SCADA IN A CLOUD-BASED ARCHITECTURE

Miguel Osório Areias

DISSERTAÇÃO

MESTRADO EM SEGURANÇA INFORMÁTICA

2013
SCADA IN A CLOUD-BASED ARCHITECTURE

Miguel Osório Areias

MESTRADO EM SEGURANÇA INFORMÁTICA

2013
Acknowledgments

Firstly I would like to thank Aurelio Blanquet, Carlos Mota Pinto and Pedro Gama from EDP that encouraged me and allow me to apply in this Master and also gave me all the necessary support throughout this period.

I would also like to thank Professor António Casimiro and Professor Alysson Bessani by the engaging way that they have motivated and supported me during this thesis.

To Nuno Pereira, whose guidance was essential during the development of this work, especially by give me interesting ideas and also being very supportive in this endeavor.
To Ana, Carolina and Madalena for their patience.
Resumo

Uma rede elétrica inteligente (Smart Grid) transforma a maneira como a energia é distribuída e utilizada, adicionando inteligência ao longo da rede para reduzir drasticamente interrupções e falhas, gerindo a procura, actual e futura, aumentando a eficiência e gestão de custos. Para fazer isso, a Smart Grid utiliza sensores, controladores digitais e ferramentas analíticas para monitorar e automatizar o fluxo e entrega de energia aos consumidores, permitindo um fluxo bidirecional de energia elétrica e de informações entre o comando central e os aparelhos do terreno, distribuídos geograficamente. Através de redes inteligentes, também é possível incorporar novas energias sustentáveis, como eólica e solar, e integrar fontes de energia distribuídas, ou veículos elétricos. Para apoiar este novo paradigma, as redes inteligentes vão impulsionar um amplo uso de sensores na rede com maior inteligência, aperfeiçoamento da eficiência energética e resposta à procura. Todos esses equipamentos na rede vão exigir um poder de computação substancialmente maior para controlo e gestão. Neste ambiente exigente, a computação em nuvem poderá proporcionar benefícios relevantes a nível de custos. Através de uma computação em nuvem é possível disponibilizar informação em tempo-real ao utilizar/consumidor dando-lhe a possibilidade de compreensão de como a energia é consumida e o que deve fazer para optimizar esse consumo. Por outro lado, o fornecimento de informação sobre os benefícios energéticos e incentivo ao consumo em determinados períodos do dia pode desencadear ajustes de consumo e, por conseguinte, reduzir a procura durante os períodos de pico de utilização. Relativamente à eficiência energética, o uso de computação em nuvem permite reduzir o poder computacional dos centros de dados através de uma gestão eficiente, aumentando a eficiência dos servidores, fontes de alimentação e sistemas de refrigeração. No entanto, os riscos associados a uma migração de actividades críticas para um ambiente de computação em nuvem podem ser inaceitáveis. Com este trabalho vamos avaliar o risco a que uma rede elétrica inteligente está exposta e o impacto, a nível financeiro, de continuidade de negócio ou de reputação para uma organização face à perda de qualquer um dos principais atributos de segurança (confidencialidade, integridade e disponibilidade). Com base nos resultados anteriores, e considerando a crescente necessidade computacional e de armazenamento de uma rede elétrica inteligente, vamos propor uma nova arquitectura baseada na computação em nuvem.

Palavras-chave: SCADA, Rede elétrica inteligente, Computação em nuvem.
Abstract

A Smart grid transforms the way the power is distributed and used, adding intelligence throughout the grid to dramatically reduce outages and faults, handles current and future demand, increases efficiency and manage costs. To do this, a Smart Grid uses sensors, digital controls and analytic tools to automate, monitor the flow and delivery of energy to consumers. In addition, Smart Grid enables a two-way flow of electricity and information between the end-points and the appliance. Through Smart Grids it is also possible to incorporate new sustainable energies such as wind and solar generation, and interacts locally with distributed power sources, or plug-in electrical vehicles. To support this new paradigm, Smart grids will boost a widespread use of intelligence data sensors on the grid improving both energy efficiency and demand response. All those equipments will require substantial computing power for controlling and managing. In this scenario, clouds computing will provide substantial cost benefits. Using real-time information through cloud computing gives to the consumer the possibility of understanding how energy is consumed and what they can do to improve it. Expectatively, the real-time feedback on energy consumption should help to improve the consumer’s behaviour. On the other hand, on the utility side, providing information about benefits, can foster incentives for consumption adjustments and, as a result, reduce demand during peak usage periods. Concerning energy efficiency, using clouds allows us to reduce the computational power of data centers through efficient application management, increasing the efficiency of servers, power supplies and cooling systems. However, the risks incurred by the migration of such critical activities to an unprotected cloud environment would be unacceptable. In our work we will assess the risk that a Smart Grid is exposed and the impact, in financial, business continuity and reputation levels, for an organization due to the loss of any of major security attributes (confidentiality, integrity and availability). Based on the previous results and the need for scalability, underlying of a Smart Grid evolution, is then proposed an architecture based on cloud computing.

Keywords: SCADA, Smart Grid, Cloud Computing.
# Contents

List of figures xv

Lista de Tabelas xvii

1 Introduction 1

1.1 Motivation ........................................... 1
1.2 Contribution ........................................ 2
1.3 Structure of the Document .......................... 2

2 Industrial Networks and Critical Infrastructure 5

2.1 Critical Information Infrastructures ............... 5
  2.1.1 The Importance of Securing Critical Infrastructure .... 6
  2.1.2 The Impact of Critical Infrastructure Incidents ...... 8

3 Smart Grids 13

3.1 The Electricity Network Evolution ................. 13
3.2 Smart Grid Technical Architecture ............. 14
  3.2.1 Smart Meter .................................. 15
  3.2.2 Concentrator ................................ 16
  3.2.3 Grid and Communication ...................... 16
  3.2.4 Central Systems ............................... 17
3.3 Smart Grid Security Requirements .............. 18
  3.3.1 Security Objectives .......................... 18
  3.3.2 Vulnerabilities, Threats and Risks ........... 20
3.4 Risk Analysis ..................................... 21
  3.4.1 Measure the Probability ....................... 22
  3.4.2 Measure the impact ........................... 22
  3.4.3 Smart Grid Risk Analysis ................... 24
  3.4.4 Final Remarks ................................ 29

4 Hosting the Smart Grid in a Cloud Infrastructure 31

4.1 What is Cloud Computing .......................... 31
## List of Figures

2.1 Critical Infrastructure Protection. ............................................ 6  
2.2 Critical infrastructure attacks. ............................................. 10  

3.1 Smart Grid Architecture. .................................................... 14  
3.2 Assess and quantify the risk. .............................................. 20  
3.3 Quantitative risk measurement. .......................................... 21  
3.4 Operational and financial impact. ...................................... 25  
3.5 Areas of greatest risk and impact. ..................................... 30  

4.1 Cloud Computing Service Models. ..................................... 34  
4.2 Cloud Computing Deployment Models. ................................. 35  
4.3 Reference architecture of the Smart Grid. ............................ 38  
4.4 Smart Grid Cloud Architecture. ......................................... 40  

5.1 Smart Meter functionalities. .............................................. 43  
5.2 Smart Meter functionalities that have physical or real-time dependencies. 48  
5.3 Smart Meter functionalities, in grey, that must be hosted on the meter. ... 51  

6.1 Present Smart Grid architecture. ....................................... 56  
6.2 Smart Grid Cloud architecture. ......................................... 56
List of Tables

2.1 The potential impact of successful cyber attacks. ......................... 9
3.1 Impact analysis - criteria for Availability. .............................. 23
3.2 Impact analysis - criteria for Integrity. ................................. 24
3.3 Impact analysis - criteria for Confidentiality. ......................... 24
3.4 Risk for the Smart Grid services regarding Availability. .......... 25
3.5 Risk for the Smart Grid services regarding Integrity. .............. 26
3.6 Risk for the Smart Grid services regarding Confidentiality. ...... 26
3.7 Risk of loss of Availability considering financial, business continuity and reputation impact. ........................................... 28
3.8 Risk of loss of Integrity considering financial, business continuity and reputation impact. ................................................. 29
3.9 Risk of loss of Confidentiality considering financial, business continuity and reputation impact. ...................................... 29
5.1 Smart meter, scalability and physical dependency. .................... 47
5.2 Smart meter, real-time dependency. ........................................ 48
5.3 Dependency between non-fundamental and fundamental on-site functionalities. .......................................................... 49
5.4 Dependency between Storage of Information and the remaining non-fundamental functionalities. ........................................ 50
6.1 Gathering information, test results. ......................................... 57
7.1 Criticality of the Smart Grid Vs SGCA regarding Availability. .... 59
7.2 Criticality of the Smart Grid Vs SGCA regarding Integrity. .......... 60
7.3 Criticality of the Smart Grid Vs SGCA regarding Confidentiality. . 60
Chapter 1

Introduction

1.1 Motivation

In the last decade, the command and control systems, including SCADA (Supervision, Control and Data Acquisition), have undergone a significant evolution. This evolution is largely driven by new technological developments and by internal pressure to streamline processes while reducing cost. This evolution led to a complete shift of paradigm in terms of systems, communications and human resources. Clear examples are the use of COTS (Commercial Off-The-Shelf) in systems previously designed and built for a specific function, or even at the communication level, where proprietary protocols give rise to standards in order to enhance the interoperability of equipment and solutions. All these changes and developments have numerous advantages, not only financial but also technical, since they can work as an enabler to integrate components from different manufacturers with different communication protocols. However, some aspects of this transition were not carefully safeguarded. Two examples are security and scalability of the solution.

Security, obtained for long by "obscurity", did not come with the technological evolution of these systems, becoming a major concern for anyone responsible for security. On the other hand, the scalability, necessary to support the massive introduction of new equipment, was not weighted, creating limitations to the evolution of a traditional SCADA into a Smart Grid. The Smart Grid is an electrical power infrastructure that makes intelligent decisions about the state of the electrical power system to maintain a stable environment. As a matter of fact, the Smart Grid is the evolution of the traditional power grid, being more efficient, innovative and focused on the clients needs.

In this new scenario, where the computer capabilities will become much more demanding, the technical evolution to a cloud architecture could be a cornerstone to a new critical infrastructure focused on scalability and able to process large amounts of data in real-time.
1.2 Contribution

Our main objective is to introduce an alternative architecture to the Smart Grid based on cloud computing and aiming to increase dependability and robustness of this critical infrastructure. This work has is starting point on the results of a European project, TClouds [1], where EDP have been involved. In the TClouds project we have defined a Smart Grid sub-system for public lighting management designed to be hosted on the cloud. This sub-system consists in a web application hosted in a cloud that enables authorized users to interact with the underlying Smart Grid infrastructure. Based on the TClouds results it is possible to use the cloud computing, in a controlled environment, to host the public lighting management sub-system.

In this present work we would like to complete the work developed in TClouds by assessing the current fragilities and limitations of the cloud computing architecture to host the electric power grid. To this end, we present a risk assessment involving current and new functionalities of Smart Grids, such as Smart Meters and their requirements in terms of privacy and data protection. This study is then used for a deeper analysis, involving all components of Smart Meters and quantifying the impact caused by the migration to the cloud of specific components and functionalities of the Smart Meter. Finally, an architecture is presented, based on the concept of cloud computing, which guarantees all the functionality of the system and takes the benefits underlying cloud computing.

All work presented here has been supported on the existing Smart Grid architecture at EDP and, despite the absence of software developments, allowed us to consolidate knowledge about the adoption of a cloud computing in such a critical infrastructure.

1.3 Structure of the Document

This dissertation is organized as follows:

Chapter 2: This chapter explains the concept of critical infrastructure enhancing its role and importance in society and the potential impact caused by an incident in this infrastructure.

Chapter 3: In this chapter it will be presented the evolution of the electrical network. Then it will be introduced the Smart Grid concept, its components and architecture. It will also be performed a risk analysis based on the criticality of the Smart Grid services regarding Confidentiality, Integrity and Availability. This paragraph will be ended with the analysis of organizational risk and depicts the impact into the organization in terms of financial, business continuity and reputation, caused by the loss of each of the principal
security attributes (Confidentiality, Integrity and Availability).

**Chapter 4:** This Chapter is related to the study performed by us in order to hosting the Smart Grid on cloud computing infrastructure. For that, the chapter starts with a definition of a cloud computing, its characteristics and models. Then, we explain the existing limitations in the present Smart Grid architecture and enumerates the advantages of using cloud computing for the critical infrastructure. A new cloud based architecture, supported by the findings of the previous chapter, will be then presented.

**Chapter 5:** This chapter explores the limitation of the Smart Meter in fulfilling all the requirements of the new cloud base architecture. For this reason, it will be conducted an assessment of the impact of move each of the Smart Meter’s functionalities to the cloud. The previous analysis will give the possibility to identify fundamental and non-fundamental functionalities of the Smart Meter and select those who must remain on the equipment and those who can easily migrate to the cloud.

**Chapter 6:** In this chapter, and after the previous analysis presented in Chapter 5, we will evaluate present limitation for deploying this new architecture on a cloud computing environment.

**Chapter 7:** In order to evaluate the new architecture presented in the Chapter 4, here we performed a second risk analysis based on the same methodology used in the Chapter 3.

**Chapter 8:** The final conclusions of the thesis are presented in Chapter 8. This includes a SWOT analysis and also a discussion of the contribution of this work in the design of a new architecture for Smart Grids that is currently under implementation at EDP.
Chapter 2

Industrial Networks and Critical Infrastructure

Industrial networks have been evolving over time. This development enhanced by technological advances have allowed these systems to provide solutions increasingly dependent on computing power and communication. Through this section we will present what is a critical infrastructure, its importance and the possible impact of a security incident.

2.1 Critical Information Infrastructures

A critical infrastructure is a complex and large-scale system whose correct operation has a high societal value, giving rise to high louses in failure scenarios, which can range from economic costs to loss of lives. Electrical networks are one of the most mature types of Critical Infrastructure (CI). Those CIs are usually remotely controlled by computers and interconnected through networks. The computational part of the CI is usually called Critical Information Infrastructure (CII) and is composed by networks, computers and software. The CII could be split into SCADA (Supervision Control and Data Acquisition) and Corporate subsystems, both with different roles in the overall system.

The Corporate subsystem hosts the IT components and can be composed by several sites interconnected by secure channels. In addition, the Corporate subsystem is connected, through a single logical connection, to the SCADA subsystem. This connection is depicted in the picture 2.1 by the control system firewall.

Supervisory Control and Data Acquisition (SCADA), on the other hand, refers generically to computer and network systems, which perform data collection and cyber control of physical processes, such as those of electrical utilities. These processes can span several sites spread out over large areas and as such, SCADA systems are today inherently distributed, although their aim is to allow supervision and control from one or a few centralized points, from/to where all information flows.
The SCADA system usually controls pipelines, water and transportation systems, utilities, refineries, chemical plans, and a wide variety of manufacturing operations. The use of those systems lies on the possibility to implement efficient control, improving plant and personnel safety, therefore reducing the cost of operation.

SCADA systems started to be used as standalone and completely isolated, i.e., with no connectivity to other systems. In addition, systems were built based on custom hardware and software. At that time, control systems were confined to a particular plant and consisted of a central unit that communicated with local controllers to interface with motors, pumps, valves, switches, sensors, and so on. In order to perform the connections between devices, companies and vendors developed their own communication protocols, many of them proprietary.

To improve both computer and networks effectiveness and reduce total cost of ownership, SCADA systems started to use standard hardware and software. Electrical utilities have also increased their reliance on the internet and communication networks and SCADA systems have evolved from standalone to distributed, inheriting some of the vulnerabilities and starting to be exposed to the same threats that plague usual computer systems.

2.1.1 The Importance of Securing Critical Infrastructure

Hardware computers, SCADA software and communication lines, as well as all the data communications transmitted through these last ones, stored on computers or processed by software, are considered cyber assets. Cyber assets are essential to the operation of crit-
ical assets infrastructures like generation plant, power lines, transformers or substations. The power of a SCADA operator to control a wide electrical infrastructure just seating in front of a computer, has brought incredible cost/efficiency advantages for electrical utilities. However it also gave rise to an increasing importance and visibility of the cyber assets. Although, cyber assets are essential to achieve our expectations for high continuity of electrical service, they also have jeopardised the service itself. They are attractive targets for malicious groups or individuals that intend to cause disruption of the service.

These kinds of attacks to critical information infrastructures often fall into cyber-crime and cyber-terrorism and cause severe financial impact to electrical companies as well as social implications in our lives. Nowadays, with the increasing quality requirements of the electrical business regulator and the penalties for power disruptions mainly after the 11th September, it becomes clear, to the electrical utilities, the importance of the cyber assets, their impact on the business as well as the need to protect them. Usually, Threat Agent is the term used to describe the potential source of a threat. To identify possible threat sources we must have a holistic view of the entire system. We need to consider all the aspects of the security discipline, starting from computers, go through physical security and go further up to operation procedures, social engineering and other security aspects. Threat Agents could be sorted out in two basic categories: internal threats and external threats. Internal threats could arise from employees or contractors that have free access to confidential and critical information and also physical access to facilities with critical cyber assets. These internal threats could be accidental or intentional; however they represent an important source of successful attacks to cyber assets. External Threat Agents, on the other hand, do not have an authorized physical access to facilities or sensitive information. These kinds of threats could be, for instance, natural or man-made disasters, that obviously are hard to avoid or predict. One of the critical external Threat Agents, belonging to the category of the former inside, that could be an ex-employee who quit and still with access to confidential information.

Security in critical infrastructures becomes even more critical once the industrial systems are built for reliability and longevity, ensuring operation without pause for months or even years, where the overall life expectancy may be measured in decades. In contrast, those systems and networks used are easily outpaced by the tools employed by an attacker, who have easy access to new exploits and can employ them at any time. Worse still, the average number of days between the time when the vulnerability is disclosed publicity and the time when the vulnerability is discovered in the control systems may be larger than one year. This gap implies that there are known vulnerabilities that can allow hackers and cyber criminals entry into the system by exploring known vulnerabilities that have not been fixed yet.
2.1.2 The Impact of Critical Infrastructure Incidents

The electrical networks have been a major concern on the part of economic stakeholders, states and the operators themselves, by fears of cyber attacks that cause instability (e.g., blackouts, technical data corruption, physical damage to power devices). In fact, society is increasingly dependent on critical services, and events that have gone unnoticed years ago, are now disclosed in average prime-time, as some recent blackouts. Even in so-called normal conditions, there is now a central concern with the quality of service. As this is crucial for business, it is attractive to hackers: damaging the quality of service could represent cash, e.g. perspective of blackmail information, or even sabotage.

Increasingly, operators have come to discover that threats against computers and control servers, can have such devastating effects as attacks on their own physical infrastructure. Cyber sabotage could result in injury or loss of life, including the loss of critical services or even catastrophic explosions.

Consequences of a Successful Cyber Incident

A successful cyber attack on a control system could be materialized in changing the intended process or altering information related to a process. The first scenario could be translated in changing the amount of energy produced at an electrical generation facility while the second scenario is related with preventing a bulk energy provider from obtaining production metrics that are used in energy trading or other business operation. In both cases the result is similar, and could be translated into penalties, financial impact of loss of production or even in the unavailability of the service, resulting in a Denial of Service (DoS).

Table 2.1 shows several incident types and, for each one, its potential impact. The solution, currently, is to architect and manage critical information infrastructures to possess at least the level of safety and reliability of traditional IT systems (if not better).

Examples of Critical infrastructure Incidents

The need to protect critical infrastructures from cyber attacks started to be a concern three years ago when stuxnet [2] destroyed 1,000 centrifuges that Iran was using to enrich uranium after taking over the computerized systems that operated the centrifuges. From that moment on, electric grid operators started to talk about the need to protect critical infrastructure from cyberattacks, and some utilities even hired a chief information security officer [3]. Stuxnet is a computer worm discovered in June 2010 which was targeted to the Iranian nuclear power station. There are previous reports related to critical infrastructures cyber attacks [4] (see figure 2.2), not only targeting standard computing platforms,
<table>
<thead>
<tr>
<th>Incident Type</th>
<th>Potential Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change in a system, operating system, or application configuration</td>
<td>Introduction of command and control channels into otherwise security system. Suppression of alarms and reports to hide malicious activity.</td>
</tr>
<tr>
<td>Change in programmable logic in remote controllers</td>
<td>Damage to equipment and/or facilities. Malfunction of the process.</td>
</tr>
<tr>
<td>Misinformation report to operators</td>
<td>Causing inappropriate actions in response to misinformation that could result in a change in programmable logic. Hiding or obfuscating malicious activities, including the incident itself or injected code (i.e., a rootkit)</td>
</tr>
<tr>
<td>Tapering with safety systems or other controls</td>
<td>Preventing expected operations, fail safes, and other safeguards with potential damaging consequences.</td>
</tr>
<tr>
<td>Malicious software (malware) infection</td>
<td>May initiate additional incidents scenarios which could impact production.</td>
</tr>
<tr>
<td>Information theft</td>
<td>Sensitive information is stolen.</td>
</tr>
<tr>
<td>Information alteration</td>
<td>Sensitive information is altered in order to adversely affect the operation.</td>
</tr>
</tbody>
</table>

Table 2.1: The potential impact of successful cyber attacks.

but even to Programmable Logic Controller (PLC) equipments. The difference between Stuxnet and other attacks lies in the method used in Stuxnet and the dimension of the attack. Estonia and Georgia attacks [5] in June 2007 and August 2008 are two good examples of earlier attacks, or later on, in 2010, the Night Dragon attack [6] that explored vulnerabilities on oil and electrical companies. In these cases, the attack collects sensitive information by exploring social engineering, fishing and Microsoft Windows operating system vulnerabilities.

Like the previous examples, Stuxnet’s purpose is also to sabotage industrial processes on a SCADA system, in this case by exploring security weaknesses to steal industrial secrets and potentially disrupting operations of critical infrastructures. Stuxnet, as Night Dragon, also explore Microsoft Windows operating system vulnerabilities to install and propagate the worm among SCADA equipments. However, the Stuxnet’s particularity is the use of a man-in-the-middle code to fake the PLC and also by exploring a zero-day vulnerability.

The SCADA systems, as many other critical infrastructures systems, are based on several backup mechanisms to ensure that a single failure of one component of the architecture does not stop the operation. To do that, those kinds of systems are built on a hot-standby architecture where the failure of one component is easily compensated, in a couple of seconds, by another component with the same role. On the other hand, to ensure reliability,
the SCADA systems have redundancy also in communications from the PLC level to the control center. Bearing in mind the redundancy implemented on the SCADA architecture and the capacity of recovering from faults, it is understandable why a direct attack aiming at stopping a single component of the architecture does not represent disruption of the overall operation. Other vectors of attack are used to increase the magnitude of the attack and many of them are based on a structured and planed attack. Stuxnet is a good example of a very well planed attack. Aware of this problem, many companies designed and implemented a common strategy of addressing security. A single security perimeter was established including in it all vulnerable critical cyber assets. All external access to the SCADA system has been protected by a strong access control scheme. In fact, all connections from the outside, established either from other corporate networks or from the Internet, were made more secure by requiring strong authentication procedures and encrypted protocols, and accesses filtered by firewalls. The security perimeter strategy, in spite of ensuring a good level of security from the outside, provides little or no security against insider attacks. The vulnerabilities and threats from the inside on the security perimeter need to be addressed in order to improve security for SCADA control systems. An attack from the inside represents a greater threat because someone who has deeper knowledge of the system architecture and has the cover of being already inside the security firewall perimeter might perform it.

Recent malwares such as Night dragon, Stuxnet or more recently, the malicious program Duqu [20], exploit exactly the security perimeter weakness on the SCADA systems.
Those are visible both by the growth of knowledge and by the processes used in these latest attacks. Indeed, the attacks on unique equipment for the sole purpose of breaking a service are already, by far, deprecated. The next generation of attacks will be even more sophisticated and comprehensive, and utilities companies must be prepared to address the new threats appropriately. To do that they must identify current risks under a holistic attack model (inside as well as outside) and develop new schemes and techniques to bring its systems to the next (and higher) level of security and dependability.

In the next paragraph we address this subject by presenting a criticality evaluation under the three fundamental security attributes (confidentiality, integrity and availability). This evaluation has also in consideration the SCADA evolution and the impact caused by the introduction of new services and components.
Chapter 3

Smart Grids

In the previous chapter we depicted the SCADA system as a mature critical infrastructure. In this chapter we describe its evolution and its main components and we assess the impact caused by specific faults.

3.1 The Electricity Network Evolution

Presently, the electricity supply system is based primarily on large, centralized and predictable energy sources, and networks to enable power flow to uncontrolled, but reasonably predictable, demand. In this scenario, the electricity networks are designed to facilitate primarily unidirectional flow from generation to demand, and to cope with the relatively low levels of short term unpredictability in demand. However, governments are now driving the transition to a secure, safe, low carbon emission, affordable energy system. This new paradigm, based on targets for reduction of greenhouse gas emissions and the decarbonization of the electricity supply, requires, from the electricity network companies, dealing with significant new challenges in order to integrate many more forms of supply and demand, in a much more dynamic and robust manner. A core element of this system will be an electricity network which has the capacity to transfer significantly more energy between a diverse range of dynamically changing generators and consumers, whilst maintaining the balance between supply and demand at multiple levels within the network. In order to achieve this, significant developments are required in integrated and intelligent monitoring and network control, resulting in a dramatic increase in the distributed nature and in the complexity of network monitoring and control systems. The resulting energy system is commonly known as the Smart Grid. Figure 3.1 presents the Smart Grid infrastructure composed and operating in three main layers. The bottom layer (right on the figure) encompasses new devices and hardware that can measure and monitor the grid behaviour through sensors on the grid or meters installed at homes. The middle layer is comprised of information technology systems that gather all the data being captured by the previous layer and deliver them to where they are needed. The top
layer is responsible for analysing all the data gathered, translating and presenting it to stakeholders.

### 3.2 Smart Grid Technical Architecture

The overall solution consists of several components which, articulated among themselves, allow us to address the objectives preconized for the system, in terms of energy management, micro-production integration and implementation of Smart Grids concepts. Therefore, the main components of this solution are:

- **Smart Meter**: devices installed at consumers/producers (including modules for measuring, actuation, processing, interface, communication, etc.);

- **Concentrator**: local control equipment installed at switching stations (including modules for measuring, actuation, processing, interface, communication, etc.);

- **Grids/Communications**: equipment and technologies for information transmission;

- **Central Systems**: systems and applications for management and central data processing.

As mentioned before, the picture 3.1 illustrates the technical architecture for the present Smart Grid, which identifies the main components and how they are joined among themselves. The following sessions address each of these components.


3.2.1 Smart Meter

The change of paradigm underway in the electrical energy system will require restructuring in the architectural model of the various components of the overall solution, with particular prominence in the Smart Meter equipment’s. The Smart Meter is a device consisting of sensors, meters, actuators, etc, which will replace the current meter. Even though, it includes a set of functions that goes well beyond power metering. Along with allowing for a detailed characterization of consumptions (accessible both locally for the consumer and remotely for the marketer), the Smart Meter sets the connection between the various low-voltage grid customers and the Switching Station, via the concentrator. The Smart Meter not only establishes the link with the rest of the system, but it also relates a set of current and future needs of each residence/consumer, grid operator, marketer, among others. We consider that all Smart Meters generally have a concentrator that manages them.

The Smart Meter needs to have an innovative architecture which not only asserts its own identity, but also should ensure modularity and evolution:

- Modular to configure, in a quickly and easily fashion, the most suitable solutions for the various consumers. To ensure this requirement, the meter must operate in a similar fashion to a “lego,” by making it possible to put together various modules for creating a single object (e.g.: the possibility of setting up value-added services for more demanding customers – domotics – by simply including additional modules/services on top of standard – central core), On the other hand, this equipment should operate similarly to “computer-peripherals,” by making it possible to externally connect/couple other devices so as to enrich services made available (e.g. possibility of connecting to more advanced/complex displays, various sensors and measuring points, etc).

- Evolutive to allow the evolution of services and functionalities made available without the need to replace the installed equipment (e.g. the possibility of adding micro-production for a consumer that also becomes a producer, and, to this end, it is enough to “add” new modules/services to the Smart Meter as already installed).

The Smart Meter’s modularity and evolutionary capacity features have presently the following characteristics:

- The ability to connect to other external components (advanced display, other meters, PDAs/laptops/PCs, etc.)

- The ability to have a basic configuration with minimum services that are indispensable to any device to be set up at the consumption site, taking into account the basic processing and the memory of the central module, namely:
- Metrology (active and reactive power and energy);
- Standard data processing for the purposes of preparing rates, load diagrams, alarms, events, managing cut-off/restoring orders and change of power, among others;
- Communication with the concentrator;
- Standard interface for communication with external devices;
- Power cut-off/connecting mechanisms and change of maximum power;
- Display with basic control and safety information.

• The ability to include and integrate other modules without the need to replace the equipment, so as to bring about an evolution of services being offered, including:
  - Additional processing capability (calculations, statistics, profiles, rates);
  - Home Area Network (HAN) communication for interaction with other devices, such as displays, equipment controllers (domotics), sensors and actuators, other meters;
  - Micro-production support, with energy management and production control capability.

### 3.2.2 Concentrator

The role of the concentrator is mainly related with the capacity of gathering information from the Smart Meters, installed at the client’s home, and transfer them to the central systems. This equipment, usually installed on the switch stations, does not only work as an interconnection bridge between the Smart Meter and the central systems but it also has a command and control role. For this reason, it is often called Distribution Transformer Controller (DTC).

In this specific area, the Concentrator is the cornerstone to boost the evolution of the electrical distribution system for an efficient combination between several micro-production technologies, to be connected to Medium-Voltage (MV) and Low-Voltage (LV) grids. Only with this integration it is possible to optimize processes involved in managing and operating the distribution grid in real-time.

### 3.2.3 Grid and Communication

In the general system, there are several different communication networks. Right from the outset, we point out the communication networks set up between the central system and the Concentrator and between the Concentrator and the Smart Meter. On top of these
communication networks, there are other networks associated with each device and with the interaction between these and the exterior.

The WAN communication network ensures the communication between the central system and the Concentrator and is nowadays supported in GPRS (General Packet Radio Service) and ADSL (Asymmetric Digital Subscriber Line) technologies, Power Line Communication (PLC), among others. There are several european initiatives to define and specify a standard for both WAN and LAN communication to be used on Smart Grid, but still a work in progress that takes into consideration the network configurations and available technologies, among other relevant features. This debate is even more complex and broad since communication technologies, such as the PLC, may vary from country to country.

The LAN communication network, set between the Concentrator and the various Smart Meters, is also be based on PLC technology and, in a few cases, can be performed by GPRS or others. As mentioned previously, there are several initiatives regarding alternative solutions, as a function of network configurations and other parameters associated with communication.

In addition, almost all european initiatives considered that the communication protocols, involved in the Smart Grid network, should be preferably public/standard. This means that the protocols comprising the various communication technologies shall preferably be part of the public domain, so as to ensure uniformity of communication with the various devices. The definition of communication protocols should be based on issues pertaining to the quality of service, standardization, communication security, among others.

3.2.4 Central Systems

The large volume of information that is made available with the structure of the Smart Grid system is (centrally) managed by an architecture of Central Information Systems (hereinafter designated as Information System), which shall interact with the other systems of the various intervening parties in the distribution grid (either existing or which will exist). The Information System is able to support the Information management of a commercial/rate-related nature, intended for billing the use of the grids, for each consumer or independent producer, as well as fraud control (involving the monitoring of consumption, energy production, quality-of-services indexes for the eventual automatic issue of compensations in the event of non-compliance with reference quality levels set in the Quality-of-Service Regulation, etc.).

This system is also responsible for the management of consumption/production infor-
information that will enable to support the services provided as part of the electricity market, including those obligations associated with sending information to marketers, the systems operator, regulatory authority, as well as the management of energy data for the purposes of calculating energy balances, establishing technical and commercial losses, determining typical consumption profiles, etc. It is also a role of the Information System to control the quality of data collected, through the implementation of functionalities pertaining to validation, editing and estimating data, taking into account the infrastructure’s technical management needs and the rules set forth for the electricity market.

Finally, the Information System should ensure automatic implementation of operations associated with the contractual life cycle of the consumption/production facilities, such as: rate changes; changes in contracted power; cut-off and restoring service due to contractual non-compliance, contract terminations/activations, or others. On the other hand, the Information System guarantees the management of technical information intended for monitoring, controlling and operating the distribution grid, via interaction with SCADA or other types of systems (powers produced and consumed, voltage levels, monitoring quality of service, etc.) as well as updating systems responsible for managing incidents and characterizing grid topology.

### 3.3 Smart Grid Security Requirements

#### 3.3.1 Security Objectives

It is imperative that any security countermeasures implemented in the Smart Grid do not impact on power availability or safety. The SCADA must be always available, since a lack or omission of information in the system, for example, during an emergency situation, could cause safety issues.

In most industries, confidentiality and integrity have higher precedence over availability. However, in the electrical power systems there is a slight difference. In these specific systems the more important security attribute is availability followed by integrity and finally by confidentiality.

**Availability**

Availability, as already mentioned, is the major security attribute of the electrical power system. These systems continuously monitor the state of the grid, in an estimated maximum latency\(^1\) of 8.3 milliseconds\([24]\) (for a typical SCADA configuration of 1200 baud, 8 data bits, 1 start bit, and 1 stop bit, transmitting one character). In this environment a

\(^1\)We discuss latency in terms of the time required to transmit a character over the long-haul SCADA communications line.
disruption in the information update can cause a loss of power. The righteousness, despite availability, of the electrical power will be dependent on the quality of the current state estimation in the power system and can be translated in integrity of input data.

Reliability and Fault Tolerance

The SCADA system relies on fault tolerance mechanisms based on hot-standby functionalities. Upon a computer failure, identified by the loss of communication, the system automatically transfers the functionality to the secondary (standby) computer. It is important to note that the failure determination is done independently from either computer, so a failure of either computer alone does not jeopardize the monitoring/control process. If the primary computer fails, the transfer to the hot standby is automatic. If the secondary computer fails, the primary continues all of the monitoring/control functions. This approach has the ability to tolerate faults and it is normally used in the most critical systems that may need to operate even while under attack by intruders, viruses, or even malfunctioning servers.

Integrity

Data integrity, in the critical infrastructures is one of the most worrying considering the main CIA (Confidentiality, Integrity and Availability) security attributes. SCADA systems are traditionally prepared to operate while some servers are malfunctioning. This is achieved, as mentioned before, by a hot standby system that ensures extreme reliability through data replication mechanisms. Loss of data integrity, in a SCADA system, can result in failures in the power supply or even blackouts. This is because all the system updates are centralized on a dashboard and shown to the operator. A malicious change on that information can induce or influence the operator to perform actions based on wrong information or influencing wrong decisions.

Confidentiality

The underlying challenges about data confidentiality on a Critical Infrastructure environment are similar to any other system and rely on ensuring that only authorized entities can gain access to that information. When unauthorized individuals or systems can have access information then, confidentiality is breached. Usually the value of confidentiality is high when it has personal information about people and its behaviour. Considering this last paragraph and in the context of our work, problems arise when the SCADA system become border and, through the Smart Grid, starting to deal with personal and private information.
3.3.2 Vulnerabilities, Threats and Risks

Based on the previous sessions and in what has already been mentioned about critical infrastructure, their impact on society and evolution, it became evident that ensuring the reliability of the electricity network infrastructure, whether Smart Grid or traditional grid, is a fundamental requirement for the functioning of modern society. Its importance to daily life means that it must be carefully designed, implemented and operated in order to ensure that risks are appropriately managed. Thus, the successful operation of the Smart Grid will be highly dependent on ICT (Information and Communication Technology) based computing systems, which will need to be sufficiently dependable in such a way that they do not negatively impact on the security of supply. Chain cyber security risks in general, and Smart Grids cyber security risks in particular, are not well understood or quantified. As a matter of fact, the risk measurement could also be quite confusing. The correct measure of how to secure a system depends much on the number and significance of the flows of the system and on the potential of the attack they may be subjected to. This means that the risk is the combination of the level of threat to which a computing or communication system is exposed, and the degree of vulnerability it possesses. In general, an attack is a malicious intentional fault, introduced in a computer or component, with the objective of exploiting a vulnerability in that system.

Figure 3.2: Assess and quantify the risk.

Figure 3.2 represents a threat that exploits a security gap in some part of the infrastructure that may generate, as a consequence, errors in the system. The risk assessment is not more than quantify the effects and impacts of a vulnerability being exploited [22]. The consequence of the above is that Smart Grid security risks can only be qualitatively assessed, need to be re-assessed on a regular basis as the threat landscape changes and new vulnerabilities are disclosed over time and, need to be actively managed to maintain acceptably low levels of risk. The next session is dedicated to this topic, deepening performing a risk analysis.
3.4 Risk Analysis

The Risk Analysis, by definition [33], is a component of risk management entered on the determination of cause-and-effect relationship between probable happenings, their magnitude and likely outcomes. The risk analysis consists also in predicting the outcomes evaluation under different perspectives and the application of qualitative and quantitative techniques to reduce ambiguity of the outcomes and associated impact, usually converted in costs, liabilities, or losses.

The qualitative risk analysis consists of using the cause-and-effect matrix, presented in Figure 3.3, to prioritize and rank the risk. It is important to highlight that the qualitative measures of risk must combine this two qualitative components: the probability of the risk occurring and the size of its impact. At the end, the result for each risk would be evaluated through a numbered raking system such as Low, Moderate, High and Very High.

The quantitative risk analysis quantifies, in terms of quantity, the ranked risks in terms of time and cost.

![Figure 3.3: Quantitative risk measurement.](image)

In our particular case, the Smart Grid, as any other complex system, is built through the integration and contribution of many different services which, according to its own specificities, have different security requirements encompassing different impacts in case of failure. In order to perform a trustworthy risk assessment it is mandatory to identify all the services available and, for each one, assess the possible impact of its failure. For this purpose we have identified eight different services covering all existing roles in the Smart
Grid architecture:

- **Grid Control and Operation** - is related with the SCADA control and operation which is performed centralized at the central system;

- **Energy Metering Management** - it is also performed at the central systems but related with the metering management;

- **Information Services** - represent the IT systems that are connected to the Grid Control and Operation and to the Energy Metering Management (billing, SAP, Asset management, ..);

- **WAN communication** - is the communication between the Smart Meter concentrator or the primary substation and the central system;

- **Primary Substation Operation** - represents the operation and data gathering performed at the primary substation;

- **Smart Meter’s Concentrator** - usually installed at the secondary substation, is responsible for collect data from the Smart Meters and to control local SCADA equipments;

- **LAN communication** - is the communication between the Smart Meter concentrator and the Smart Meters;

- **Smart Meter** - is installed at the client’s home and it is responsible for collect consumer data, perform some calculation and provide information to the client.

### 3.4.1 Measure the Probability

The probability in the risk analysis, estimates the likelihood of uncertain events occur within a specified period. However, this previous sentence should not be misread, the risk event will not occur deterministically with a specific frequency, thereby, the probability of an event occurs can range anywhere from just above never to just below certain. It is important to note that a probability in any of those extremes (never or certain) represents a certainty not a risk. With this notion in mind, our probability rank was defined between rare and almost certain.

### 3.4.2 Measure the impact

Impact is a measure of importance (negative) for the operation caused by the loss of the listed proprieties. For that, we consider that two resources with the same level of impact in relation to a failure can have a complete different probability of failure among them. What we refer here is, assuming a failure, how critical is the lack of this functionality. To
illustrate this previous paragraph, we can consider two resources with high impact concerning Integrity. In this scenario, resource A has a high probability of losing Integrity (almost certain) while resource B, on the other hand, has a low likelihood (rare). We also consider a third resource, C, with low impact. In this abstract example, the operational risk imposed by the integrity of the resource A is considerably higher comparing to the resource B. Accordingly, the protection of integrity, which must be considered in both cases, should be higher for resource A. Nevertheless, they may use the same mechanisms but implemented differently in terms of settings and parameters. Resource C, by having a low impact, can earn simpler mechanisms.

The criteria identified for the evaluation of the operational impact of the major categories of services in Smart Grids, concerning loss of Availability, Integrity and Confidentiality are:

**Availability**

Availability is the proportion of time a service is in a functioning condition, i.e., is the maximum delay time admissible to a service response. In our work we considered that a service that can be more than 2 hours off-line is a service with low Availability requirements. On the opposite, a service is considered very high in Availability terms, if it cannot be off-line more than 30 minutes. Table 3.1 depicts all the Availability levels considered in our work.

<table>
<thead>
<tr>
<th>Availability</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very High</td>
<td>The service cannot be off-line more than 30 minutes</td>
</tr>
<tr>
<td>High</td>
<td>The service can be off-line between 30 minutes and 1 hour</td>
</tr>
<tr>
<td>Moderate</td>
<td>The service can be off-line between 1 hour and 2 hours</td>
</tr>
<tr>
<td>Low</td>
<td>The service can be off-line more than 2 hours</td>
</tr>
</tbody>
</table>

Table 3.1: Impact analysis - criteria for Availability.

**Integrity**

Integrity is regarded as the honesty and truthfulness or accuracy of a system or process, and can be measured as the impact caused by a malicious change on the information. In our work we considered a system with low Integrity requirements whose who the unauthorized modifications do not have any impact on the process. On the opposite, a system is considered very high if it unauthorized modifications represents serious impact on the service. Table 3.2 depicts all the Integrity levels considered in our work.
Chapter 3. Smart Grids

<table>
<thead>
<tr>
<th>Integrity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very High</td>
<td>Modification have serious impact on the service</td>
</tr>
<tr>
<td>High</td>
<td>Modification have notable impact on the service</td>
</tr>
<tr>
<td>Moderate</td>
<td>Modification only have a minor impact on the service</td>
</tr>
<tr>
<td>Low</td>
<td>Modification do not have impact on the service</td>
</tr>
</tbody>
</table>

Table 3.2: Impact analysis - criteria for Integrity.

Confidentiality

Confidentiality is a requirement that limits access or places restrictions on certain types of information. In our work we considered a system with low Confidentiality requirements if the information that it deals with is public domain. On the opposite, a system is considered very high if it the information that it deals with is confidential. Table 3.3 depicts all the Confidentiality levels considered in our work.

<table>
<thead>
<tr>
<th>Confidentiality</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very High</td>
<td>The information is confidential</td>
</tr>
<tr>
<td>High</td>
<td>The information in restricted internally</td>
</tr>
<tr>
<td>Moderate</td>
<td>The information in internally</td>
</tr>
<tr>
<td>Low</td>
<td>The information is public</td>
</tr>
</tbody>
</table>

Table 3.3: Impact analysis - criteria for Confidentiality.

3.4.3 Smart Grid Risk Analysis

The criteria defined and presented in Tables 3.1, 3.2 and 3.3 are considered the impact for our risk analysis which, complemented with the likelihood of happening, will identify the risk for each of the Smart Grid’s services. However, the Smart Grid, as any other complex system, has a number of stakeholders with different requirements and expectations. For our analysis we have defined three different level of stakeholders involving operational and financial impacts.

The operational impact analyzes the criticality of the system from an internal point of view, i.e., evaluates the probability of a hazard and the impact that it causes in critical services.

The financial impact determines the potential impact, this time from an external point of view, resulting from the interruption of a specific service and how it is reflected in consumers and, in the last instance, in the market. To this second analysis we have considered that the impact could be translated in terms of cost (financial), provisioning (business continuity) and the impact caused by a hazard on the society’s opinion (reputation).
Operational Impact

Through Table 3.4 it is possible to see that the level of risk concerning loss of Availability is the same (moderate risk) for all functionalities of the Smart Grid. Although, even with the same risk level, it is important to highlight the probability of the loss of Availability assigned to the Smart Meter and the LAN communication which, comparatively, it is higher than the other services. The reason for this lies in the fact that this equipment is installed in the customers’ homes and, therefore, it is impossible to create physical barriers of security.

<table>
<thead>
<tr>
<th>Service</th>
<th>Probability</th>
<th>Loss of Availability</th>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Grid Control and Operation</td>
<td>Rare</td>
<td>Very High</td>
<td>Moderate</td>
</tr>
<tr>
<td>Energy Metering Management</td>
<td>Rare</td>
<td>Very High</td>
<td>Moderate</td>
</tr>
<tr>
<td>Information services</td>
<td>Rare</td>
<td>Very High</td>
<td>Moderate</td>
</tr>
<tr>
<td>WAN communication</td>
<td>Unlike</td>
<td>High</td>
<td>Moderate</td>
</tr>
<tr>
<td>Primary substation operation</td>
<td>Unlike</td>
<td>High</td>
<td>Moderate</td>
</tr>
<tr>
<td>Smart Meter's Concentrator</td>
<td>Unlike</td>
<td>High</td>
<td>Moderate</td>
</tr>
<tr>
<td>LAN communication</td>
<td>Possible</td>
<td>Moderate</td>
<td>Moderate</td>
</tr>
<tr>
<td>Smart meter</td>
<td>Possible</td>
<td>Moderate</td>
<td>Moderate</td>
</tr>
</tbody>
</table>

Table 3.4: Risk for the Smart Grid services regarding Availability.

Table 3.5 represents the same study that was done in Table 3.4 but now assessing the impact in terms of Integrity.

The evaluation in terms of Integrity gives us the possibility to segregate the Smart Grid services in two main groups: 1) the group of SCADA functionalities that have a clear influence on the command and control of the electric network and, 2) the group caused by the lack of integrity throughout the metering process. The first group includes the Grid...
Table 3.5: Risk for the Smart Grid services regarding Integrity.

Control and Operation and the Primary Substation Operation, here the lack of Integrity is high at the Primary Substation because they may hold wrong decisions. As a matter of fact, the electric control network is performed centrally and entirely based on information received from the field, in this case, by the command and control equipment at the substations level. This hierarchical dependency supports the impact on the Grid Control and Operation in terms of loss of Integrity once this system collects information from the substations, computes and remotely controls the substations. Even with several differences in terms of impact, due to loss of Integrity, the risk is the same. The reason for that lies on the security mechanisms, implemented at the central systems layer, which reduce the hazard probability at the Grid Control and Operation.

The second group defined for the risk analysis for the loss of Integrity involves the Smart Meter, the Concentrator and the Energy Metering Management. Here it is important to mention that, similar to the previous analysis, the probability decrease from the bottom to the top, e.i., is possible at the Smart Meter, unlike at the Smart Meter’s Concentrators and rare at the Energy Metering Management.

Table 3.6: Risk for the Smart Grid services regarding Confidentiality.
Table 3.6, focusing on the loss of Confidentiality, shows evidences that services related to SCADA (Grid Control and Operation and Primary Substation operation) present a very low risk in face of loss of Confidentiality. The reason for this is related to the fact that those services only treats technical data related to the electric network and, because of that, the Confidentiality is not a requisite. The same situation is no longer present in the metering components (Energy Metering Management, Concentrator and Smart Meter). Here, as in the case of loss of Integrity, the likelihood is higher in Smart Meters compared with the central systems. In addition, the impact of loss of Confidentiality grows towards the central systems.

It is also important to mention that WAN and LAN communications are considered high in terms of confidentiality when placed in the Smart Grids context. The reason for that lies in the fact that this new Smart Grids paradigm involves not only control and operations processes but also customer and consumption information, required for the metering process, and much more demanding in terms of Confidentiality requirements. Traditionally, in a independent analysis assumes that control and operation as critically low concerning Confidentiality.

**Financial Impact**

Tables 3.4, 3.5 and 3.6 gives us a view of the impact, in term of criticality, for each of the Smart Grid’s services, evaluated them in terms of Confidentiality, Integrity and Availability. Despite the goodness of this analysis, the assessment based only on criticality might not be enough. Actually, even considering the CIA[23] a widely used benchmark for security evaluation, there are organizational risks that must be considered in addition to those which have already been discussed. These risks must have impact into the organization in terms of financial, business continuity and reputation for the loss of Availability, Integrity and Confidentiality.

Tables 3.7, 3.8 and 3.9 present, respectively, the risk of loss of Availability, Integrity and Confidentiality, from the perspectives of financial, business continuity or reputation impact for an organization. What is important and noteworthy is that the introduction of the commercial component of the Smart Grid, referred in the tables as energy metering management, expressively increases the risk for the organization in all three analyses.

The financial risk measures the increase in costs and decrease in revenue resulting from losses of each one of the security attributes. The same methodology was used to evaluate the impact of business continuity on the organization. The business continuity analysis complements the previous one, the financial, by integrating the possible costs associated with the technical impact. Lastly, we assessed the impact on the company’s reputation re-
sulting from loss of each security attributes. This final analysis, the reputation, represents a social assessment of the organization and may hold negatively the financial results of the organization.

<table>
<thead>
<tr>
<th>Service</th>
<th>Risk of loss of Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Financial</td>
</tr>
<tr>
<td>Grid Control and Operation</td>
<td>Moderate</td>
</tr>
<tr>
<td>Energy Metering Management</td>
<td>Very High</td>
</tr>
<tr>
<td>Information services</td>
<td>High</td>
</tr>
<tr>
<td>WAN communication</td>
<td>Moderate</td>
</tr>
<tr>
<td>Primary substation operation</td>
<td>Moderate</td>
</tr>
<tr>
<td>Smart Meter’s Concentrator</td>
<td>High</td>
</tr>
<tr>
<td>LAN communication</td>
<td>Moderate</td>
</tr>
<tr>
<td>Smart meter</td>
<td>Moderate</td>
</tr>
</tbody>
</table>

Table 3.7: Risk of loss of Availability considering financial, business continuity and reputation impact.

Table 3.7, gives us the possibility to draw some conclusions about the risk of loss of Availability in a Smart Grid architecture. On one hand, the introduction of the Energy Metering Management represents an increase in the financial risk, which influences negatively the reputation security risks. The reason for the increase of the financial risk is related to the services provided to customers which, as in the case of consumption, have high requirements in terms of availability and impact on reputation. On the other hand, real-time operation is a prerequisite of any SCADA system and, as that, requires availability and dependency on communications.

A second analysis, presented in the Table 3.8, assesses the risk resulting from loss of Integrity. This analysis can be analyzed in two different perspectives. On one hand, the impact of the hazard in the technical components (Grid Control and Operation and Primary Substation Operation) and the impact on the metering components (Energy Metering Management, Smart Meter’s Concentrator and Smart Meters). Considering the technical components, which only deals with technical data, the impact of loss of Integrity is bigger at the business continuity and reputation level if compared with the financial impact. The lack of Integrity in the SCADA system could influence negatively the operation of the electrical grid, misleading to wrong decisions at the command and control level that may cause interruptions in the power distribution. The coherence of the system is, in this scenario, compromised and influence negatively the business continuity and, in cause of power outages, also the reputation of the organization.

In terms of metering, the loss of Integrity represents a financial impact that may influence negatively the revenue. The impact on business continuity and reputation are moderate not representing a real risk to the organization.
A final analysis now considering Confidentiality, allows the measurement of the extreme impact that Smart Grids introduce on this security attribute. There are two factors that alter our intuition about Confidentiality in an environment dedicated to the power distribution. On the one hand, with the introduction of Smart Grids are also introduced services that process sensitive contents, such as consumption and client’s habits. On the other hand, may now less intuitive, the SCADA information itself represents a quite high Confidentiality requirements, as confirmed by recent attacks on critical infrastructure (presented in Chapter 2) which, exclusively targeted critical infrastructure with the intention to sabotage and to get operational information. The results of this final analysis are presented in the table 3.9.

<table>
<thead>
<tr>
<th>Service</th>
<th>Risk of loss of Confidentiality</th>
<th>Financial</th>
<th>Continuity</th>
<th>Reputation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Grid Control and Operation</td>
<td>Moderate</td>
<td>Moderate</td>
<td>Low</td>
<td></td>
</tr>
<tr>
<td>Energy Metering Management</td>
<td>Very High</td>
<td>Moderate</td>
<td>Very High</td>
<td></td>
</tr>
<tr>
<td>Information services</td>
<td>High</td>
<td>Moderate</td>
<td>High</td>
<td></td>
</tr>
<tr>
<td>WAN communication</td>
<td>High</td>
<td>Moderate</td>
<td>High</td>
<td></td>
</tr>
<tr>
<td>Primary substation operation</td>
<td>Low</td>
<td>High</td>
<td>Moderate</td>
<td></td>
</tr>
<tr>
<td>Smart Meter’s Concentrator</td>
<td>High</td>
<td>Moderate</td>
<td>High</td>
<td></td>
</tr>
<tr>
<td>LAN communication</td>
<td>High</td>
<td>Moderate</td>
<td>High</td>
<td></td>
</tr>
<tr>
<td>Smart meter</td>
<td>High</td>
<td>Moderate</td>
<td>High</td>
<td></td>
</tr>
</tbody>
</table>

Table 3.9: Risk of loss of Confidentiality considering financial, business continuity and reputation impact.

### 3.4.4 Final Remarks

The analysis carried out in this chapter was been achieved through the analysis of internal documents and analysis of the combined degree of vulnerabilities and threat levels. As
shown earlier, a risk analysis can identify the areas where the efforts must be placed in order to reduce the fragility of a system. The major objective is to reduce the highest values, both in terms of probability of occurrence and impact caused. The following section presents an alternative architecture for Smart Grids that, in addition to present significant advantages in terms of scalability, significantly decreases the highest risks identified in this session.

![Risk Analysis Table]

<table>
<thead>
<tr>
<th>Probability</th>
<th>Low Risk</th>
<th>Moderate</th>
<th>High</th>
<th>Very High</th>
</tr>
</thead>
<tbody>
<tr>
<td>Almost Certain</td>
<td>Moderate</td>
<td>High Risk</td>
<td>Extreme</td>
<td>Extreme</td>
</tr>
<tr>
<td>Likely</td>
<td>Moderate</td>
<td>High Risk</td>
<td>High Risk</td>
<td>Extreme</td>
</tr>
<tr>
<td>Possible</td>
<td>Low Risk</td>
<td>Moderate</td>
<td>High Risk</td>
<td>Extreme</td>
</tr>
<tr>
<td>Unlikely</td>
<td>Low Risk</td>
<td>Low Risk</td>
<td>Moderate</td>
<td>High Risk</td>
</tr>
<tr>
<td>Rare</td>
<td>Low Risk</td>
<td>Low Risk</td>
<td>Moderate</td>
<td>Moderate</td>
</tr>
</tbody>
</table>

Figure 3.5: Areas of greatest risk and impact.
Chapter 4

Hosting the Smart Grid in a Cloud Infrastructure

On the Smart Grid the near-real-time data generated by Advanced Meter Infrastructure (AMI) is expected to present unique challenges and opportunities. The ability to effectively translate this huge amount of data from raw information into valuable, actionable insight can lead to superior customer engagement, new product offerings, increased revenue, and operational efficiencies for utilities that do so. In this scenario, where the computer capabilities will become much more demanding, the technical evolution to a cloud architecture could be a cornerstone to a new critical infrastructure focused on scalability and able to processing, in a real-time fashion, large amounts of data.

As previously mentioned, the deployment of Smart Meters in a Smart Grid is not only large but also costly, requiring high up-front investment in hardware. On the other hand, one of the major arguments for cloud computing is that outsourcing processing and storage can reduce hardware costs once the cloud provider is able to offer the same resources at lower cost due to economies of scale.

Through this chapter, we will explore the concept of cloud computing by presenting their characteristics and models with the main goal of defining a new architecture for the Smart Grid.

4.1 What is Cloud Computing

Cloud computing is an emergent computing technology enhancing collaboration, agility and viability and providing, at the same time, the potential for cost reduction through optimized and efficient computing. More specifically, cloud computing separates applications and information providing an on-demand model with the ability to scale up, down, or out automatically as workload requirements change. Enabling network access to a shared pool of configurable computing resources such as networks, servers, storage, applications
and services in a scalable environment provides an opportunity to significantly reduce costs through optimization and increased operating and economic efficiency. Furthermore, cloud computing services are provided over an internet network connection, making it broadly available and accessed through standard mechanisms and client platforms. Another characteristic of cloud computing relies on the capability to provide computing resources designed to serve multiple users, supported on different physical and virtual resources dynamically assigned according to the consumer demand. Those resource pooling capabilities, based and constructed over business demands, could provide specific service levels to meet particular needs.

4.2 Cloud Computing Characteristics

Mistakenly, cloud computing is sometimes considered as a service that provides universal access to data and applications from the internet[16], but in reality it is much more than that. In October 2009, the National Institute of Standards and Technology (NIST)[17] published a definition of cloud computing, based on five essential characteristics, and detached the concept of cloud computing from the previous simplistic definition. These characteristics are presented below in more detail.

4.2.1 Scale and Elasticity

From a service provider’s perspective it is impossible to anticipate the usage volumes or demands for services or how the services will be used by customers. However, a service needs to be available all the time, even if it is used three times a year during peak selling seasons or if the service requests drastically increase in a short time. The ability to dynamically allocate the needed resources to meet the required quality of service is called elasticity and enables the management of the service according to the number of requests. High-availability (HA) requirements, typically identified in the design phases, are architected with failure in mind and designed in order to ensure that if any element fails there is another that can, almost immediately, take its place. The HA functionalities are those usually implemented either at hardware or software level, and used as fail-over mechanisms to enforce redundancy. At the application level, the redundancy of elements can be architected through a primary node (denominated as server) with a secondary being designed as the backup, which remains idle in standby mode. This architecture assumes HA through a replication process that ensures the same session, obtained by synchronization mechanisms, between the active and the standby elements. This mechanism, notwithstanding the HA, has a flip side in the sense that its scalability is limited and extremely costly. A second solution, already used but boosted by the cloud computing, foresees an active-active server solution supported by a load balancer component. This solution is architected not with failure in mind but with scale in mind, enabling elasticity (scale out,
scale in) and based on the ability of rapid delivery of required resources. In addition, new
instances can be added to the service, as the demand increases, to ensure that performance
and availability remain adjusted to the current needs.

### 4.2.2 On-Demand and Self-Service Provisioning

One of the greatest benefits of cloud computing is that consumers are able to procure
cloud services in an automatic faction and only when needed. On-demand and Self-
Service provisioning in addition to elasticity is able to dynamically provide an upgrade
on a service in terms of computing hardware, software, services, or process resources.
This characteristic is often referred as pay-as-you-grow subscription method. On-demand
provisioning capabilities of cloud services eliminate many of the time delays inherent in
the typical data center provisioning process, mainly because it is possible to assess, for all
requests, the availability of existing resources versus the need to purchase new hardware.

### 4.2.3 Broad Network Access

The broad network access is also a cloud computing characteristic once it promotes the
use of diverse client platform, such as mobile phones, tables, laptops and workstations, to
access a service wherever and whenever it is needed.

### 4.2.4 Measured Service

The measured service represents the capability to monitor, control and report both the
provider and consumer of the utilized service. Through this service it is possible to control
and optimize resources adjusting it to current needs.

### 4.2.5 Resource Pooling

In a cloud computing environment the provider’s computing resources are pooled to serve,
in a multi-tenant model\(^1\), multiple consumers. Those resources are then dynamically
assigned and reassigned according to consumer demand. In this scenario, the consumer
may be able to specify location, in a higher level of abstraction, of the provided resources
allowing to address across border problems related to legal issues. This high level of
abstraction can represent a specific country, a state or even a specific datacenter. The
resource pooling is transversal to all other characteristics and represents the cost efficiency
of the solution.

\(^{1}\)Represents the ability to use the same software and interfaces to configure resources and isolate
customer-specific traffic and data
4.3 Service Models

According to the NIST definition[17], cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. There are three services models of cloud computing in order to address different customer’s needs. Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). Figure 4.1 illustrates and summarizes the characteristics of each of these models. A more detailed description follows.

Figure 4.1: Cloud Computing Service Models.

4.3.1 Infrastructure as a Service (IaaS)

Infrastructure as a Service (IaaS) is the delivery of a computing foundation (servers, networking technology, storage, and data center space) as a service. It also includes the delivery of operating systems and virtualization technology to manage the resources. This service is a contract between two parts, therefore the service can be negotiated to ensure that peaks are handled.

4.3.2 Platform as a Service (PaaS)

The provider is able to deliver more than infrastructure with Platform as a Service (PaaS). In this case, it delivers an integrated solution based on a solution stack for both software development and runtime environment. Platform as a Service can be considered an evolution of Web hosting as, for example, complete software stacks for developing Web sites. Platform as a Service is inherently multi-tenant and naturally supports the whole set of Web services standards and it is usually delivered with dynamic scaling. Platform as a Service typically addresses the need to scale as well as the need to separate concerns of access and data security for its customers.
4.3.3 Software as a Service (SaaS)

Software as a service, also referred as “on-demand software”, is a cloud service model based on the software delivery model in which software and associate data are hosted on a cloud in a centralized maner. The Software as a Service business has its roots in an early kind of hosting operation carried out by Application Service Providers (ASPs) and on-demand computing software delivery model. Benefits of the SaaS model includes easy administration and collaboration as well as compatibility since it will be accessed by users with standard software, i.e., all users use the same software version.

4.3.4 Deployment Models

There are at least three types of cloud computing deployment scenarios. Figure 4.2 illustrates the fundamental models.

![Figure 4.2: Cloud Computing Deployment Models.](image)

The public cloud is the most commonly referenced regarding the topic of cloud computing, where the infrastructure and applications are owned, off-premises and external, by the organization selling cloud services. Private cloud, on the other hand, is internal and supplied on-premises. This service is usually supplied behind the firewall, and maintained within the premises of the host organization. Figure 4.2 depicts the classification, in two dimensions, of the various deployment models. However, since many traditional vendors and users are not quite ready to jump into public cloud computing or are restricted from doing so, the cloud service tiers are replicated within a private cloud environment. It will rely on a delicate balance of public and private models resulting in a hybrid cloud solution. Hybrid cloud is a composition of, at least, two clouds (one private and other public) that remain unique entities but are bound together, offering the benefits of both models.
4.4 The Computational needs of the Smart Grid

As mentioned in Section 3, the Smart Grid transforms the way power is distributed and used, adding intelligence throughout the grid to dramatically reduce outages and faults, improving responsiveness, handling current and future demand, increasing efficiency and management costs. The Smart Grid uses sensor meters, digital controls and analytic tools to automate and monitor the flow and delivery of energy to consumers, enabling a two-way flow of electricity and information among the power plant, the appliance and the points in between. Through Smart Grids it is also possible to incorporate new sustainable energies such wind and solar generation, and interact locally with distributed power sources, or plug-in electrical vehicles.

One of the things we are starting to see is a kind of shift in investment trends, moving from the supply side to increasingly focusing on the demand side. That means, for example, that in the future, instead of getting a bill that gives the consumer just a total aggregate amount they consumed over a month or so, the consumer will know where that energy was consumed, per specific equipment, like the refrigerator, or the heating and cooling systems, and will even receive information about whether there is an efficient alternative that could help to reduce its bill. To support this new paradigm, Smart Grids will boost widespread use of intelligent sensors on the grid improving both energy efficiency and demand response. It is not surprising, then, that the power grid is under immense pressure today from inability to scale to current demands, and is growing increasingly fragile, even if the repercussions of power outages grow more serious. Upgrading to a ”smarter grid” will require substantial computing power for controlling and management, to which cloud computing may provide interesting benefits in terms of costs.

Smart Grids also imply a change in the way the data is captured. We are facing a shift from a single regional power system to a more decentralized model, enabling distributed generation and facilitating data sharing and visibility to neighboring power grids. Decentralized Smart Grid is a subject on which there are several researches, and among them we highlight the work developed by Tomasz Kaminski[18] , a research analyst specialized in renewable energy for Frost & Sullivan, who recently focused on distributed generation related technologies. He argues that the Smart Grid is the enabler for the addition and control of distributed generation and this proliferation will drive the market for grid-scale energy storage. According to this researcher, the decentralization of the Smart Grid is already in place and will be faster adoption rates all over the world, mainly to be complied with the European Union climate and energy package, usually called by Kyoto protocol or by the “20-20-20” plan (20 percent decrease in greenhouse gases, 20 percent increase in energy efficiency and a 20 percent increase in renewable energy use by the year 2020). This trend in decentralization is also present in the analysis carried out in January 2013 by
Bloomberg New Energy Finance (BNEF)[19] showing that the investment in Smart Grid technology reached US$ 14 billion in 2012, 7% more comparing to 2011.

Viewed at a global scale, the Smart Grids are also changing consumers’ habits and behaviours. The present consumer is becoming more sophisticated about pricing, shifting consumption from peak periods to off-peak periods and controlling his consumption, likely in real-time. This new paradigm will also shift a substantial new load into the grid while the operation of the grid itself will continue to grow in complexity. Actually, The International Energy Agency (IEA) estimates a European investment of 1.5 trillion euros over 2007-2013[25] to renew the electrical system from generation to transition and distribution. This investment includes the Smart Grid implementation and for maintaining and expanding the current electricity system. In addition, a recent report by Pike Research [35] forecast that the accumulative European investment for Smart Grid technologies will reach 56.5 billion euros during the period from 2010 and 2020. The same report appraisals 240 million of Smart Meter deployed in the European Union by 2020.

All this momentum allows, as a side effect, the entire infrastructure modernization translated into a high technology upgrade. This is a key factor to address new challenges not only at data collection level but also at processing and dissemination level. Smart Grid stakeholders leverage the introduction of cloud computing in order to indexing and searching data, managing data that might contain petabytes of information, coordinating actions and implementing cloud scale databases.

As a matter of fact, cloud computing is taking over all computing and storage solutions, replacing traditional information technology operations and business models all over the world. Economies of scale enable cloud providers to reduce service costs by operating massive datacenters, comprising tens or even hundreds of thousands servers.

Recently, researchers have studied how to use Cloud Computing to manage, or at least, to help the Smart Grid management procedures. Simmhan et al.[26] focused their work on the benefit of using a Cloud platform to optimize the Smart Grid demand response. Rusitschka et al.[27] presented a model for the Smart Grid data management based on the Cloud Computing architecture. This model takes advantage of distributed data management for real-time data gathering, parallel processing for real-time information retrieval, and ubiquitous access. Kim et al.[28] proposed a Cloud-based demand response architecture for fast response time in large scale deployments. Finally, György Dán et al.[29] study the cases where the cloud may be useful for Power Systems.
4.5 Present constrains of the Smart Grid reference architecture

SCADA systems are distributed geographically and usually controlled from one location. In this architecture there are distributed components, endpoints, responsible for data collecting and physical operations execution. As a matter of fact, endpoints establish the connection between the application, the human operation and the hardware execution. On the other hand, computational power, data storage and network operation are provisioned according to a centralized architecture. This mix of distributed and centralized architectures is fundamental to ensure a timely, accurate and global overview of the system. As already mentioned previously, the evolution of the Industrial Control System (ICS) and its integration with the metering components will cause an exponential growth in terms of equipment, computational power requirements and data. Figure 4.3 depicts the major components of the Smart Grid architecture.

![Figure 4.3: Reference architecture of the Smart Grid.](image)

The central systems, residing in the data center, contain, as seen previously in chapter 3, the control and operation system as well as the energy metering management system. Besides the large storage capacity and computing requirements, this level provides connection to all IT systems, responsible for handling and management of customer’s consumption and/or production. The central system is also responsible for the connection with the outstanding components that compose the Smart Grid. Here, beyond Smart
Meters and concentrators, there is still older equipment that guarantees large part of the control and operation of the electrical grid and as such, has to be integrated. For this, there are several connections, established through serial interfaces, which ensure the integration of all legacy equipment. In this architecture, all communication between the central systems and smart metering is accomplished through the concentrator. Concentrators and Smart Meters have modules for processing and storage, allowing the treatment and provision of information to the end user.

Adapting this architecture to the growing needs of Smart Grids points out a model with more distributed computational power where each endpoint (concentrators and Smart Meters) would assume an even more important role in the overall solution. Following this client-server architecture, would required a network equipment with more resources installed locally and could result in a higher cost of ownership, introduces complexity and security risks. As seen in Chapter 3, the Smart Meters pose a high risk to the organization, either financially or in terms of reputation in case of loss of confidentiality. The increase in computational power and storage, if performed by these equipments, will increase the risk identified anteriorly. In addition it is important to mention that a most demanding equipment represent necessarily higher costs which, considering the final size of a Smart Grid, represents a fairly high amount of money.

4.6 A new architecture for the Smart Grid

A completely different approach carried out by this work and depicted in the figure 4.4, is also supported on the same client-server architecture, however here we come up with a solution that migrates most of the resources, including storage and processing power, to the central systems. This new model, which we have called SGCA (Smart Grid Cloud Architecture) reduces the operations that are performed on the endpoints preventing that clients end-up getting muddled with too many lines of code, configurations, updates and files.

4.6.1 Components of the Smart Grid Cloud Architecture (SGCA)

The SGCA’s architecture envisages the use of two private cloud with different roles. Its main functionalities and responsibilities are described in the next paragraphs.

Computational Area and Operational Area

The Computational Area (CA), presented in the figure 4.4, has a complex role in this new architecture, being the bridge between the Operational Area (OA) and the endpoints, and having the responsibility to ensure the bidirectional communication between these two
entities. Besides, the CA is also responsible for processing all information previously executed by both concentrators and Smart Meters. By doing that, we are able to reduce the endpoint’s demands in computational and storage requirements. The existence of a second cloud, defined as the Operational Area, ensures a complete segregation of duties and, simultaneously, provides all the necessary connections to the IT and legacy components. As a matter of fact, the Operation Area gives the possibility to explore the cloud computing advantages in the SCADA system and, by taking advantage of this new architecture, reduce the impact and technical limitations caused by the inherited components.

This vision for the Smart Grid architecture evolution is much more aligned with the efforts performed by governments, research institutes, and industry leaders to undertake cloud computing to solve their ever increasing computing and storage problems. Decentralizing computational power and data storage required by Smart Meters represents financial benefits and security improvements [30][31]. On the one hand, transforming and limiting those devices only to their basic functions, which are mostly related with physical interactions, significantly reduce the Total Cost of Ownership (TCO). In addition, removing all critical information management from the Smart Meters confers them an innate immunity to attacks with possible sensitive data disclosure.
The role of the concentrator in the SGCA architecture

In the SGCA, the concentrator’s role has been greatly reduced, getting free of all issues related with the metering functionalities. In the reference architecture, figure 4.3, the concentrator has a dual job. On the one hand, it was responsible for gathering the Smart Meter data, process them and make the results available to the central systems. In addition, the concentrator was and still, the responsibility for the SCACA functionalities. The migration of the metering functionalities of the concentrator to the CA reduces their computational requirements. Nevertheless the concentrator, sill connected through PLC (Power Line Communication) to the Smart Meters and, with the present limitation in using PLC in the cloud, it will work as a bridge between the Smart Meters and the CA. The overcome of this limitation represents, not only a direct connection between the Smart Meter and the CA but also dependability benefits, at reliability and availability level, once a single point of failure was eliminated. Today, a possible alternative for this dependency could be using GPRS (General Packet Radio Service) for the communication between the Smart Meter and the CA, although the costs associated tho this migration are unbearable at the present moment. For this reason, the SGCA is designed this the concentrator in the network and working as a communication hub between the Smart Meter and the CA.

The role of the Smart Meter in the SGCA architecture

A similar approach was taken concerning the relocation of Smart Meter functionalities to the cloud. However, removing all measurement components it is not feasible in the sense that this equipment not only collects metering information but also has physical connections that have to remain on-site. With this limitation in mind, we developed a study, and presented in the following chapter, focused on Smart Meters and its migration to a cloud. To do that, we break down the Smart Meter into their main functionalities and gauged them according to the following criteria: physical connection, real-time requirement and dependency with other functionalities.
Chapter 5

Adapting the Smart Meter to private clouds

The advantages brought by the SGCA architecture are founded on the cloud computing benefits presented in the session 4 and with which it is possible to ensure, at once, scalability and computational power, safeguarding simultaneously the integration of legacy components and IT systems. However, as shown in the previous session, the migration of Smart Meters to the cloud requires a deeper and careful analysis.

5.1 Smart Meter Functionalities

In this chapter we present the main functionalities implemented for this equipment in EDP and evaluate, for each of these functionalities, its dependence on physical connections and their reliance on real-time. The Smart Meters measure electricity consumption in households and communicate their readings at regular intervals to back-end system. To do that the Smart Meter uses the functionalities presented in the Figure 5.1 and described

<table>
<thead>
<tr>
<th>Public Lighting</th>
<th>Storage of Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rates</td>
<td>Clock</td>
</tr>
<tr>
<td>Communication</td>
<td>Power Measurement</td>
</tr>
<tr>
<td>Parameterization and Remote Actuation</td>
<td>Anti-fraud Mechanisms</td>
</tr>
<tr>
<td></td>
<td>Firmware Update</td>
</tr>
<tr>
<td></td>
<td>Quality of Service</td>
</tr>
<tr>
<td></td>
<td>Interface with the Consumer</td>
</tr>
<tr>
<td></td>
<td>Technical Management</td>
</tr>
<tr>
<td></td>
<td>Energy Efficiency</td>
</tr>
</tbody>
</table>

Figure 5.1: Smart Meter functionalities.
herein:

**Power Measurement:** Measurement of active and reactive power in both directions. Measurement of maximum power during a configurable integration period from 1 to 60 minutes.

**Storage of Information:** Figures for consumptions and productions occurring during configurable integration periods of 15, 30 or 60 minutes of the active energy and reactive energy, consumed and produced. The system shall store data regarding the quality of service during a period of at least one year.

**Rates:** The Smart Meter needs to consider at least 5 different types of days (summer and winter weekdays, summer and winter Saturdays, Sundays or holidays) and, at least, two seasons. It is possible to remotely program cycles (daily, weekly, . . .), standard time periods (winter, summer), holidays, etc.

**Communications:** Communications may be divided into three groups:

1. **LAN/WAN communication** - The system enabling communication between the Smart Meter and the concentrator should make it possible to use various types of communication technologies, by transparently performing communication migration via a physical change (hardware) in the communication module;

2. **Home Area Network (HAN) communication between devices** - The Smart Meter is designed to support interconnections with other devices. This interconnections could be a mere acquisition of analogue or digital signals involving only one I/O module for interaction with the outside or something more complex, involving for example, Ethernet or ZigBee communications [32];

3. **Internal communication between modules** - The various modules of the Smart Meter should communicate among themselves so as to ensure information exchange and sharing.

**Parametrization and remote actuation:** Parametrization and remote actuation may be divided into four groups:

1. **Change of rate option** - The system should allow for remote change of contractualized rate option;

2. **Regulation of power control** - The system should enable the contracted power value to be remotely changed;
3. Possibility of outage/reactivation of supply - The system should make it possible to remotely and totally switch off/reactivate a customer, for reasons of contract non-compliance, deactivating/reactivating contracts, technical faults at the customer’s facility (fraud detection), among others;

4. Remote date/time synchronization - The Smart Meter should be synchronized by the concentrator.

**Interface with the consumer:** Interface with the consumer may be divided into three groups:

1. Access to the instantaneous load / power value - The system should make sure the customer can see the instantaneous power value, while showing the percentage of the integration period;

2. Presentation of accumulated values for comparing with billing values - The system should provide the customer with access to billed consumption and a history of measurements;

3. Notice of maximum power taken - The system should show the value of maximum power attained within the current rate period, as well as the value history when selected.

**Quality of service:** Quality of service may be divided into three groups:

1. Record of the number of long supply outages - The system should record the number of service outages lasting more than a given period of time, remotely configurable by the grid operator (for example, more than 3 minutes), depending on the Quality-of-Service Regulation;

2. Record of the duration of long outages - The system should record the duration of the outages referred to under the previous requisite;

3. Record of the accumulated time when the voltage level exceeds the limits set forth by the Quality-of-Service Regulation.

**Anti-fraud mechanisms:** Change of the Smart Meter - The system should comprise control and alarm mechanisms for changes to the system, so as to dissuade users from eventually carrying out fraudulent acts (such as, alarm when removing the meter module cover, etc.).

**Firmware Update:** Smart Meter remote firmware update - Should be a log associated with firmware updates. Every change carried out on the equipment should be auditable.

**Technical Management:** Technical Management may be divided into two groups:
1. The system should be prepared to proceed with the power supply outage, in order to meet grid management requirements (processing branch congestions, restoring service, among others);

2. The system needs to be prepared to momentarily limit the maximum power value in order to meet grid management requirements (processing branch congestions, among others). This functionality may be implemented in the form of a reduction corresponding to percentage value of the contracted power and, as a supplement, via a fixed value.

**Energy Efficiency:** Promoting energy efficiency. There needs to be an application to be used by the consumer, which will make it possible to acquire and process consumption data, including the ability to view the load diagram, produce analyses of change to consumer data, convert kWh to CO2 figures based on reference terms, among others.

**Clock:** The system should include a real-time clock (RTC) for supporting rate-related activity, among others.

**Control of Public Lighting:** The system should provide the control and management of public lighting providing information in real-time and simultaneously allowing control remotely.

### 5.2 Criteria Description

Decoupling the Smart Meter in components, presented in the previous session, allows us to identify the role of each functionality. Now, during this session, we will analyse the impact of migrate to the cloud each of the features previously identified, according to the following criteria: physical connection, real-time requirements and dependency with other functionality.

#### 5.2.1 Physical Connection

In the Smart Grid architecture, the consumers are physically connected to the grid by having a Smart Meter installed in their households. This physical connection, as seen in the previous chapter, limits the migration to the cloud of the Smart Meter. In this session, we will examine for each functionality of the Smart Meter, which is actually its physical dependence and identify those that, even part of the Smart Meter, do not have physical limitations.

Table 5.1 depicts the physical dependencies of each component. In this table it is possible
to identify a clear separation of functions that have dependencies or physical connections. From the results presented in the table, those who can raise some doubts are the clock and the control of public lighting. The physical dependency of the clock is related with the necessary precision with which events are timestamped. On the other hand, the control of public lighting is directly related to a SCADA functionality, which are only present in some Smart Meters, that have the role of controlling and monitoring the public lighting service through sensors and actuators.

<table>
<thead>
<tr>
<th>Functionality</th>
<th>Physical connection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power Measurement</td>
<td>x</td>
</tr>
<tr>
<td>Storage of Information</td>
<td></td>
</tr>
<tr>
<td>Rates</td>
<td></td>
</tr>
<tr>
<td>Communication</td>
<td>x</td>
</tr>
<tr>
<td>Parametrization and remote actuation</td>
<td></td>
</tr>
<tr>
<td>Interface with the consumer</td>
<td></td>
</tr>
<tr>
<td>Quality of service</td>
<td></td>
</tr>
<tr>
<td>Anti-fraud mechanisms</td>
<td>x</td>
</tr>
<tr>
<td>Firmware update</td>
<td></td>
</tr>
<tr>
<td>Technical management</td>
<td></td>
</tr>
<tr>
<td>Energy efficiency</td>
<td></td>
</tr>
<tr>
<td>Clock</td>
<td>x</td>
</tr>
<tr>
<td>Control of public lighting</td>
<td>x</td>
</tr>
</tbody>
</table>

Table 5.1: Smart meter, scalability and physical dependency.

### 5.2.2 Real-time Requirements

Table 5.2 is a complement to the results obtained with previous analysis. Here the aim is to identify which functionalities have also real-time requirements. The result of this analysis, in conjunction with the previous one, identifies the functionalities that have dependencies either on physical or real-time, and therefore must remain on-site. Figure 5.2 identify, in grey, all functionalities with physical or real-time dependency.

### 5.2.3 Dependency Between Functionalities

In the previous session we have identified all functionalities with physical dependency or with real-time requirements. All these functionalities, as we have seen, are not elected to a cloud migration making them fundamental on-site functionalities. For the remaining functionalities (non-fundamental on-site functionalities) is now mandatory to assess the dependence that exist between these functionalities and those previously identified. Table 5.3 depicts the dependency between non-fundamental and fundamental on-site functionalities. After this analysis we can draw some conclusions:
Chapter 5. Adapting the Smart Meter to private clouds

<table>
<thead>
<tr>
<th>Functionality</th>
<th>Real Time Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power Measurement</td>
<td>x</td>
</tr>
<tr>
<td>Storage of Information</td>
<td></td>
</tr>
<tr>
<td>Rates</td>
<td></td>
</tr>
<tr>
<td>Communication</td>
<td>x</td>
</tr>
<tr>
<td>Parametrization and remote actuation</td>
<td></td>
</tr>
<tr>
<td>Interface with the consumer</td>
<td></td>
</tr>
<tr>
<td>Quality of service</td>
<td></td>
</tr>
<tr>
<td>Anti-fraud mechanisms</td>
<td></td>
</tr>
<tr>
<td>Firmware update</td>
<td></td>
</tr>
<tr>
<td>Technical management</td>
<td></td>
</tr>
<tr>
<td>Energy efficiency</td>
<td></td>
</tr>
<tr>
<td>Clock</td>
<td></td>
</tr>
<tr>
<td>Control of public lighting</td>
<td>x</td>
</tr>
</tbody>
</table>

Table 5.2: Smart meter, real-time dependency.

Figure 5.2: Smart Meter functionalities that have physical or real-time dependencies.
Table 5.3: Dependency between non-fundamental and fundamental on-site functionalities.

1. All non-fundamental functionalities are dependent on the power measurement functionality;

2. Storage of information, parameterization and remote actuation, firmware update and technical management are functionalities that are already rely on external communications to perform their tasks;

3. Anti-fraud mechanisms are a functionality that only depends on storage information;

4. Clock is well used in the system and only the interface with the consumer do not use them;

5. Public lighting depends on the storage information and the energy efficiency functionalities.

Through the analysis of dependencies, performed in Table 5.3, it was possible to identify a set of functionalities that should remain on-site. However there are functionalities, even not elected to remain in the equipment, that deserve further analysis since they have significant dependency with the fundamental on-site functionalities. For that we have selected all non-fundamental functionalities that have more than two dependencies with the fundamental on-site functionalities and, for those, we performed an additional analysis. This second analysis evaluates the dependencies of a specific non-fundamental functionality with the remaining non-fundamental functionalities. By doing this, we can have
a much more concrete idea of the best place to put each of these functionalities. The functionalities that we have selected are: Storage of Information, Parametrization and remote actualization, Quality of service, Firmware update and Energy efficiency. Through

<table>
<thead>
<tr>
<th>Functionality</th>
<th>Storage of Information</th>
<th>Parametrization of information</th>
<th>Quality of Service</th>
<th>Firmware update</th>
<th>Technical management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage of Information</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rates</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Parametrization of Information</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interface consumer</td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Quality service</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Firmware update</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Technical management</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Energy efficiency</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 5.4: Dependency between Storage of Information and the remaining non-fundamental functionalities.

the analysis of Table 5.4 we are able to ascertain that the number of dependencies that Storage of Information has in relation to the remaining non-fundamental functionalities is higher than their dependencies that it has with the fundamental on-site functionalities. As a result, this functionality should migrate to the cloud. The same analysis was performed for the remaining four functionalities and, through the dependency comparison, it was possible to infer that all four functionalities must remain on-site. Figure 5.2 uses the same model previously presented in figure 5.3 highlighting, in grey, all the features of the Smart Meter that must remain locally in the equipment.

**Final Remarks**

In the definition of the new architecture for the Smart Grids (SGCA), performed in the session 4, we have identified the Smart Meter as complex and physical dependent equipment. For this reason, we devote this section to the study of each of the Smart Meter functionalities, evaluating for each, the advantages and disadvantages of migrate each of them to the cloud. Complementarily to the previous sessions, the next session will evaluate the present cloud limitations in hosting such a critical infrastructure.
Figure 5.3: Smart Meter functionalities, in grey, that must be hosted on the meter.
Chapter 6

Present limitations for deploying the SGCA architecture

In the session 4 we have defined an architecture for Smart Grids based on a cloud computing model. Then, in the session 5 we analyzed all the functionalities, from the Smart Meter point of view, that could migrate to the cloud. Now with all the SGCA architecture defined, it is important to assess the present limitations on the cloud computing for deploying such a critical infrastructure.

6.1 Cloud Computing Weaknesses

Cloud computing brings together a number of computational system advantages at software, hardware, and system design and architecture levels. To use them, robust hardware and networks communication are needed. This section presents both technical and legal constraints to the use of cloud computing.

6.1.1 Virtualization

Virtualization[36] is the most common application being used for Hardware’s virtualization enabling the creation of a virtual machine (VM) that emulates a physical computer by creating different Operation System (OS) environment that is logically separated from the hosting system. A single physical system/hardware can be used to create several VMs that can run different OSs independently and at the same time. Virtualization, in addition to server’s virtualization, may also virtualize networks, applications and storage.

Network virtualization allows the complete reproduction of a physical network in software offering operational benefits and independence of hardware. Through the network virtualization is possible to ensure rapid provisioning, nondisruptive deployment, automated maintenance and support for both legacy and new applications.
Application and storage virtualization encapsulates the application software from the underlying operating system on which it is executed. Application virtualization can provide high availability, disaster recovery and speed and agility as well as cloud-readiness. However not all software can be virtualized or can require heavy OS integration.

Despite the great benefits of virtualization it also offers certain security disadvantages. There are data latency concerns in a multi-tenant environment and additional risk considering the fact that all tenants will share the security level of the least security tenant. In addition, virtual machines communicate over the virtual machine communication interface (VMCI)\(^1\), rather than a network. This drawback, present in all virtual machines who are sharing the same hardware, result in the impossibility of implement standard network security controls. Solutions like virtual firewalls [38], design to address this issue, are now available in the market but its applicability and effectiveness still not a consensus among the community[39].

### 6.1.2 Weak Consistency

Usually distributed systems only work in environments with specific and simple protocols such as Nasper or Verisign. (both based on DNS and WWW), using large scale and more complex distributed systems might represent some architectural issues[40]. Some of these issues are related to the guarantee offered by a system, to store the state consistent, even when it is explicitly changed by an external factor which can be triggered, e.g., by simultaneous processes of reading and writing. On the other hand, a distributed system need to be always on and the service should operate fully ensuring, at same time, scalability capacities.

### 6.1.3 Legal Concerns and Constraints

Cloud computing creates new dynamics in the relationship between an organization, its information and the cloud provider, creating new challenges in understanding how laws apply to a wide variety of information management scenarios[41]. Cloud computing creates considerable legal issues that must be consider, specifically those around any data that might be collected, stored and processed. There will likely be state, national or international laws that must be considered to ensure a broadly legal compliance. Failure to adequately protect the organization’s data can have a number of consequences, including the potential for fines by one or more government or industry regulatory bodies.

---

\(^1\) is an infrastructure that provides fast and efficient communication between a virtual machine and the host operating system and between two or more virtual machines on the same host[37].
6.1.4 Security and privacy

Security is the biggest concern when it comes to cloud computing. By leveraging a remote cloud-based infrastructure, a company essentially gives away private data and information, things that might be sensitive and confidential. The preceding paragraph leads us to short and complex challenges in terms of data loss. Usually, the measures implemented to mitigate one can exacerbate the other. A common sense would tell us to encrypt data in order to reduce the impact of a security breach, but if you lose the encryption key, you will lose the data. To prevent this situation, you could opt to keep offline backups to prevent data loss, but doing that increases the exposure to data breaches. Through this simple example, it is possible to infer the complexity of the security in the cloud environment and the difficulty in selecting the best solution to fulfill all security needs. In addition, Denial of service attacks represents also a huge concern in the age of cloud computing when organizations are dependent on the availability of one or more services.

6.1.5 Dependency and vendor lock-in

One of the major problems of cloud computing, when using the public cloud model, is the implicit dependency on the provider. This is called by the industry as “vendor lock-in” since it is difficult, and sometimes almost impossible, to migrate from a provider once you have rolled with him. The decision to switch to some other provider, when made, can be really painful and cumbersome to transfer huge data from the old provider to the new one.

6.2 Network constraints

At first glance, entirely based on intuition, leads us to consider that the proposed change to the new architecture of Smart Grids represents a big flop. In fact, our solution removes from the data collector, the Smart Meter in our case, considerable effort on processing and storage. This change, without any room for doubt, has significant impacts on the performance of the Smart Grid since its entire functionality lies on the communications.

A more pragmatic approach about this subject allows us to find some advantages in this new architecture bringing to light what appeared to be doomed to failure. Indeed, the fact that almost all computational power are performed in the cloud implying that the Smart Meter only has to send the raw data reducing, by that, the packets size and thus the transition time. All the arguments presented previously, while theoretical, have a negligible value. For this reason, we developed a couple of tests in order to measure the performance between the Smart Meters and the concentrators. These tests were performed with equip-
ment already installed in the EDP Smart Grid and part of the architecture presented in the chapter 4. This way, all results were obtained directly from the field.

6.2.1 Communication field test

The tests were conducted on the infrastructure installed at the EDP, using five Smart Meters from Landis manufacturer and a concentrator from the Current manufacturer. All the Smart Meters have the same firmware version and the communication between the concentrator and the Smart Meters is performed in a PRIME\textsuperscript{2} version of PLC (Power Line Communication). Through these tests we would like to evaluate the communication impact involved in the migrating of several core components of the Smart Meter to the cloud. For that, we had selected two types of scenarios:

1. A first one supports the actual Smart Grid architecture where all the computational power is local, i.e., in the Smart Meter. This scenario is presented in Figure 6.1;

   ![Figure 6.1: Present Smart Grid architecture.](image1)

2. A second scenario, Figure 6.2, this time simulating the existence of a cloud, considers that the Smart Meter sends the data without any previous treatment.

   ![Figure 6.2: Smart Grid Cloud architecture.](image2)

\textsuperscript{2}PRIME (PoweRline Intelligent Metering Evolution) is a worldwide PLC standard for advanced metering and grid control applications
At this point it is important to note that the communication between the concentrator and the Smart Meter is, most of the solutions implemented in Europe, based on a master-slave communication where the Smart Meter waits to be hierarchically stimulated to send data[42]. The tests were performed according to the following use cases:

- **Gathering load diagrams:** represents the power consumption diagrams on each home. The load diagram is computed locally by the Smart Meter and collected by the concentrator one time a day. This use case fits in the first scenario and explores the need of computational power on the Smart Meter;

- **Gathering daily events:** represents all the events of the current day. Daily events are collected by the concentrator in a raw format and represent the transmission of all the information available on the Smart Meter’s side. This use case fits in the second scenario;

- **Gathering daily absolute:** represents the final value of the day. The daily absolute represents a single value, computed by the Smart Meter, and collected by the concentrator. This use case fits in the second scenario;

- **Gathering daily billing:** represents all the billing data. The daily billing is similar to the daily absolute, but related with the billing. This use case fits in the second scenario.

### 6.2.2 Results

By performing those tests it was possible to assess the impact caused by the transmission of a large amount of data, load diagrams, versus the transmission of raw data whenever there is asked by the concentrator. The results of this test present a significant success rate

<table>
<thead>
<tr>
<th>Service</th>
<th>Success</th>
<th>Samples</th>
<th>Average</th>
<th>Deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gathering load diagrams</td>
<td>96%</td>
<td>50</td>
<td>00:43</td>
<td>00:12</td>
</tr>
<tr>
<td>Gathering daily events</td>
<td>98%</td>
<td>50</td>
<td>00:26</td>
<td>00:16</td>
</tr>
<tr>
<td>Gathering daily absolute</td>
<td>100%</td>
<td>50</td>
<td>00:05</td>
<td>00:02</td>
</tr>
<tr>
<td>Gathering daily billing</td>
<td>100%</td>
<td>45</td>
<td>00:06</td>
<td>00:16</td>
</tr>
</tbody>
</table>

Table 6.1: Gathering information, test results.

for the last two cases, when data is sent without any treatment. The reason for the decrease in the success rate in the gathering load diagrams and in the gathering daily events lies on the PLC limitation under wider in time.

### 6.2.3 Final Remarks

A conclusion of those tests, supported by the table 6.1 shows us that there is a significant advantage in transmitting data, by request without any treatment. In addition, these results
support the studies and analysis performed so far, giving evidence of the benefit obtained by using the cloud to accommodate non-fundamental functionalities of Smart Meters.
Chapter 7

SGCA Security Evaluation

In the session 4 we presented the Smart Grid Cloud Architecture (SGCA) in order to address the scalability and computational power requirements of the Smart Grid and safeguarding, at the same time, the integration of legacy components and IT systems. In this session we will evaluate, using the same methodology presented in the session 3, the possible advantages that we can obtain in terms of security.

7.1 Operational impact regarding the SGCA

To perform this analysis we will use the results obtained in section 3, and for each of the three fundamental attributes of security, we will evaluate its performance with this new architecture.

<table>
<thead>
<tr>
<th>Service</th>
<th>Availability in Smart Grids</th>
<th>Availability in SGCA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Grid Control and Operation</td>
<td>Very High</td>
<td>Very High</td>
</tr>
<tr>
<td>Energy Metering Management</td>
<td>Very High</td>
<td>Very High</td>
</tr>
<tr>
<td>Information services</td>
<td>Very High</td>
<td>Very High</td>
</tr>
<tr>
<td>WAN communication</td>
<td>High</td>
<td>Moderate</td>
</tr>
<tr>
<td>Primary substation operation</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Smart Meter’s Concentrator</td>
<td>High</td>
<td>Moderate</td>
</tr>
<tr>
<td>LAN communication</td>
<td>Moderate</td>
<td>Low</td>
</tr>
<tr>
<td>Smart meter</td>
<td>Moderate</td>
<td>Low</td>
</tr>
</tbody>
</table>

Table 7.1: Criticality of the Smart Grid Vs SGCA regarding Availability.

Table 7.1 presents the impact caused by the lack of Availability in Smart Grid, identified previously in the session 3, and compares the results with the same lack in a SGCA architecture. With this comparison it is possible to verify, highlight in bold, a significant reduction in the Smart Meter, LAN and WAN communication and Smart Meter’s Concentrator. The result was expected and reflected the migration of all metering functionalities from the distributed components, in this case, the concentrator and the Smart Meter. As a matter of fact, the impact of loss of Availability it inversely proportional to the depen-
dency of information.

It is important to mention that the concentrator in this new architecture works as a hub that collects information from the Smart Meters and send them to the central systems. The presence of this equipment in the SGCA, is mainly supported by the present impossibility of connect the Smart Meter to the central system directly through PLC (Power Line Communication). Although they no longer have the responsibility to process data from the Smart Meters and, as a result, the value assigned to the Smart Meter’s Concentrator have been decreased from high to moderate. This architectural change performed at the concentrator level, also has a positive impact in the WAN communication.

<table>
<thead>
<tr>
<th>Service</th>
<th>Integrity in Smart Grids</th>
<th>Integrity in SGCA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Grid Control and Operation</td>
<td>Very High</td>
<td>Very High</td>
</tr>
<tr>
<td>Energy Metering Management</td>
<td>Very High</td>
<td>Very High</td>
</tr>
<tr>
<td>Information services</td>
<td>Very High</td>
<td>Very High</td>
</tr>
<tr>
<td>WAN communication</td>
<td>Very High</td>
<td>High</td>
</tr>
<tr>
<td>Primary substation operation</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Smart Meter’s Concentrator</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>LAN communication</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Smart meter</td>
<td>High</td>
<td>High</td>
</tr>
</tbody>
</table>

Table 7.2: Criticality of the Smart Grid Vs SGCA regarding Integrity.

Regarding loss of Integrity and loss of Confidentiality, presented in Table 7.2 and Table 7.3 the conclusion are not so straightforward, at the first glance, the new architecture did not grind any advantage beyond those already referred to the loss of Availability. As a matter of fact, the impact remain the same because it is associated with the disclose, in the case of Confidentiality, or modification, in the case of Integrity, and not exactly with the place where the data is processed and saved. Nevertheless, the concentrator and the Smart Meter have a much lower role in the system without the need to process and archive data, in this circumstances, the amount of information possible to obtain is considerably lower.

<table>
<thead>
<tr>
<th>Service</th>
<th>Confidential. in Smart Grids</th>
<th>Confidential. in SGCA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Grid Control and Operation</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Energy Metering Management</td>
<td>Very High</td>
<td>Very High</td>
</tr>
<tr>
<td>Information services</td>
<td>Very High</td>
<td>Very High</td>
</tr>
<tr>
<td>WAN communication</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Primary substation operation</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Smart Meter’s Concentrator</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>LAN communication</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Smart meter</td>
<td>High</td>
<td>High</td>
</tr>
</tbody>
</table>

Table 7.3: Criticality of the Smart Grid Vs SGCA regarding Confidentiality.
7.2 Final Remarks

There are two important points to retain from these comparative assessment. On one hand, the SGCA was effective in reducing the impact caused by the loss of Availability and the results would be even better if it were possible to migrate to the cloud all the concentrator functionalities. This migration, when possible, will reduce a simple point of failure and eliminate the LAN communication which is, nowadays, responsible for the communication between the controller and the Smart Meter. On the other hand, this new architecture do not change significantly the risk associated to the loss of Integrity or Confidentiality. The inference about this topic, based first on the intuition and then validate by the results, lead us to implement additional security mechanisms on the Smart Meter and on the concentrator.
Chapter 8

Conclusion

The exponential growth of equipment and its information, generated in a distributed way, requires rethinking the existing architecture for a command and control system for the electric network. This new paradigm of Smart Grids also incorporates a significant change in the security requirements, in fact, the introduction and integration of information related with client’s consumption raises serious problems related to data privacy. Through the customer consumption is possible to identify patterns of behaviour that can be easily translated into habits or interests. As a matter of fact, a significant reduction in consumption could mean that a person is on vacation.

The analysis of customer consumption can go further, creating patterns of behaviour that allow us to identify people who, for example, have a habit of watching TV after dinner, people who have a pool at home or who mainly use the oven to cook. All this information is financially valued because they allow direct campaigns focused on customer interests.

This thesis addresses two major dilemmas for the area of power distribution. On the one hand, the growth, completely inevitable, of equipment and information causing the adaptation of processes and systems to this new paradigm much more complex and demanding and. On the other hand, the introduction of business data, deriving from the Smart Meters, which require to consider the privacy as a security requirement with high impact on the Smart Grid architecture. The work presented here was carried out in three complementary phases: 1) operational and organizational risk assessment, 2) definition of a new Smart Grid architecture and 3) evaluation the benefits and drawbacks of this new architecture. In the first phase we carried out a risk assessment of each of the Smart Grid's components in terms of three security attributes: Confidentiality, Integrity and Availability. In this phase we have also performed an analysis of the risk associated with the loss of each of the security attributes. This analysis, based on three axes (financial, business continuity and reputation), create the possible to identify the real impact, for the organization, in case of security losses. All the previous findings are then used in the phase.
2 to support the definition of a new architecture, this time, based on cloud computing to increase dependability, scalability and robustness of the Smart Grid platform. In the phase 3, we presented an evaluation of all functionalities of Smart Grid, using the same methodology defined on the phase 1, and rated the impact of their migration to a cloud solution.

In the new Smart Grid architecture (SGCA) the Smart Meter starts to assume a lower risk in the system while ensuring, simultaneously, a better performance in terms of availability and scalability. Simultaneously, this new architecture reduce also production costs, which multiplied by the number of customers, represent a real financial benefit.

The migration of a mature system to a completely different, complex and demanding environment must end with a cost-benefit analysis, here translated in a SWOT analysis in order to strategically measure strengths, weaknesses, opportunities and threats.

**Strengths**

One of the major Strengths of the cloud computing is the ability to scale up services obviating the need for underutilized servers in anticipation of peak demand and the capability to request more computing resources on the fly. The availability and broad network access are also an advantage that cloud computing can offer. In addition, it can provide an immediate access to hardware resources, with no upfront capital investments for users, leading to a faster time to market in many businesses. All these benefits make the Smart Grid prepared to address the expected increase the level of processing and information storage that will be required for this system.

**Weaknesses**

The current weaknesses of cloud computing are mainly related to security aspects either within the own infrastructure or at the level of communications. In addition, the dependency on the cloud provider is considered also as a drawback since the costs of a possible migration can be extremely high. Lastly, and also related with the vendor lock-in, is the possible impact of an outage in the service. All these constraints lead us to assume that the migration of a Smart Grid solution must be based on a private cloud computing model. The use of a public cloud should only be considered for functionalities not dependent on real-time and always in a hybrid model. One possibility is the use the public cloud computing to implement disaster recovery mechanisms.
Opportunities

Cloud computing creates opportunities to support innovative new services and business models that decrease time to market, create operational efficiencies and engage customers in new ways. In addition to these global resources that support organizations to create lasting competitive advantage, cloud computing brings along the cost-effective and scalable solutions facilitating and promoting the use of applications and tools on a global scale. The opportunities for Smart Grid can be divided into two groups. Firstly the ability to ensure the timely information delivery requirement to the customer and, secondly, the ability to respond properly to constant increase of the computational and storage needs.

Threats

The biggest obstacle in the adoption of a cloud service is related with the security and privacy issues. On the top of the security problems we can find issues related with data loss or leakage but there are many others, representing similar impact. Among them there are at least two that are important to mention. The first one is related with insecure interfaces that consumers use to manage and interact with cloud service. The second is related with the malicious insiders, which is amplified in a cloud environment by the convergence of IT services and customers under a single management structure.

Final Remarks

As a final remark, the evolution and adoption of cloud services is crucial for effectively address the computational needs imposed by the Smart Grid evolution. Although the present study and results allow us to conclude that critical infrastructures have specific requirements for security, resilience and availability that postpone a migration in part or totally, to a public cloud. We really believe that Smart Grids will adopt private clouds at short-term and, only for non-critical components, the use of a public cloud in a hybrid model.

EDP has been working on the feasibility of adopting cloud computing to host the Smart Grid architecture. A first initiative was led through the participation in the European project, TClouds, where EDP drew a use case, based on public lighting management has a specific functionality of the Smart Grids architecture. The involvement in the TClouds project, complemented with this thesis, gave us the possibility to assess the benefits and limitations of a migration to the cloud and the possible to establish the necessary steps for migration in a progressive and sustained way. This migration process has already begun, and its first phase foresees the creation of a private cloud to accommodate of all servers
that constitute the Smart Grid of EDP.

In the proposal for this thesis we had predicted a practical component to evaluate the implementation of the architecture presented here. This objective was not completely fulfilled since some components of the Smart Grid, for example Smart Meters, were disaggregated and analyzed separately. Accordingly, the realization of a prototype is unfeasible since it is not possible to transfer selected components of the equipment to the cloud without having access to the equipment code. However, in the chapter 5 we have performed a test comparing the traditional Smart Grid architecture with the SGCA.
Bibliography


[22] Cynthia Lynn Bellefeuille and Dartmouth College, Quantifying and managing the risk of information security breaches to the supply chain, Massachusetts Institute of Technology, 2005.


[31] Expert Group 3 First Year Report, Options on handling Smart Grids Data, January 2013.


[50] Lan Foster, Yong Zhao, Ioan Raicu, Shiyong Lu, Could Computing and Grid Computing 360-Degree Compared.