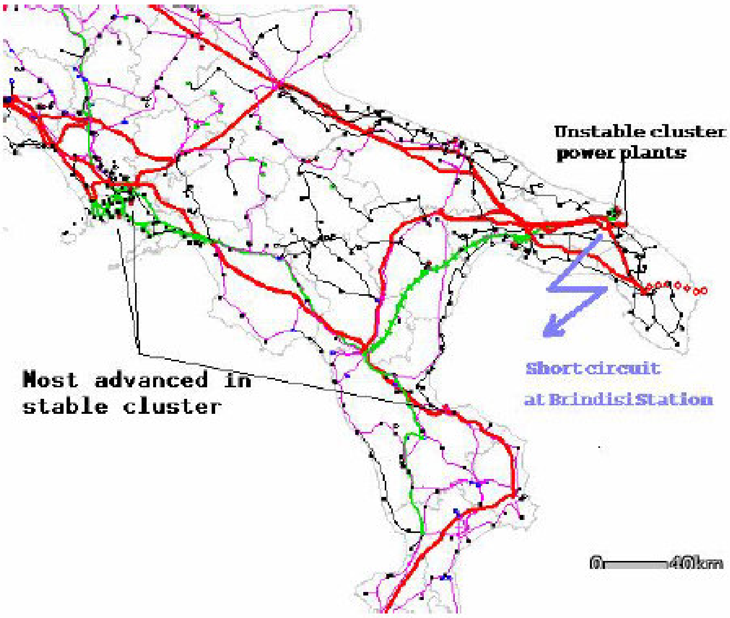


Figure 5-23: “Stable” and “Unstable” clusters

The evolution of “stable” and “unstable” clusters are presented in the flowing pictures, in order to have a simple vision of the behaviour of the generation groups involved in the contingency under consideration.

In Figure 5-24 the angle of the equivalent machines to “stable” cluster and “unstable” cluster are shown for the limit case, that is for a Short Circuit of 100 ms.

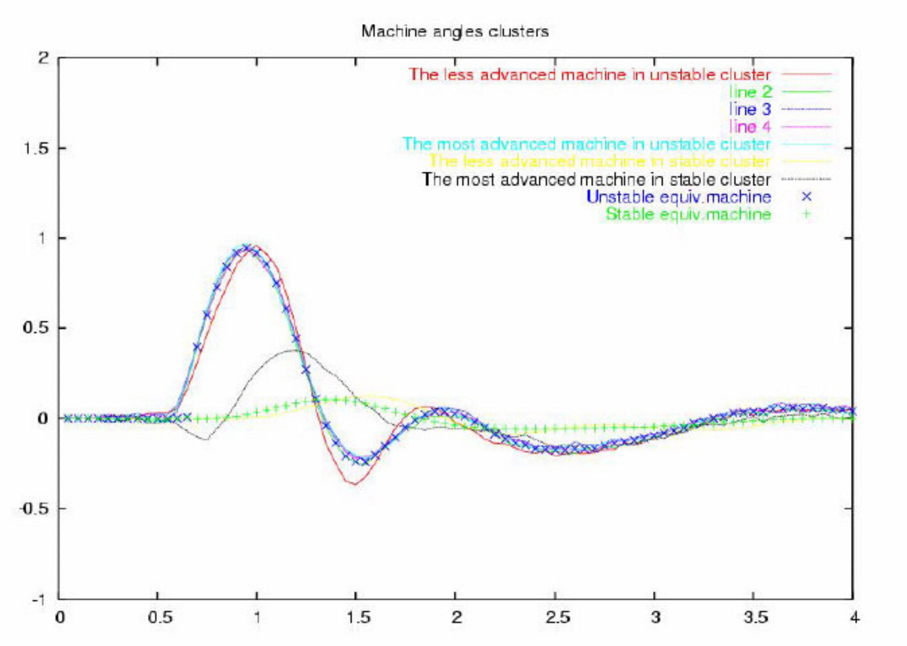


Figure 5-24: Angles of equivalent machines to “Stable” cluster and “Unstable” cluster for the limit case (100ms)

In Figure 5-25 the angle of the equivalent machines to “stable” cluster and “unstable” cluster are shown for the unstable case, that is for a Short Circuit of 125 ms.

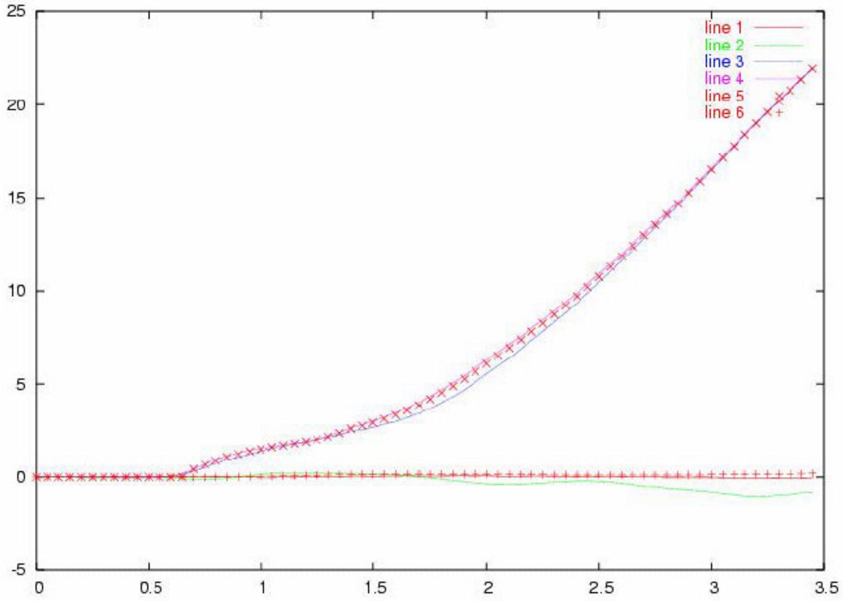


Figure 5-25: Angles of equivalent machines to “Stable” cluster and “Unstable” cluster for the unstable case (125ms) without any remedial action

The remedial action to recover the system, must happen by 400 ms from the short circuit clearing event. The effectiveness of this action, constituted by the trip of G2 and G3 units of

Brindisi Power Plant is shown in Figure 5-26. In this figure are represented the equivalent machines angle for the “stable” and “unstable” clusters in the controlled case (trip of G2 and G3).

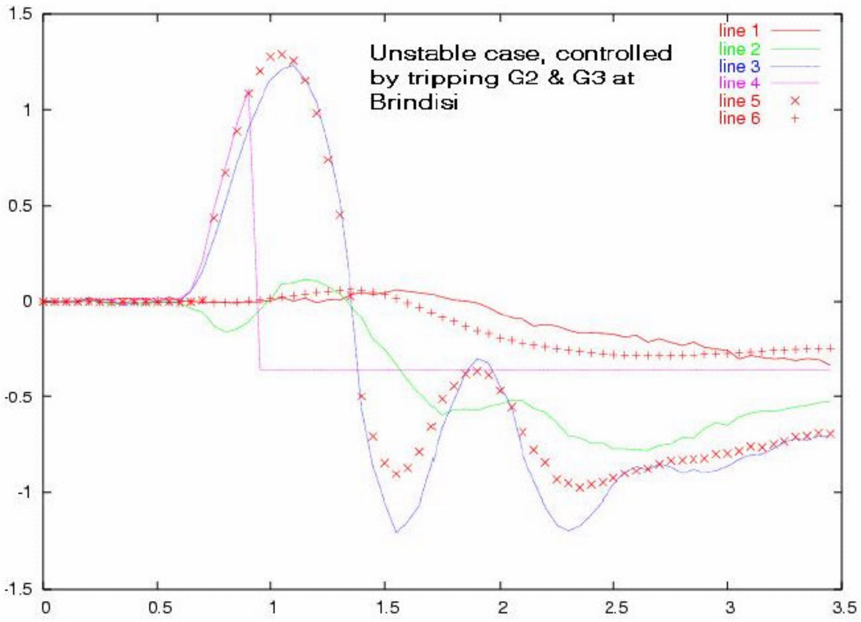


Figure 5-26: Machines angle for the unstable case (125ms) but controlled by tripping G2 and G3 Brindisi’s machines

Some off-line tests show that the remedial action after or equal 450 ms cannot recover the system, as put in evidence in Figure 5-27, which shows the system behaviour, when the remedial action, due to transmission delay from and to the plant, comes at 450 ms. Figure 5-25 shows the system transient when no remedial action is taken for the same condition.

For both the last two cases the Brindisi area lost synchronism.

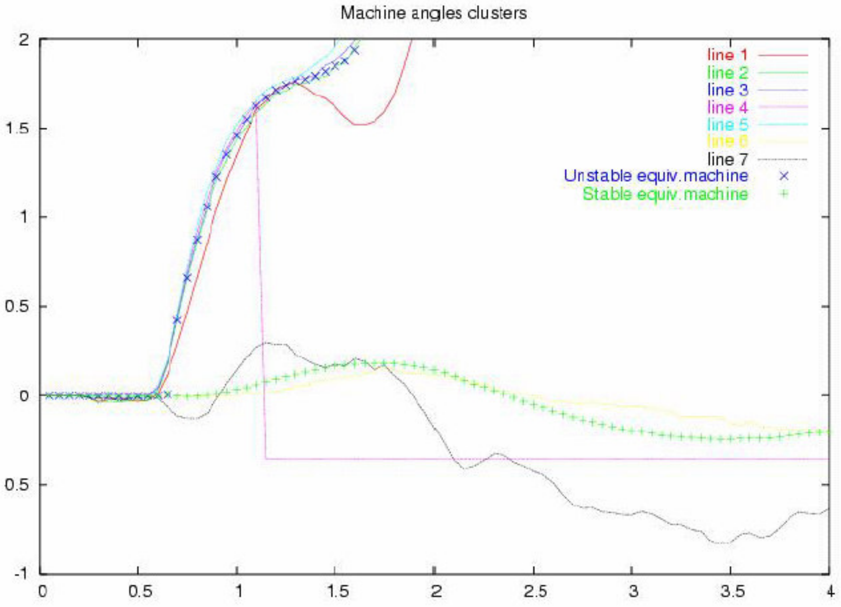


Figure 5-27: Equivalent machines angle to “Stable” cluster and “Unstable” cluster for the unstable case (125ms) when remedial action is taken at 450 ms, by tripping G2 Brindisi’s unit

To verify that excessive and superfluous remedial action does not drive the system to other sort of instability, two units are tripped, at the same time. The system is stressed, but it survives (see Figure 5-26).

This condition comes out to be typical for the analysed network. It is real, even if not probable, that short circuit of 100 ms up to 150 ms can occur and that areas with characteristics like the studied one can temporary be present.

In Figure 5-28 are shown local machines measures at Brindisi Power Plant, without transmission delay, in the “unstable” case but controlled, that is a short circuit of 125 ms of duration.

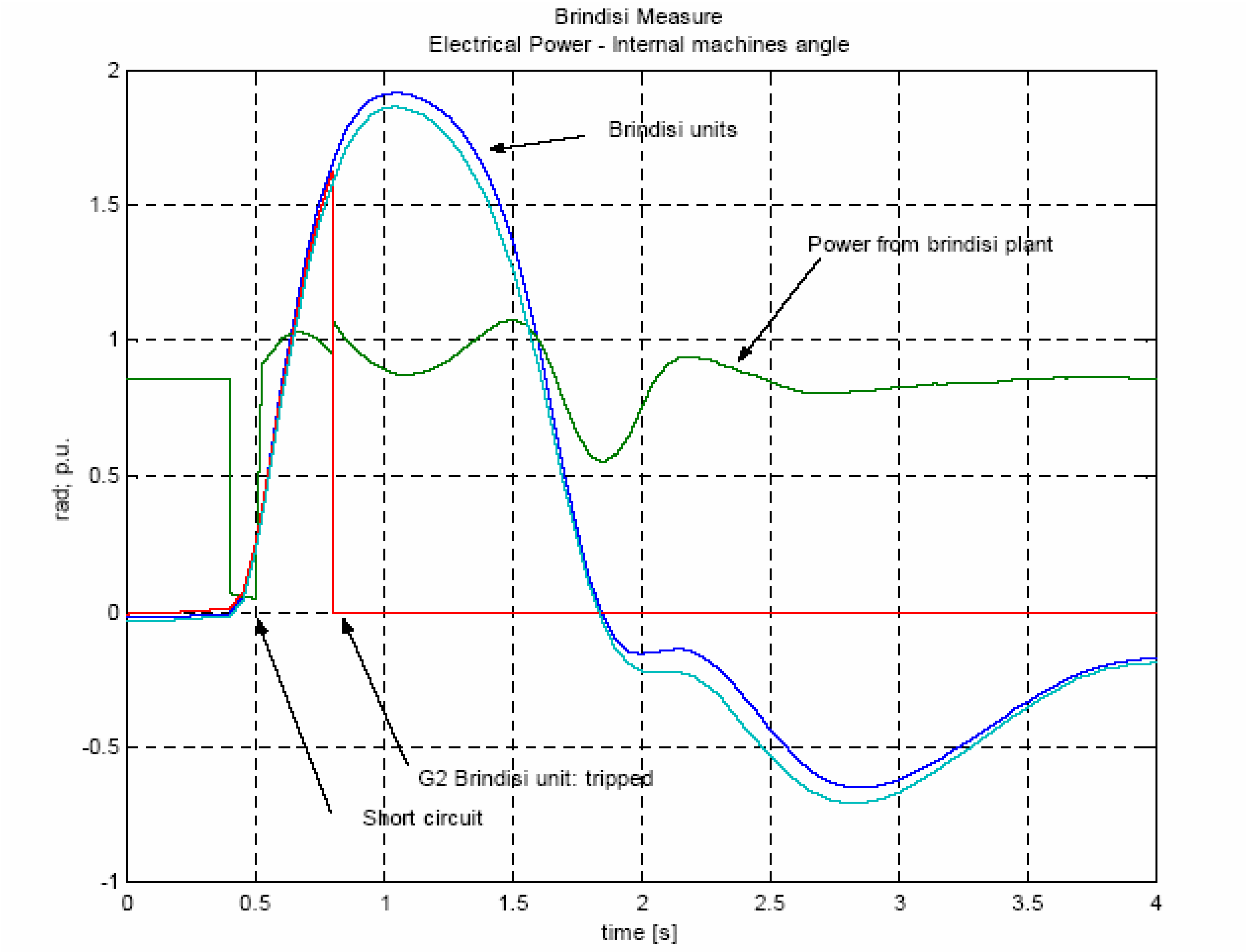


Figure 5-28: Local machine measures at Brindisi power plant with no transmission delay. Unstable but controlled case (125ms)

Stakeholders involved:

- GENCO
- TSO
- TSP of GENCO
- TSP of TSO

Information Control Systems involved:

- Systems of TSO and GENCO involved (see Figure 5-17):
- AVR-PSS (GENCO)

- PQR (GENCO)
- PFR (GENCO)
- SFR (TSO NCC)
- SCADA (GENCO)
- RTS (TSO ACC)
- NTS (TSO NCC)

Information Flow:

The information flow is classified as follows:

- Measurements: from AVR, PQR, PFR and Substation to SCADA, SFR, RTS and RTS
- Signals: from AVR, PQR, PFR and Substation to SCADA, SFR, RTS and NTS
- Commands: from PQR, SFR, RTS, NTS and SCADA to AVR and PFR
- Information flow AVR, PQR, RVR, NVR, PFR, SFR, Substation and SCADA

Real-time requirements:

Commands have a response time within the time required by PQR, AVR, PFR, RVR and NVR.

Meanwhile the trip of the adequate generators must happen by 400ms.

Power contingencies:

The interconnected electric power systems under short circuit can lead to have problems of loss of synchronism.

Goals:

The main purpose of the scenario consist to show the interdependencies among the different power plants of the Power Infrastructure, i.e. how a power disturbance, as the short circuit, may propagate through the Grid to various Power Plants causing the loss of synchronism of some generators

This situation requires an intervention of TSO to avoid the situation that could cause cascading effects of loss of synchronism

ICT Threats:

The most plausible ICT threats are:

- ***Viral infections*** propagating from a PC on the network.
- ***Intrusion*** into the TSO Centre/Power Plant communications flow followed by the execution of faked commands (like modify parameters settings)
- ***DoS*** attacks to the telecontrol communications, generated by enemies located on the Power Plant, Telecom IP backbone or TSO centres

Cascading Effects and possible countermeasures:

In Figure 5-29 referring to the state of the Power System (see **Figure** 3-1) are depicted possible sequences of the cascading effects, that may collapse into an *IN EXTREMIS* situation.

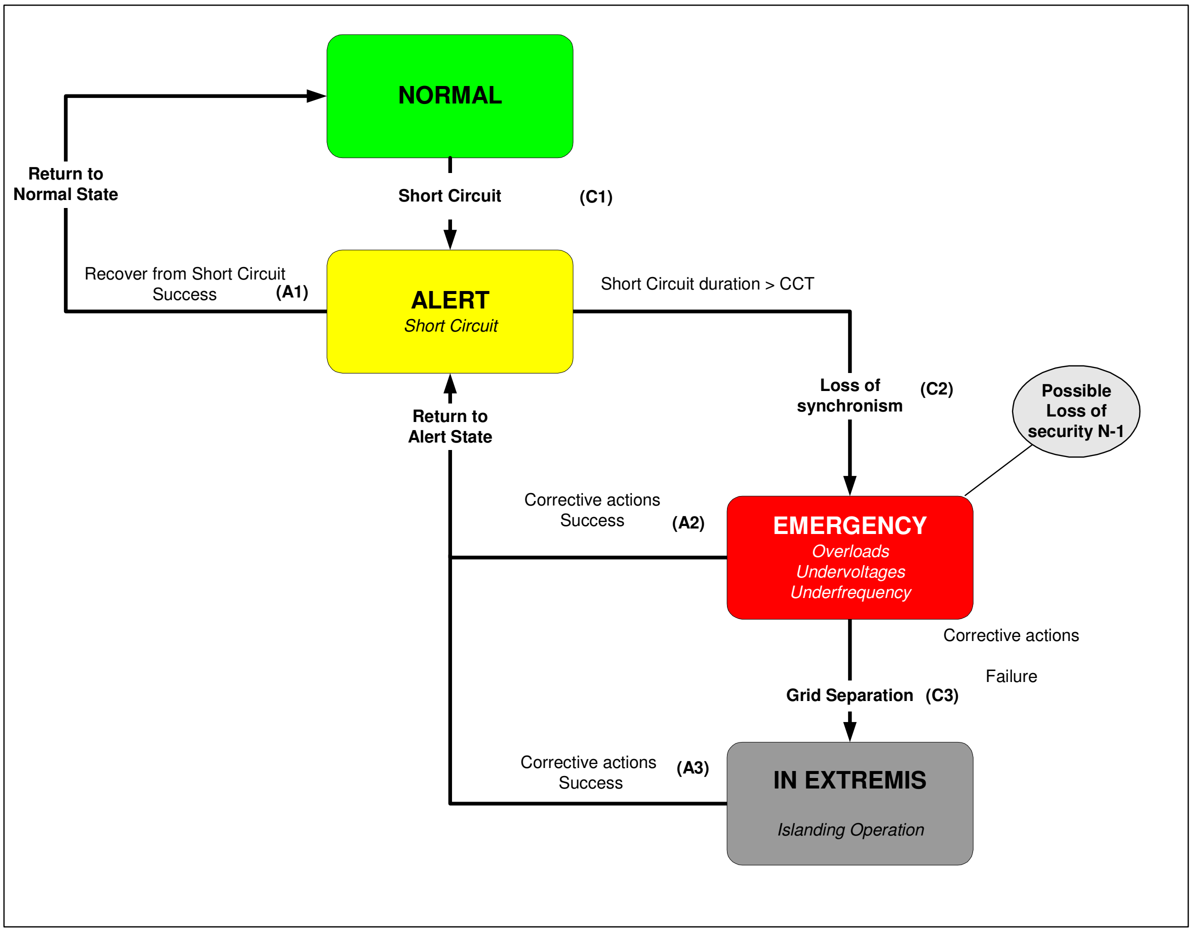


Figure 5-29: Short Circuit - Sequence of possible Cascading Effects

5.5.5 Transmission Grid Voltage Instability (Scenario 9)

This scenario explores the Voltage collapse due to voltage regulation by ULTC – Under Load Tap Changer. In order to put in evidence the main characteristics of the control scenario regarding the topics of voltage instabilities three cases on Italian network are taken into consideration. They deal with the voltage problems that can arise e.g. at Candia station, which is placed in Central Italy, see the Figure 5-30.

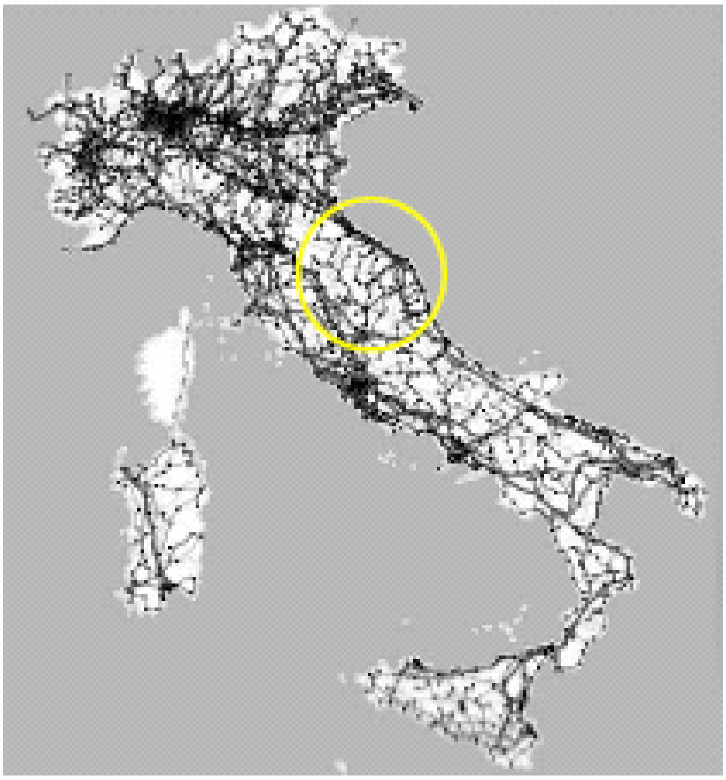


Figure 5-30: The placement of CANDIA station in respect to Italy

The CANDIA STATION contains three electrical nodes at respectively 400kV, 240 KV and 132kV., as indicated in Figure 5-31.

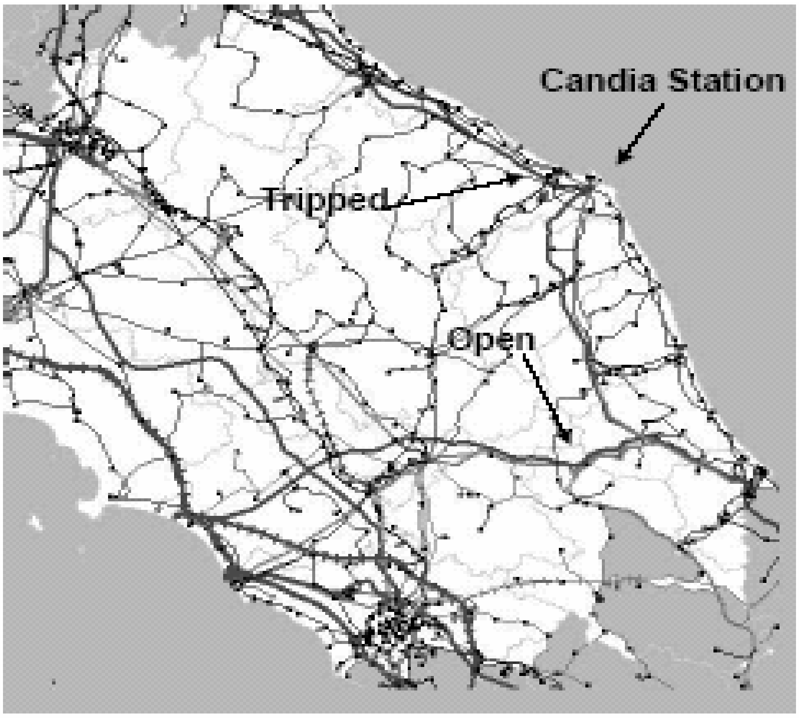


Figure 5-31: Neighbouring of CANDIA station

The three cases about voltage instability refer to a **voltage drop at Candia** and are analyzed by the use of the simulator of electric power system named SICRE:

- In **case 1**, despite the increase in P0 and Q0 which are the references for electric active power and the reactive power, voltage drops below unacceptable value but it does not collapse.
- In **case 2**, the static solution cannot be reached since the load flow algorithm performed at each simulation step fails to converge.
- For **case 3** the tap changer, which has its lowest limit set to zero, in order to allow voltage to collapse, is acted continuously, with the following integral regulation law v the gain equal to 1/10 seconds.

Case of Voltage Instability due to Voltage Regulation by ULTC.

Case Description

In the Figure 5-32 has been shown the one-line diagram of CANDIA area. At Candia station, three transformers are regulated to maintain voltage at 132 kV bus-bar constant. The loads on these busses are modelled with quadratic voltage dependence.

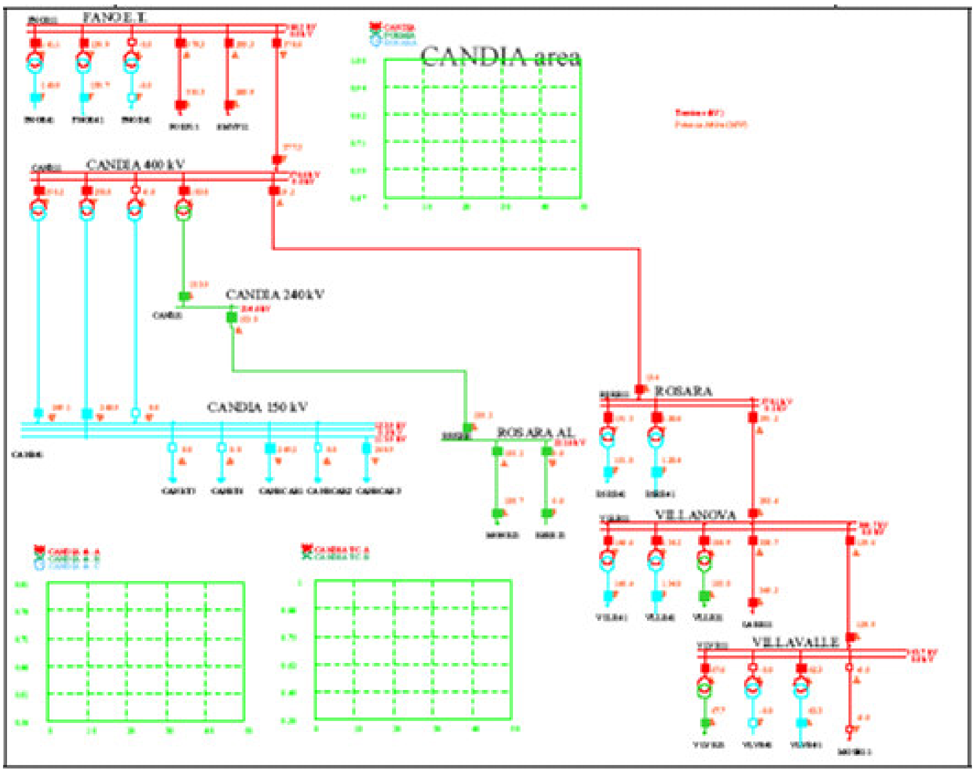


Figure 5-32: On line diagram of CANDIA Area

As initial condition, the Candia station is supplied practically by CANDIA-FANO line, where 380 MW are flowing on 400 kV and the rest on 240 kV lines. The total load is about 500 MW.

Case 1

This case refers to load increment at CANDIA when VILLAVALLE-MONTALTO line has been tripped at 5 s. After system reached new steady state, ramp up on Candia loads is started at 100 s. Load reference is incremented at 10 [.]/s

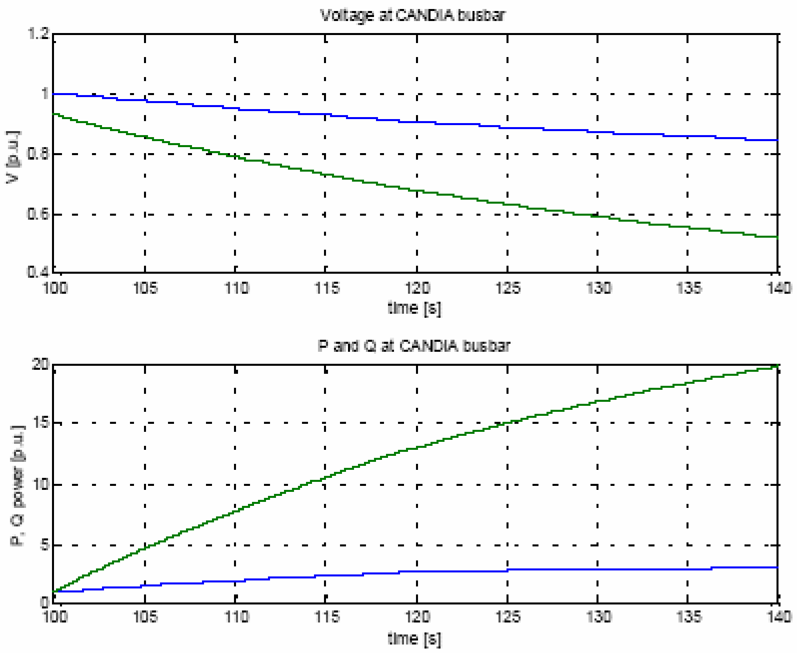


Figure 5-33: Trend of voltage and power at CANDIA bus-bar during P and Q loads increment (case 1)

Case 2

This case refers to load increment at CANDIA 132 kV bus-bar, when CANDIA-FANO and VILLAVALLE-MONTALTO lines have been tripped at 10 s. Load references are incremented at 10 [.]/s from t = 100 s.

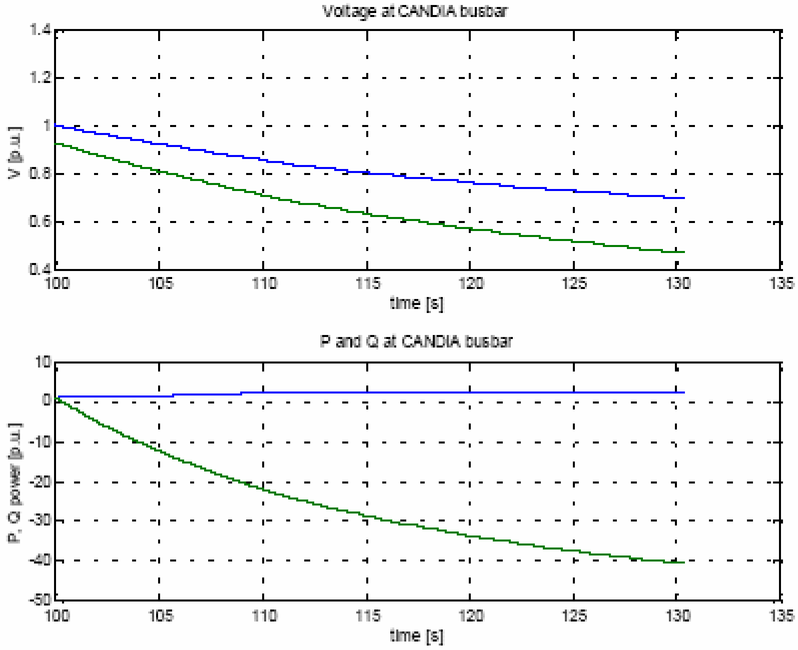


Figure 5-34: Trend of voltage and power at CANDIA bus-bar during P and Q loads increment (case 2)

Case 3

This case refers to instability due to ULTC (Under Load Tap Changer) control when CANDIA-FANO trips at time 30 s. The previous discontinuity refers to Candia's load set at 5 s.

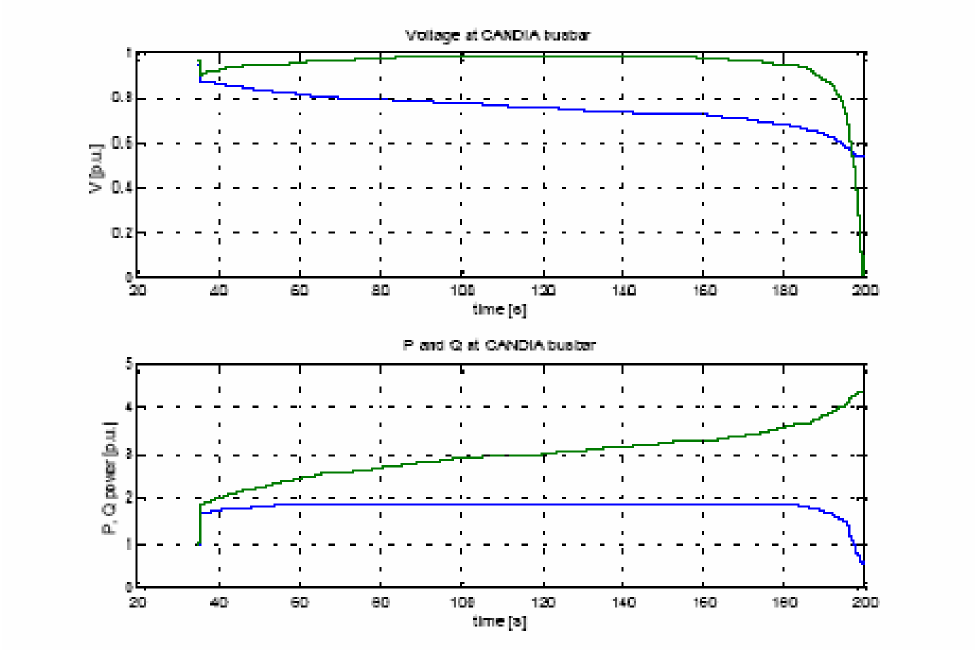


Figure 5-35: Trend of voltage and power at CANDIA bus-bar during ULTC instability

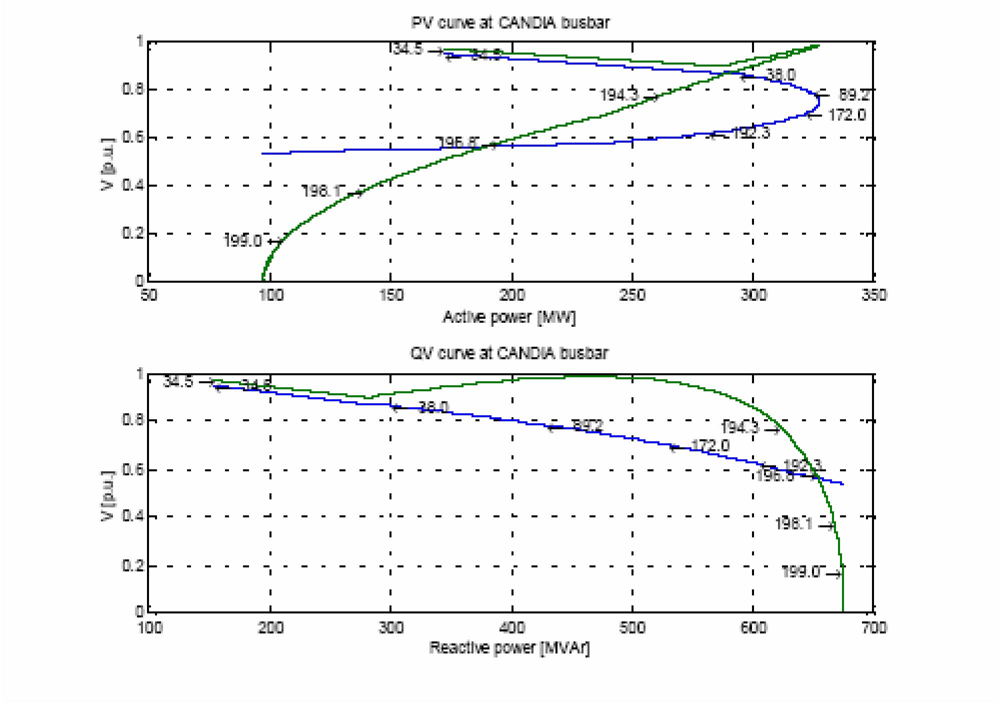


Figure 5-36: PV and QV curves at CANDIA bus-bar during ULTC instability

Simulated case of Voltage Instability due to Voltage Regulation by ULTC

Case Description

In Figure 5-32 the one-line diagram of CANDIA area is showed. At Candia station, three transformer are regulated to maintain voltage at 132 kV bus-bar constant. The loads on these busses are modelled with quadratic voltage dependence.

As initial condition, the Candia station is supplied practically by CANDIA-FANO line, where 380 MW are flowing on 400 kV and the rest on 240 kV lines. The total load is about 500 MW.

The critical event is CANDIA-FANO 400 kV line tripping.

The critical event is the tripping of the line CANDIA-FANO, in fact following this event, as can be observed in Figure 5-37, the voltage drops down from 370 kV to 320 kV. The sub-network bus-bars drop consequently from (0.93,0.86) p.u. to (0.81, 0.75) p.u. (voltage reference 132 kV. In figure the voltage reference is 150 kV).

The voltage regulation tries to restore the initial voltage condition moving the tap changer.

During the simulation, the limits on tap changer are removed to emulate the global effect of all the low voltage sub-network tap changer regulations. To get more realistic scenario, noise is added on system with the following parameter:

• NVAR = 0.005	noise variance of load demand
• Pmin = 5.0	minimum power to modify load demand
• BasV_noise_Var = 0.0001	noise variance on measure
• delay = 150 ms	transmission delay

Loads with greater than 5 MW demand, are randomly chosen with 10% of probability, at every simulation step with 0.005 p.u. variance.

On this hypothesis, if no corrective actions are taken, both 132 kV networks reach voltage collapse.

The voltage transient and equivalent tap changers position are also plotted in Figure 5-37.

Both high voltage and low voltage at Candia station are monitored by *VIDA (Voltage Instability Detection Algorithm)* protection.

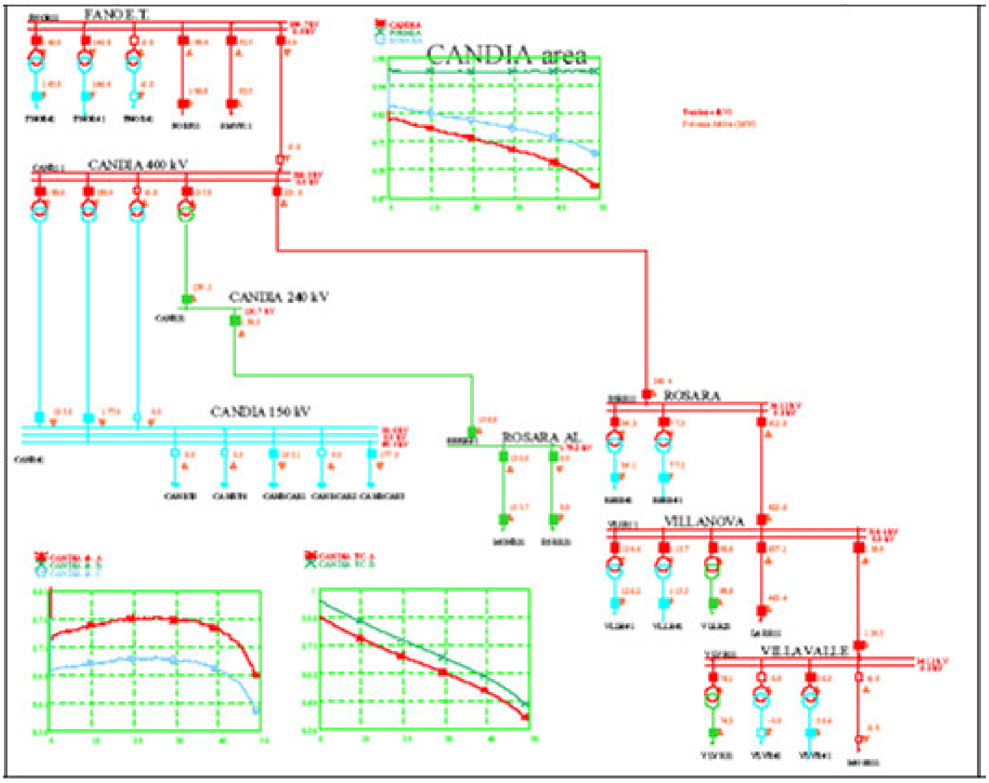


Figure 5-37: The one-line diagram of CANDIA area with the plot of the voltages

The result for “no noise” test is shown in Figure 5-38.

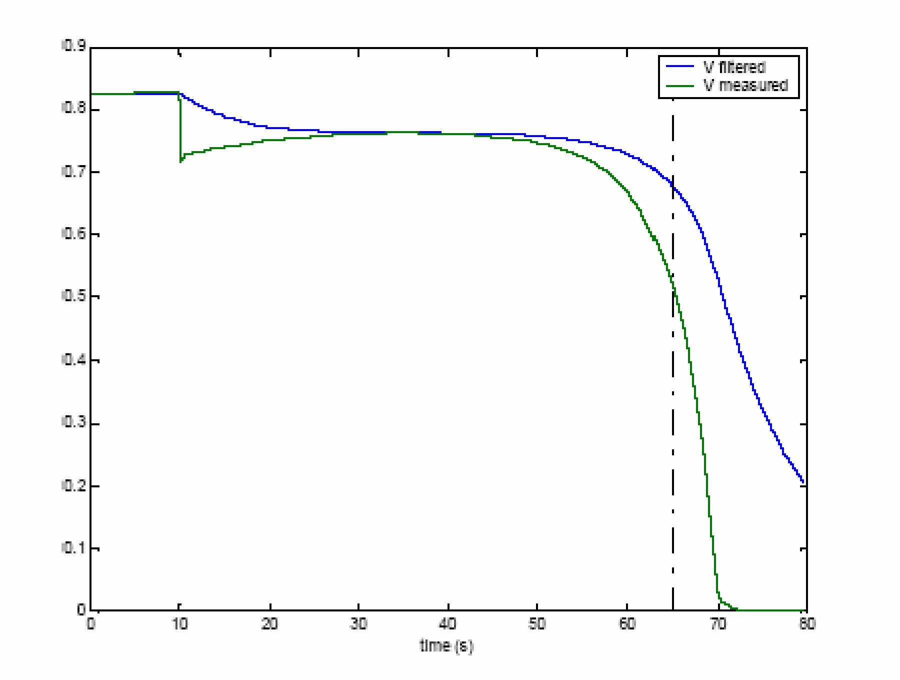


Figure 5-38: Transient of voltage at 132 KV bus-bar of CANDIA during the collapse

In order to implement corrective actions able to avoid voltage instability and possible voltage collapse a WAVP (Wide Area Voltage Protection) could be used. One type of these WAVP is presented in [Corsi *et al.* 2006].

Stakeholders involved:

- GENCO
- TSO
- TSP of GENCO
- TSP of TSO

Information Control Systems involved:

Systems of TSO and GENCO involved (see Figure 5-17):

- AVR-PSS (GENCO)
- PQR (GENCO)
- SCADA (GENCO)
- RTS (TSO ACC)
- NTS (TSO NCC)

Information Flow:

The information flow is classified as follows:

- Measurements: from AVR, PQR and Substation to SCADA, RTS and RTS
- Signals: from AVR, PQR and Substation to SCADA, RTS and NTS
- Commands: from PQR, RTS, NTS and SCADA
- Information flow AVR, PQR, RVR, NVR, Substation and SCADA

Real-time requirements:

Commands have a response time within the time required by PQR, AVR, RVR and NVR.

Power contingencies:

The loss of a line without a corrective action could bring the grid to voltage collapse.

Goals:

The main purpose of scenario is to show the interdependencies among the different power plants of the Power Infrastructure, i.e. how a power disturbance, as the trip of a line, may propagate through the Grid to provoke voltage collapse.

ICT Threats:

The most plausible ICT threats are:

- ***Viral infections*** propagating versus PC on the network.
- ***Intrusion*** into the TSO Centre/Power Plant communications flow followed by the execution of faked commands (like modify parameters settings)
- ***DoS*** attacks to the telecontrol communications, generated by enemies located on the Power Plant, Telecom IP backbone or TSO centres

Cascading Effects and possible countermeasures:

In Figure 5-39 referring to the state of the Power System (see Figure 3-1) are depicted possible sequences of the cascading effects, that may collapse into an *IN EXTREMIS* situation.

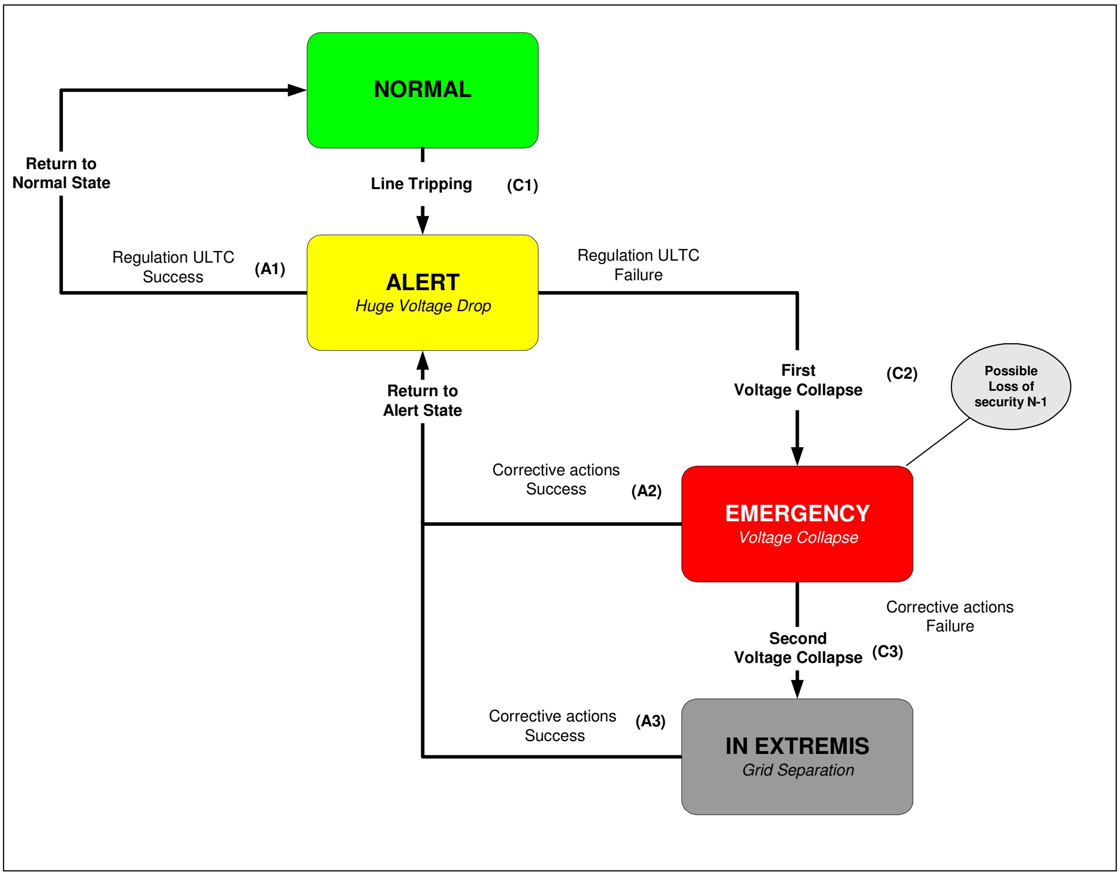


Figure 5-39: Voltage instability - Sequence of possible Cascading Effects

6 CONTROL SYSTEM SCENARIOS: MICROGRIDS

In the included scenarios some typical series of events in a distribution grid are presented and the control system reaction is estimated using various computer simulations. In the scenarios, faults are also injected to see their impact on the system as a whole. Of course 'impact' is hard to define: this could be (in order of importance) the system availability, economical cost or power quality problems. These problems are also highly correlated: lower system availability will have an economical impact; severe power quality problems lead to increased wear out of electrical devices or even trigger protection devices, leading to lower system availability, and so on.

In these control system scenarios the most common operational mode of the system is presented, namely the *grid connected mode* of the AEG. Although the AEG is able to operate in *islanded mode* when sufficient power generation capacity is available, and this capability is able to boost the availability of the electrical system, this mode is not dealt with here. This is due to the relatively low probability of islanding and the lack of load shedding schemes with a fine enough granularities (needed to overcome the inevitable lack of generation capacity of DG) in the current power grid. Also other impediments, such as protection issues, will defer islanded operation of DG in the near future

6.1 Simulation Scenario

6.1.1 Simulation algorithm

The algorithm used to simulate the behaviour of the microgrid with distributed control, simulates both the electrical and ICT level of the application. Since we are working in a radial distribution segment, power flow calculations are relatively simple when it is connected to transmission level. Primary control will, when the system is grid connected, only control active power output based on local voltage levels, since frequency is kept stable by the strong external power grid. The agent behaviour (primary and secondary control loop) and the overlay network are simulated too. For these simulations we assume that communication delays and gossiping intervals are a few orders of magnitude larger than the time needed for settlement of the primary control loop (proportional controller and power). This means that power flow calculations and the primary control action are calculated first until convergence is observed. Only then generators will gossip, and adjust their parameters for the primary control loop according to the results of secondary and tertiary control loop. When all generators finished gossiping, new power flow calculations are done until convergence, and so on. The number of iterations is chosen in advance.

```
for(i=0; i<nb_of_iterations; i++){
        applyScript(i);          ←———— Apply script, e.g. fault injection
        for(each agent A){
                A.gossip();          ←———— Gossiping:
                                             secondary and tertiary control loop
                A.adjustPQ();
        }
        while(no convergence){
                doPowerFlow();
                for(each agent A){           ←———— Powerflow calculations and
                        A.applyDroopControl();       primary control until convergence
                }
        }
}
```

6.1.2 Simulation environment: Loads, Generators and Distribution Grid

Distribution Grid Layout

The distribution net shown in Figure 6-1 is used in the simulations, the colours correspond to the colours used in the graphs resulting from the simulations. There are three branches which all contain both passive loads and small generators, of which both active and passive power output levels are controllable. It is presumed that the relatively small load changes in these scenarios will not influence voltage levels on the high voltage grid. So at point *F* near the feeding transformer *16* will always be at nominal voltage (230V) because of the connection to the strong grid.

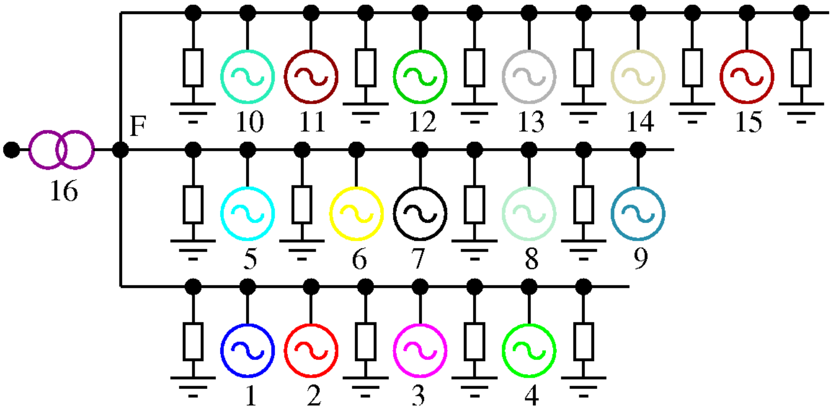


Figure 6-1: Distribution net layout used in simulations, containing one feeder transformer and three branches with both passive loads and DG units.

Marginal Cost Curves

Marginal cost curves of the generators are chosen as a simple monotonically increasing linear function with some marginal cost for zero output (which is not necessarily zero) and some marginal cost for the generator maximum output. The feed-in transformer has no bounds on the amount of power it can inject into the distribution net (which is realistically for power levels needed in the presented scenarios). Also, the transformer has a relatively high marginal cost curve which increases when injected power increases. This high price encourages local generators to produce.

Power Consumption

In all scenarios presented similar loads are applied. In the beginning all generators have a certain set point P_0 for their desired power output and the loads have fixed power consumption. Unbalances between local supply and demand are automatically dealt with by the transformer. At time (or iteration) 21 several loads increase their power consumption and at time 121 several loads drastically decrease their power consumption.

Following these load changes, one will typically observe three phases during a simulation:

- t = [1..20]: Steady settlement of initial settings to global Pareto optimum.
- t = [21..120]: Demand suddenly increased, feeder will resolve unbalance initially, some DG units might also react slightly (if local voltage drop is high enough). Afterwards, DG units will adjust power output to steadily evolve towards Pareto optimum.
- t = [121..181]: Demand suddenly decreased, feeder will resolve unbalance initially, some DG units might also react slightly (if local voltage rise is high enough). Afterwards, DG units will adjust power output to steadily evolve towards Pareto optimum.

Dead Zone

Unless stated differently, the 'dead zone' in which primary control does not react to voltage changes extends from 229V to 231V. Obviously, as long as primary control is not active, there is no difference between power output set point P_0 and actual power output P, and also secondary control will not be active.

Graphical Simulation Results

Simulation results are displayed using three graphs, showing information on all generators and the feeder transformer at every time step.

1. The first graph shows the *active power output P (full line) of every generator, and the power offset P_0 (dashed line)* which is the power the generator should produce at the nominal voltage level. If the local voltage level is within certain bounds of the nominal value (in the 'dead zone'), the actual power output P will equal this P_0. When primary control is activated (thus if voltage levels exceed the dead zone), there will be a difference between P and P_0, called ΔP. Secondary control will try to decrease the overall ΔP, and consequently bring voltage closer to its rated value.
2. The second graph shows the *voltage levels near each generator*. Also the dead zone is indicated. Mind that as long as voltage levels stay in this zone, no secondary control action will be seen. Also notice that voltage level at the feeder transformer is always at the rated value of 230V due to the connection with the strong grid.
3. The third graph shows the *marginal costs of the actual power output* (P) of each generator. In this graph the action of tertiary control should be visible when convergence between these costs occurs. Mind here that sometimes a generator may seem not to converge, although tertiary control works just fine. This is because a generator is producing maximally at its maximum marginal cost, when overall marginal cost is higher than this value; or the other way around, a generator is producing its minimal output (0W) at its minimal marginal cost (which is not necessarily 0), when overall marginal cost is lower than this value.

6.2 Primary Control Only (Reference Scenario)

In this scenario the AEG is operated without secondary or tertiary controls, and only the local primary control loop is used. This will give us a benchmark to show the effect of secondary and tertiary control, and their combined effect.

Stakeholders Involved

- DG owners
- DSO
- To some lower extent:
    - Local loads
    - TSO

Systems Involved

- Distributed Generators (+ grid connected inverters)
- Local control systems (voltage/frequency measurement device + embedded controller)
- LV/MV Distribution grid

Resulting Behaviour

Following load changes at time t=21, only the power output of the feeder transformer increases. This is because the load change does not cause a large voltage decrease near the DG units. Primary control increases active power output only if voltage levels go under the lower bound of the 'dead zone', which is the case for only a limited number of DG. Since insufficient extra local power is produced to feed the increased loads at time 21, the transformer connected to the transmission grid (indirectly via the MV distribution grid) feeds the shortage. Comparing the power output graph (Figure 6-2) and the voltage level graph (Figure 6-3), it is easily seen that only generators that are below the lower voltage bound diverge lightly from their power output setting P_0 (dashed lines in the power graph), and thus increase production (full line in the power graph) due to primary control. Looking at the economical graph in the figure showing marginal output costs, we see that power production is not at an economically optimal level, since marginal production costs are different.

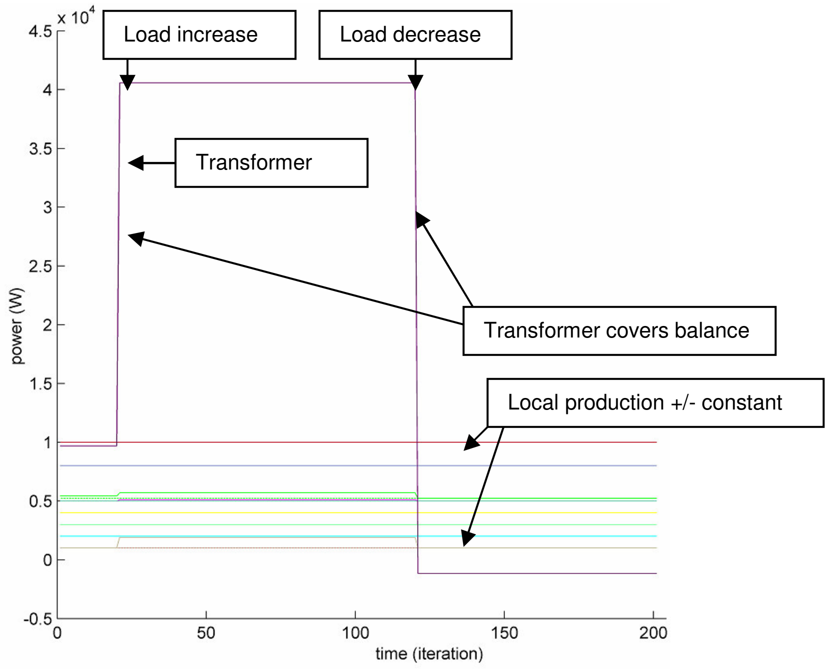


Figure 6-2: Active power outputs and power output setpoints P0

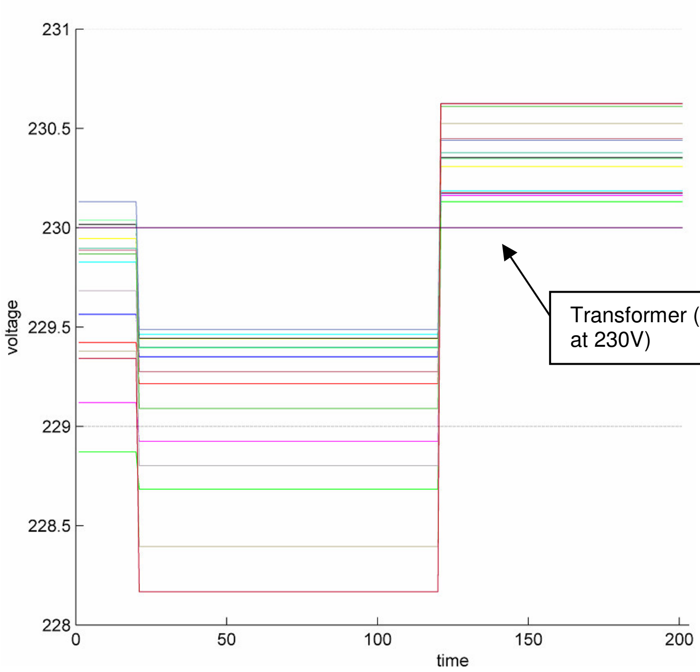


Figure 6-3: Voltage levels

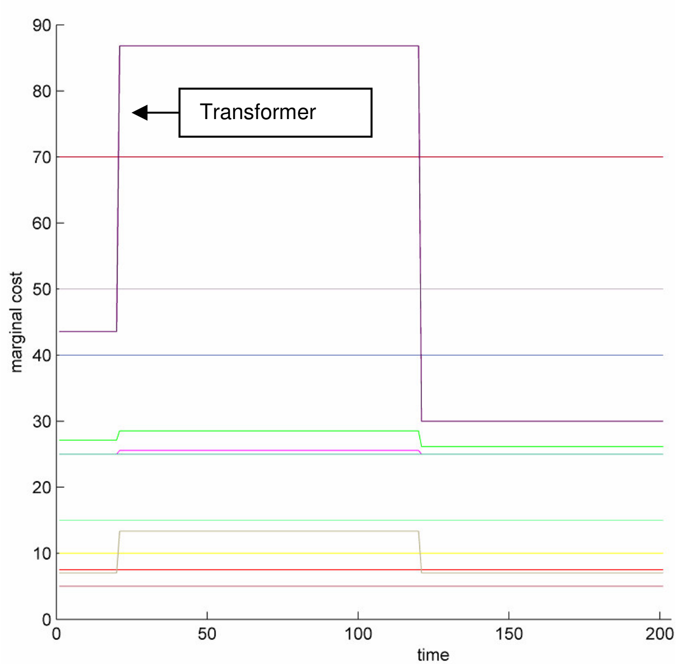


Figure 6-4: Marginal power costs

6.3 Normal behaviour, all control loops operational (Reference Scenario)

This first simulation shows the behaviour of the AEG under normal circumstances. All generators are directly or indirectly interconnected over a random overlay network. Each node in the overlay network has five neighbours. Both secondary and tertiary control are operational, and no faults have occurred in the system.

Stakeholders Involved

- DG owners
- DSO

- To some lower extent:
    - Manageable loads (possibly in economical control loop)
    - Local loads
    - TSO

Systems Involved

- Distributed Generators (+ grid connected inverters)
- Local control systems (voltage/frequency measurement device + embedded controller)
- Controller agents (PC with agent software)
- TCP/IP communications over LAN, WAN and/or the Internet
- LV/MV Distribution grid

Resulting Behaviour

Looking at the simulation graphs one sees strong fluctuations in power outputs at iteration t=1, t=21 and t=121, which last for about 20 iterations. After that, DG power output remains constant. The reason for the fluctuations is the combination of secondary and tertiary control converging to the Pareto optimal point that equalizes marginal costs along the system while taking voltage levels into account.

Time period t=[21,120] is the most interesting in this simulation. After the load increase, convergence occurs and all generators generate power at the same marginal costs, except for generators 9 and 15. There are large loads near generator 15, which pull down local voltage. For this, generator 15 generates at a higher marginal cost (higher production) as to minimize this voltage divergence. The load on the line containing generators 5 to 9 is rather low, causing these voltage levels to be high. Generator 9 produces below the global marginal cost as to limit the voltage on that line. Generator 6 also seems to diverge from global economical optimum, but this is not the case; generator 6 has a marginal cost below the optimum, but already produces its maximum output. The same holds for the feeder transformer during the other time periods: its marginal cost is above global optimum (in this case it is 30), but its production is 0.

Another interesting fact to point out is that load fluctuations are instantly balanced by the feeder transformer and nothing else. Afterwards, DG units start to adjust their power output because they have a different marginal cost than the feeder. Finally, one can also see in Figure 6-5 that the feeder transformer sometimes has a negative power production. This means it absorbs the surplus power production after the large load decrease.

In the presented scenario, one observes the ‘normal’ behaviour of the AEG. Convergence using the distributed gossiping scheme is quite fast after a sudden power demand change; it takes less than 10 gossiping rounds to settle around a global optimum. If we choose the gossiping steps to occur every second, optimization takes about ten seconds. If we account for inertia of involved DG units, this is more than fast enough, because these units can’t adjust their output any faster. In larger overlay networks (and larger underlying distribution grid, of course), or overlay networks with a less random structure, convergence might be a little slower.

Bandwidth Demand

The proposed system has a constant bandwidth requirement, which is dependent on the number of nodes in the system and the time interval between gossiping steps. Every node makes a single TCP-connection with a random neighbour at a fixed time interval (here an iteration step corresponds with a single time interval), and sends a few parameters (ΔP, P_0 and its cost graph) to its gossiping buddy. This communication is not all over a single communication line, but distributed over the Internet. The interval between gossiping steps can be adjusted in function of the available bandwidth and control system demands.

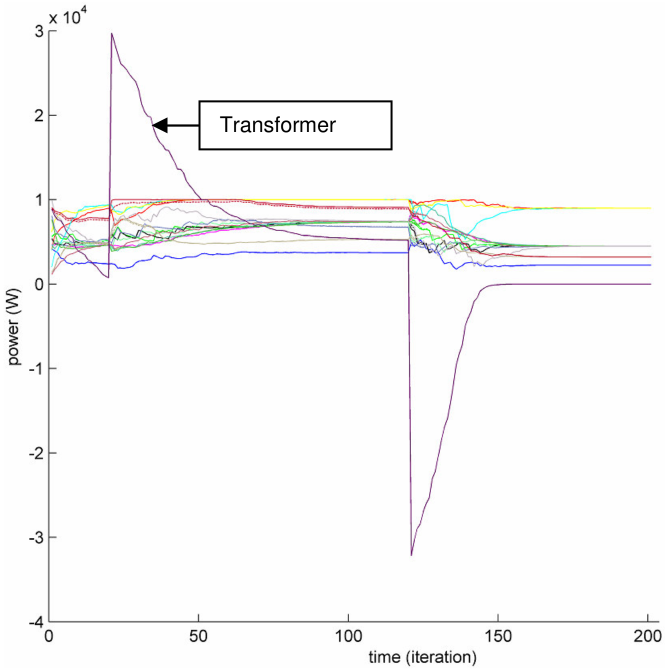


Figure 6-5: Power outputs

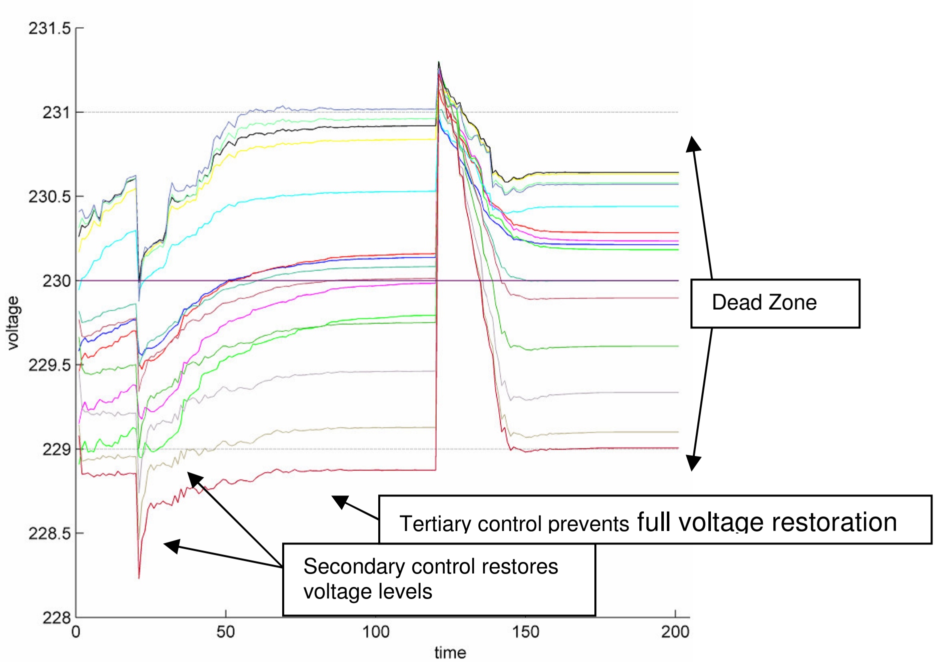
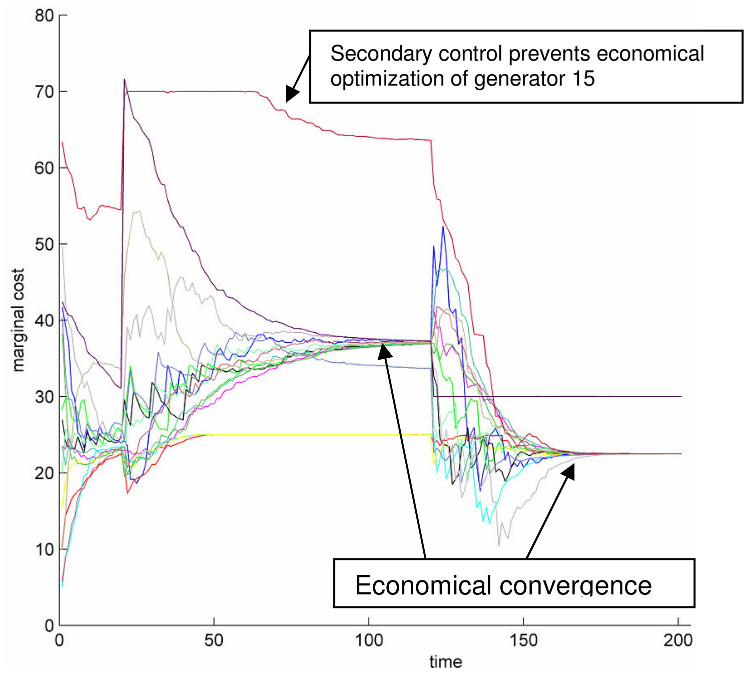


Figure 6-6: Voltage levels



Secondary control prevents economical optimization of generator 15

Economical convergence

Figure 6-7: Marginal production costs

6.4 Secondary control only (Reference Scenario)

To study the influence of secondary control on the application, or the influence of the absence (or failure) of tertiary control, some simulations are presented in which only secondary control is enabled.

Stakeholders Involved

- Same as scenario in section 6.3

Systems Involved

- Same as scenario in section 6.3

Resulting Behaviour

When the load increases at time step t=21, we see (as we have seen in previous simulations) that the grid mainly feeds necessary extra power. Simultaneously, some voltages locally exceed the dead zone which triggers primary control and overall average □P (= P_0-$P_{effective}$) no longer equals zero. This in turn triggers secondary control which steadily adjusts power output (actually P_0) of all generators (by the average ΔP). All DG units gradually increase their production, and as a consequence the voltage rises towards the nominal value. Due to the distributed gossiping based averaging algorithm the local calculation of the average ΔP takes some time (in the algorithm used here, convergence is assumed after 10 gossiping steps). This inevitably leads to a trade-off: using a shorter time than 10 rounds might speed up the system to adjust to the new situation, but the shorter the number of rounds, the worse the local estimation of the system-wide average ΔP. A too rough estimation might lead to undesirable oscillations.

It is easily seen in Figure 6-10 no economical optimization is done, and an economically suboptimal situation is created in which generators produce at different marginal cost. In this situation opportunity costs are suffered, which does not necessarily mean that real economic losses are suffered!

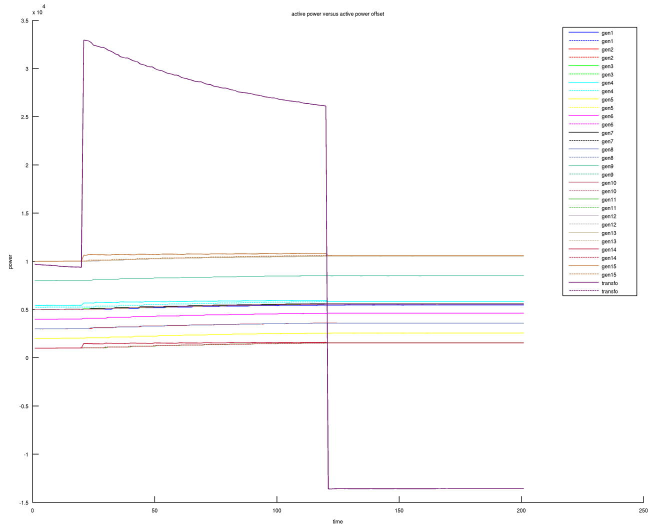


Figure 6-8: Active power output

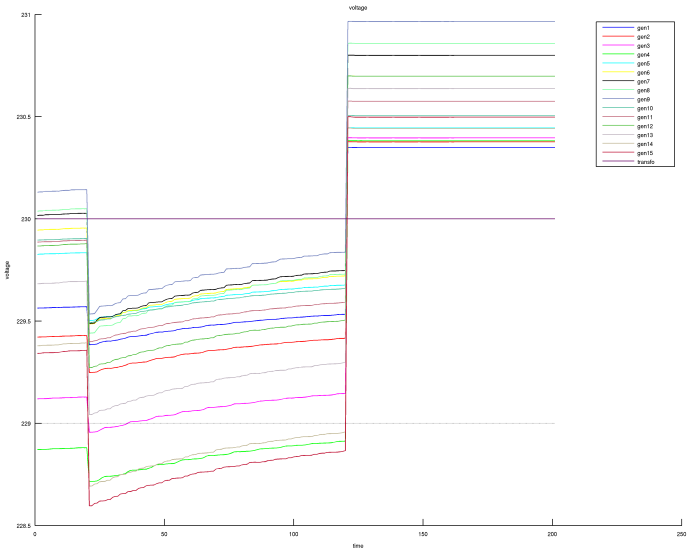


Figure 6-9: Voltage levels

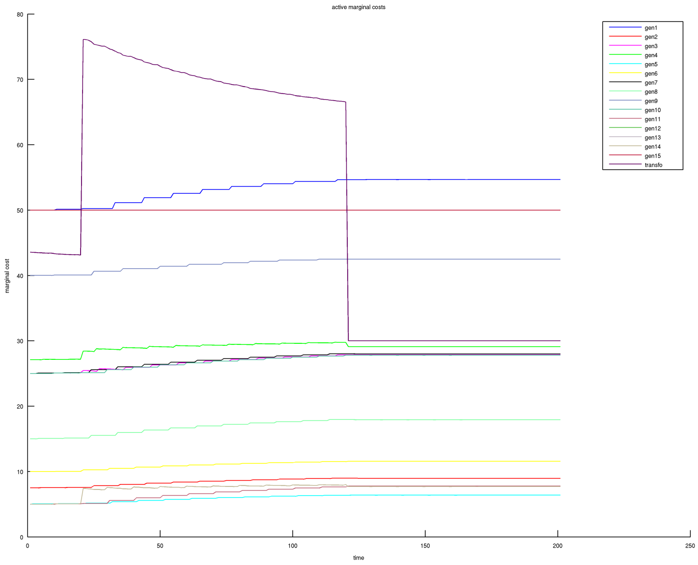


Figure 6-10: Marginal production costs

6.5 Tertiary control only (Reference Scenario)

Analogously to previous scenario, in this scenario only tertiary control is enabled while secondary is disabled. This shows the influence of tertiary control and the influence of the absence (or failure) of secondary control on the application.

Stakeholders Involved

- Same as scenario in section 6.3

Systems Involved

- Same as scenario in section 6.3

Resulting Behaviour

If we compare the results of this simulation with the ones of section 6.3 where both secondary and tertiary control are enabled, we see great similarities between these results. The main difference is the noticeable larger divergence of voltage levels near generators 14 and 15 at time t=[21,120] in this simulation. This of course is a result of the purely economical optimization policy, while power quality is ignored.

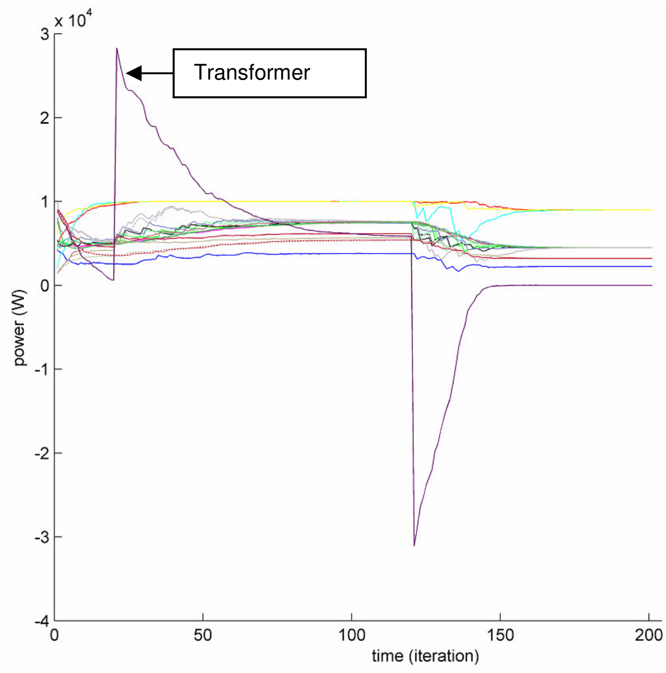


Figure 6-11: Power outputs

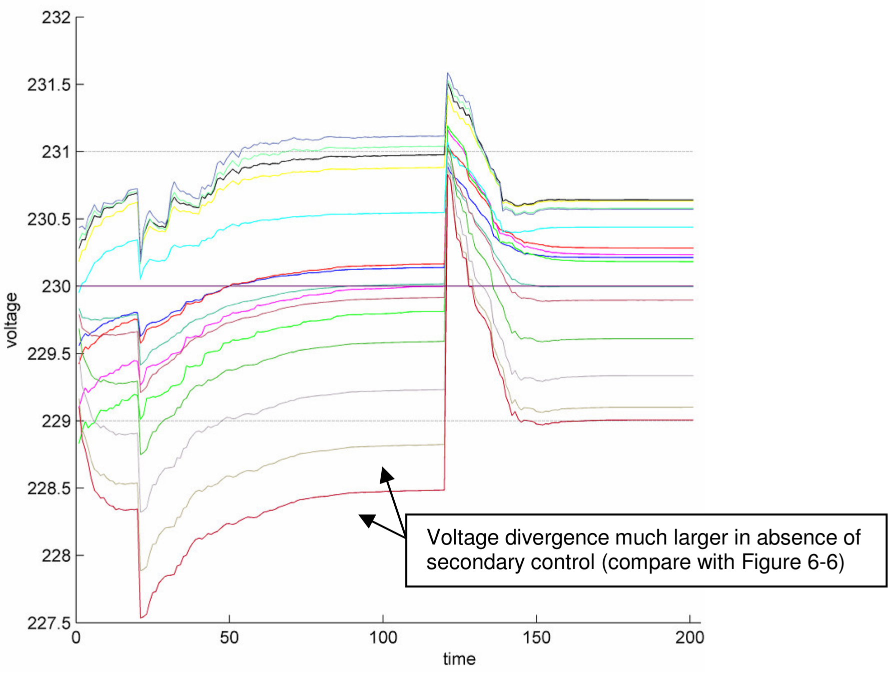


Figure 6-12: Voltage levels

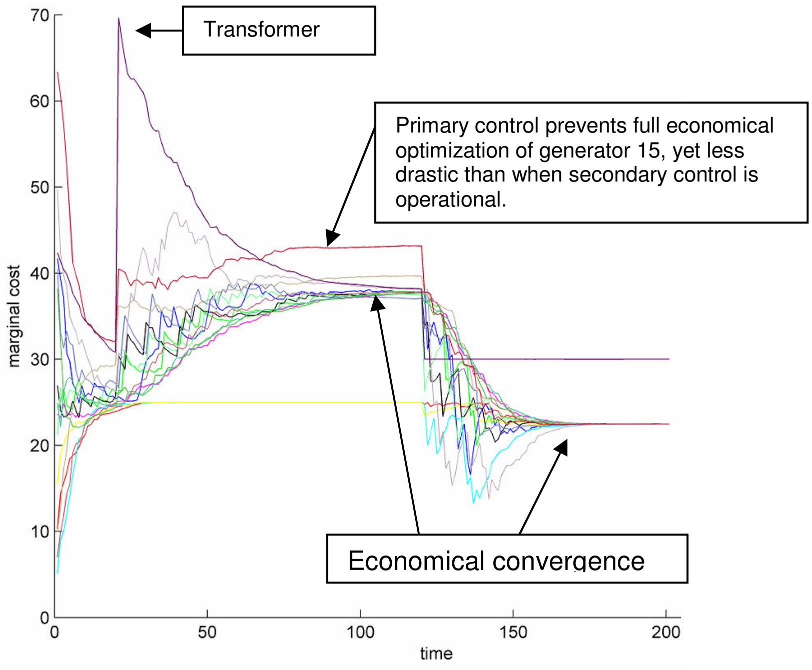


Figure 6-13: Marginal production costs

6.6 Network latency (Scenario 10)

Packet switched public networks such as the Internet can't give any guarantee about latency of packet delivery. The reason for this unpredictable and possibly unbounded packet delivery latency is because there are no bounds on the amount of packets that can be sent by any user at any time over any connection. This may cause contingencies at some routers (which have a store and forward mechanism), causing packets to be queued longer in the input and/or output buffer of the router. Ultimately this may lead to packet loss if the router input and/or output buffers are full.

Stakeholders Involved

- Same as scenario in section 6.3

Systems Involved

- Same as scenario in section 6.3

Resulting Behaviour

In the gossiping based averaging schemes of both secondary and tertiary control, gossiping steps are done in a timeframe of a second to a couple of seconds. There is a stochastic convergence time of these algorithms of about 30 to 100 gossiping cycles, mainly dependent on the overlay network structure. This means that generator control parameters are adjusted to a Pareto optimal point in about half a minute to a couple of minutes. Knowing typical generator inertia and rate of change in loads (or power consumption) and non-dispatchable generators, there is no need for any faster convergence. Now, in the Internet as we know it today typical latencies (round trip times in fact) are in the order of magnitude of 150ms, and it is gradually improving (see Figure 6-14). Certainly if we are considering short distance communication (AEGs cover only a single distribution net) the delays are rather small (about 30ms) in relation to the time between gossiping steps (about 1 to 2 seconds). From this we can conclude the influence of network delays on control system behaviour, even with cheap public networks, may be neglected.

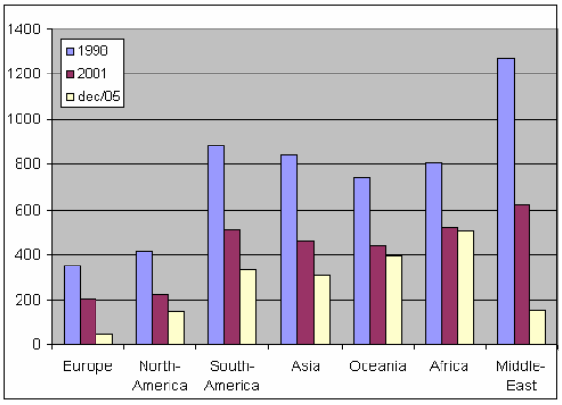


Figure 6-14: Average round-trip-time in milliseconds between Ghent (Belgium) and other parts of the world world (measured by the Department of Information Technology, Ghent University)

6.7 IP-packet losses (Scenario 11)

As explained in previous scenario, packets can get lost on packet switched networks such as the Internet, due to routers dropping packets when their buffers are almost full or when packets are corrupted during transmission (leading to faulty CRC). How will these packet losses influence the functionality of the distributed control system?

Stakeholders Involved

- Same as scenario in section 6.3

Systems Involved

- Same as scenario in section 6.3

Resulting Behaviour

Looking at Figure 6-15 showing typical packet loss over the Internet, we see that nowadays only a small percentage of sent packets is lost (especially when sent to a nearby location), and this rate is gradually improving. Also, during a gossiping step, a TCP-connection is set up between the gossiping partners. The TCP transport protocol will cover packet loss by retransmitting lost packets. As a consequence, even when networks are heavily loaded (and consequently packet loss is high), this will be seen as a connection with somewhat larger delays than usually. Given the low probability of packet losses, this situation is covered by previous scenario (section 6.6) and will not be discussed here any further.

In the extreme, the TCP connection may suffer so many packet losses that subsequent timeouts lead to the point where the TCP-connection is closed. From application level this is seen as a network failure or a node crash (one cannot distinguish these). This situation is discussed later in the following scenario (section 6.8).

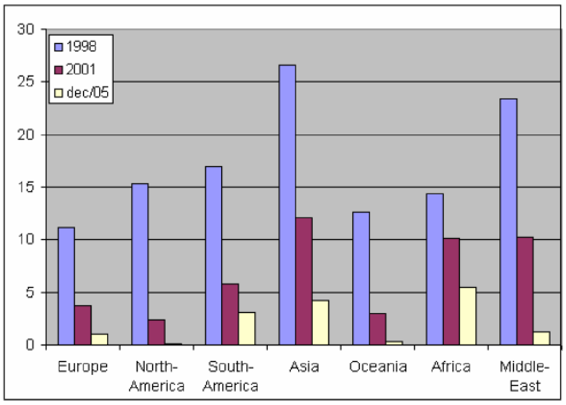


Figure 6-15: Average packet loss percentage between Ghent (Belgium) and the rest of the world (measured by the Department of Information Technology, Ghent University)

6.8 Agent control system (or network) unavailable (Scenario 12)

By a non-critical control system failure we mean the failure of the non-critical part of the control system of a single node, which is responsible for secondary and tertiary control. Critical functions, such as primary control, are still functional in this scenario.

We can distinguish two different scenarios: the node was part of the overlay control system and then fails, or the node has never been connected to the rest of the control system. The former will always occur due to a failure (computer crash/network failure), while the latter may also follow from the fact that not all generators in the distribution net have this kind of control system (which is very likely in a deployment in distribution systems of nowadays). Mind that in both cases, although there is no connection on ICT-level between the node and the rest of the system, they are still connected electrically.

Stakeholders Involved

- Same as scenario in section 6.3

Systems Involved

- Same as scenario in section 6.3

Resulting Behaviour

In a typical real world deployment of this AEG system it would be very likely to have some DG units in the distribution net that don’t participate in the distributed control system. Coarsely spoken, these are just ‘negative loads’ for our AEG. If these non-participating DG are small enough, they will be negligible (they have no influence on voltage levels). Larger DG units (which have a non negligible influence on voltage levels) have a mandatory voltage regulator (some sort of droop control), and so they should not cause a too large deviation from rated voltage. Voltage at the injection point of this DG unit will not optimal, but when installed properly, it should be within allowable limits. Of course the system will not be economically optimal, since a generator is not taking part in the tertiary control scheme.

Another scenario in which non-critical control systems are unavailable for a single DG unit is the case in which the control system (or the communication link) fails while it is participating in the secondary and primary gossiping schemes. At first sight the system degenerates to the previously discussed case of a distribution net with a generator that is not taking part in the distributed control system. Although there is more to it for what is concerned the secondary control. Unanticipated loss of a node which is taking part in the distributed averaging algorithm may lead to small divergences in the calculated global average. These errors can, even if the crash is discovered or the crashed node comes back online, not be solved easily.

Figure 6-16 illustrates this behaviour. The real global average is 6 (in the beginning). In the third step a node is lost. This changes the real global average to '5.333'. The algorithm settles after convergence on '5.666', which is different from both the real current average '5.333' and the original average '6'. These errors may accumulate over time, since they can't be easily detected in a distributed way.

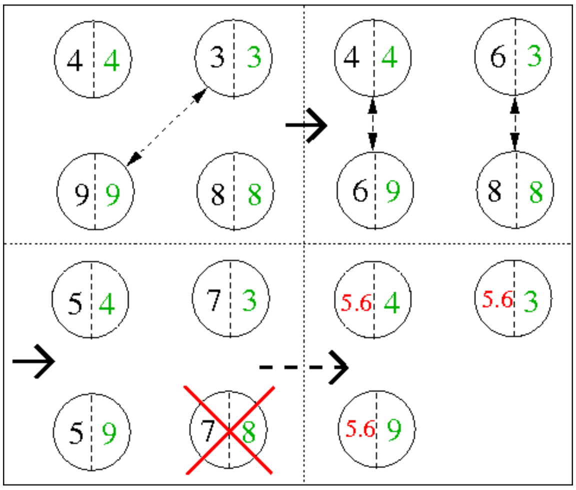


Figure 6-16: Consequence of node failures for distributed averaging.

These general remarks on gossiping based averaging lead to following conclusions:

> *When a controller fails when the secondary control is not in a converged state, and this controller does not re-enter the system, or is reset when it re-enters the system, a system wide divergence of the estimated average value of ΔP will follow, which cannot be restored automatically.*

When we are dealing with totally random failures with nodes not re-entering or being reset (so typical network failures are not part of these), the divergence should be limited due to the fact that the system converges quite rapidly (and thus the lost value will be close to the system wide average), and due the fact that faults may cancel each other. A periodic system wide reset might however be needed to limit divergence in the long run.

6.9 Critical Control System Failure (Scenario 13)

If the primary control system of a DG unit fails, or any other part of the DG unit, local physical protection devices should act to decouple the unit from the distribution net. This is to protect the rest of the distribution net from a possibly escalating fault. When local protection fails after for example a short circuit, a local blackout of a power distribution segment might follow when other protection devices isolate the segment from the rest of the grid; but the latter will happen only exceptionally, since physical protection devices that protect against overcurrents (e.g. after short circuit) are very reliable. The most important consequence will thus be the loss of a single production unit.

Stakeholders Involved

- Same as scenario in section 6.3

Systems Involved

- Same as scenario in section 6.3

Resulting Behaviour

In grid connected mode the instant loss of a DG unit will immediately be covered by the transformer that connects the segment with the grid. The transformer is dimensioned as to be able to feed the whole low voltage segment and the grid has –seen from distribution level- an infinite power supply. Afterwards, secondary and tertiary control can take the microgrid back to a Pareto optimal state.

6.10 Denial of service attacks on IP-network (Scenario 14)

Denial of Service (DoS) attacks try to disturb the functionality of some system or service. Since we are using public communication channels, these attacks can be executed on these channels. They can be generic (caused by a worm or virus attacking random computers/networks) or aimed at this specific control system. An aimed DoS attack may use the overlay-network mechanisms to perform the attack; an example may be constantly joining and leaving the overlay-network, which triggers a bandwidth consuming algorithm searching new neighbours. This may lead to a denial of all communications over one or more channels.

Stakeholders Involved

- Same as scenario in section 6.3
- Telecom Provider

Systems Involved

- Same as scenario in section 6.3

Resulting Behaviour

Whatever the underlying reason or mechanism for the DoS attack, as a result we get very long communication delays, which lead to loss of connection between some or all agents. The resulting behaviour is thus covered by previous section 6.8.

6.11 Attack on overlay network topology (Scenario 15)

The basic idea of overlay networks is letting nodes connected to some common communication infrastructure (e.g. computers on the Internet) organize themselves in a distributed way, as to be able to retrieve certain nodes or resources on those nodes when needed. The structure or topology of these overlay networks is dependent on the rules for these nodes to choose their direct neighbours in the overlay network. The fault tolerance and resource discovery ability of overlay networks is dependent on the right application of these rules. One attack scenario could be an attack on this topology by some malicious node(s). These would send wrong query results to nodes searching for new neighbours as to make themselves the new neighbour of these nodes. After some time, these malicious nodes can become the centre of the overlay network.

In the overlay network used in the microgrid application, a malicious node can fake its identity by sending false XML descriptions to other nodes. These descriptions determine the choice of the direct neighbours of a node. If the malicious node chooses this fake description in function of the requesting node, it can make the semantic distance to this node very small which will mislead the other node in choosing the malicious node as a new neighbour. Continuing this process makes the malicious node(s) the centre of the whole overlay network. There is no easy way for the other nodes to detect this attack.

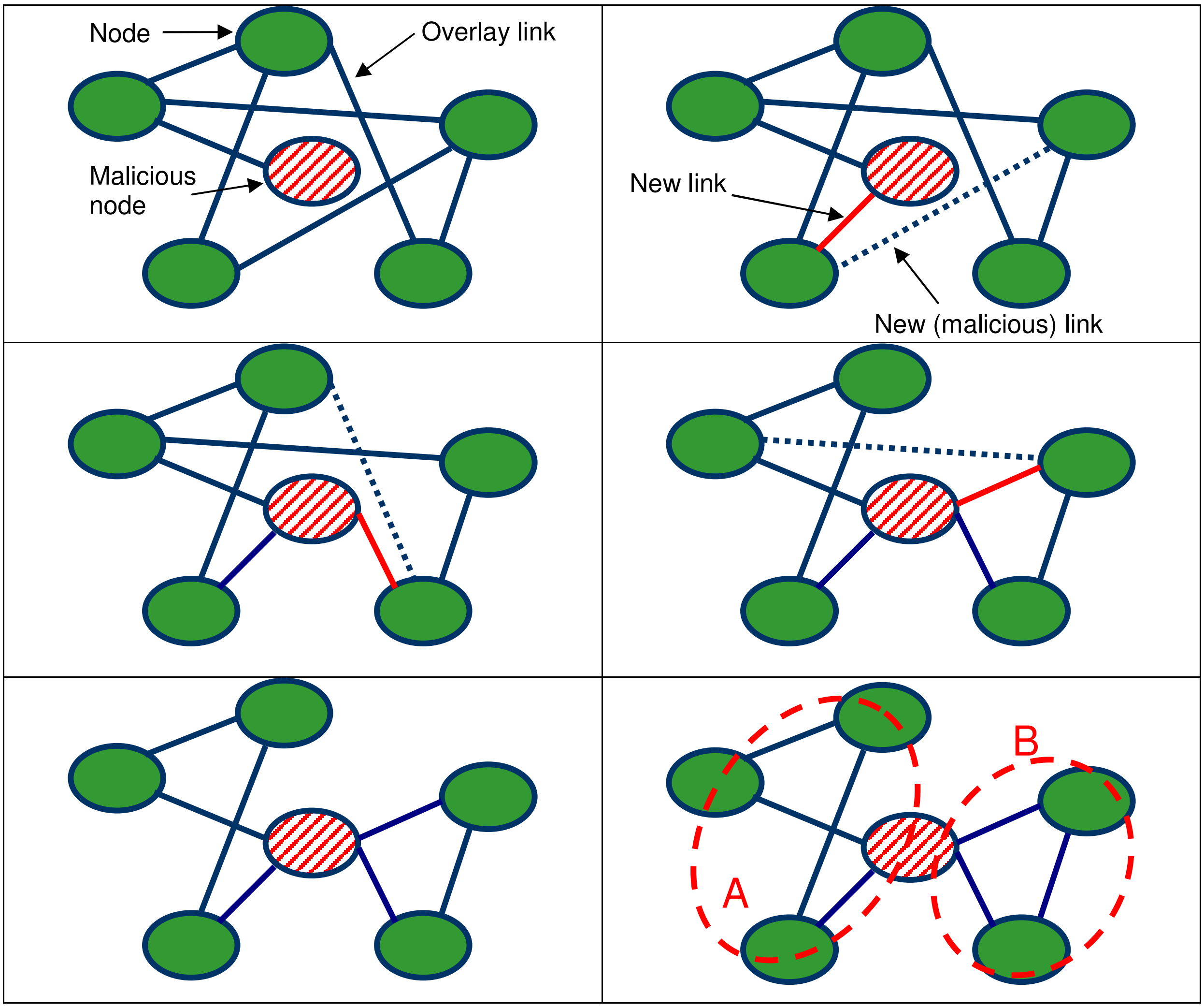


Figure 6-17: Example of an attack on overlay network topology which makes malicious node the sole connection between two groups (group A and group B) of overlay nodes.

Stakeholders Involved

- Same as scenario in section 6.3

Systems Involved

- Same as scenario in section 6.3

Resulting Behaviour

This attack on the middleware level (which is the overlay network) does not necessarily influence application level (secondary and tertiary control). Yet, it gives the attacker more power over the overlay network, and consequently over the applications that use this structure. Next two scenarios show how this power can be abused.

6.12 Overlay network partitioning (Scenario 16)

An interesting scenario occurs when the overlay network partitions. This may be caused by a bad overlay network structure (not enough neighbours per node or insufficient randomness in chosen neighbours leading to clustering), by major communication infrastructure failures, which may partition the underlying physical network (e.g. failures of routers), or more probable, by a malicious attack on the overlay network (see previous scenario).

In this scenario we have partitioned the overlay network in two groups:

1. Generator 1 to generator 9 controller agents
2. Generator 10 to generator 15 controller agents + grid connected transformer

Note that the system remains connected electrically.

Also, no load updates occur during the simulations; like this one can observe the steady convergence from initial generator settings towards some stable point. This makes underlying control system functionality much clearer.

Stakeholders Involved

- DG owners
- Local loads
- DSO

Systems Involved

- Distributed Generators (+ grid connected inverters)
- Local control systems (voltage/frequency measurement device + embedded controller)
- LV/MV Distribution grid

Resulting Behaviour

Figure 6-18, Figure 6-19 and Figure 6-20 show the results of this scenario. The influence of the splitting of the overlay network can easily be seen, as two clearly distinct groups are observed, especially in the graph plotting the power production (marginal) costs. This is clearly sub-optimal behaviour, since marginal costs are equal in the economical optimum. In some cases secondary control may also be hampered, where voltage levels are below or above the dead zone in one overlay partition, but the generators which are able to mend this are in the other partition.

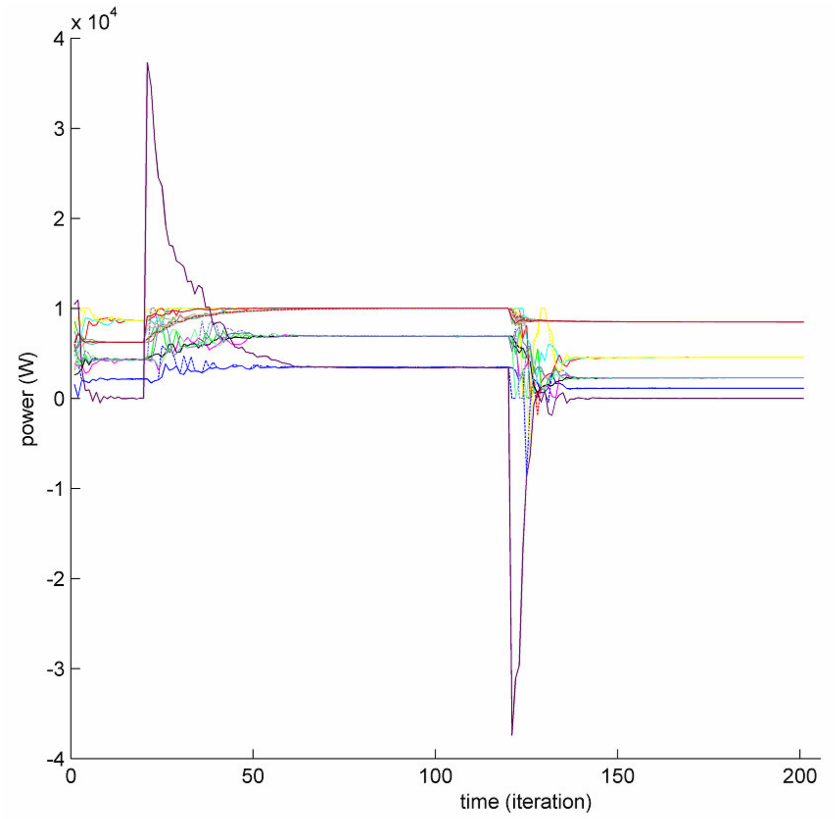


Figure 6-18: Power output

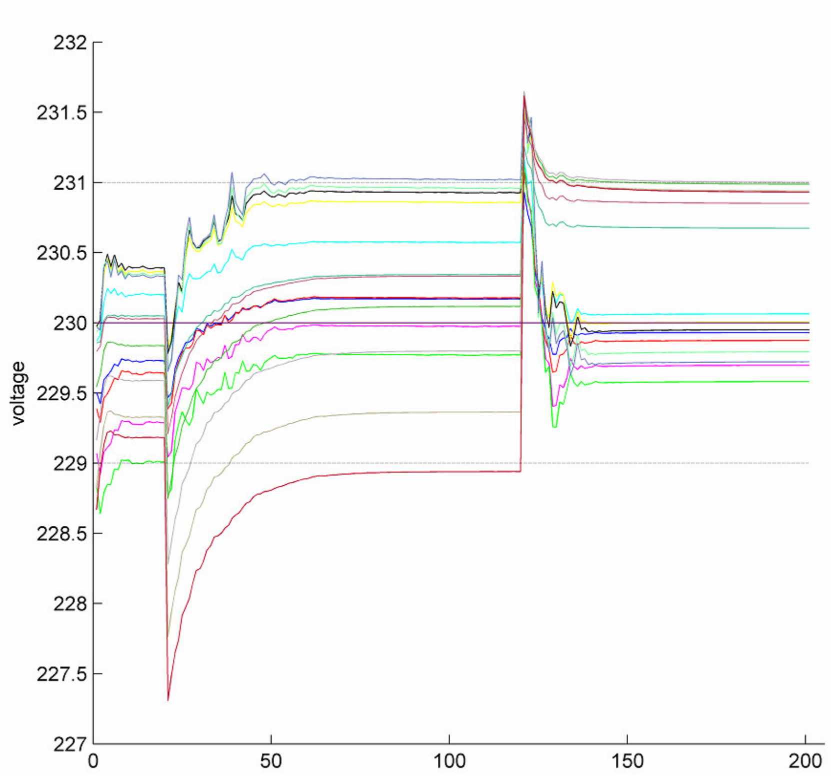


Figure 6-19: Voltage levels

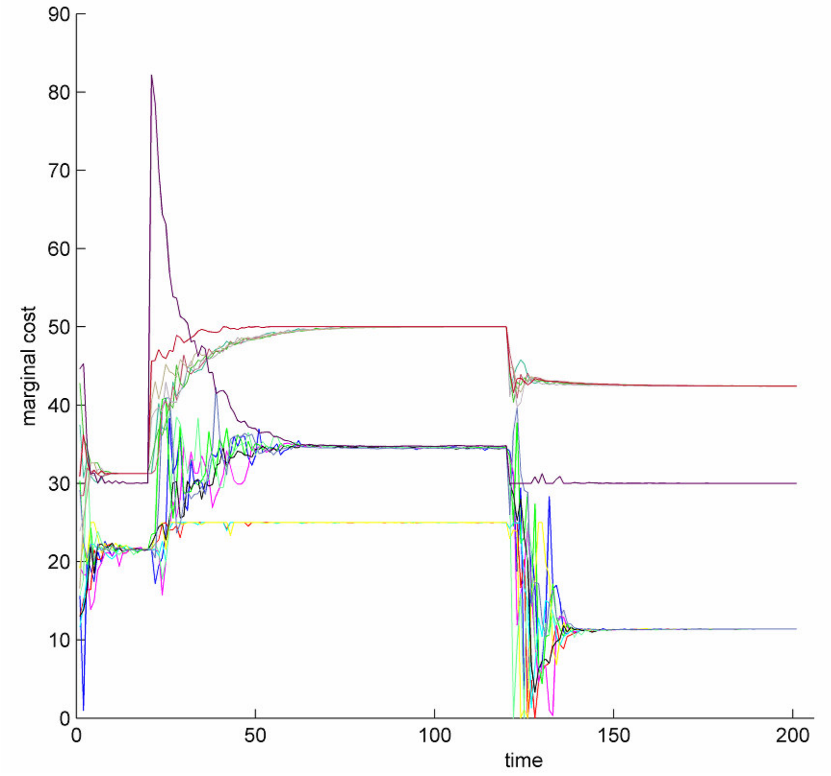


Figure 6-20: Marginal production costs

6.12.1 Representing the Control System Scenarios by means of UML diagrams

In this section, we represent by means of UML state diagrams, the effects of a network partitioning, as described in the Scenario16. The other forms of attack described in the other scenarios are represented in section 8.2.8(appendix).

Figure 6-21 depicts the possible states of the a malicious agent, i. e. an agent joining the overlay network with the aim of performing some kind of malicious attack to the network. Such an agent is initially in the state *Created*, then it turns to the *UnderRegistration* state in order to join the overlay network. When this activity is completed, the malicious agent turns to the state *Active* representing the situation where the agent is performing its malicious activity. Actually such state is a super-state whose sub-states represent the possible forms of attack that the malicious agent may perform; such sub-states are: *VoltageLevelAttack*, *DosAttack*, *ChangingTopology, ManInTheMiddle*. The state *ManInTheMiddle* is in turn a super-state containing the substates *PartitionNetworkAttack* and *EconomicalTampering* representing the attempt to partition the overlay network and the dispatch of faked economical information respectively. Both sub-states are reachable from the state *ChangingTopology* representing the situation where the malicious agent establishes some malicious links in the overlay network. This step is necessary to perform both the malicious partitioning of the network and the economical tampering.

When the agent leaves the *Active* state, it turns to the state *RemoveRegistration* representing the stage where the agent leaves the overlay network. When the agents quits this state, it turns to the final state *Removed*.

With respect to the state diagram of the non malicious agent (Figure 3-30), the state diagram of the malicious agent (Figure 6-21) differs for the malicious activities inside the *Active* state.

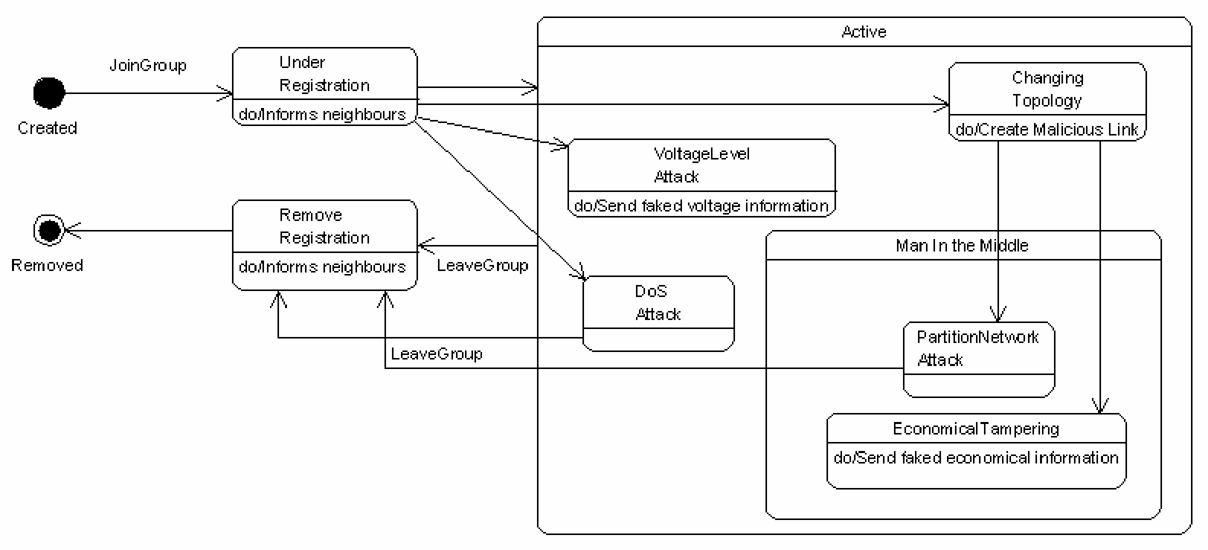


Figure 6-21: State diagram of a malicious agent

The possible states of the overlay network are shown in the state diagram in Figure 6-22 where the state transitions are due to the effects of the activity of a malicious agent (the states of a malicious agent are described in Figure 6-21).

The overlay network is initially in the *Normal* state, and turns to the state *SinglePointOfFailure* when a malicious agent turns to the state *ManInTheMiddle* (see the state diagram in Figure 6-21). In other words, such state transition occurs when a malicious agent is able to partition the overlay network or is able to send malicious economical information.

The overlay network turns from the state *SinglePointOfFailure* to the state *Partitioned* when the same malicious agent has determined the partition of the overlay network.

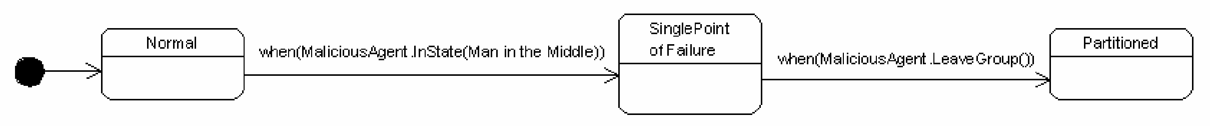

Normal
when(MaliciousAgent.InState(Man in the Middle))
SinglePoint of Failure
when(MaliciousAgent.LeaveGroup())
Partitioned

Figure 6-22: State diagram of the overlay network

The state diagram in Figure 6-23 shows how the voltage regulation in the distributed generation is affected by the attack of a malicious agent (the states of a malicious agent are shown in Figure 6-21). According to such state diagram, the primary voltage regulation is not affected by the attack (the primary voltage regulation does not change its state). The secondary voltage regulation is initially in the *Optimal* state where no attack has been performed. From the *Optimal* state, the secondary voltage regulation can turn to the state *Degraded* if the overlay network is partitioned by the action of a malicious agent. Otherwise, the secondary voltage regulation can turn from the state *Optimal* to state *DangerouslyOutOfRange* if a malicious agent is negatively influencing the secondary voltage regulation by transmitting malicious information about the voltage levels.

The tertiary voltage regulation is initially in the state *Optimal* where no attack has been performed. From this state, the tertiary voltage regulation can turn to the state *SubOptimal* if a malicious agent performs the partition of the overlay network, or if a malicious agent performs the economical tampering. The tertiary voltage regulation turns from the state *Optimal* to the state *Abnormal* if a malicious agent is negatively influencing the secondary voltage regulation by transmitting malicious information about the voltage levels.

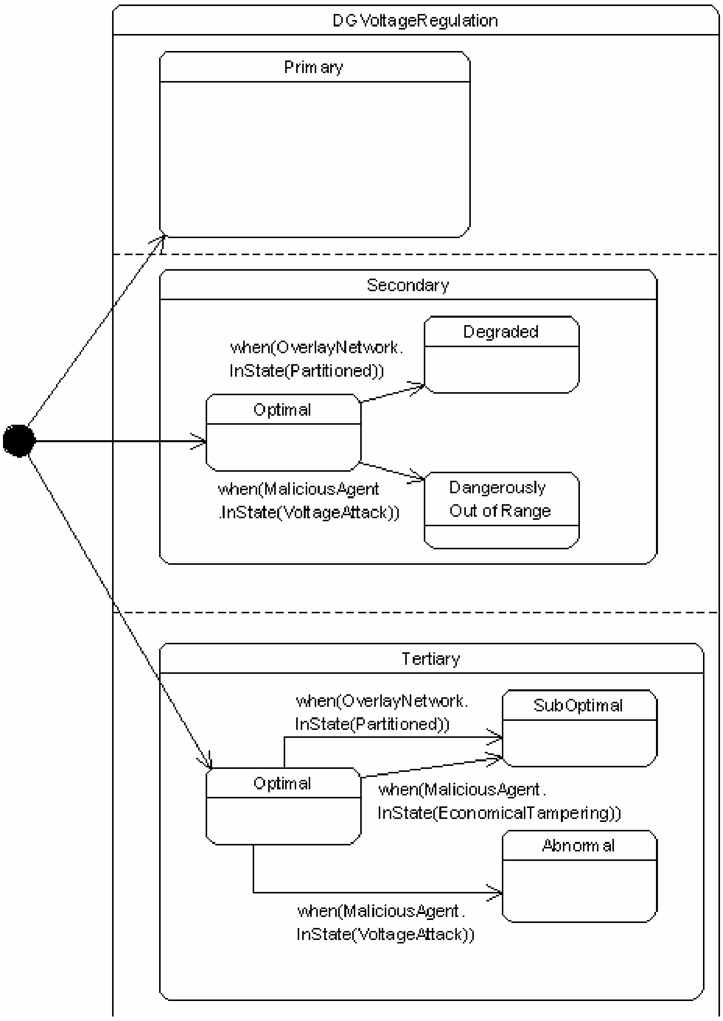

DGVoltageRegulation
Primary
Secondary
when(OverlayNetwork.InState(Partitioned))
Degraded
Optimal
when(MaliciousAgent.InState(VoltageAttack))
Dangerously Out of Range
Tertiary
when(OverlayNetwork.InState(Partitioned))
SubOptimal
Optimal
when(MaliciousAgent.InState(EconomicalTampering))
Abnormal
when(MaliciousAgent.InState(VoltageAttack))

Figure 6-23: State diagram of the voltage regulation in distributed generation system

6.13 Economical tampering attack (Scenario 17)

The single biggest reason for people to misconduct or to hack into a system like this is personal financial gain. Since a power market based mechanism is used, which determines the income of the respective DG owners, the economical control loop may be a tempting target. Various types of malicious attacks can be expected here: passive eavesdropping, altering messages sent from one generator to the other or spoofing another legitimate generator. The attacker can try to influence the market price using any of these mechanisms, lowering the price if the hacker is a consumer or raising the price if he is a producer. An example of a market tampering attack is shown in Figure 6-24 where a malicious node can determine all price information flowing from one side of the overlay graph to the other following the topology attack described in section 6.11.

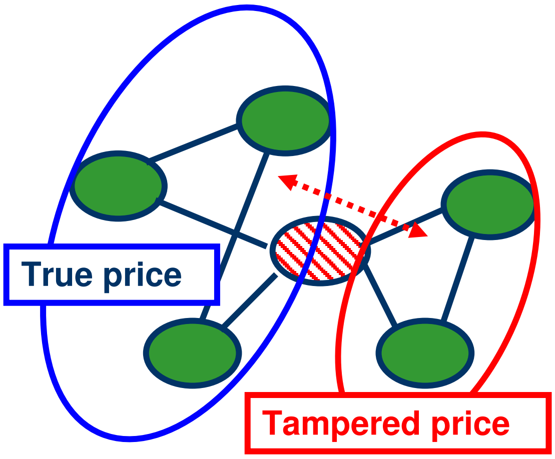


Figure 6-24: Market price tampering attack

Stakeholders Involved

- DG owners
- Local loads
- DSO

Systems Involved

- Same as scenario in section 6.3

Resulting Behaviour

If one subgroup is connected to a transformer broadcasting the true spot market price, the malicious node(s) can fake this spot market price as to decrease or increase the price, dependent on the fact whether the attacker is a producer or a consumer. The exact attack pattern will of course be dependent on market and metering mechanisms used for these kinds of applications.

6.14 Voltage level attack (Scenario 18)

The secondary control loop implemented by the multi agent system optimizes the voltage level in all points of the distribution grid segment as to minimize the divergence from rated values. Since over-voltages are dangerous for all equipment attached to the power grid, attacks on the secondary control loop are very tempting for attackers who want to inflict physical damage to the system. The most probable course of action would be the injection of false values in the secondary control loop (which is based on a distributed averaging algorithm). Over time these errors accumulate and the global average will diverge from its true value, leading to too high or too low active power injection in the grid.

Stakeholders Involved

- DG owners
- Local loads
- DSO

Systems Involved

- Same as scenario in section 6.3

Resulting Behaviour

If one succeeds in raising the power output of many generators simultaneously, voltage levels may become dangerously high. This may destroy certain assets (sensitive loads, generators, power cables…) or, more likely, over-voltage switches may disconnect DG units or whole distribution segments from the power grid, leading to loss of production capacity or even a local black-out.

The simulation, from which the resulting graphs are depicted in Figure 6-25 and Figure 6-26, shows the result of a single agent injecting way too large values for DP into the distributed averaging algorithm. A large average ∆P normally means that voltage levels are low in most parts of the distribution grid, and this encourages generators to increase active power production. It is easily seen in Figure 6-25 that all local generators increase their production, and that the feeding transformer has a large negative production. This means that excess power flows back to the transmission grid. Large active power injections also increase local voltage levels, leading dangerously high voltage levels, and thus a successful voltage level attack.

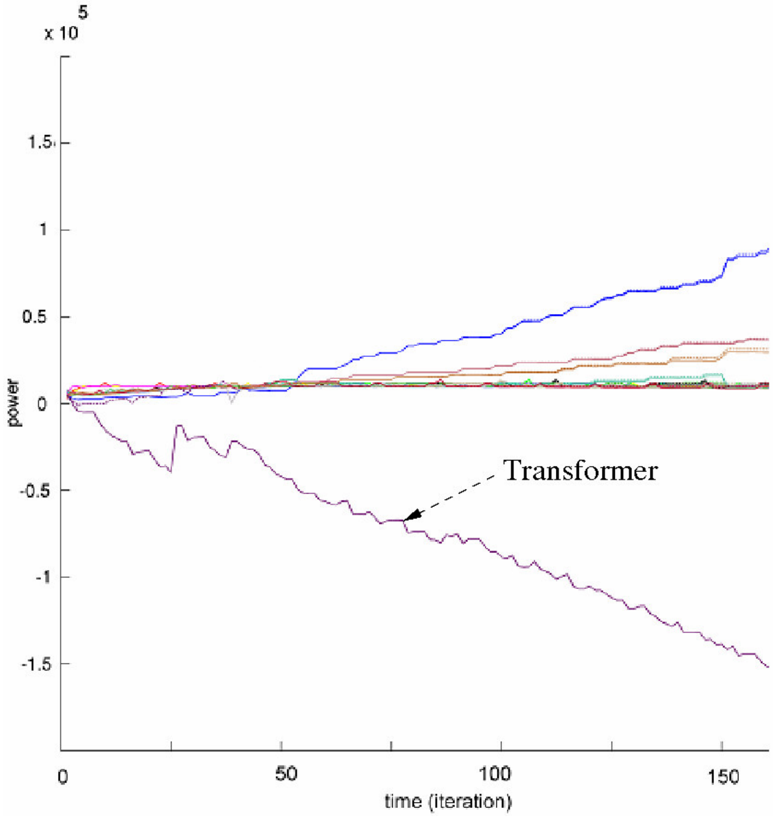


Figure 6-25: active power output

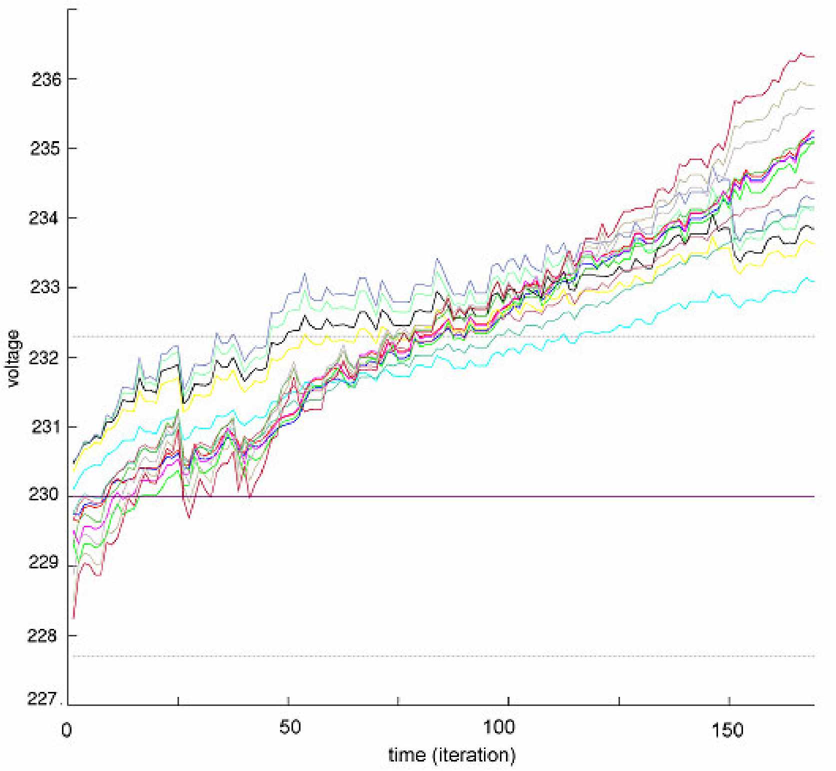


Figure 6-26: voltage levels

6.15 Alternative approach, centralized control (Scenario 19)

The secondary control loop has been implemented in a distributed way. What would be the consequences for the system to have a centralized client-server topology with dedicated communication lines? This scenario investigates the use of such a centralized architecture.

Using a centralized architecture radically changes the control system on architectural, infrastructural and organizational level. Centralized secondary and tertiary control is a common practice in the power grid, where power output of large power plants is centrally controlled in order to keep voltage and frequency stable. Tertiary control has somewhat changed with the advent of the power markets, but the basic idea can still be applied within a single generation company. Consequently, this means that the standard centralized algorithms can also be applied on a system like a single distribution grid (radial MV/LV segment) in order to optimize voltage and production costs.

Looking at architectural level of the ICT part of this system, the infrastructural requirements are also very different. First of all, we need a single centralized server with enough processing power to execute the system wide optimization problem for the two optimization loops. This server has to be very reliable, since it forms a single point of failure to this system. For this, backup servers may be an indispensable asset. Secondly, bandwidth usage is totally different from the distributed system. In the centralized system, all agents (or clients) have to send their parameters (current production, marginal cost curve…) to the server, and after the server receives all these parameters and has calculated the new settings, it replies with to each client once. This process has to be repeated with some fixed time interval. The amount of messages sent is thus *O(2n)* with *n* the number of agents in the system. In the gossiping based system, the amount of messages sent per gossiping cycle is $O(n^2)$, but these messages are distributed all over the communication infrastructure, while in a centralized system they all go over a single communication channel to the server. This means that next to a reliable server, a reliable broadband communication channel will be needed for the server.

Stakeholders Involved

- Server provider (DSO, third party?)
- DG owners
- DSO
- To some lower extent:
    - Manageable loads (possibly in economical control loop)
    - Local loads
    - TSO

Systems Involved

- Server(s) for centralized secondary control
- Distributed Generators (+ grid connected inverters)
- Controller agents (PC with agent software)
- TCP/IP communications over LAN, WAN and/or the Internet
- Local control systems (voltage/frequency measurement device + embedded controller)
- LV/MV Distribution grid

Consequences

- A trusted party has to install a reliable server. The question of who will have to take this responsibility remains. The server and broadband channel are an extra cost for this layout.
- Attack scenarios are totally different than with the fully distributed approach. DoS attacks are very likely, and probably easier to pull off since only a single server/communication channel has to be blocked. Identity spoofing or man-in-the-middle attacks on the central server have a much bigger impact on the system than with the distributed approach. Yet, strong authentication with a single certified server is easier than certification and trust within a peer-to-peer system.
- A single algorithm cycle is enough to reach the optimal system state (send parameters to server-calculation of optimal settings-replies to clients), while in gossiping approach the system will probably be constantly evolving towards a near-optimal point. Bandwidth demand is constant in both cases (both approaches send a fixed number of messages within a certain time interval). Which of the two has the fastest convergence is dependent on the calculation speed of the server, the chosen (in function of bandwidth) intervals between algorithm cycles, and the specific bandwidth availability on the communication channels.

7 CONCLUSIONS

This document reports the results of the activities performed in the Work Package 1 “Identification and description of Control System Scenarios” of the “CRitical UTility InfrastructurAL resilience (CRUTIAL)” project, as described in the Annex 1 to the EC contract n° 027513.

The Work Package 1 of the CRUTIAL project was devoted to the identification of critical control system scenarios to be used by the other Work Packages of the program.
The concept of control system scenarios revealed a valuable support for starting the discussion on the interdependencies of power and ICT infrastructures during the first year of the project running. A lot of information has been acquired and exchanged within the consortium allowing to build several cross-references with the other active work packages.

The specification of the (portion of) Electrical Power system that is of interest for CRUTIAL is given in the form of natural language with the support of picture with drawings and symbols that are commonly used by electrical people, as well as in the form of a collection of UML diagrams, a language with whom computer science people are more familiar.

A set of reference control system scenarios have been identified, covering emerging themes involving ICT for Power System bulk and distributed generation, transmission and distribution infrastructures, like the following ones:

- Communication security in the supervision and control systems of grid and generation operators
- Possible breaches caused by interactions between the corporate and the process networks
- Interactions among Transmission, Distribution and Generation ICT systems
- Possible problems related to the ICT system’s remote maintenance.

The investigation on the ongoing technological renewal in the regulation and control systems of (bulk) power generation, transmission and distribution allowed to derive an integrated view of the many ICT systems involved. The control scenarios selected represent examples of inter-infrastructure and inter-operator platforms to be further developed in the future project studies: different level of protections have to be integrated in the infrastructures of the different operators for providing an adequate resilience to the management of the whole Electrical Power System.

Both the computer simulation studies presented in the distributed generation scenarios and lab simulations show that this microgrid functions quite well under normal circumstances, independent of the fact whether the system is islanded or not. In islanded mode, the generator capacity has to be sufficient to feed the loads connected to the distribution segment. Automatic balancing by load shedding or load management is not supported yet. Although the computer simulations presented here do not account for dynamic electrical system behaviour or frequency regulation, they are a useful tool to supplement lab experiments in order to simulate a larger environment than is feasible in a lab. Also, doing fault injections are somewhat safer in a computer simulation then when using a real laboratory set-up.

The results from these simulation show that the main challenges the current microgrid has to deal with are concerned with IT-security issues, certain weaknesses in the overlay network protocols and some weaknesses in the generator control loops (mainly secondary) implemented on this overlay network. Further work within the CRUTIAL project will thus look into these weaknesses and try to mitigate these. This can be done by implementing best-practices for security (firewalls, cryptography, certification, strong access control mechanisms, etc.), but also extensions to its current functionality and adaptations of current algorithms are envisioned.

The specification using UML diagrams has been used in WP1 as a way to elicit information from domain experts, as well as a way to communicate domain information to experts of computer science with limited knowledge in Electrical Power Systems. The plan is to use the UML specification as a basis for completing the initial proposal of the modelling framework in WP2 and for the specification of the analysis scenarios to be implemented in WP3 and WP5.

The WP1 material shared within the CRUTIAL consortium forms now a solid common know-how for the future developments of the project. In the next two years of the CRUTIAL project the control system scenarios identified in WP1 will be used as a reference for the analysis of interdependencies among ICT and power devices, for the development of the test beds, for studying and evaluating the resilience of architectures.

8 APPENDIX: UML

8.1 UML representation of the Electric Power System

8.1.1 Power System Infrastructure

Figure 8-1 shows the UML class diagram of the general Electric Power System; the aim of this diagram is indicating which are the main subsystems of the electric power system (or Power System Infrastructure). The main class is *PowerSystemInfrastructure* representing the whole electric power system; this class is the aggregation of the classes representing the main subsystems of the electrical system:

- *PowerGeneration* represents the set of power plants for the generation of electric power; this class is the aggregation of the class *PowerPlant* representing the power plants;
- *PowerGrid* represents the infrastructure used to transport the electric power from the power plants to the consumers; this class is the aggregation of these classes:
  - *TransmissionGrid* represents the grids transferring the electric power from the power plants to the distribution grids;
  - *DistributionGrid* represents the grids transferring the electric power to the consumers.
- *Automation&ControlSystem* represents the system dedicated to the automation and the control of the power grid; this system is considered from the logical point of view and from the physical point of view; so the class *Automation&ControlSystem* is the aggregation of these classes:
  - *PhysicalAutomation&ControlSystem* represents the set of the sites realizing the automation and control system by acting on the state of power plants and substations; therefore, the class *PhysicalAutomation&ControlSystem* is the aggregation of instances of the class *Site* which is in turn the aggregation of instances of the class *PhysicalHos*t representing a generic device connected to the communication network;
  - *LogicalAutomation&ControlSystem* represents the set of software applications performing the automation and control functionalities; therefore the class *LogicalAutomation&ControlSystem* is the aggregation of instances of the class *Application* representing software applications.

  The classes *PhysicalHost* and *Application* are associated because an application runs on a certain physical host. Moreover, the class *Application* is associated with the class *Function* because an application performs an automation and control function.
- *ProtectionSystem* represents the system preserving the safety of the power grid.
- *Load* is the class representing the loads

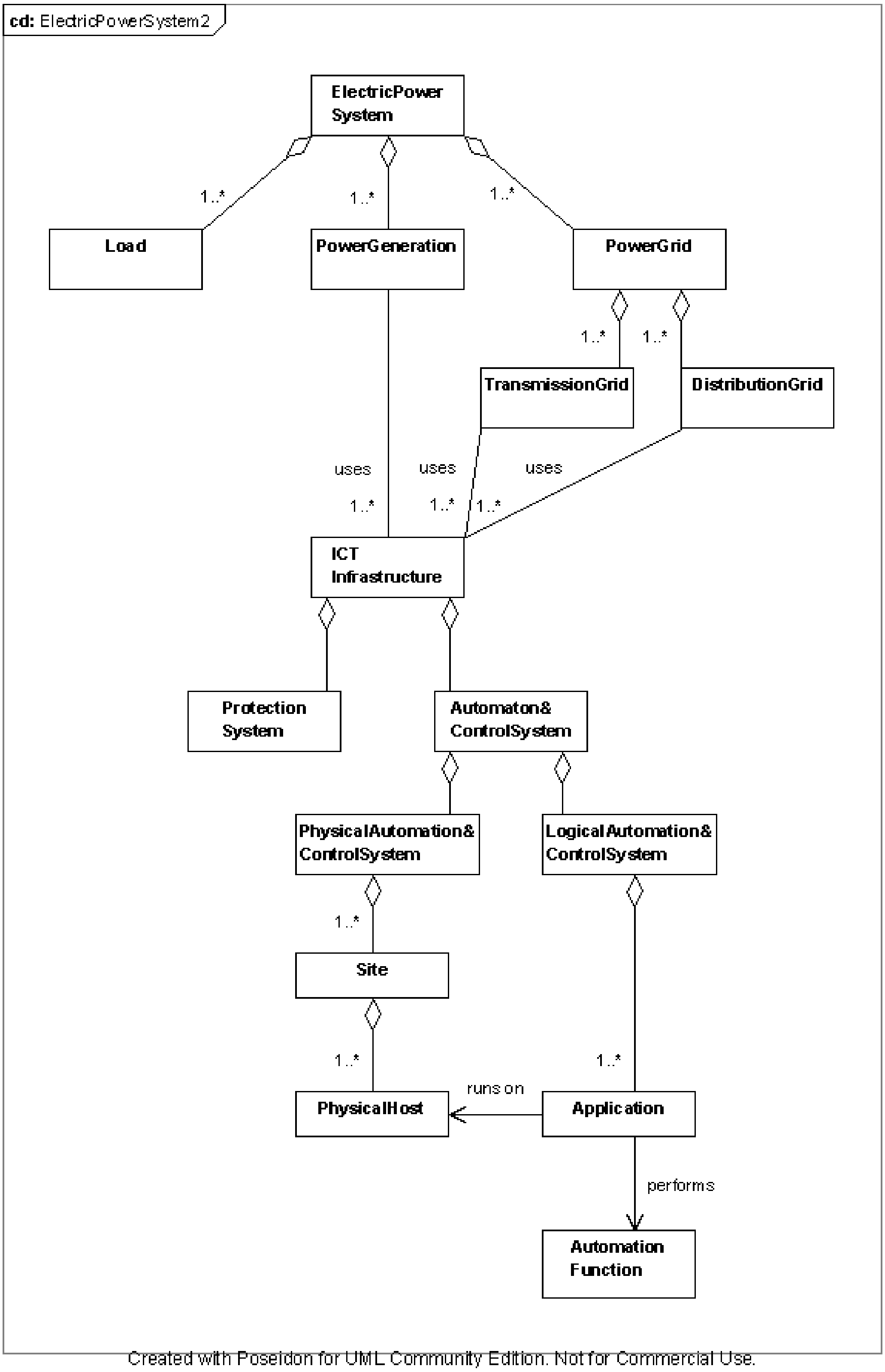


Figure 8-1: Class diagram of the power system infrastructure

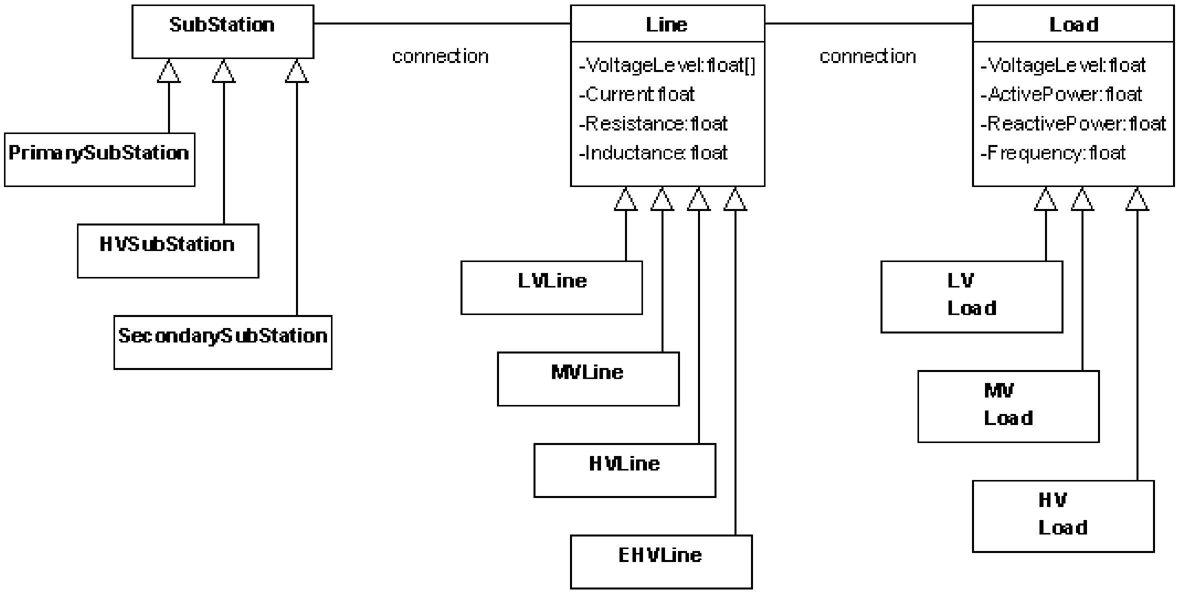
8.1.2 Electric lines

Figure 8-2 shows the class diagram describing the electric lines and the power grid elements connected by electric lines. In the class diagram in Figure 8-2, the class *Line* represents the electric lines, while the class *SubStation* and the class *Load* represents the substations and the loads respectively. The class *Line* is associated with both the class *SubStation* and the class *Load* because an electric line can connect a substation or a load to the power grid.

Moreover, the class *Substation* is specialized in the following classes representing the several kinds of substation:

- *PrimarySubStation* represents the primary substations transforming the HV electric power coming from a HV line, into MV electric power transferred along a MV electric line;
- *SecondarySubStation* represents the secondary substations transforming the MV electric power coming from a MV line, into LV electric power transferred along a LV electric line;
- *HVSubStation* represents the substations transferring the electric power from EHV lines to HV lines.

The class *Load* is specialized in the classes *LV Load*, *MV Load* and *HV Load* according to the voltage level of the load. The class *Line* is specialized in the classes *LVLine*, *MVLine*, *HVLine* and *EHVLine* according to the voltage level of the electric power transferred along the electric line.



Created with Poseidon for UML Community Edition. Not for Commercial Use.

Figure 8-2: Class diagram of the grid elements

8.1.3 Power Generation and Power Grid

Figure 8-3 shows the class diagram representing the power generation together with the power grid; the power generation consists of the set of power plants, while the power grid is the infrastructure necessary to transfer the electric power from the power plants to the consumers distributed on the territory.

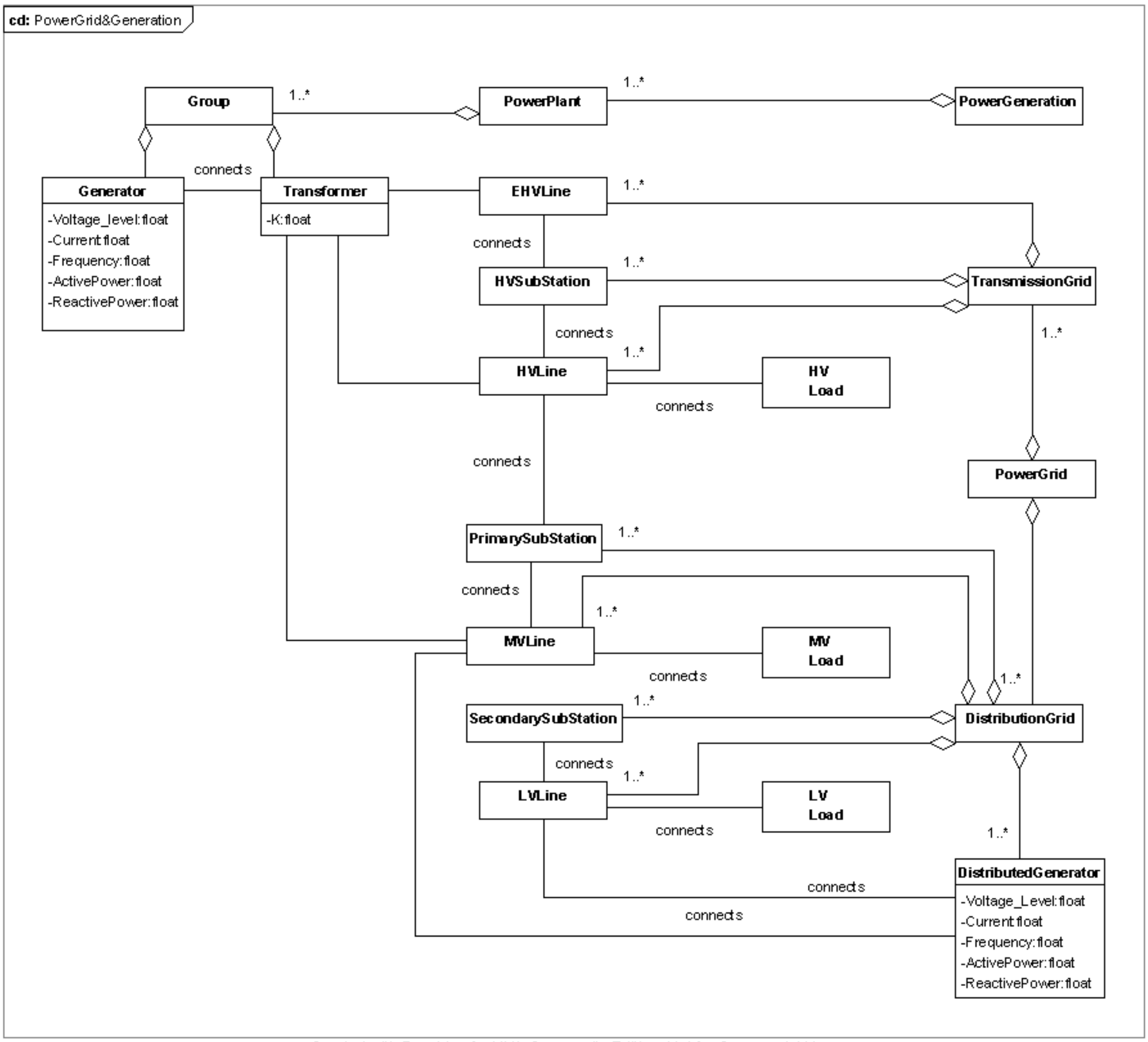
The power generation is represented by the class *PowerGeneration* which is the aggregation of the class *PowerPlant* which represents the power plants for the production of electric power. These two classes are already present in the class diagram in Figure 8-1. The class *PowerPlant* is the aggregation of instances of the class *Group* which is in turn the aggregation of the classes *Generator* and *Transformer* representing power generators and transformers respectively. The cardinality (1) of the aggregation arcs between *Group* and *Generator*, and between *Group* and *Transformer*, indicates that a group is composed by one generator and one transformer. Moreover, the classes *Generator* and *Transformer* are associated because a generator is connected to a transformer in order to raise the voltage of the produced electric power, to the level used on EHV lines.

The power grid is represented by the class *PowerGrid* which is the aggregation of the class *TransmissionGrid* and of the class *DistributionGrid* representing the transmission grid and the distribution grid respectively.

The class *TransmissionGrid* is the aggregation of the classes *HVSubstation*, *EHVLine* and *HVLine*; these classes are already present in the class diagram in Figure 8-2 and they are described in section 8.1.2. The class *EHVLine* is associated with *Transformer* due to the fact that a transformer conveys the electric power from the generator to the to an EHV electric line. The class *HVSubStation* is associated with both the class *EHVLine* and with the class *HVLine* because HV substations transform the EHV electric power coming from a EHV electric line, into HV electric power transferred along a HV electric line. The class *HVLine* is associated with *HV Load* in order to represent that a HV electric line is used to connect a HV load to the transmission grid.

The class *DistributionGrid* is the aggregation of the following classes: *PrimarySubstation*, *SecondarySubStation*, *MVLine* and *LVLine*; these classes are already presented in Figure 8-2 and they are described in section 8.1.2. The class *PrimarySubStation* is associated with the class *HVLine* (composing the class *TransmissionGrid*) because a primary substation is connected to the transmission grid by means of a HV electric line. A primary substation is instead connected to the distribution grid by means of a MV line (a primary substation transforms HV electric power into MV electric power); so, the class *PrimarySubStation* is associated also with the class *MVLine*. *MVLine* is associated also with *MVLoad* and *DistributedGenerator* because a MV load or a distributed generator is connected to the distribution grid by means of a MV electric line.

A secondary substation transforms the MV electric power into LV electric power; for this reason, the class *SecondarySubStation* is associated with the classes *MVLine* and *LVLine*. *LVLine* is associated also with the class *LVLoad* and *DistributedGenerator* because a LV load or a distributed generator is connected to the distribution grid by means of a LV electric line.



Created with Poseidon for UML Community Edition. Not for Commercial Use.

Figure 8-3: Class diagram of the power generation and the power grid

8.1.4 Sites

A site hosts the ICT infrastructures dedicated to the automation, control and management of a portion of the power grid. The class diagram in Figure 8-4 represents a site in terms of classes. The main class is *Site* consisting of an aggregation of the class *PhysicalHost*; moreover the class *Site* is associated with itself to represent the fact that automation sites can communicate exchanging information and orders. The class *Site* is already present in the class diagram in Figure 8-1.

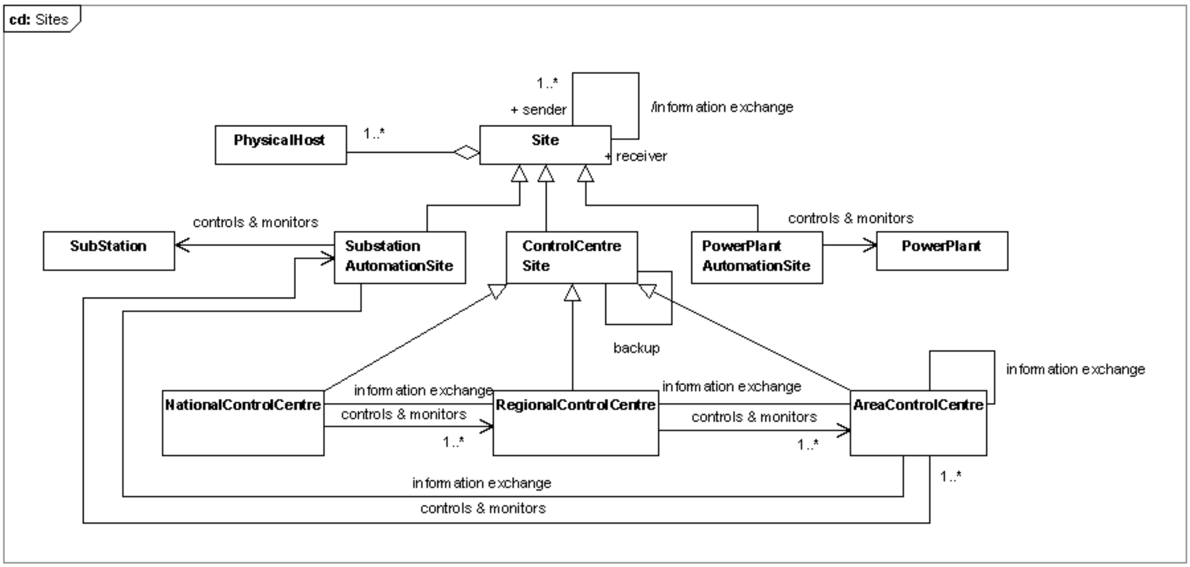
A site can directly control a substation or a power plant; otherwise a site can control other sites. In order to represent this fact, the class *Site* has been specialized in these classes:

- *SubstationAutomationSite* represents the automation sites controlling a substation in direct way; for this reason, this class is associated with the class *SubStation*.
- *ControlCentreSite* represents the sites controlling other sites on the power grid; the sites of this kind are organized in geographical way, so the class *ControlCentreSite* is specialized in the following classes:
    - *NationalControlCentre* represents the automation sites monitoring the national grid and controlling the regional sites;

- *RegionalControlCentre* represents the sites monitoring a regional grid and controlling the area (local) sites;
- *AreaControlCentre* represents the automation sites monitoring and controlling a local area of the power grid; this class is associated with itself to model the possibility for an area control centre to be replaced by another one in case of malfunctioning, or the possibility to realize the redundancy in the normal functioning of the area control.

- *PowerPlantAutomationSite* represents the automation sites controlling a power plant in direct way; for this reason, this class is associated with the class *PowerPlant*.

The associations between the class *NationalControlCentre* and the class *RegionalControlCentre* indicate that there is an information exchange between a national control centre and a regional one. The same relations hold between the class *RegionalControlCentre* and the class *AreaControlCentre*. The class *ControlCenterSite* is associated with itself to indicate that a control centre site may be replaced by another one in case of malfunctioning.



Created with Poseidon for UML Community Edition. Not for Commercial Use.

Figure 8-4: Sites classification

8.1.5 Stakeholders

The class diagram in Figure 8-5 refers to the stakeholders in the electric power system. The main class is Stakeholder associated to several classes representing the entities in the electric power system that a stakeholder may own or manage. For instance, the association between the class *Stakeholder* and the class *DistributionGrid* indicates that a stakeholder may own the distribution grid; in this case, the stakeholder is a distribution company, as indicated by the role of the class *Stakeholder* in the association with the class *DistributionGrid*. In a similar way, the other associations in the class diagram in Figure 8-5 represent the possible roles of a stakeholder.

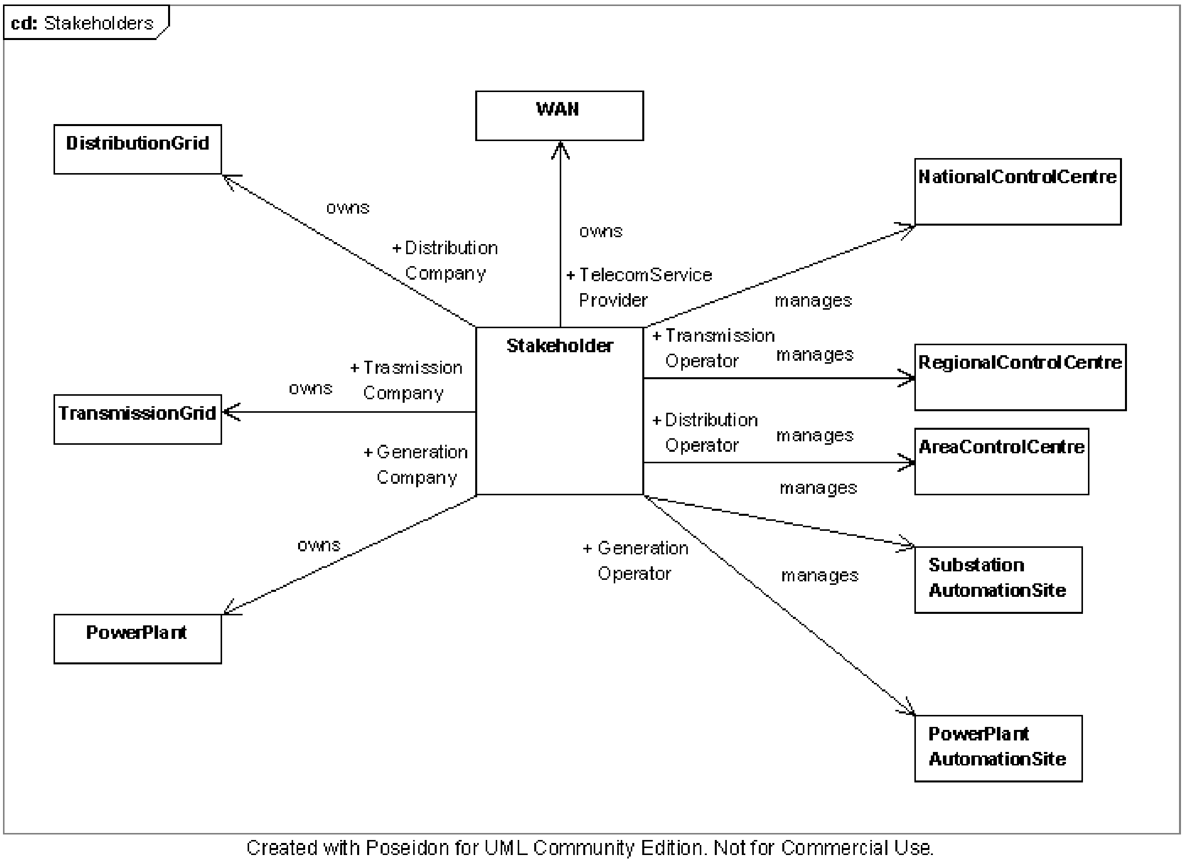


Figure 8-5: Stakeholders

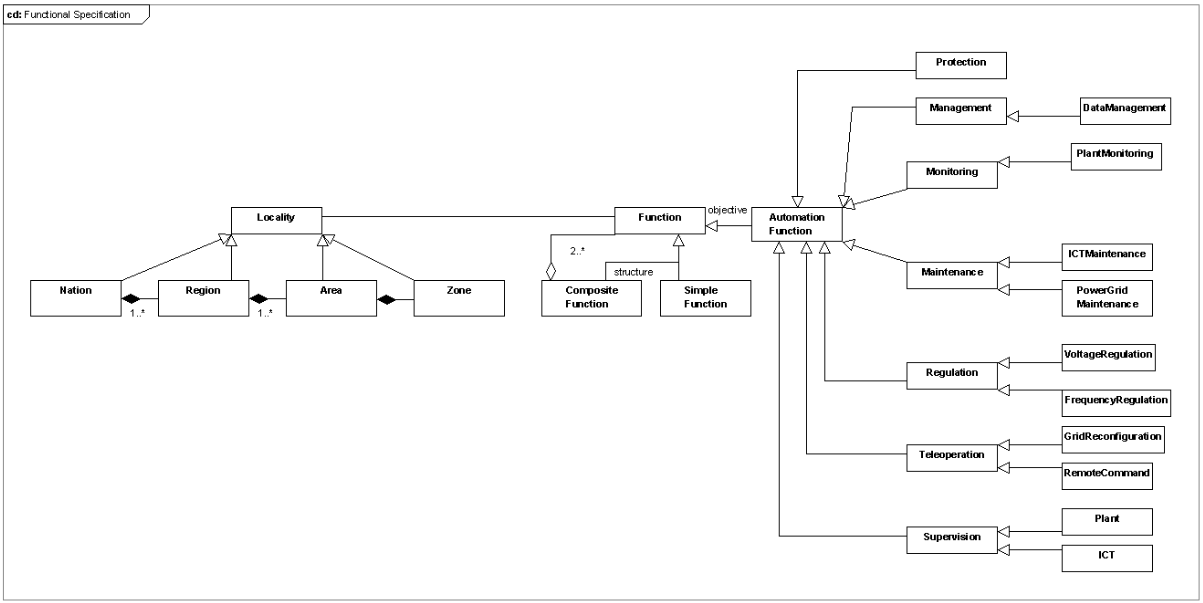
8.1.6 Functions

Activities such as management, monitoring, maintenance and control can be classified as functions, where each function can be composed by a set of simpler functions: in the class diagram in Figure 8-6 the class *Function* is specialized in *SimpleFunction* and *CompositeFunction* where the latter is an aggregation of *Function* so recursively we can define a hierarchical structure of composite functions. In particular, an automation function is realized in automatic way. The class *Function* is specialized in *AutomationFunction* which is in turn specialized in several classes representing the main automation functionalities: *Protection*, *Management*, *Monitoring*, *Maintenance*, *Regulation*, *Teleoperation* and *Control*.

The class *Management* is in turn specialized in *DataManagement* representing the management activity concerning the data. The monitoring activity can concern the power plants; therefore the class *Monitoring* is specialized in the class *PlantMonitoring*. The ICT components and the power grid can be object of maintenance, so the class *Maintenance* is specialized in *ICTMaintenance* and *PowerGridMaintenance*. Moreover, the class *Regulation* concerning the generic activity of regulation, is specialized in *VoltageRegulation* and *FrequencyRegulation* modelling the voltage regulation and the frequency regulation respectively.

The teleoperation functions are represented by the class *Teleoperation* specialized in the class *GridReconfiguration* and the class *RemoteCommand*; the supervision functions are represented by the class *Supervision* specialized in the classes *Plant* and *ICT*.

Moreover, each function has its own geographical scope: the class *Function* is associated in a biunivocal way with the class *Locality* which is in turn specialized in *Nation*, *Region*, *Area* and *Zone* classes. In this way we can distinguish, e.g. the state of the regional Teleoperation of Lombardia from the state of the regional Teleoperation of Piemonte.



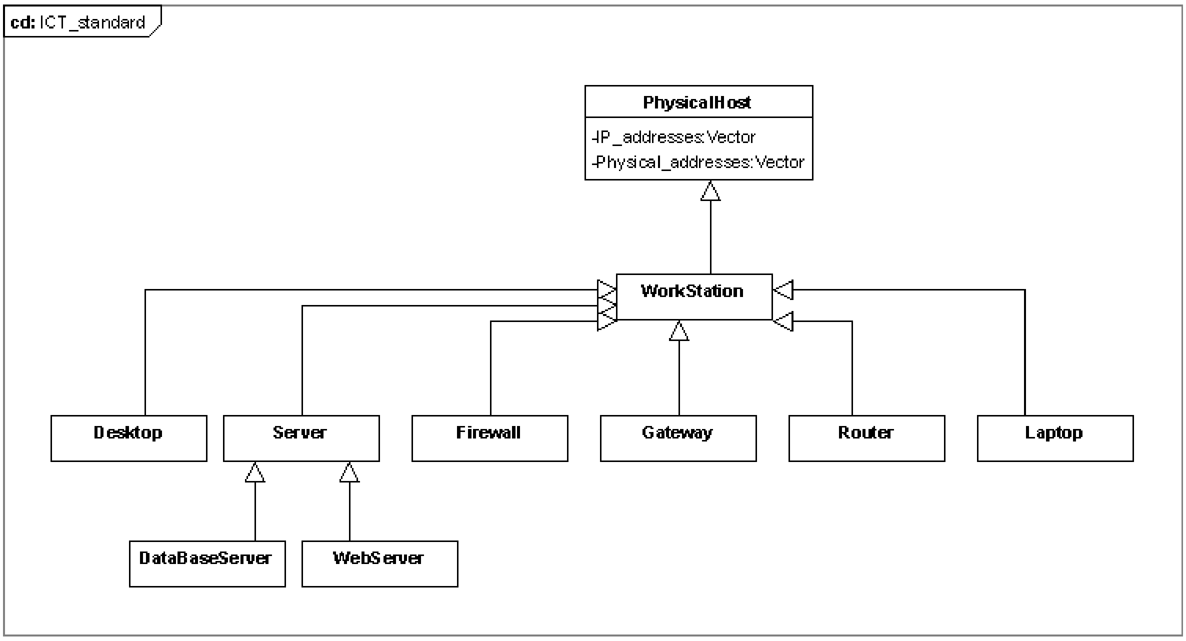
Created with Poseidon for UML Community Edition. Not for Commercial Use.

Figure 8-6: Class diagram of the functions performed by ICT elements

8.2 Representing the Control System Infrastructure in UML

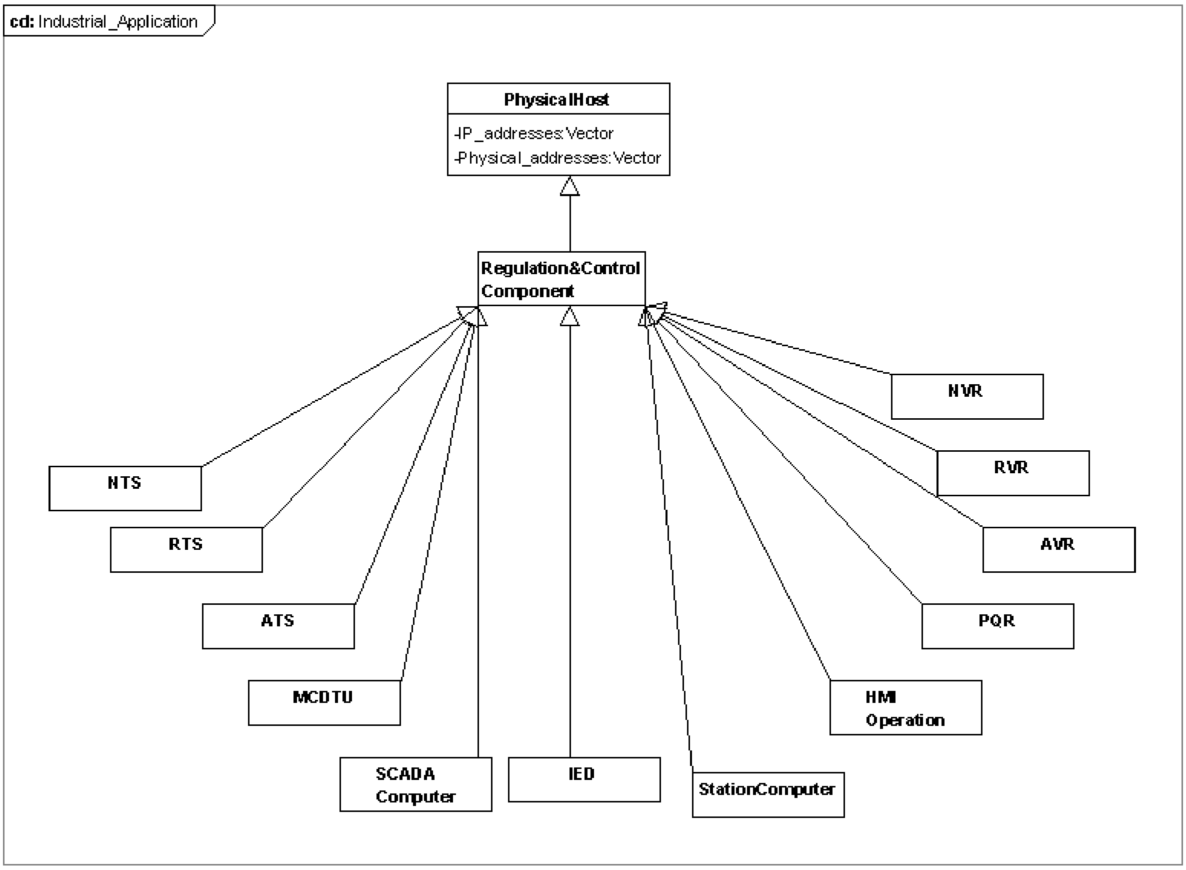
8.2.1 ICT Elements

The ICT elements present in the electric power system are represented in the class diagrams in Figure 8-7. The class *PhysicalHost* represents the generic device connected to the communication network. This class is already present in the class diagram in Figure 8-1 and can be specialized in two classes: *WorkStation* (Figure 8-7) and *Regulation&ControlComponent* (Figure 8-8). The class *WorkStation* represents generic computers and has several specializations, one for each role of a workstation: *Desktop*, *Server*, *Firewall*, *Gateway*, *Router*, *Laptop*. Moreover, the class *Server* is specialized in *DataBaseServer* and *WebServer*.



Created with Poseidon for UML Community Edition. Not for Commercial Use.

Figure 8-7: Class diagram of the ICT elements



Created with Poseidon for UML Community Edition. Not for Commercial Use.

Figure 8-8: Class diagram of the industrial application components

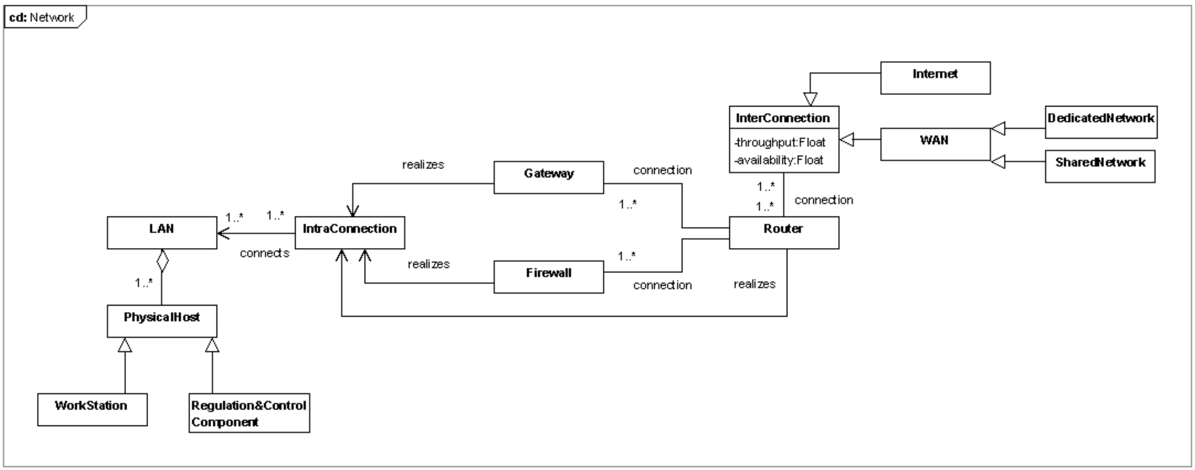
8.2.2 Industrial application components

In Figure 8-8, the class *PhysicalHost* is specialized in the class *Regulation&ControlComponent* identifying the industrial application components, e.g.: the components dedicated to the regulation and control of a node of the power grid; the class *Regulation&ControlComponent* is therefore specialized in *IED*, *MCDTU*, *SCADAComputer*, *PQR*, *HMIOperation*, *AVR, StationComputer*, etc.

8.2.3 ICT Network

Figure 8-9 shows the class diagram of the ICT Network of a site; the class *PhysicalHost* is present in this diagram and is specialized in *WorkStation* and *Regulation&ControlComponent*. The class *LAN* identifies the local networks of a site; *LAN* is the aggregation of instances of *PhysicalHost*. This class is already present in the class diagrams in Figure 8-1, Figure 8-4, Figure 8-7 and Figure 8-8. The connection between the local networks of a site, is represented by the class *IntraConnection* associated with *LAN*. This form of connection is realized by means of gateways, firewalls and routers identified by the classes *Gateway*, *Firewall* and *Router* respectively and associated with the class *IntraConnection*. Gateways and firewalls are also connected to the routers of the site; the router is the point of connection between the local networks of the site and the external network necessary for the communication with other sites.

The class *Router* identifies the routers and is associated with *Gateway*, *Firewall* and *InterConnection*. The class *InterConnection* represents the connection of the control site with other sites by means of the public network (Internet) or by means of a private network. Therefore, the class *InterConnection* is specialized in *Internet* and *WAN*; *WAN* is specialized in *DedicatedNetwork* and *SharedNetwork*. The class *DedicatedNetwork* identifies private networks dedicated exclusively to the interconnection of sites; the class *SharedNetwork* identifies private networks used to connect sites, but also used to other purposes. The class *WAN* is already present in the class diagram in Figure 8-5.



Created with Poseidon for UML Community Edition. Not for Commercial Use.

Figure 8-9: Class diagram of the networking elements

8.2.4 Voltage Regulation

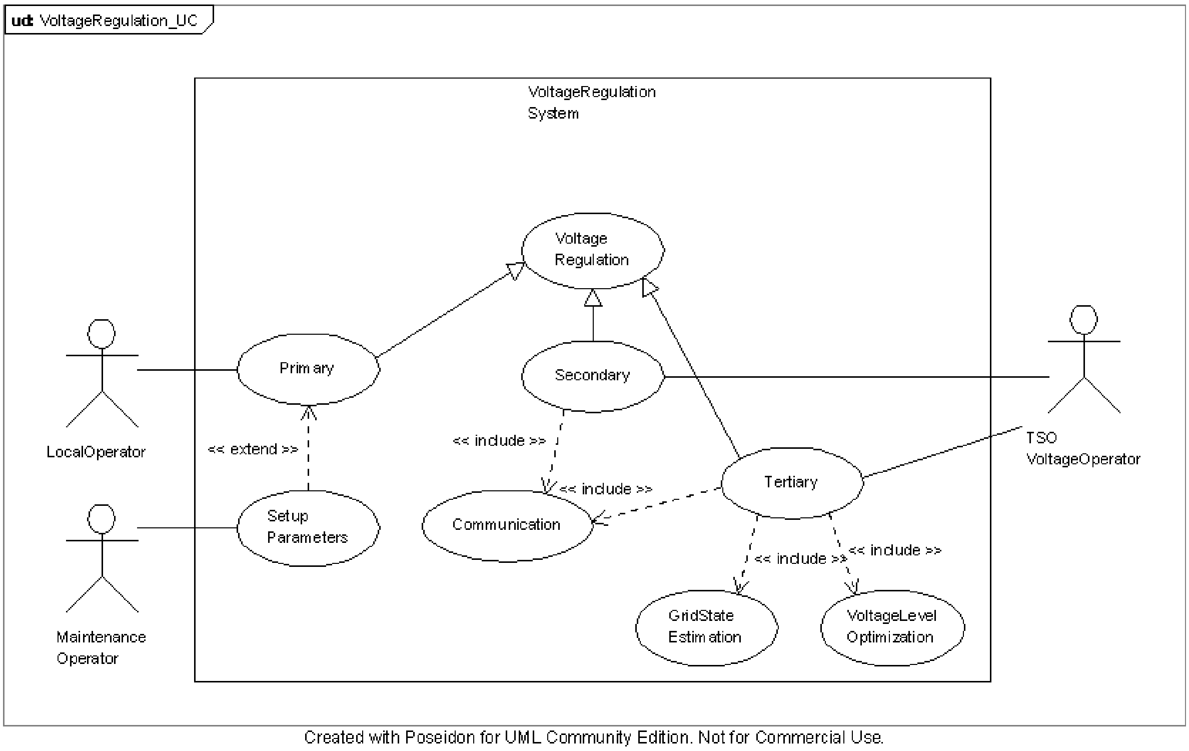


Figure 8-10: Use case diagram of the voltage regulation

The use case diagram in Figure 8-10 shows the functionalities of the Voltage Regulation System. The use case called *VoltageRegulation* represents the general function of the Voltage Regulation System. Such use case is specialized in the use cases *Primary*, *Secondary* and *Tertiary* representing the primary, secondary and tertiary voltage regulation respectively. The use case *Primary* is associated with the actor named *LocalOperator* identifying the operator dedicated to the primary voltage regulation on a local area. The same use case is extended by the use case named *SetupParameters* representing the setup of the parameters influencing the AVR functioning. The use case *SetupParameters* extends the use case *Primary* because the parameter setup may be eventually perfomed inside the primary voltage regulation. The actor *MaintenanceOperator* is associated with the use case *SetupParameters*; such actor identifies the operator dedicated to setup the parameters concerning the primary voltage regulation.

The use case *Secondary* specializing the use case *VoltageRegulation*, includes the use case named *Communication*; this means that each time the secondary voltage regulation is performed, the communication function is exploited (to connect the regulation components involved in the secondary voltage regulation).

The use case *Tertiary* includes the following use cases: *Communication*, *GridStateEstimate* and *VoltageLevelOptimization*. This means that the tertiary control regulation includes these functions: the communication between the components involved in the tertiary voltage regulation, the estimate of the grid state and the optimization of the voltage level in the grid.

The actor *TSOVoltageOperator* is associated with the use case *Secondary* and with the use case *Tertiary*; such actor identifies the operator dedicated to the secondary and tertiary voltage regulation.

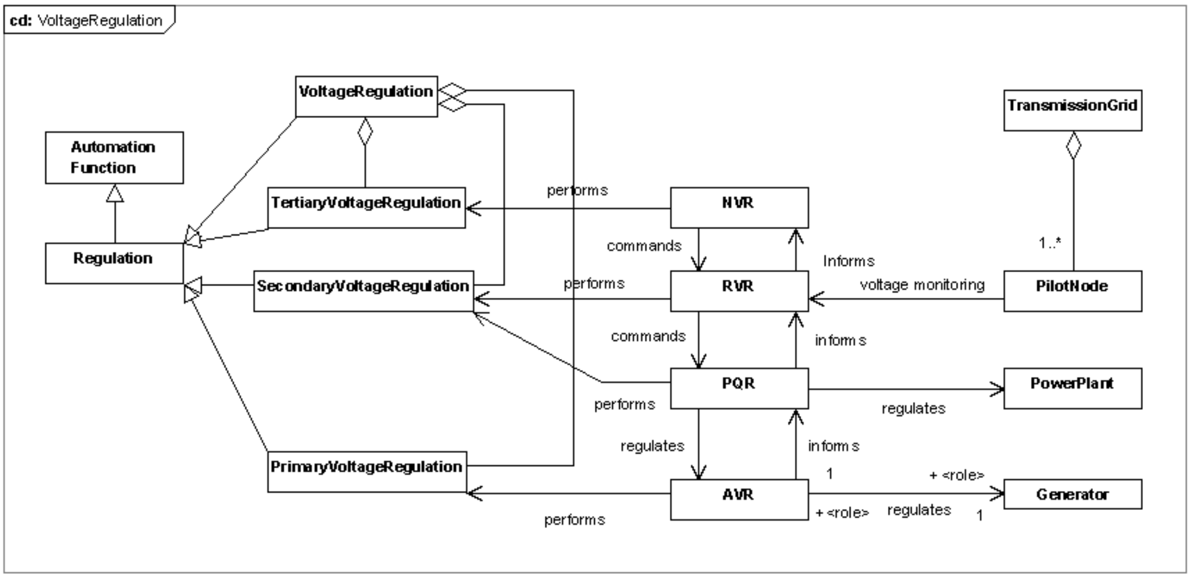
The structure of the voltage regulation system of the electric power system is represented by the class diagram in Figure 8-11 where the main class is *VoltageRegulation* extending the class *Regulation* identifying the regulation functions. The class *Regulation* is already present in Figure 8-6. *VoltageRegulation* is the aggregation of three classes extending the class *Regulation*; such classes reflect the geographical organization of the voltage regulation; they are: *PrimaryVoltageRegulation*, *SecondaryVoltageRegulation* and *TertiaryVoltageRegulation*.

Besides the description of the voltage regulation in terms of functions, the class diagram in Figure 8-11 indicates also the components performing each function. The classes *NVR*, *RVR*, *AVR* and *PQR* represent the components realizing the regulation operations on the power plants or on the substations. The class *NVR* models the national voltage regulator performing the tertiary voltage regulation: *NVR* is associated with the class *TertiaryVoltageRegulation*. The class *RVR* represents the regional voltage regulator performing the secondary voltage regulation together with the reactive power regulator represented by the class *PQR*; *RVR* and *PQR* are associated with the class *SecondaryVoltageRegulation*. Finally, the automatic voltage regulator performing the primary voltage regulation, is represented by the class *AVR* associated with the class *PrimaryVoltageRegulation*.

NVR and *RVR* are associated since the national voltage regulator can send commands to the regional voltage regulators, while a regional voltage regulator can send information about the state of the corresponding portion of power grid, to the national voltage regulator. Similarly, the class *RVR* is associated with the class *PQR* because a regional voltage regulator can send commands to the reactive power regulator. Finally, the classes *PQR* and *AVR* are associated because the reactive power regulator sets the reference voltage values.

The class diagram in Figure 8-11 shows also which elements of the power grid are influenced by the components realizing the voltage regulation. The class *RVR* is associated with the class *PilotNode* because the regional voltage regulator monitors the voltage levels in the pilot nodes. The class *PQR* is associated with *PowerPlant* since the reactive power regulator influences the state of the power plant. The class *AVR* is associated with the class *Generator* because the automatic voltage regulator influences the state of the generators of a power plant.

The class *PowerPlant* is already present in the class diagrams in Figure 8-3 and in Figure 8-4 respectively; *Generator* is already present in the class diagram in Figure 8-3; the classes *PQR* and *AVR* are already present in the class diagram in Figure 8-8.



Created with Poseidon for UML Community Edition. Not for Commercial Use.

Figure 8-11: Class diagram of the voltage regulation

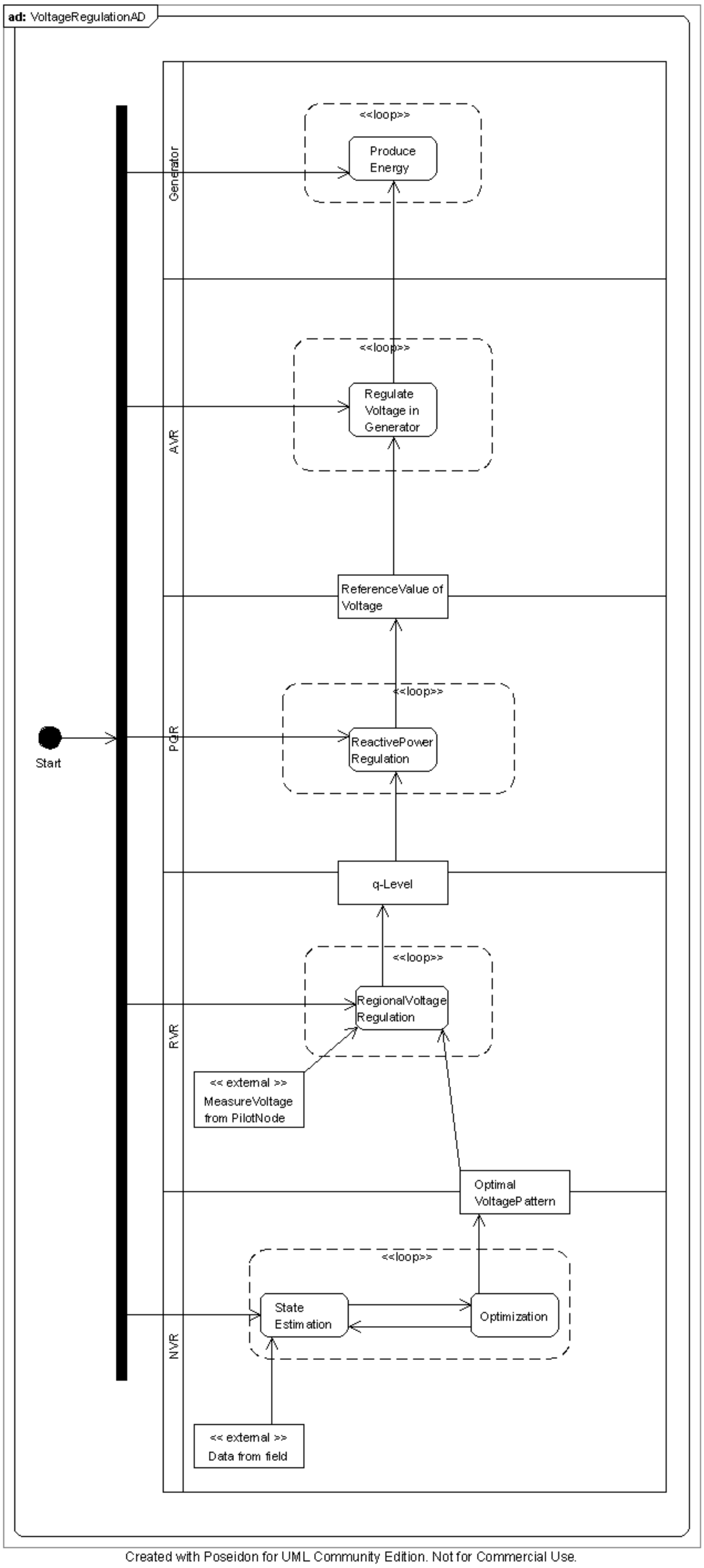

ad: VoltageRegulationAD
Generator
<<loop>>
Produce Energy
AVR
<<loop>>
Regulate Voltage in Generator
ReferenceValue of Voltage
PQR
<<loop>>
ReactivePower Regulation
Start
q-Level
RVR
<<loop>>
RegionalVoltage Regulation
<< external >> MeasureVoltage from PilotNode
Optimal VoltagePattern
NVR
<<loop>>
State Estimation
Optimization
<< external >> Data from field
Created with Poseidon for UML Community Edition. Not for Commercial Use.

Figure 8-12: Activity diagram of the Voltage Regulation

8.2.5 Teleoperation

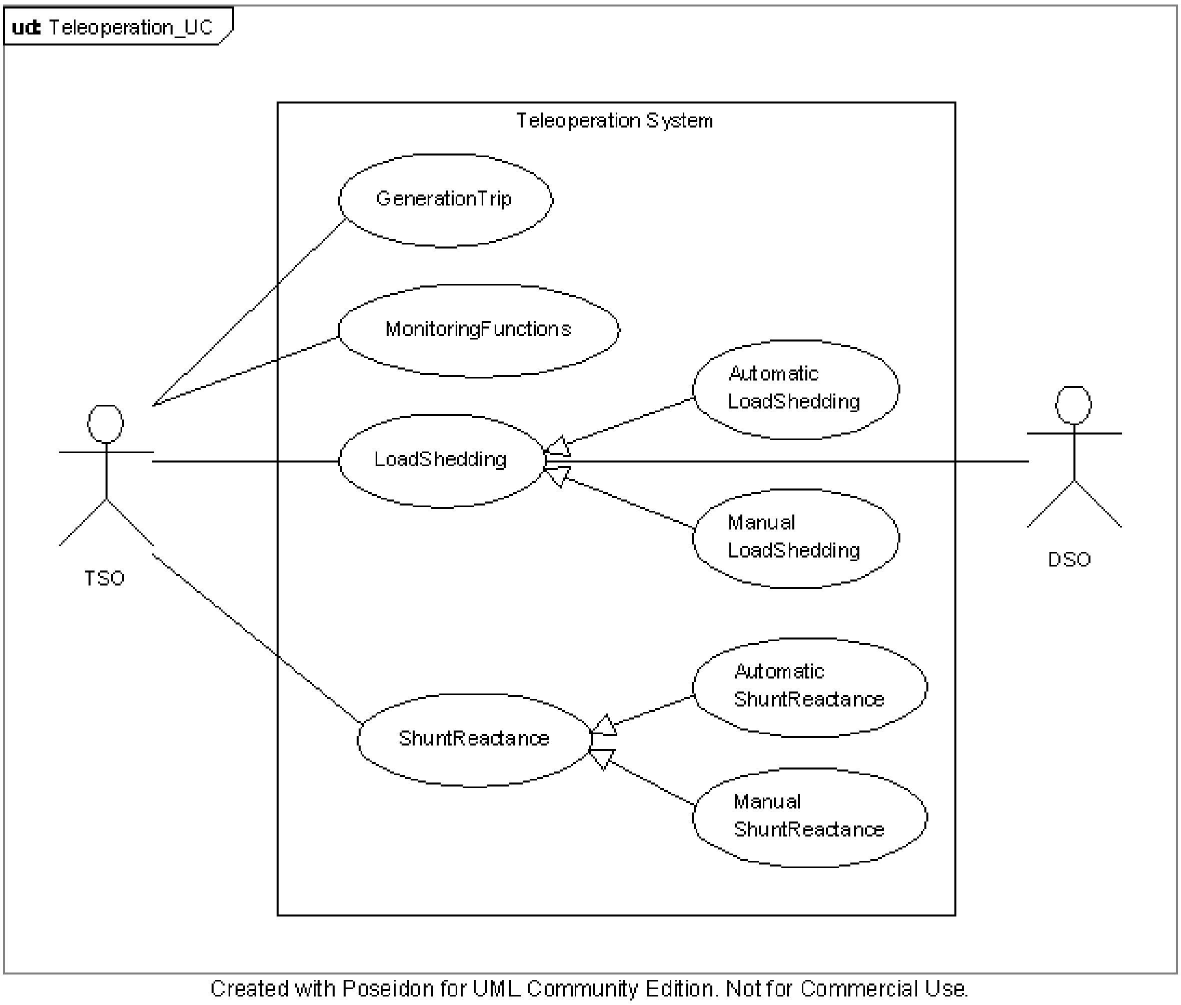


Figure 8-13: Use case diagram of the Teleoperation system

In Figure 8-13 we show the use case diagram of the teleoperation. The use case diagram describes with a high level of abstraction who are the relevant users interacting with the system, and the services provided by the system. In this type of diagram the focus is on the purpose of the service provided not on its implementation. In our case the TrasmissionServiceOperator (TSO actor) and DistributionServiceOperator (DSO actor) interact with the Teleoperation system in order to coordinate different services: Generation Trip, Monitoring Functions, Load Shedding, Shunt Reactance.

In our case, the TSO interacts with all the provided functions whereas the DSO interacts only with load shedding activities because it authorizes the TSO to perform them.

The structure of the teleoperation system of the electric power system is represented by the class diagram in Figure 8-14 where the main class is *Teleoperation* specialized in *RemoteCommand*. *RemoteCommand* is the aggregation of three classes extending the class *Function* identifying the functions (*Function* is already present in the class diagram in Figure 8-6); these classes reflect the geographical organization of the Teleoperation; they are: *NationalTeleoperation*, *RegionalTeleoperation* and *AreaTeleoperation*.

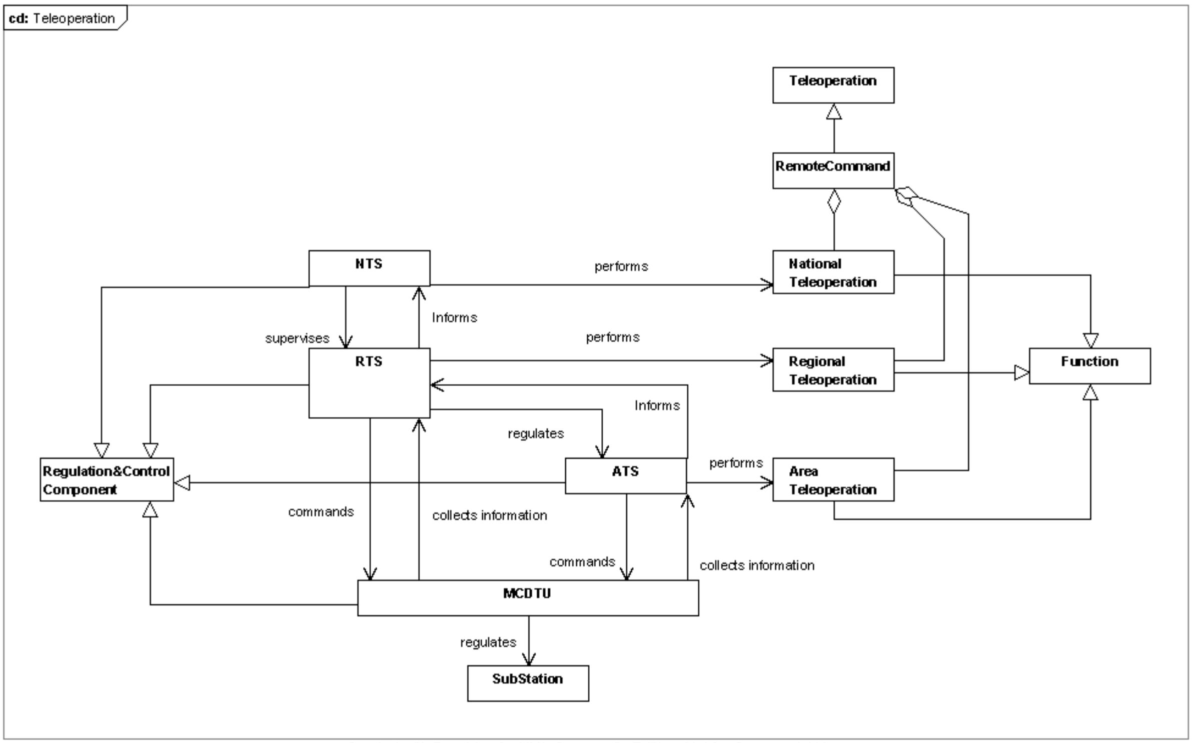
Besides the description of the Teleoperation in terms of functions, the class diagram in Figure 8-14 indicates also the automation components performing each function. The classes *NTS*, *RTS*, *ATS* and *MCDTU* extend the class *Regulation&ControlComponent*

representing the hardware components realizing control operations on the power plants or on the substations. The class *Regulation&ControlComponent* is already present in the class diagram in Figure 8-8.

The class *NTS* is associated with the class *NationalTeleoperation* because *NTS* represents the automation component performing the national Teleoperation; analogously, the class *RTS* is associated with the class *RegionalTeleoperation*, the class *ATS* is associated with the class *AreaTeleoperation*. *NTS* and *RTS* are associated since the national Teleoperation can send commands to the regional Teleoperation, while a regional Teleoperation can send information about the state of the corresponding portion of power grid, to the national Teleoperation. Similarly, *RTS* and *ATS* are associated since the regional Teleoperation commands the area Teleoperation, while the regional Teleoperation is informed by the area Teleoperation.

A *MCDTU* exchanges commands and information also with the regional Teleoperation system, so the class *MCDTU* is associated with the class *RTS*.

The class *MCDTU* is associated with the class *ATS* because the area Teleoperation system collects information from the MCDTU automation components; the class *MCDTU* is associated also with the class *SubStation* because the automation components represented by the class *MCDTU* influence the state of the substations.



Created with Poseidon for UML Community Edition. Not for Commercial Use.

Figure 8-14: Class Diagram of the teleoperation

8.2.6 ICT threats

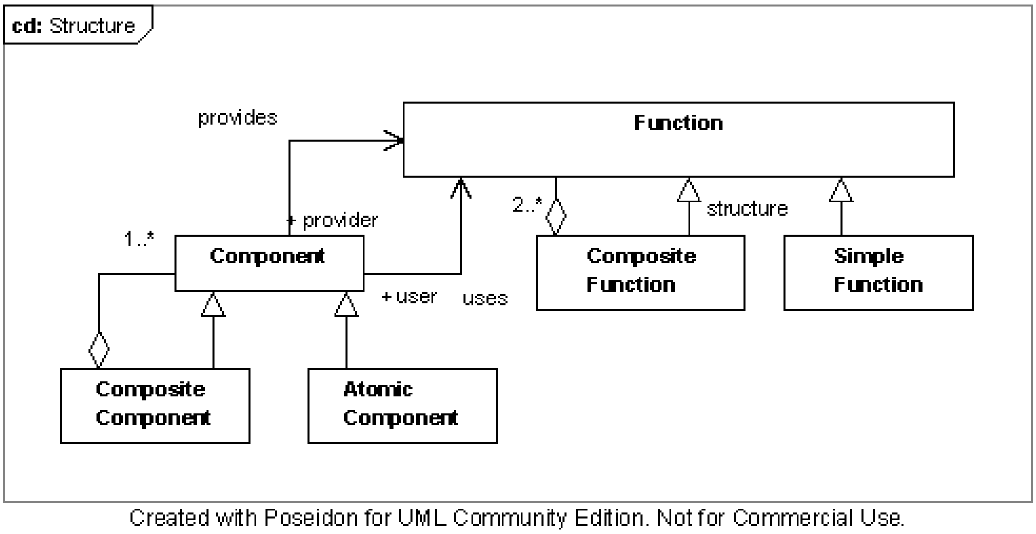


Figure 8-15: Class diagram of function classification

The class diagram in Figure 8-15 concerns the function classification. The main class in such diagram is *Function* representing the generic function; this class can be specialized in the class *SimpleFunction* and in the class *CompositeFunction*. In particular, the class *CompositeFunction* is the aggregation of the class *Function*. In this way, we represent that a composite function can be composed by simple functions or by further composite functions. The class *Function* is associated with the class *Component* in order to express that a certain component provides a certain function. The class *Component* is specialized in the class *AtomicComponent* and in the class *CompositeComponent*. Moreover, the class *CompositeComponent* is the aggregation of the class *Component*; in this way, we represent that a composite component can be composed by atomic components or by further composite components.

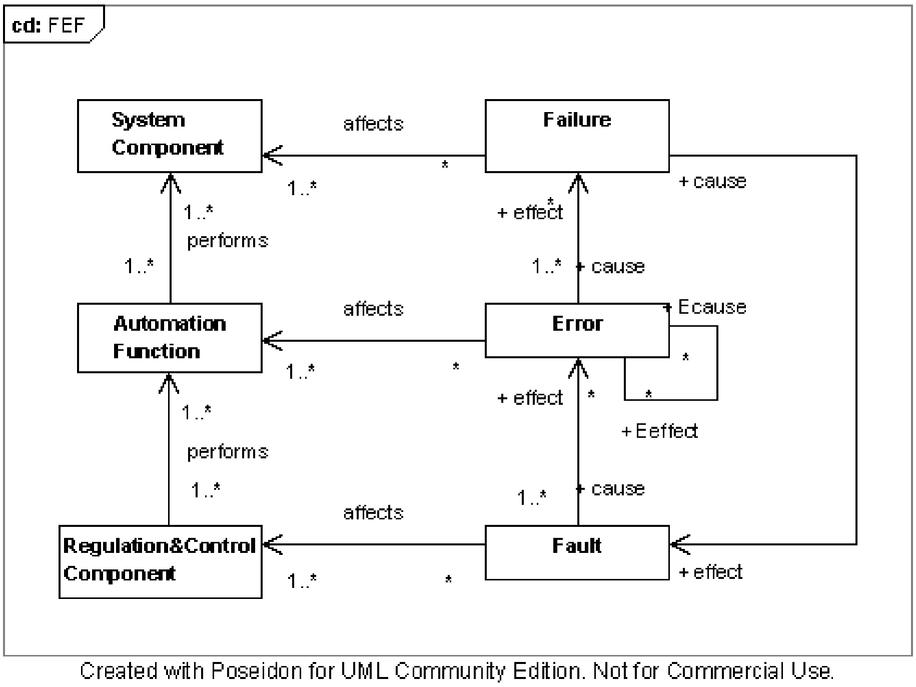


Figure 8-16: Class diagram of Fault-Error-Failure

The class diagram in Figure 8-16 represents the Fault-Error-Failure (FEF) chain [Avizienis *et al.* 2004]. The class *Fault* is associated with the class *Error* in order to express that a fault may cause an error; the class *Error* is in turn associated with the class *Failure* because an error may cause a failure. The class *Failure* is associated with the class *Fault* in order to express that a failure may cause another fault. The class diagram in Figure 8-16 shows also the elements affected by the FEF chain: a fault affects a regulation & control component, an error affects an automation function, a failure affects a system component.

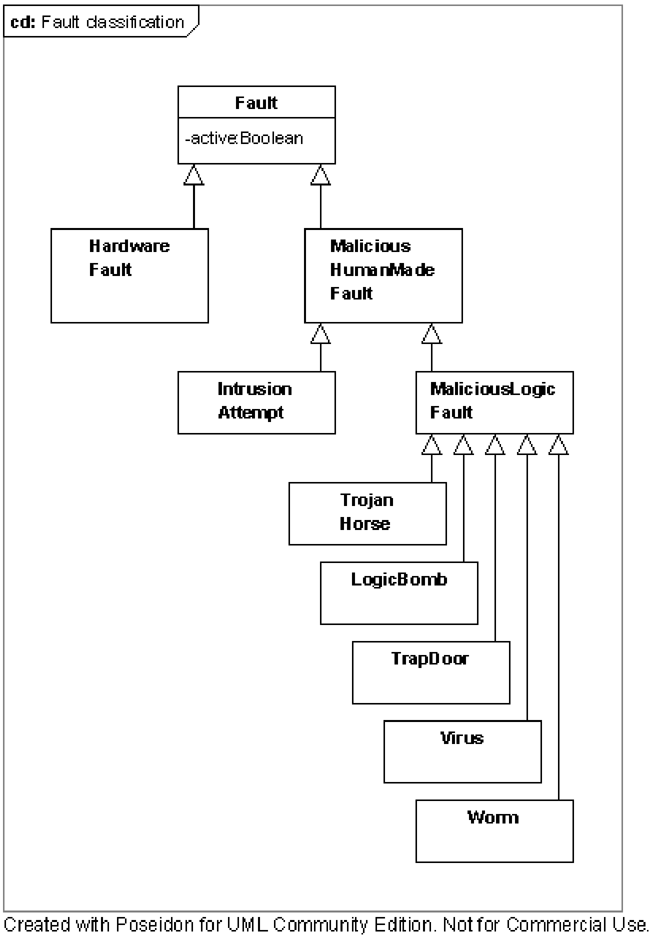


Figure 8-17: Fault classification

The class diagram in Figure 8-17 represents the fault classification according to [Avizienis]. The class *Fault* represents the generic fault and is specialized in the class *HardwareFault* and in the class *MaliciousHumanMadeFault*; the class *HardwareFault* represents the fault depending on the hardware characteristics of a component; the class *MaliciousHumanMadeFault* represents the fault due to some malicious attack by a human actor. Such kind of fault can be an intrusion attempt or malicious logic fault; the class *MaliciousLogicFault* is specialized in *TrojanHorse*, *LogicBomb*, *TrapDoor*, *Virus*, *Worm*; these classes represent the several forms of malicious logic faults.

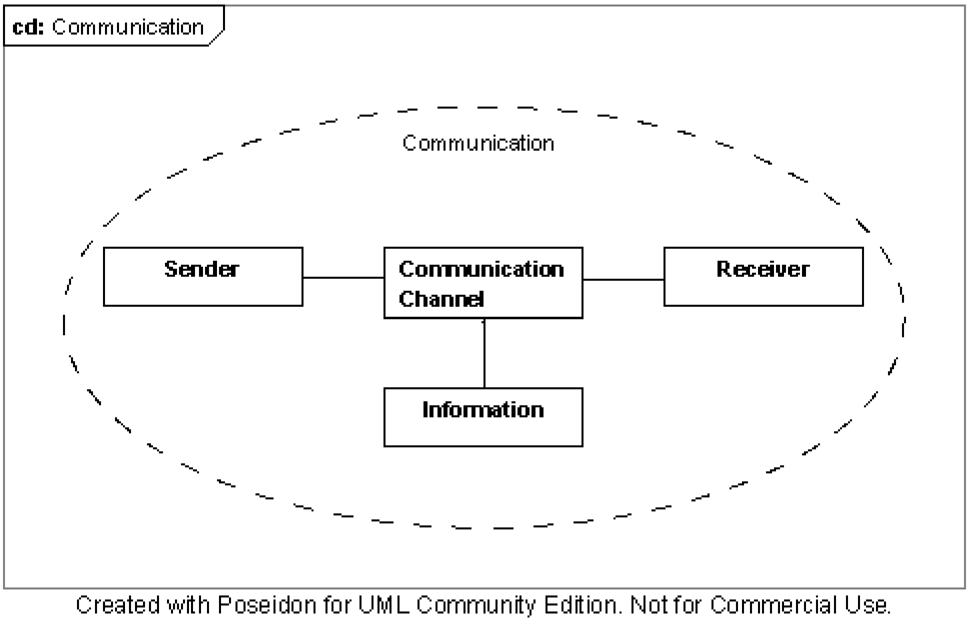


Figure 8-18: Collaboration of the communication function

The diagram in Figure 8-18 shows the classes involved in a generic communication between a sender and a receiver, together with the collaborations between such classes. This diagram indicates that a sender and a receiver exchange information by means of a communication channel.

The packet delivery in normal conditions is depicted in the sequence diagram in Figure 8-19 where a packet is sent from the sender to the receiver through the communication channel without any delay. In the sequence diagram in Figure 8-20, we represent the situation of the communication in case of denial of service with delay in the packet delivery. The sequence diagram in Figure 8-21 shows the loss of the packets still in case of denial of service.

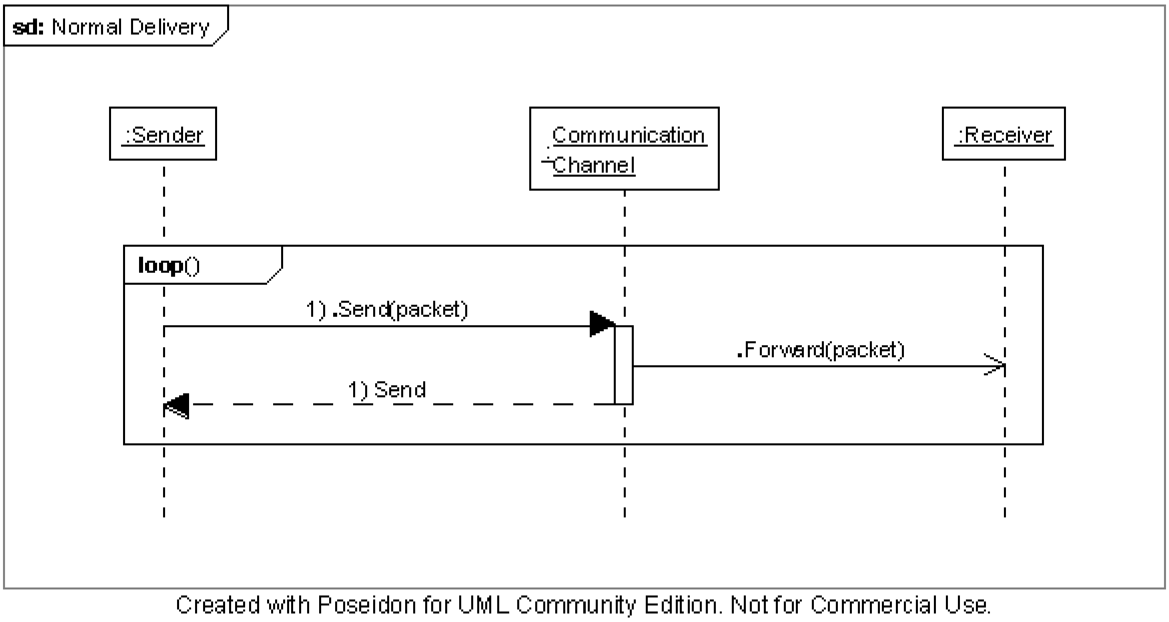
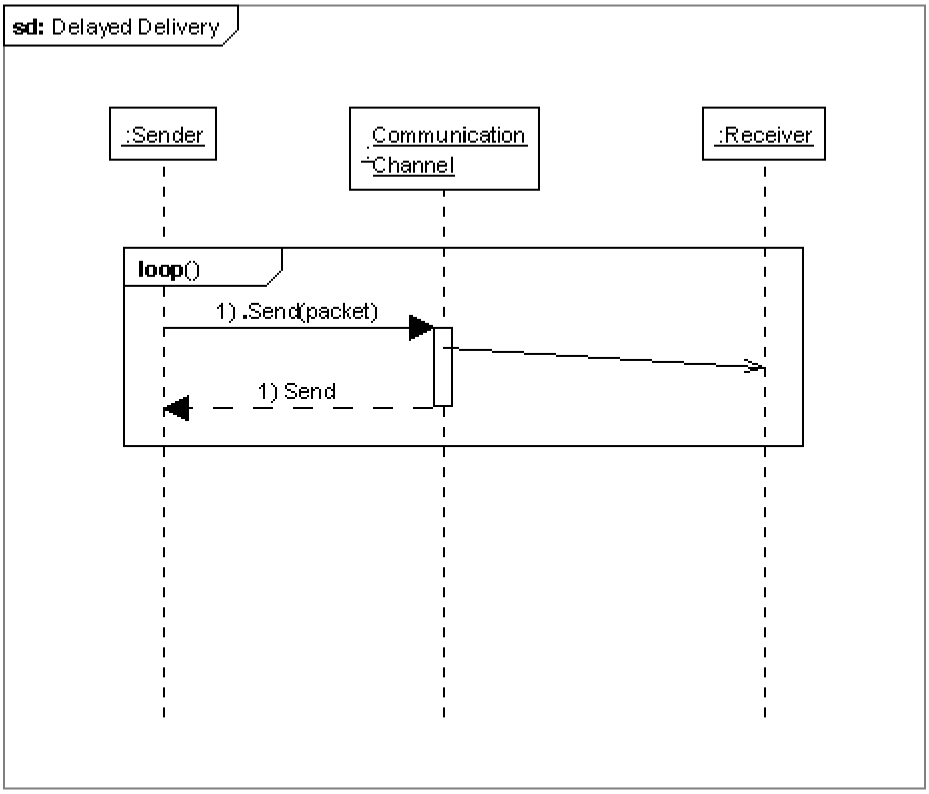
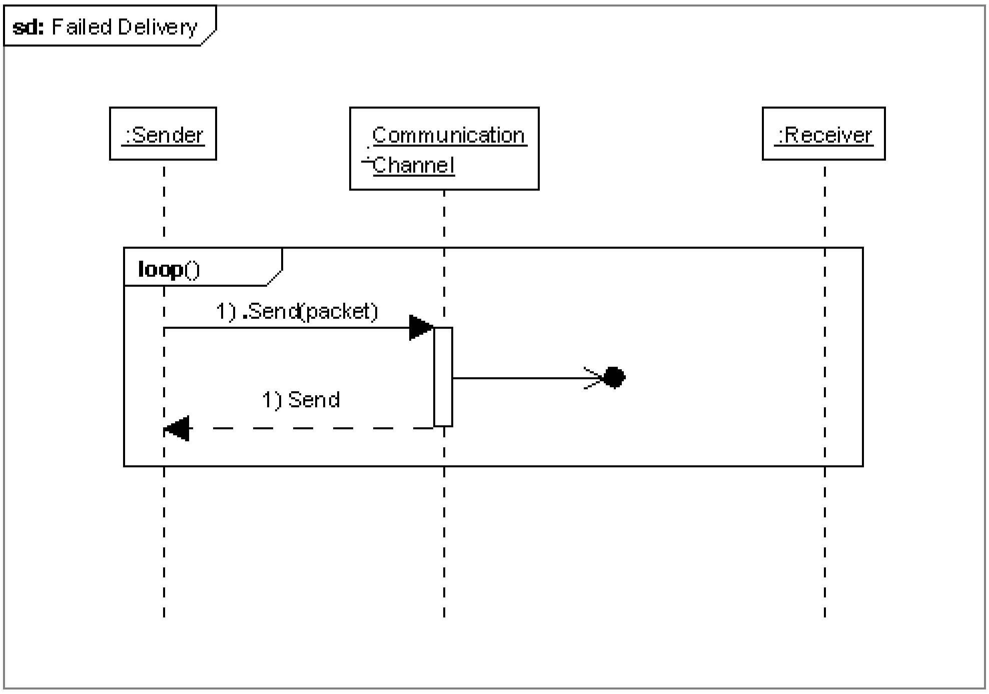


Figure 8-19: Interaction fragment of a normal communication



Created with Poseidon for UML Community Edition. Not for Commercial Use.

Figure 8-20: Interaction fragment of a delayed communication



Created with Poseidon for UML Community Edition. Not for Commercial Use.

Figure 8-21: Interaction fragment of a failed communication

The sequence diagram in Figure 8-22 is the composition of the previous ones showing the several stages of the denial of service: initially we are in a normal situation even though in parallel way, an attacker is performing the denial of service. When the denial of service begins to influence in a negative way the packet delivery, the communication can be in two alternative situations: the case with delayed packet delivery and the case with failed packet delivery.

In the sequence diagram in Figure 8-23, we represent an intrusion in the communication: initially we have the normal communication conditions depicted in the sequence diagram in Figure 8-19; after the intrusion, the intrusion can send faked commands through the communication channel.

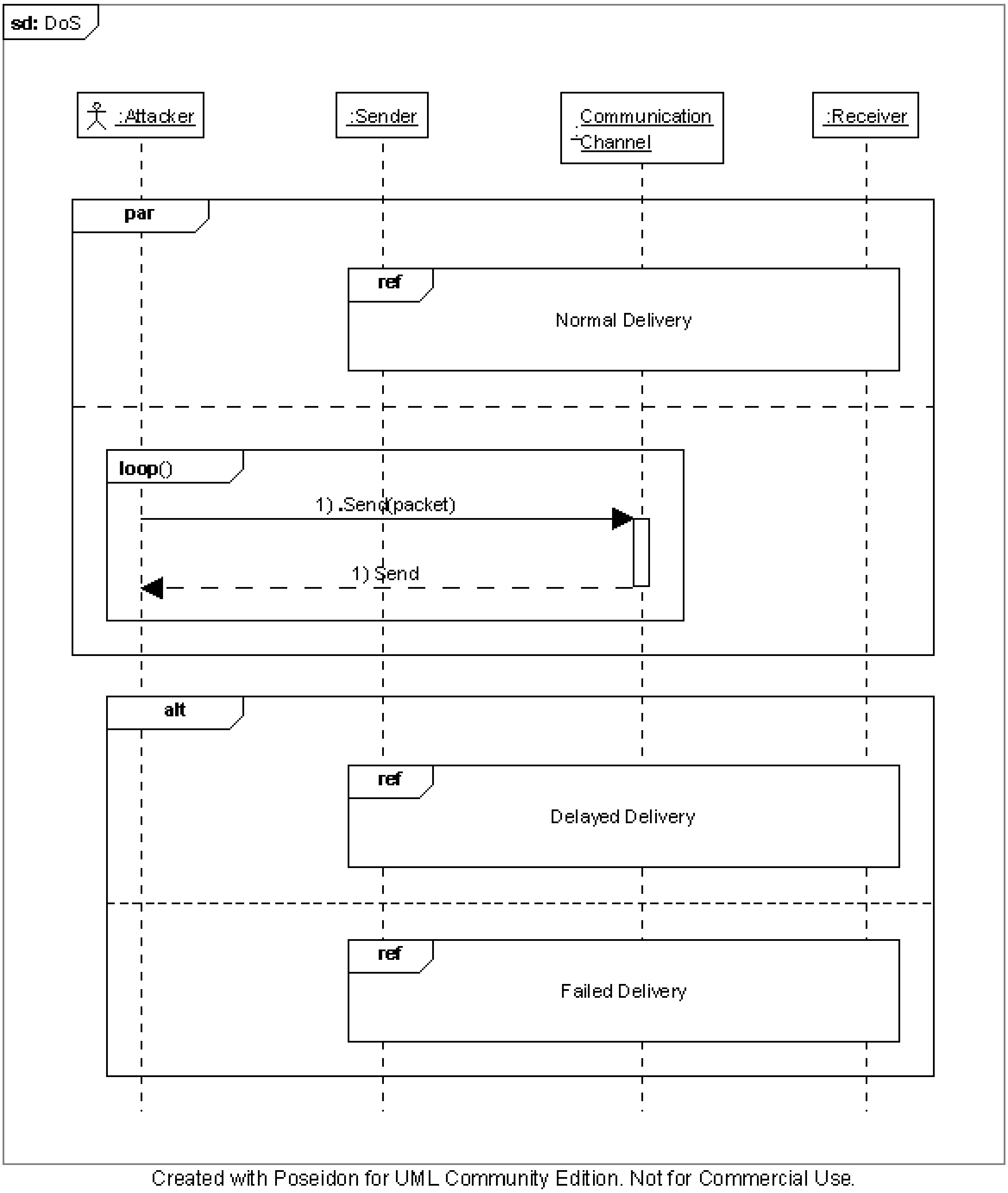
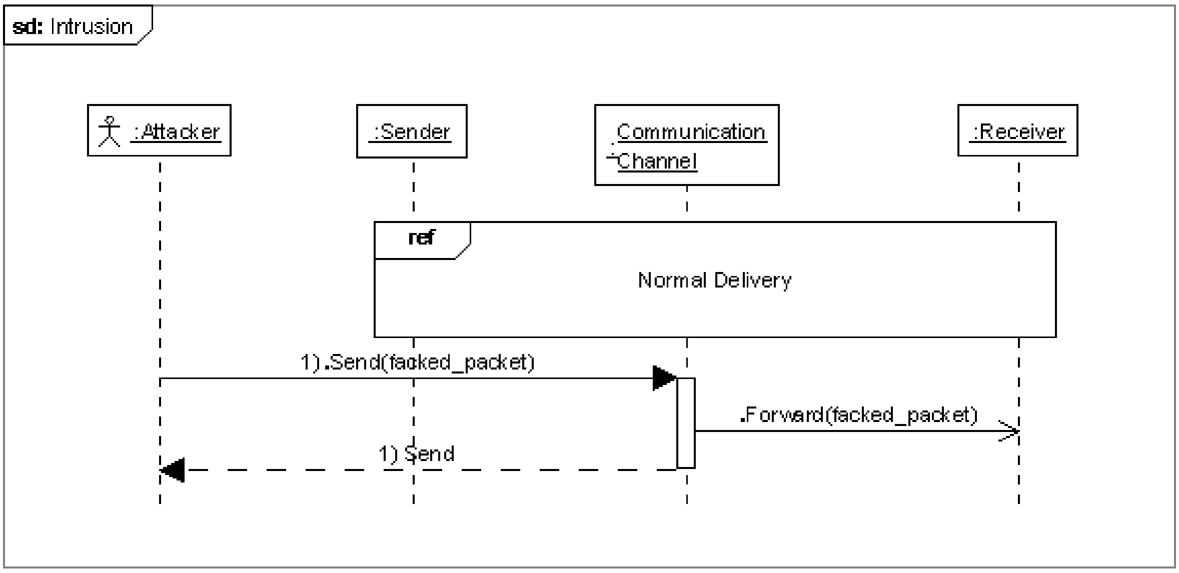


Figure 8-22: Sequence diagram of a denial of service attempt

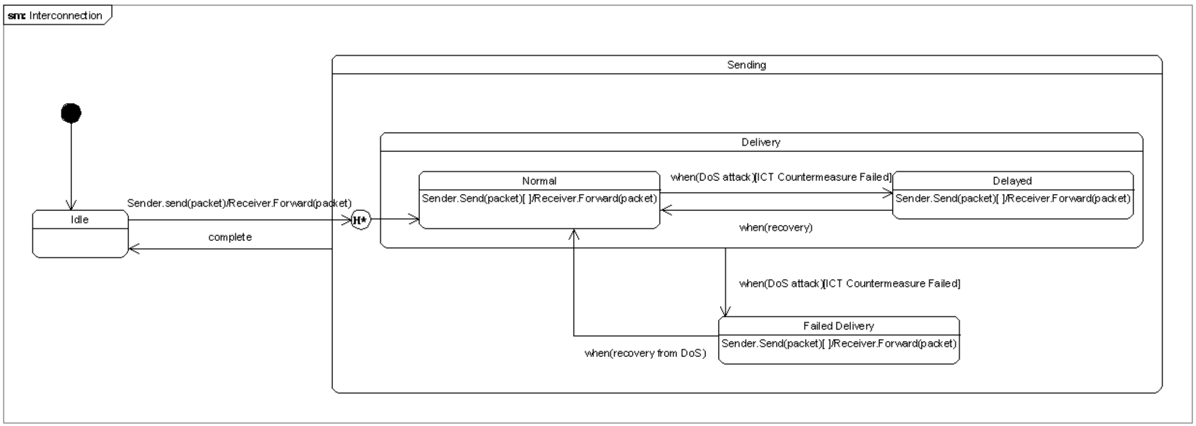


Created with Poseidon for UML Community Edition. Not for Commercial Use.

Figure 8-23: Sequence diagram of an intrusion attempt

Figure 8-24 shows the possible states of the interconnection (the class *Interconnection* in Figure 5-11) in case of denial of service according to scenario 1: the interconnection is initially *Idle* and turns to the state *Sending* when the transmission of packet begins; such state contains an inner state machine composed by the states *Delivery* and *Failed Delivery*, where *Delivery* is the initial one. The state *Delivery* represents the situation where the packets are delivered, possibly with a delay; the state *Failed Delivery* represents the situation where the packets are not delivered. The state transition from *Delivery* to *Failed Delivery* is due to the combination of a denial of service affecting the interconnection, and the failure of the corresponding countermeasure. The inverse state transition, from *Failed Delivery* to *Delivery*, is due an action of recovery from the denial of service.

The state *Delivery* contains a further inner state machine composed by the states *Normal* and *Delayed*; in the state *Normal*, the packets are delivered without any delay; in the state *Delayed* the packets are delivered on delay. The state transition from *Normal* to *Delayed* is determined by the begin of a denial of service; the inverse state transition from *Delayed* to *Normal* is determined by an action of recovery from the denial of service.


sm: Interconnection
Sending
Delivery
Idle
Sender.send(packet)/Receiver.Forward(packet)
complete
H*
Normal
Sender.Send(packet)[ ]/Receiver.Forward(packet)
when(DoS attack)[ICT Countermeasure Failed]
Delayed
Sender.Send(packet)[ ]/Receiver.Forward(packet)
when(recovery)
when(DoS attack)[ICT Countermeasure Failed]
Failed Delivery
Sender.Send(packet)[ ]/Receiver.Forward(packet)
when(recovery from DoS)

Created with Poseidon for UML Community Edition. Not for Commercial Use.

Figure 8-24: States of the interconnection in case of Denial of Service

8.2.7 UML representation of the Scenario 1

8.2.7.1 Denial of service

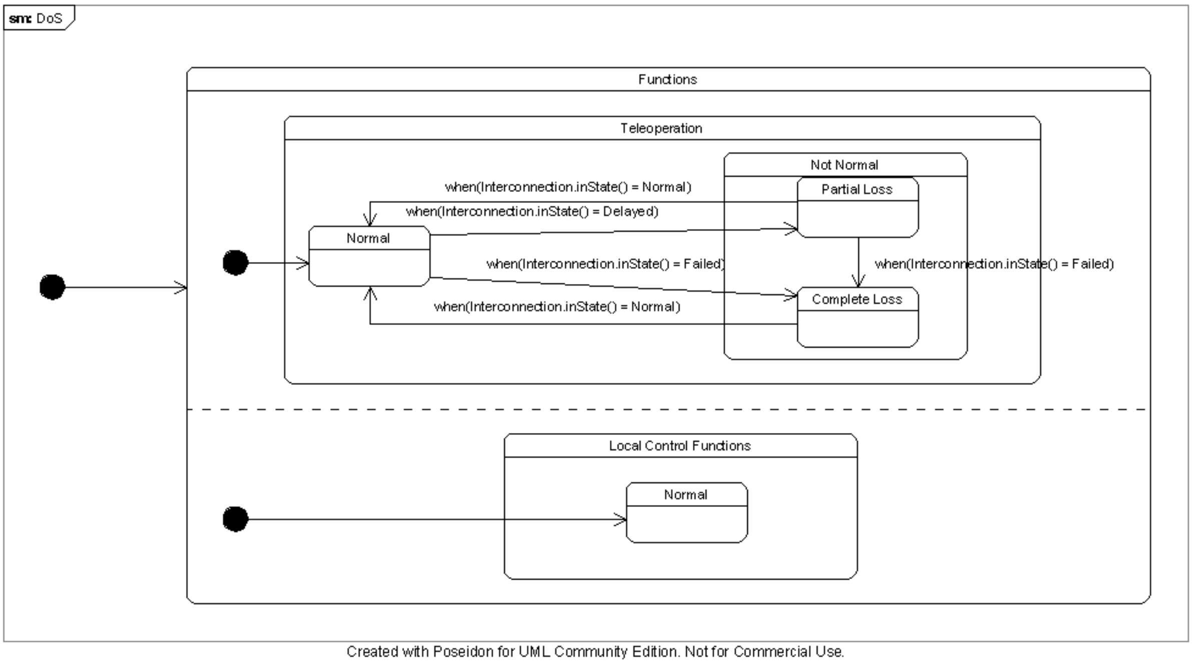

sm: DoS
Functions
Teleoperation
Not Normal
Partial Loss
Complete Loss
Normal
when(Interconnection.inState() = Normal)
when(Interconnection.inState() = Delayed)
when(Interconnection.inState() = Failed)
when(Interconnection.inState() = Normal)
when(Interconnection.inState() = Failed)
Local Control Functions
Normal
Created with Poseidon for UML Community Edition. Not for Commercial Use.

Figure 8-25: States of the Teleoperation and of the Substation local control functions, in case of denial of service

Figure 8-25 shows the states of the Teleoperation and of the local control functions of the substation, in case of denial of service according to scenario 1. The state transitions in the state machine in Figure 8-25 are determined by the possible states of the interconnection shown in Figure 8-24.

The Teleoperation can turn from the state *Normal* to the state *Partial Loss* if the interconnection is in state *Delayed* (see the state machine in Figure 8-24). In the state *Partial Loss*, we have a partial loss of the Teleoperation commands. The inverse state transition, from *Partial Loss* to *Normal*, occurs if the interconnection turns back to the state *Normal* (see the state machine in Figure 8-24).

In Figure 8-25, the state transition of the Teleoperation, from *Normal* to *Complete Loss*, is determined by the state *Failed* of the interconnection; the inverse state transition is due to the state *Normal* of the interconnection.

The states *Partial Loss* and *Complete Loss* compose the global state *Not Normal* of the Teleoperation. Moreover, inside such global state, a state transition is possible from *Partial Loss* to *Complete Loss* and is due to the state *Failed* of the interconnection.

The state machine diagram in Figure 8-25 shows also the state of the local control functions of the substation; such state is permanent because it is not influenced by the state of the interconnection.

8.2.7.2 Intrusion

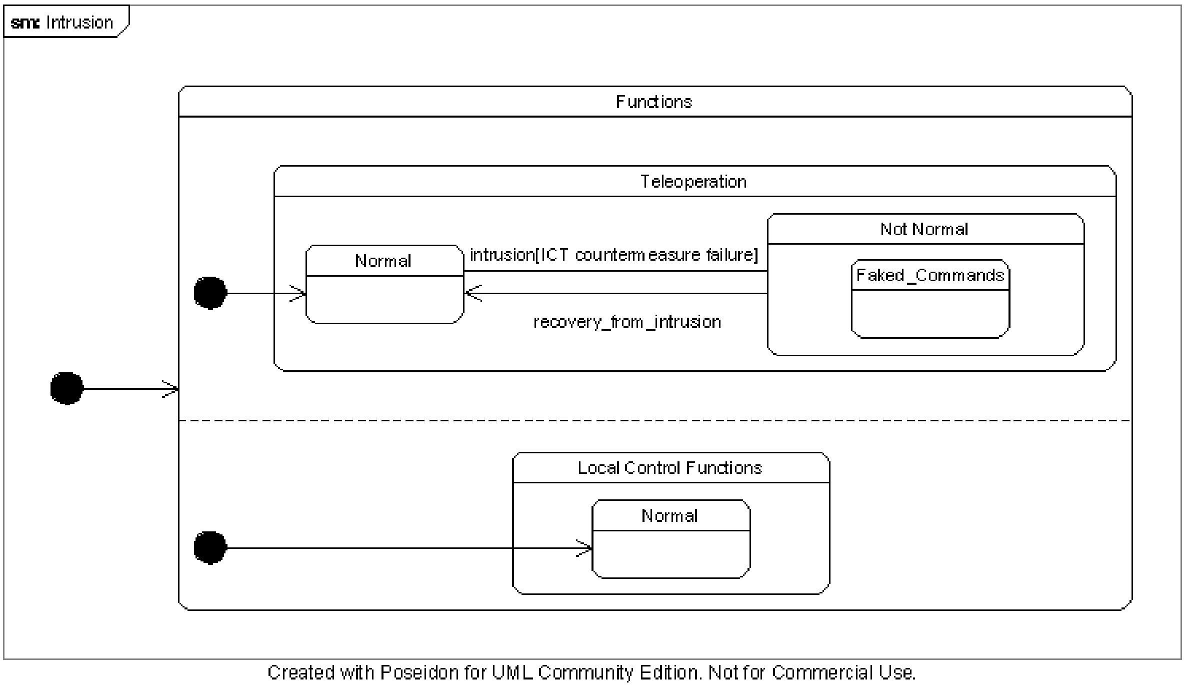


Figure 8-26: States of the Teleoperation and of the Substation local control functions, in case of intrusion

The state machine in Figure 8-26 concerns the Teleoperation and the local control functions in case of intrusion according to the Scenario 1. The Teleoperation turns from the state *Normal* to the state *Faked_Commands* in an intrusion occurs and the corresponding countermeasure fails. The inverse transition is due to a recovery action. The state *Faked_Commands* is an internal state of the global state *Not Normal* already present in the state machine in Figure 8-25.

The local control functions are not influenced by the intrusion, so they keep the *Normal* state.

8.2.8 UML representation of the Distributed Generation Scenarios

8.2.8.1 Non malicious Agent

The state diagram in Figure 8-27 shows the possible states of a non malicious agent. In such diagram, the agent is initially in the state *Created*, then it turns to the state *UnderRegistration*; in this state, the agent has been recently created and its neighbours are being informed of its presence. At the end of this process, the agent turns to the *Active* state; in such state, the agent is known by all its neighbours and is performing its activity. If the agent decides to leave the overlay network, then the agent turns from the *Active* state to the *RemoveRegistration* state; during such state the agent is removed by the overlay network by informing the neighbours of the agent about the fact that the agent is being excluded from the network. At the end of the removing activity, the agent turns to the final state *Removed*.

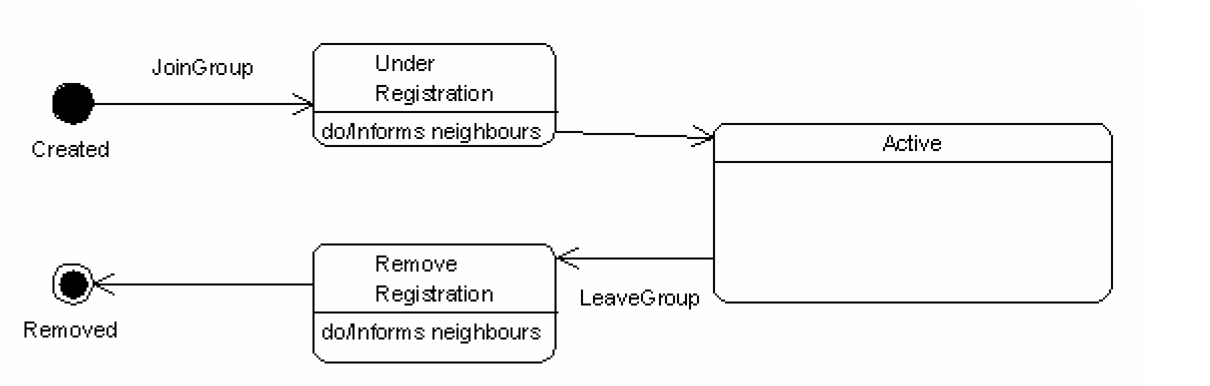


Figure 8-27: State diagram of a non malicious agent

8.2.8.2 Malicious Agent

Figure 8-28 depicts the possible states of the a malicious agent, i. e. an agent joining the overlay network with the aim of performing some kind of malicious attack to the network. Such an agent is initially in the state *Created*, then it turns to the *UnderRegistration* state in order to join the overlay network. When this activity is completed, the malicious agent turns to the state *Active* representing the situation where the agent is performing its malicious activity. Actually such state is a super-state whose sub-states represent the possible forms of attack that the malicious agent may perform; such sub-states are: *VoltageLevelAttack*, *DosAttack*, *ChangingTopology, ManInTheMiddle*. The state *ManInTheMiddle* is in turn a super-state containing the substates *PartitionNetworkAttack* and *EconomicalTampering* representing the attempt to partition the overlay network and the dispatch of faked economical information respectively. Both sub-states are reachable from the state *ChangingTopology* representing the situation where the malicious agent establishes some malicious links in the overlay network. This step is necessary to perform both the malicious partitioning of the network and the economical tampering.

When the agent leaves the *Active* state, it turns to the state *RemoveRegistration* representing the stage where the agent leaves the overlay network. When the agents quits this state, it turns to the final state *Removed*.

With respect to the state diagram of the non malicious agent (Figure 8-27), the state diagram of the malicious agent (Figure 8-28) differs for the malicious activities inside the *Active* state.

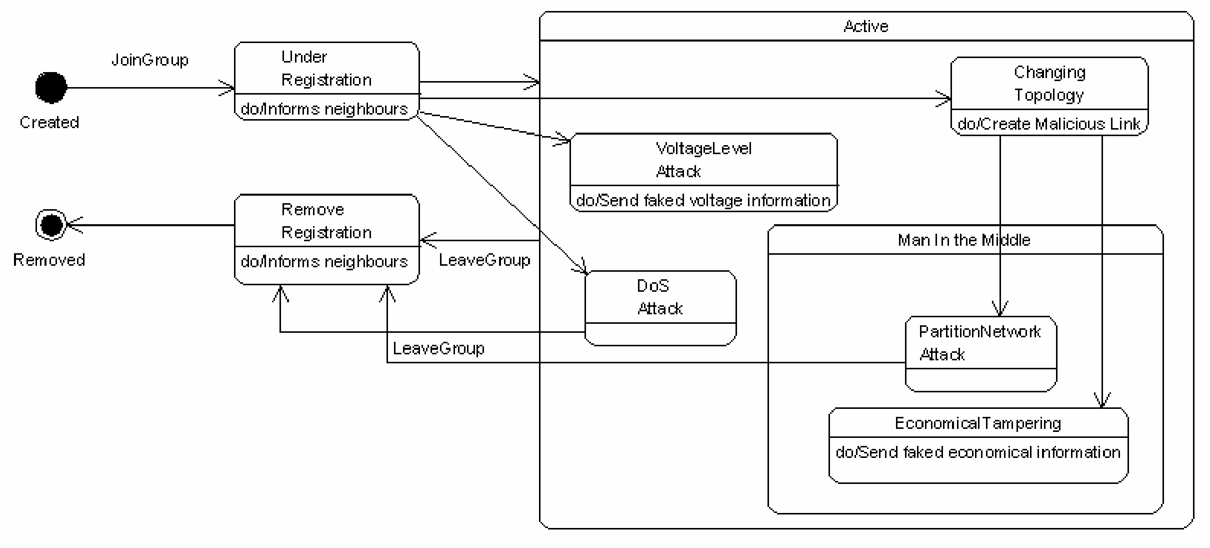


Figure 8-28: State diagram of a malicious agent

The possible states of the overlay network are shown in the state diagram in Figure 8-29 where the state transitions are due to the effects of the activity of a malicious agent (the states of a malicious agent are described in Figure 8-28).

The overlay network is initially in the *Normal* state, and turns to the state *SinglePointOfFailure* when a malicious agent turns to the state *ManInTheMiddle* (see the state diagram in Figure 8-28). In other words, such state transition occurs when a malicious agent is able to partition the overlay network or is able to send malicious economical information.

The overlay network turns from the state *SinglePointOfFailure* to the state *Partitioned* when the same malicious agent has determined the partition of the overlay network.

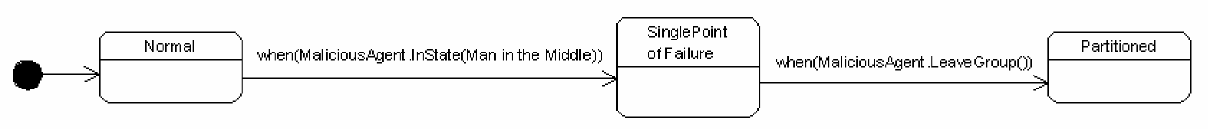

Normal
when(MaliciousAgent.InState(Man in the Middle))
SinglePoint of Failure
when(MaliciousAgent.LeaveGroup())
Partitioned

Figure 8-29: State diagram of the overlay network

The possible states of the portion of internet exploited to realize the overlay network in the distributed generation, are depicted in the state diagram in Figure 8-30. Actually such states concern the consume of the internet bandwidth due to the execution of the distributed algorithm necessary to add or remove an agent from the overlay network (the states of an agent are indicated in the diagram in Figure 8-28).

The initial state of the internet portion is *Normal* where the bandwith is consumed in an ordinary way. If the algorithm is executed for an amount of agents exceeding a certain threshold, then the internet state turns to the state *DelayedDelivery* where the packets are delivered with a certain delay due to the consume of the bandwith in a not ordinary way. The state *DelayedDelivery* is actually a super-state containing the substates *Busy* and *VeryBusy* representing two different levels of consume of the bandwith and consequently two different degrees of delay in the packets delivery.

If the number of agents requiring the execution of the distributed algorithm, keeps on growing, the internet can turn to the state *FailedDelivery* where the packets delivery fails.

If instead the number of agents to add or to remove decreases, the internet can turn back from *FailedDelivery* to *DelayedDelivery*, or from *DelayedDelivery* to *Normal*.

A possible form of denial of service attack affecting the internet portion exploited to realize the overlay network, may consist of generating a huge number of useless agents joining and leaving the overlay network.

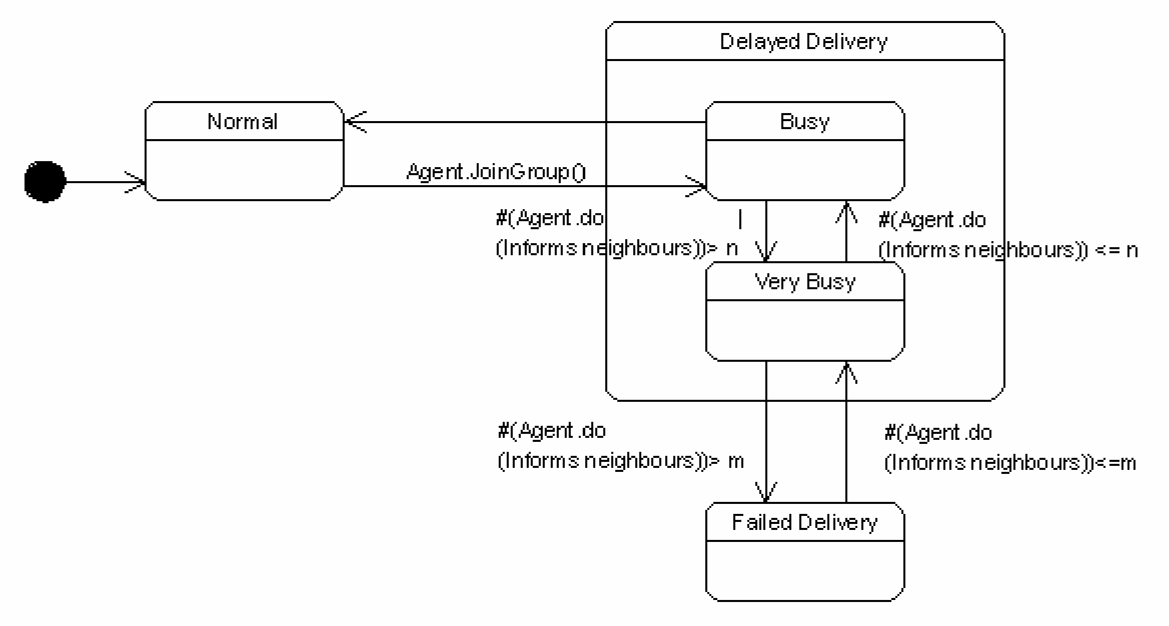


Figure 8-30: State diagram of portion of internet exploited to realize the overlay network

The state diagram in Figure 8-31 shows how the voltage regulation in the distributed generation is affected by the attack of a malicious agent (the states of a malicious agent are shown in Figure 8-28). According to such state diagram, the primary voltage regulation is not affected by the attack (the primary voltage regulation does not change its state). The secondary voltage regulation is initially in the *Optimal* state where no attack has been performed. From the *Optimal* state, the secondary voltage regulation can turn to the state *Degraded* if the overlay network is partitioned by the action of a malicious agent. Otherwise, the secondary voltage regulation can turn from the state *Optimal* to state *DangerouslyOutOfRange* if a malicious agent is negatively influencing the secondary voltage regulation by transmitting malicious information about the voltage levels.

The tertiary voltage regulation is initially in the state *Optimal* where no attack has been performed. From this state, the tertiary voltage regulation can turn to the state *SubOptimal* if a malicious agent performs the partition of the overlay network, or if a malicious agent performs the economical tampering. The tertiary voltage regulation turns from the state *Optimal* to the state *Abnormal* if a malicious agent is negatively influencing the secondary voltage regulation by transmitting malicious information about the voltage levels.

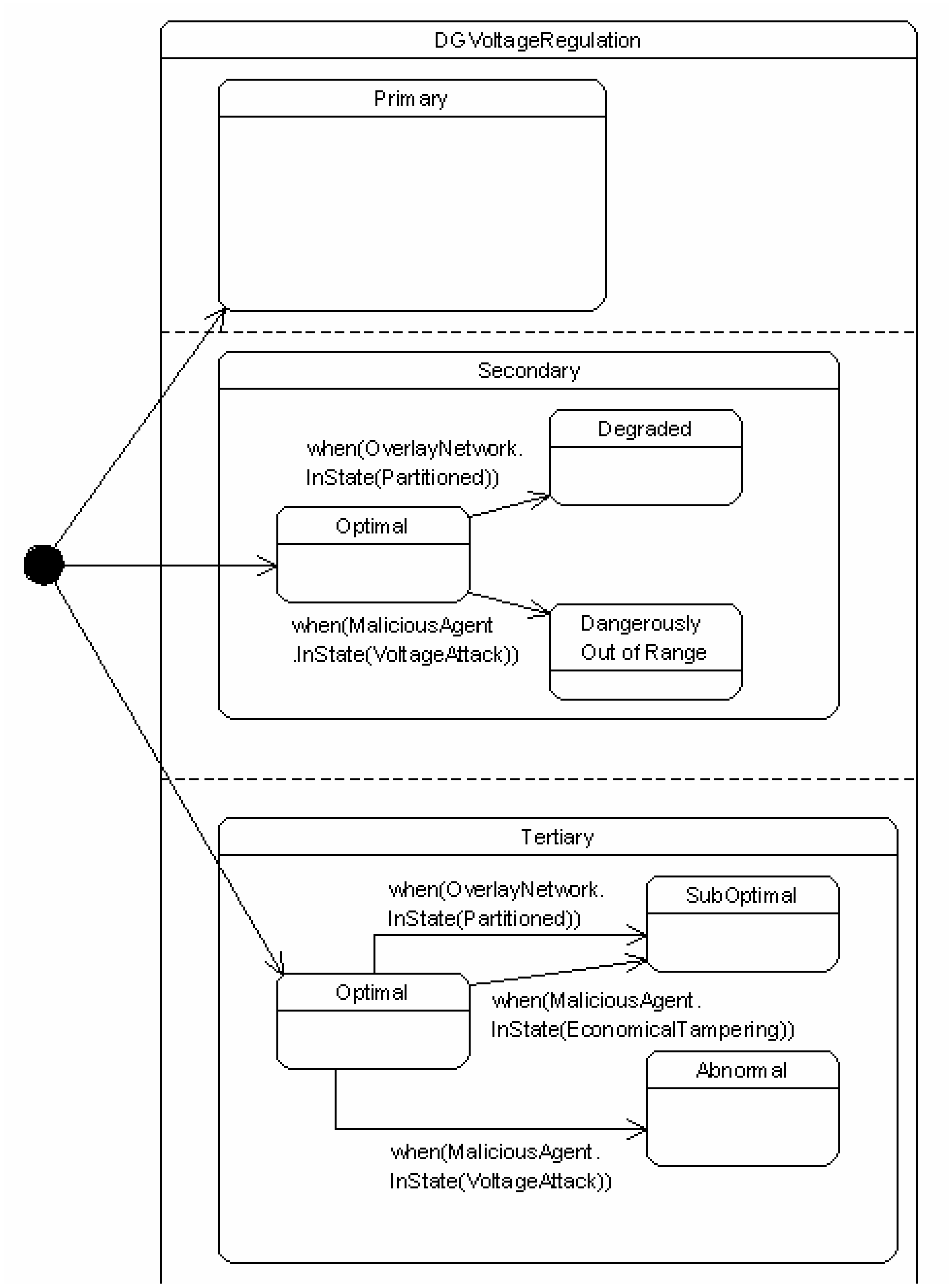


Figure 8-31: State diagram of the voltage regulation in distributed generation system

REFERENCES

[Ackermann *et al.* 2001] Ackermann, T., G. Andersson and L. Söder. “Distributed Generation: a definition”, Electric Power Systems Research, vol. 57, 2001, p.195-204.

[Amin & Wollenberg 2005] Amin, M. and B.F. Wollenberg. “Toward a Smart Grid”, IEEE Power & Energy Magazine, September/October, Vol. 3, No. 5, 2005, pp. 34-41.

[Avizienis *et al.* 2004] Avizienis, A., J. C. Laprie, B. Randell and C. Landwehr. “Basic Concepts and Taxonomy of Dependable and Secure Computing”, IEEE Transaction On Dependable and Secure Computing Vol. 1, No. 1, January-March 2004.

[Brand *et al.* 2003] Brand, K-P, V. Lohmann and W. Wimmer. “Substation Automation Handbook”, Utility Automation Consulting Lohmann, 2003.

[CIRED WG04 1999] CIRED. “Dispersed Generation, Preliminary Report of CIRED Working Group WG04”, June, 1999, p. 9 + Appendix (p.30).

[CNSS I4009 2006] Committee on National Security Systems. “CNSS Instruction n° 4009: National Information Assurance Glossary, May 2003 revised June 2006, http://www.cnss.gov

[Corsi *et al.* 2006] Corsi, S., G. Cappai and I. Valadè. “Wide Area Voltage Protection”, Cigré 2006 Paris Session, Paris, August-September 2006.

[De Brabandere *et al.* 2004] De Brabandere, K., B. Bolsens, J. Van den Keybus, A.Woyte, J. Driesen and R. Belmans. “A voltage and frequency droop control method for parallel inverters”. In Proceedings of the IEEE Power Electronics Specialists Conf. (PESC-2004), pages 2501–2507, Aachen, Germany, Jun 2004.

[DeMarco & Braden 2006] DeMarco, C.L. and Y. Braden. “Threats to Electric Power Grid Security through Hacking of Networked Generation Control”, CRIS, Third International Conference on Critical Infrastructures, Alexandria, VA-USA, September 2006.

[Dimeas & Hatziagryriou 2005] Dimeas, A.L. and N.D. Hatziagyriou, “Operation of a Multiagent System for Microgrid Control”, IEEE Transactions on Power Systems, Vol. 20, No. 3, August 2005.

[Dondi *et al.* 2002] Dondi, P., D. Bayoumi, C. Haederli, D. Julian and M. Suter. “Network Integration of Distributed Power Generation”, Journal of Power Sources, vol. 106, 2002, p. 1-9.

[Dondossola & Lamquet 2006] Dondossola, G. and O. Lamquet. “Cyber Risk Assessment in the Electric Power Industry”, Electra N°224, February 2006, pp. 36-43, http://www.cigre.org/gb/electra/electra.asp

[Dondossola *et al.* 2006a] Dondossola, G., J. Szanto, M. Masera and I. Nai Fovino. “Evaluation of the effects of intentional threats to power substation control systems”, International Workshop on Complex Network and Infrastructure Protection, CNIP 2006 March 28-29 Rome, Italy.

[Dondossola *et al.* 2006b] Dondossola, G., O. Lamquet and A. Torkilseng. “Key issues and related methodologies in the security risk analysis and evaluation of electric power control systems”, Cigrè 2006 Paris Session

[Dunn & Mauer 2006] Dunn, M. and V. Mauer (eds,). International CIIP Handbook 2006, Vol. II, “Analyzing issues, challenges, and prospects”, Center for Security Studies (CSS), ETH Zurich.

[Fink & Carlsen 1978] Fink, L.H. and K. Carlsen. “Operating Under Stress and Strain”, IEEE Spectrum, March 1978, p. 48-53.

[FIPS 200 2006] Federal Information Processing Standards. “FIPS PUB 200: Minimum Security Requirements for Federal Information and Information Systems”, March 2006.

[Flower 2003] Flower, M. “UML Distilled: A Brief Guide to the Standard Object Modeling Language”, Addison Wesley, September 2003.

[Huang *et al.* 2002] Huang, J. and S.S. Venkata. “Wide Area Adaptive Protection: Architecture, Algorithms and Communications”, Proceedings of Power Systems and Communications Infrastructures for the Future, Beijing, September 2002.

[IEA 2002] IEA. “Distributed Generation in Liberalized Electricity Markets, Paris”, 2002, p. 128.

[IEC 60870-5 2006] International Standard IEC 60870-5. “Telecontrol equipment and systems - Part 5-104: Transmission protocols – Network access for IEC 60870-5-101 using standard transport profiles”, International Standard, Second Edition, Reference Number IEC 60870-5-104(E), June 2006.

[IEC 60870-6 2002] International Standard IEC 60870-6. “Telecontrol equipment and systems - Part 6-503: Telecontrol protocols compatible with ISO standards and ITU-T recommendations – TASE.2 Service and protocol”, International Standard, Second Edition, Reference Number IEC 60870-6-503(E), April 2002.

[IEC 61850-5 2003-07] International Standard IEC 61850-5. “Communication network and systems in substations – Part 5: Communication requirements for functions and device models”, First edition 2003-07.

[IEC 61850-6 2004] International Standard IEC 61850-6. “Communication networks and systems in substations – Part 6: Configuration description language for communication in electrical substations related to IEDs”, First Edition, Reference Number IEC 61850-6-2004(E), March 2004.

[Kaâniche *et al.* 2006] Kaâniche, M., J.C. Laprie and K. Kanoun. “Link between LAAS models for describing interdependencies and CESI Power System finite state model”, CRUTIAL Lisboa Meeting October 17, 2006.

[Kaâniche *et al.* 2007] Kaâniche, M., et alter. “Methodologies Synthesis”, CRUTIAL Workpackage 2 deliverable D3, January 2007.

[Kato *et al.* 2005] Kato, T., H. Kanamori, Y. Suzuoki and T. Funabashi. “Multi-Agent Based Control and Protection of Power Distribution System - Protection Scheme with Simplified Information Utilization”, Proceedings of the 13th International Conference on Intelligent Systems Application to Power Systems, 2005.

[Kok *et al.* 2005] Kok, J.K., C.J. Warner and I.G. Kamphuis. “PowerMatcher: Multiagent Control in the Electricity Infrastructure”, Autonomous Agents and Multi-Agent Systems, July 25-29, 2005, Utrecht, Netherlands.

[Laprie *et al.* 2006] Laprie, J.C., K. Kanoun and M. Kaâniche. “Modelling cascading and escalading outages in Interdependent Critical Infrastructures”, Fast Abstract DNS 2006, Philadelphia, USA.

[Lund *et al.* 2006] Lund, P., S. Cherian and T. Ackermann. “A Cell Controller for Autonomous Operation of a 60kV Distribution Area”, International Journal of Distributed Energy Resources, Vol. 2 No. 2 April-June 2006.

[Marwali *et al.* 2004] Marwali, M.N., J.-W. Jung and A. Keyhani. "Control of Distributed Generation Systems - Part II: Load Sharing Control", IEEE Transaction on Power Electronics, Vol. 19, No. 6, November 2004.

[OMG 2002a] Object Management Group. “UML 2.0 Infrastructure Specification. Final Adopted Specification”, Object Management Group, 2002, http://www.uml.org

[OMG 2002b] Object Management Group. “UML 2.0 Superstructure Specification. Final Adopted Specification”, Object Management Group, 2002, http://www.uml.org

[Pender 2003] Pender, T. “UML Byble”, Wiley Pubblishing Inc., September 2003.

[Schainker *et al.* 2006] Schainker, R., J. Douglas and T. Kropp. “Electric Utility Responses to Grid Security Issues”, IEEE power & energy magazine, march/april 2006 edition.

[Tsikalakis *et al.* 2006] Tsikalakis, A.G., A. Dimeas, N.D. Hatziargyriou, J.A. Pecas Lopes, G. Kariniotakis and J. Oyarzabal. “Management of Microgrids in Market Environment”, International Journal of Distributed Energy Resources, Vol. 2 No. 3 July-September 2006.

[UCTE Handbook] UCTE. “UCTE Operation Handbook”, https://www.ucte.org

[UCTE Report 2002] UCTE. “The Effects of System Extension On Inter-Area Oscillations”, https://www.ucte.org, UCTE Annual Report 2002, p.24-25.

[UCTE Report 2003] UCTE. “Final Report of the Investigation Committee on the 28 September 2003 Blackout in Italy”, https://www.ucte.org

[Vanthournout *et al.* 2004a] Vanthournout, K., G. Deconinck and R. Belmans. “Building Dependable Peer-to-Peer Systems”, Supplemental volume of international conference on dependable systems and networks (DSN-200), Florence, Italy, June, 2004; pp. 297-301.

[Vanthournout *et al.* 2004b] Vanthournout, K., G. Deconinck and R. Belmans. “A Small World Overlay Network for Resource Discovery”, In M. Danelutto, D. Laforenza, and M. Vanneschi, editors, 10th Int. Euro-Par Conference(Euro- Par 2004), Lecture notes in Computer Science Vol.3149, Springer, Berlin, Pisa, Italy, Aug/Sept., 2004; pp. 1068-1075.

[Vanthournout *et al.* 2005] Vanthournout, K., K. De Brabandere, E. Haesen , J. Van den Keybus, G. Deconinck and R. Belmans. ”Agora: Distributed tertiary control of distributed resources,”15th Power Systems Computation Conference , 2005 , Liege, Belgium, August 22-26, 2005.

[Vidrascu *et al.* 2006] Vidrascu, A., F. Lenoir and J-M. Delbarre. “Cyber Security in Substation Automation: Design and Supervision”, Cigré 2006 Paris Session.