Chapter III

# Cyber security in the emerging systems of the electrical sector

Jorge Cuéllar Jaramillo

## Abstract

There are many forces that have led modern societies to embrace a new concept for the production and distribution of electricity in the future: the smart grid. They include the scarcity of fossil fuel and the ecological impact of current energy sources. The intelligence of the future grid will depend on the use of technologies of information and communication. Indeed they will be indispensable to meet the challenges of the new energy sources which are intermittent and distributed. The energy supply infrastructures are among the most critical for the modern world, and the reliability of the distribution is the most important requirement to be met. This implies that ensuring the IT security of the smart grid will be of pivotal importance. But this will only be feasible with a demanding and large effort to cope with the security issues, conducted in a determined way by the different sectors of our society, including government authorities and private organizations, research groups and in particular all the different actors that will take part in the new electric grid.

The purpose of this article is to provide an overview of the security landscape of processes related with the management of command and control information and personal data in the context of the Smart Grid. Without entering into technical details that would distract us, we will discuss the purpose and use of smart technologies in the future grid, the risks associated with them, the security requirements that they must meet, and the means to implement them. We conclude that it is crucial to understand and treat the risks. This endeavour will convey a set of new challenges that our society will have to face.

**Keywords:**

IT Security, Technology, Information, Communication, Threats, Strategy, Attacks, Grid, Internet, Cyber-security, Vulnerabilities, Critical Infrastructures, SCADA, Cyber threats, Smart Grid

## The smart distribution grid

### *The threshold of the third industrial revolution*

It was already clear to the inventor Thomas Edison that the creation of new individual electrical solutions, such as the electric light bulb or energy generators, was not enough to have a large-scale impact on society. It is also necessary to build an energy distribution system in order to place these advance within the reach of the general public. Hence, their efforts were not restricted to creating individual electrical systems, but also to the transmission of electrical energy to private homes. The first energy distribution grid started in 1882. This rapidly led to the practical utility of the technological advances and an explosive increase in their use. However, it used direct current (DC), which turned out to be only useful for transmitting energy over short distances.

Nikola Tesla discovered that alternating current was capable of going beyond the limitations on energy transmission and it was more suitable for electrical transmission over long distances. In 1895, George Westinghouse used this technology to connect a generator at Niagara Falls and transfer electrical alternating energy to the city of Buffalo, some 35 kilometres away, thus beginning what Marshall McLuhan called the Electricity Age.

Since then, the structure of the distribution grid has maintained the same basic architecture: generation does not have to be close to consumption and electricity flows unidirectionally, with centralised distribution from the generator plants to the end consumers, whether households or industry. The system's reliability is assured by an excess of capacity (reserves) in order to respond to potential demand at practically any time. Electrical systems were designed and constructed in times in which primary energywas relatively plentiful and cheap thus not having the imposing need to save energy, or to optimise consumption at all costs. The abundance of electrical energy has been an extremely important factor in the industrialisation and development of Spain, Europe and, of course, the whole world.

The information society and the third industrial revolution have been in the making since the second half of the last century, with the electrical and ICT advances such as the transistor, television, computing, robotics, Internet, etc. But there are several authors, such as Jeremy Rifkin who consider the Smart distribution Grid to be the door to the third industrial revolution ("The Third Industrial Revolution", New York, Macmillan, 2011). The five pillars of the third industrial revolution, according to Rifkin are:

I. The replacement of the conventional energy sources by renewable energies.

II. The transformation of the buildings and houses in power micro-plants that can access sources of local renewables recourses.

III. The installing of energy storage technologies, such as those for the creating, storing and processing of hydrogen. These technologies will be used in buildings, houses or cities in order to effectively use the intermittent or surplus energy at times of demand troughs.

IV. Use information and communication technologies, and Internet in particular, so as to create hub grids having locally generated energy, negotiate prices and sell surpluses to the local or global grid.

V. The replacing of the existing conventional transport fleets by electrical vehicles, which can store energy and thus purchase it at times of elevated supply and sell it at times of greater demand.

The use of information and communication technologies will make it possible to decentralise both production and control. It will allow the optimization of electrical energy distribution in a way that is unprecedented and radically different form todays, geared toward the centralised generation of electricity in large electrical plants.

## *Forces that lead to Smart Networks*

There are many reasons that currently make it essential to re-design the architecture and functioning of the electrical network and that lead us to Smart Networks. We sub-divide these into reasons of security supply, of the protection of the environment, changes in the market and the need for new grid optimisation mechanisms.

### Supply security

Fossil fuels –coal, oil and natural gas- are limited, oil particularly is now close to its production zenith. Since before the first energy crisis in 1973, fuel prices have been rising in waves and times of great shortfalls in the supply of oil, electricity and other energy resources have appeared. These crises adversely affect the rest of the economy, increasing the likelihood of recession: as energy costs raise the costs for all industries also go up, while the price of petrol leads consumers to reduce their costs and to less confidence in the economy. Oil-dependent countries have great motivation to save energy and search for and integrate alternative sources. None of these will be as cheap, as convenient or as simple to transform in energy terms as oil, but they will be necessary to assure the energy supply.

### Ecology and the protection of the environment

Many reasons have led us to become aware of the need to preserve the environment and oblige us to look for renewable low-emission energies that have few harmful residues. Two examples are: the growing atmospheric pollution, as for example, has been observed so drastically in China in recent years, and the increasingly imminent risk of climate change that could turn out to be disastrous in the field of nuclear technology security, as Fukishima showed. The great difficulties that Japan faced with nuclear plants following the tsunami have been the main reason why the German government decided to opt for energy transition ("Energiewende").

### The market

One of the stimuli for this change in the system is the de-regulation and privatisation of the markets, as well as the re-structuring of industry in general and the electrical sector in particular. Many governments are expecting growth in innovation and competitiveness, as well as a reduction in prices and supply efficiency. Even nowadays, energy grids are still mostly handled by generating and transmitting monopolies, but these structures are evolving towards a large network of many competitive energy producers and other participants in the system.

### Optimisation of the distribution system operations

On the other hand, the necessity of making use of alternative energy sources leads to greater investment costs and production cost. This naturally incites the search for optimal methods of using energy generation surpluses. It will be possible to maintain such high reserves, which cover the existing demand at any time: alternative energy is mostly *intermittent*, that means, there is a huge fluctuation in energy, depending on the state of the weather (wind and sun), the waves, of the quantity of rainfall, etc. In order to resolve this problem, it will be necessary for end consumers to actively participate in optimal energy usage, levelling out demand curves. It would be ideal if users take less energy from the grid at times of low production. This is achieved using *demand response (DR)* mechanisms, providing incentives to the general public to reduce electricity usage at times when demand is high. It will also be necessary for users not just to consume, but also to produced and store within the same grid.

Another consequence of the use of renewable energy sources will be that electricity grids will stop being unidirectional. Depending on the climate conditions in the different regions, electricity could, for example, flow from north to south. In order to adapt the grid and achieve a situation in which the system remains stable, it is necessary to have very detailed information about the electrical characteristics as well as meticulous supply and demand forecasts.

### *What are Smart Grids?*

Briefly, the functionality of a Smart Grid is the distributed, quasi-optimal coordination of the actions of generators, distributors, consumers and prosumers (which perform the dual roles of producing and consuming energy) in an efficient, sustainable, economic, and secure way, that facilitates the dynamic integration of regenerative energy sources, beneficial to the environment. For this purpose it is necessary that consumers actively participate in optimising the operations of the system, and the system must offer them greater amounts of information and the opportunity to interact. Smart Grids use information and communication technologies (ICT) in both innovative services and in smart technologies for monitoring, control, communication and auto-regeneration.

We begin by saying the Smart Grid is not a static concept, but rather a *vision* with the goal of handling energy resources in an efficient way. This proposal is specified in the use of innovative technologies, many of which are still being developed, in order to efficiently manage the generation, distribution, measurement, storage and consumption of electrical energy, responding to needs of growing energy demand and of creating a sustainable energy base that is capable of reducing the climate and ecological impact. To do this, it is absolutely essential to use ICT, entrusted with vital tasks at all of the levels of the system, from the acquisition and processing of signals, up to the technical control of the dynamic system of electrical energy flow and the integration of the actions of all of the players in one single coherent system.

Many authors consider Smart electrical distribution Grids to be humanity's largest technological project. An endeavour of such magnitude cannot be undertaken in one single strike. Constructing Smart Grids will have several stages, investments will increase over time and the profits obtained will gradually become visible. Smart Grids will not be developed at the same pace everywhere. On the contrary: bit by bit, smart local management and distribution islands are appearing, called micro-grids, at universities, industrial or commercial centres, etc. These grids use small energy sources, which are relatively cheap and reliable, such as micro-turbines, photovoltaic panels, and fuel batteries, fitted in client's premises. A micro-grid operates as a controllable module, connected to the global network, with the aim of supplying electrical power and local heating, reducing the maintenance of local voltages, achieving greater efficiency in using residual heat and reducing total emissions.

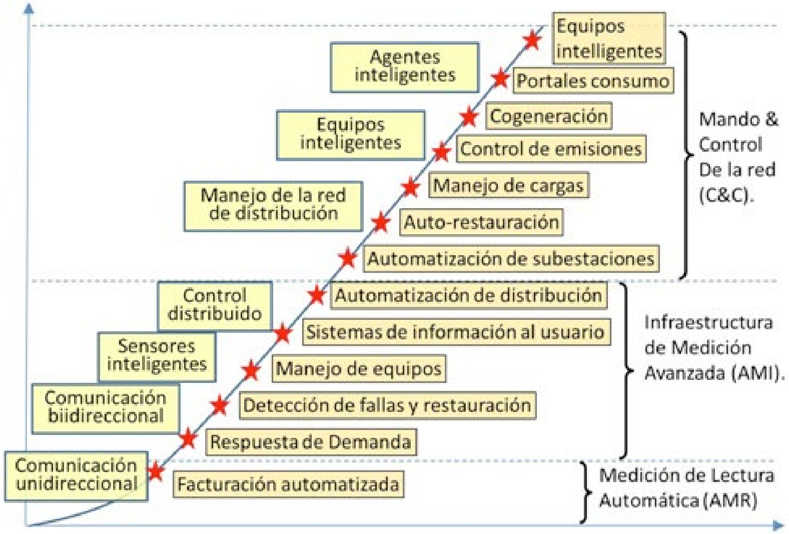
Agentes inteligentes
Equipos inteligentes
Manejo de la red de distribución
Control distribuido
Sensores inteligentes
Comunicación biidireccional
Comunicación unidireccional
Equipos intelligentes
Portales consumo
Cogeneración
Control de emisiones
Manejo de cargas
Auto-restauración
Automatización de subestaciones
Automatización de distribución
Sistemas de información al usuario
Manejo de equipos
Detección de fallas y restauración
Respuesta de Demanda
Facturación automatizada
Mando & Control De la red (C&C).
Infraestructura de Medición Avanzada (AMI).
Medición de Lectura Automática (AMR)

**Figure 1. Stages of network construction. Both investments in technology and infrastructure (left boxes) as well as the system features and benefits as returns investments (right boxes) will occur over time (horizontal axis). Some of these concepts will be discussed in Section: THE ROLE OF TIC´s IN THE INTELLIGENT NETWORK. The intelligent network features.**

Figure 1 shows the three main phases of implementation of the grid: the introduction of automatic ways of measuring, the introduction of advanced measurement and the infrastructure of command and control mechanisms, including the provision of tools for electronic energy markets. The illustration also shows the return on investment that will be achieved in the different steps, according to the main architect of the first micro-grid in Canada, Professor H. Farhangi[1].

Smart Grids will cover the entire electrical energy business chain, and they will integrate other players in adjacent areas, such as water and gas. Moreover, they will cross geographical and political borders. This is because in many cases it will be necessary to complement the generation and storage services of the different countries. For example, it is easier to generate solar energy in southern Europe. In Scandinavian countries, the energy is stored in hydro-electrical reservoirs. Even more so with functions that go beyond energy supply, including the supervising of transport, the distribution of assets, the well-being of the inhabitants, the quality of water and many more. There are already a large number of projects that are building these Smart Grids, in particular in the context of smart cities.

[1] Hassan Farhangi: The Path of Smart Grid, SISS Power & Energy Journal, Jan 2010, Vol 8, No 1.

## The current electrical supply system

### *Architect and characteristics of the current system*

The electricity supply system covers a set of useful resources for generating, transporting and distributing electrical energy. Figure 2 shows the current electrical distribution system in a very schematic way. The current network is unidirectional and divided into several parts that operate with a certain degree of independence between each other, controlled by pieces of SCADA equipment that share any information in a very limited way. All of these grid characteristics will change in the future grid.

This system is fitted with a supervision system that acts in real time, comprising control, security and protection mechanisms whose priority goal is to maintain the quality of service, balancing generation with users' demand and compensating from the possible incidents and faults that may appear. It is not easy to maintain this balance because electricity flows nearly at the speed of light and cannot be easily stored in a profitable or immediate way. Therefore, it has to be used at the time it is produced. Electricity flow cannot be controlled as is the case with liquids, opening or closing valves, nor does it stop like telephone connections. Electrical energy moves freely through all of the other paths, being divided in accordance with the physical rules of impedance.

On the other hand, the network is fitted with a business management and administration system consisting of mechanisms for forecasting resources planning and managing trade, including both energy auctions such as invoicing and remunerating the different market agents.

These two, the supervision and control system and the business management, are both distributed and largely depend on information and communications technologies.

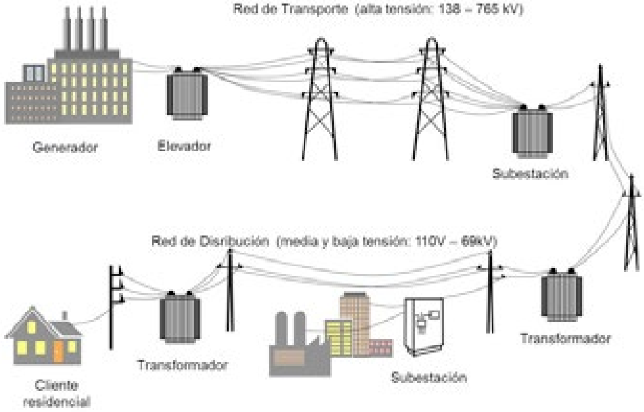
Red de Transporte (alta tensión: 138 – 765 kV)
Generador
Elevador
Subestación
Red de Disribución (media y baja tensión: 110V – 69kV)
Transformador
Cliente residencial
Transformador
Subestación

Figure 2. The current electrical distribution system (simplified diagram).

Very often, different parts of the system are operated and run by distinct companies. Therefore, the control system is of a distributed and hierarchical nature: the controlling equipment at the generating plants, in the transport network, in the sub-stations the sharing network and the distribution grid, and supervised and controlled by stand-alone pieces of equipment, but these communicate between each other so as to achieve overall equilibrium.

Sub-stations or transformers frequently have Remote Terminal Units, better known as RTUs, devices fitted with micro-processors, which obtain the signals from processes with integrated sensor equipment or, for instance, by means of phase measurement units. The RTUs send the accumulated information to a remote site where SCADA equipment is located. This processes the information from a large number of signals from different places, with accuracy measured in terms of milli-seconds. SCADA systems, the acronym for the Supervision, Control and Acquisition of Data, make it possible to monitor, control and supervise remote electrical distribution processes, automatically controlling the processes. In addition, these pieces of equipment are connected with control rooms, making it possible for the visualising of the state of the grid and the entry of control commands, with the field devices feeding back data in real time.

With the Smart Grid already having been announced, transmission and distribution lines are being fitted with smart devices that locally control sensors and triggers. One example is provided to us by measurement and protection relays, capable of calculating the operating conditions of the circuits and hence, detecting and locating the faults and, depending on its level of intelligence and conditions, it can even diagnose the type of fault, and activate smart switches when problems are detected. These switches are necessary in order to isolate pieces of equipment and networks. In this way it can protect them and minimise the number of users affected when outages take place.

We can conclude that ICT is already essential nowadays to maintain the stability of the electric supply system.

The business administration and management systems related to the electric system also rely hugely on ICT. But these systems are rather less interesting for our purposes, for two reasons. First, they are less critical because the stability of the grid does not depend on them and because they are easier to keep redundant. Second, they are similar to those that are conventionally used in the diversified commercial world, where the problems of cyber security have been well studied.

### *Reliability*

Aninfrastructure is considered crtical, when serious supply problems occurs due to an error of it.. The 8/2011 Act for the Protection of Critical Infrastructures, defines these in the following way: a service is called *essential,* if it is necessary for the maintaining of basic social functions, health security the social and economic well-being of citizens, or the effective functioning of the state. A set of grids, installations, systems,- physical and ITC equipment on which the function of an essential service rests, is called *critical infrastructure,* if its functionality is indispensable and does not allow for alternative solutions. Therefore its disturbance or destruction would have a severe impact on essential services.

Reliability is the most prioritized demand of modern society for any of the structures used in critical infrastructures.

The frequency of the electrical energy sector infrastructure is frequently considered. This encompasses both electrical generation and transmission as the most critical of the infrastructures. When the latter stops working, all of the others are paralysed as well. This includes the distribution of comply-used goods, the health service in hospitals and clinics, public communication networks, etc. For example, the damage to the Auckland electrical system in New Zealand in 1996 forced 60,000 of the 74,000 employees in the areas affected to work from home or from alternative offices, while most of the residents of the 6,000 apartments affected were compelled to move while a solution to the problem was sought out.

The electrical system's reliability can be defined in terms of the system's capacity to deliver electrical power to consumers in an accepted way and in the quantities established and desired.

The North American Electrical Reliability Corporation (NERC) divides reliability into two categories, suitability, or static reliability, and security, or dynamic reliability.

*Suitability* means that the necessary resources are present and accessible to generate, operate, transmit and supply electricity in the planned way, and in accordance with the quality requirements for continuously expected waves. This includes the cases of very high demand, during routine repairs or when there are faults, contingencies, or foreseeable problems, such as those due to heavy electrical storms in the area. Amongst these resources, we can find demand response programmes which, as we shall see, reduce energy demand peaks.

*Security*, on the other hand, is the system's capacity to bear unexpected disturbances, such as short circuits or the loss of elements due to natural causes, as well as intentional and unintentional attacks, either physical or cybernetic, of non-malicious consumers, internal workers, competitors, terrorists or enemies. In particular, security means that the system as it is will be intact after discharges or other faults occurring in the equipment. Security includes the capacity to recover from the problems when they appear in the swiftest possible way, restoring the provision of the service and the performance of the elements.

NERC has developed a method and several standards in order to ensure the reliability of the electrical supply based upon various fundamental principles. The most important as already mentioned, is to continuously balance demand and supply and to keep the system stable, in spite of the contingencies or faults that may appear. The demand goes to a certain predictable point, and this is also the case with the expected statistical deviations. The demand curves are analysed and constantly updated. Above all, the danger of this imbalance between supply and demand lies in the frequency of alternating current (50 or 60 Hz, normally), which can be substantially affected, rising if there is less demand, or going down if there is higher demand. Small variations in the frequency are not problematic, but if it rises too much, the speed at which electricity generators turn starts to fluctuate, causing vibrations that could damage them. Low frequencies are automatically handled by means of cuts of the energy supply in towns or in districts, each one in turn, so as to avoid a complete outage. An imbalance could also be the effect of unexpected contingencies, and when parts of the grid are isolated, could lead in turn to a cascade effect. Another threat lies in the loss or rising of voltage, which could damage motors or provoke instabilities in the network, it can also exceed the capacity limits of the insulators and cause disruptive discharges and very dangerous electrical arcs that happen when electricity bursts jump from one electrical conductor to another one. Instability problems could appear in the matter of fractions of a second. In North America, in August 2003, a part of the Eastern interconnection system became destabilised, leading to a very big blackout in a very large area.

Maintaining the reliability of the electrical network is a continuous and complex process that requires very skilled and highly trained operators, specialised smart equipment and extremely careful planning, design and development. It is interesting to understand, how despite the possible problems and dangers that could appear in the energy system, the system remains relatively stable. The reasons for this are: firstly, there is a standardised and rigorous system, in order to maintain and check operation plans, including long-term systematic evaluations, the analysis of contingencies, and quite detailed plans, on the short, medium and long term. Secondly, the system is always made ready for all of the potential simple contingencies (where only one pieces of equipment fails), even in the worst of cases. Thirdly, the system is made ready to provide swift responses if there are multiple faults. Lastly, the system has extra capacities for all of its functions, such as for example, redundant equipment, but also reserves in the production and transmission capacities.

What we have to ensure is, that these security and reliability processes are also applied in the Smart Grid, adapting them to the cyber security needs and the threat to information and communication technologies that the future distribution grid is going to require.

### *ICT security requirements in the electrical supply*

ICT security is a very broad concept, which covers different properties with many qualifications, a large quantity of technical mechanisms that can be implemented in hardware or in software and a series of processes that have to be secure throughout the entire system cycle, from the definition of requirements to the use of the system or its upgrading or correction. Wikipedia limits the concept of ICT security (http://es.wikipedia.org/wiki/Seguridad_informática), in such a way that it is wholly insufficient for us: "Computer security spans [...] everything than an organisation values (assets) and it entails a risk if this confidential information reaches the hands of other people, converting itself, for example, into privileged information". While generally speaking it is true that *confidentiality* is one of the most important aspects of computer security, there are a further three properties which are even more important for smart distribution grids: *integrity, availability and privacy* (the latter concerns the protection of the personal information of an individual or a group of them. Privacy is very close to confidentiality and they are sometimes seen as synonyms, but for our purposes it is convenient to consider them separately. In this context, any information related to private individuals, which can be used together with other sources of information, in order to identify, contact or locate that specific person directly or indirectly, is called Personally Identifiable Information, or PII, which is predominant in the United States).

As far as distribution grids are concerned, the most crucial security property is undoubtedly *integrity*. In the common sense of the word, this concept is related to *completeness* (the state of not lacking any of its parts), *coherence, or the state of being impeccable.* The technical sense of the expression in the context of ICT –while being quite precise– covers many different aspects. In a Smart Grid, a large quantity of data is generated, by sensors or by users inputting data or by interfaces with other systems. These data can be modified, and they will be read at any time, for the purpose of processing, accumulation, filtering or analysis. The rules that determine who can create or modify data, and under what conditions, are the rules of *integrity*. The rules that define who can read the data is the rules of as *confidentiality*. The rules that govern the use of personal data, the valid purposes for using them, the third persons to who they can be distributed, are the rules of *privacy*. *Availability*, in its ICT security aspect, is the system's resistance to the so-called denial of service attacks, which will be discussed later on.

The four security requirements –integrity, privacy, confidentiality and availability– are top level requirements and they are independent of the devices made available and the technology that is going to be implemented. In order to guarantee these requirements, it is necessary to systematically reduce them to certain more particular and specific ones. Some examples of such specific requirements are: alarm systems, intrusion or attack detection systems, mechanisms for resisting intrusions or attacks and recovery if this is necessary, methods of identifying, authenticating, authorising and controlling access, as well as protocols to protect the distribution of cryptographic passwords and systems to calculate the reliability of the elements in the system.

This article will not try to discuss how or with what technologies it is possible to guarantee these requirements.

### Integrity

In order for the grid to function correctly, it is necessary for the data processed by the system to be complete and for them to correspond to what is expected. This means they have to be consistent with the values of the sensors with parameters that are inputted by the administrators, with user's input and with the data that come from other systems, such as data fromweather forecast systems, e.g., the intensity of the winds and the volume of the water.

This property, expressed precisely, is the integrity of the system. In order for this to be completed, it is necessary that the data cannot be modified without authorisation when it passes through the communication channels, or when it is in a databank or in another memory, temporarily or permanently. These aspects of integrity can be implemented using cryptographic methods, such as digital signatures. The two difficulties in this context lie in the need to use such mechanisms in processors that have little computer capacity (such as sensors) and in the need to distribute the passwords that are necessary to protect them against attackers. Another aspect of integrity is that the data is solely generated by the authorised entities. To do this, it is additionally necessary to have access control methods which, at least in theory, are well understood and do not present great difficulties, except for the large quantity of elements that work in the system. The next aspect of integrity is the hardest one to ensure: using the correct process that createe, modify or communicate the data. It is no use to make sure that only one very reliable administrator is capable of changing the system configuration, if the programme that is used to do administration is malicious and it performs in an unexpected way.

### Privacy

Before anything, the protection of privacy means respecting the limits set by law for the compiling and utilisation of personal data. The text of reference within the European context in this regard is the European

Directive 95/46/EC. This directive defines the main guidelines and the principles of orientation for data protection. The member states have implemented this kind of directives as well as independent national bodies that are responsible for supervising the protection of the private data; they set the terms for judicial appeals in case that privacy rights are not respected. In Spain, this controlling body that is responsible for complying with the Spanish Data Protection Act is the Spanish Data Protection Agency (SDPA), which was created over twenty years ago. The directives and the legislations are not only applied to the data processed by computerised ICT, but also those that are dealt with on paper in traditional files.

The privacy of a piece of information provided, in a given moment, may take on different levels of importance, depending on the particular situation, the practices and the culture of the individuals in question and of the society in which they live. This is especially valid for that information that gives away the practices, activities, convictions, family status, etc. of an individual. For a person in a particular social context it is not problem to disclose that someone is a Muslim or his family has 6 children, but for someone else, in another context, this situation could be very delicate.

There are two reasons why this is pertinent for Smart Grids: first, the person himself who is interested is entitled to oppose certain forms of handling his data, the way it is used in, or the level of detail that is contained. Second, the personal details that are processed with a Smart Grid can provide information about matters that are really personal to the individual. There are already rather a large number of doubts nowadays concerning privacy of personal information of consumers, with the appearance of smart meters. Data about the electrical consumption in a family –should they be very detailed and taken very frequency– can offer a lot of details about the family life: at what time a device was switched on or off, e.g, the television, the oven, the washing machine, etc.. It is possible to know if the family is not at home or if they have guests, if a shower was taken hurriedly or if there was breakfast, etc. Data from an electric car can show evidence about the places the user has visited, and this could maybe be evidence of related activities. If users access the system remotely, the data could perhaps indicate whether they are on holiday and where.

To put this very briefly, the basic principles of privacy are as follows: the data have to be compiled and processed for certain purposes which are particular and legitimate, and only for them. The interested person has to know the way his data is handled; he is entitled to access his data an must have given his consent to it being used; certain categories or types of data (that could reveal something about his racial or ethics origin, his political convictions, religious or philosophical persuasions, his membership of a trade union, the state of his health, his sexual orientation or activity, or his personal or family situation) cannot be collected, or special permissions and provisions are required; the competent authorities must receive information about the unlawful, alteration, dissemination or unauthorised access to personal data. Lastly the data has to be handled in a secure system that offers confidentiality.

In this list we can clearly see the difference between confidentiality and privacy: privacy presupposes confidentiality, but the former covers a lot more.

### Confidentiality

In general terms, confidentiality is the property that the data stored in information systems or that is transmitted by communication networks are not within the reach of people who do not have the authorisation to read the data. In the case of the supply network, there is quite a large quantity of data that needs to be protected in this respect. For example, details about the physical architecture are important to secure because they could bring about a physical attack if they fall into the hands of terrorists. Similarly, the data about contingency plans, production or transmission reserves, consumption forecasts, economic data about the system, etc. must also be protected. Personal data about the users, about their consumption and their accounts have special important value for reasons of privacy, as we have discussed above.

### Availability

Availability is the property that the systems are at the disposal of the users or those that can access them at the times when they need them. In this general sense, this is practically the same as the system's reliability. But there is a very particular sense of the word, related to the security requirements of information and communications technologies. This means that such systems have to be immune or highly robust when faced with the so-called denial of service attacks. One typical form of attack is that of saturating the communication networks service, blocking that service with a huge number of requests or overloading the network with artificial messages that make legitimate access difficult or impede it. There are other more sophisticated ways of putting the system availability at risk, attacking its integrity, for example, changing the credentials that it uses. There is a broad range of mechanisms that that can be implemented in the ICT infrastructure: the use of systems with redundancy, fixing disks, high-availability equipment, mirror servers, virtualisation, data replication, storage networks, redundant links, etc. The suitable solution depends on the services or that have to be protected, and the service level that it is necessary to provide.

### Cyber security rules in the current electrical supply system

Here is not the place to discuss the attacks that have been discovered in the electrical distribution system in depth. Going beyond casual attacks, the ones that make us concerned are those that are called Advanced Persistent Threats, which are advanced ways of clandestinely gaining intelligence about a company, a sector, a critical infrastructure or a particular group of individuals, continuously and persistently.

It is necessary to understand what the dangers are in general terms, how advanced attacks work and what needs to be done to lessen the relevant risks, without going into a discussion about the techniques that are used. In very general terms, an advanced attack is achieved in the following stages: Firstly, relevant information for the initial attack is compiled. Attackers search for information on Internet and in other media that is provided for public access to in order to know which employees of the different electrical companies or the associated company can be attacked. To complete this information so-called social engeneering methods are employeed. For instance, this entails asking for data by telephone, pretending to be somebody who is authorised to have the information. Now, attackers have got a list of their first victims, of their positions, work environment, the names of their colleagues, etc. Then they send them fraudulent electronic messages, which are fake but appear to come from their boss, from a work colleague, from a centre that arranges conference of professional interest, of companies that provide protection systems etc. This type of e-mail fraud is used in order to obtain further information, or to steal the victim's credential and so be able to enter servers where the victim has access. On certain occasions, it is possible to use these fraudulent e-mails in order to inject a malicious code into the victim's system. This method of using malicious messages that are constructed for certain people in particular, and then sent to a pre-established target is called *spear-phishing*. This enables the stealing of credentials, secret passwords or codes in order to manage to *impersonate an identity*. Once inside the organisation, they look for new passwords, vulnerable programmes, communication or administration services that could be abused. They inject malicious codes within the programmes that already exists and known, trying to conceal their true character and intentions. This malware usually has capacities to contact a malicious server that controls it or guides it and opens up a channel so that the attacker can "enter" in the compromised system. This is known as a *Backdoor*.

Other Trojans are commonly injected into the more important files for the computer's operating system, until they manage to make the attack succeed. In this way, even though the computer is re-started, the Trojan, having infected files from the operating system, remains present. It can now spy on the activities of the administrators and even read what is written on the keyboard (known as *keyloggers*) or send messages to other computers, searching for cryptographic passwords, etc. In the meantime, it is waiting for the right time for the final attack, maybe coordinating itself with other malicious programmes by means of the malicious server, and it can carry on selecting information about the physical defence or cybernetic systems, the structure of SCADA systems, and the logic programmes, relevant documents, peoples' names or e-mail addresses, parameter values, etc. In certain cases, the malware could even stay inactive for weeks or months before starting the internal attack that it was designed for.

### *Stuxnet*

Stuxnet is the name of the malicious code (Trojan, or malware), discovered in July 2010 due to a functional anomaly that caught the operators' attention. There is recent evidence that preliminary versions (version "0.5") had already appeared in 2005. This was the first malicious code found that reprogrammed control systems and the supervision of SCADA programmes, as well as the programmable logic controllers (PLCs) connected to these. The malware analysis took many months, because it uses different type of coding and very advanced obfuscation. The software can spy, affect and damage the critical infrastructures that are infected, without the administrative staff being capable of recognising the damage in time.

Stuxnet is a piece of software that has never been seen before, which certainly required a very complete team of expert programmers, with very detailed knowledge about different programming techniques, the equipment that the attacks are targeting and the industrial processes that they want to manipulate. The scale of this endeavour means, that it must have been very costly to programme and that the construction of it most likely had the support of a large organisation or a state body of some country. Stuxnet employs four vulnerabilities in the Microsoft Windows operating system which where unknown until then, in order to penetrate the Siemens SCADA system. In addition, Stuxnet can generate digital signatures with two genuine certificates stolen from certification authorities.

There are a lot of indications that Stuxnet was specifically designed to delay the start-up of the Bushehr nuclear plant in Iran. For example, most of the computers contaminated by Stuxnet are found in that country.

Since many of the pieces of industrial control equipment cannot be accessed via Internet, Stuxnet has the ability to infect using USB memory sticks. Moreover, it is capable of using other means of communication, and it has the capability to upgrade itself when necessary.

Until march 2011, a total of 24 Siemens' clients in the industrial sector had been notified worldwide, which had been infected by the Trojan. It was possible to eliminate the malicious code in all of these cases. Siemens is providing programmes to detect the presence of Stuxnet for public access on Internet (http://support.automation.siemens.com) as well as a list of steps and tools to eliminate the Trojan.

### *Stuxnet relatives: Flame, Duqu, Gauss and Madi*

Flame, also called Flamer or sKyWIper, is a modular malware that was discovered in 2012 that is highly complex and of a very substantial size. The organisations that have studied it, like the cryptography laboratory of the Budapest University, and Kaspersky agree that it is one of the most complex pieces of software and that it is very hard to fully understand. This is because of the fact that it has various obfuscation methods, various particular file formats, and at least five encrypting mechanisms. It also uses special methods to inject code into its victims.

Flame has a very advanced form of functionality in order to steal information, to store and communicate it, in addition to advanced mechanisms that spread it from one computer to another. It is capable of practically intercepting all of the computer's interfaces including USB sticks, the keyboards cameras, Bluetooth, microphones, and internet connections. Therefore it can record conversations and Skype conversations, capture the images from screens or keystrokes from the keyboard, etc. This data together with the stored documents are sent to one of various malicious servers spread around the world. The programme then waits to receive new instructions from those servers, and download additional modules that extend its functionality.

The programme has been used to carry out cyber-espionage attacks in Middle Eastern countries and it has infected 1,000 machines. In June 2012, the Kaspersky published evidence that reveal that Stuxnet and Flame authors had been in contact and they had worked together on at least the first stage of development. One example of this collaboration between the two groups of attackers was the USB infection mechanism code, which is identical in Flame and Stuxnet.

Duqu is a variant of Stuxnet, appearing at the end of 2011, which contains a variety of software tools that offer different types of services to attackers including the theft of sensitive information, such as cryptographic certificates and private passwords. Using these allows signing for malignant software and passing it off as upgrades of the systems under attack. Furthermore it has kernel (or core) controllers and tools for injecting code into existing programmes and read keystrokes. Duqu searches for information that could be handy for attacking industrial control systems although it seems that its objective is not to directly destroy, but rather to spy. It is possible that the information extracted is then used to create very specialised attacks. In personal computers it has indeed been observed that Duqu destroys information that is stored on drives.

Duqu is still being analysed by security experts, who have not been able to decipher all of the code and understand exactly how the Trojan works and, in particular, how it is distributed and multiplied. It seems that the code eliminates itself after about a month, which makes it harder to identify.

Duqu has been found in a limited number of companies, including those engaged in building industrial control systems, such as SCADA. The information extracted can maybe be used as a basis for designing and perpetrating new attacks such as the Stuxnet one.

Gauss, discovered at the end of 2012, is able to spy on bank transactions, steal information about access to social networks or electronic mail and attack critical infrastructures. Gauss is a complex set of cybernetic espionage tools, highly modern and apparently related to Flame. It contains encrypted binary code, which is not yet understood. It is activated in certain system configurations. Gauss would seem to have been used to steal authentication information from people in the Middle East, the Lebanon in particular.

Kaspersky and Seculert further studied the "Madi" Trojan. They identified over 800 victimis in various countries, such as critical infrastructures in Iran and Israel, financial institutions, Middle Eastern engineering students, but also think tanks and governmental agencies, some of them in the electrical sector, and foreign consulates in the United States. The attackers use social engineering methods to identify specific people and pieces of equipment in which –once they have been compromised– Madi is capable of searching for, and stealing the information stored in files, of reading electronic mails and instantaneous messages and even of recording keystrokes, reading what the user is writing on his keyboard for example codes and passwords. It sends all of this information to a spy server. It is also capable of upgrading itself to new versions.

### *Other attacks on SCADA centres and on the Smart Grid*

In its edition of April 8 2009, the "Wall Street Journal" reported that the American electrical network had been penetrated by spy countries that put Trojans in place, capable of disturbing the system, according to the report security officers, who did not offer details. The same year, an update of a piece of software in a Georgia (USA) nuclear plant initiated an unexpected energy stop at the plant's SCADA control and supervision system.

It is even possible that attacks on the Internet in general or on certain types of systems that are not directly associated with the energy supply affect the SCADA sectors. This had happened both in 2004 with the SQL Slammer worm and with the Conflicker virus in 2009.

It is hard to know how may attacks there actually are against SCADA servers, especially those that are targeted at one system in particular and are of an advanced nature. It is easier to calculate how often the indiscriminate attack attempts on SCADA servers take place. In 2013 TrendMicro reported on an investigation which, a few hours after activating a SCADA system that was not very well-defended with the sole purpose of watching cyber-attacks, demonstrated such continuously. The final statistics showed 28 days of continuous attacks with a total of 39 different attacks coming from 14 countries. At the Black Hat 2013 conference it was proven, that it is possible to take control over PLC control units so as to turn them on and off in a simulate situation.

However it is important to mention that although the SCADA controllers and the associated computers have vulnerabilities that are easy to find if one has direct access to the equipment, taking benefit of these vulnerabilities remotely and crossing the protection measures that are usually used is rather more difficult. In many cases, the continuous monitoring of these systems stops an attack that gaining information by means of trial and error. In contrary, a malicious code such as Stuxnet proves that the current measures are insufficient, if an attacker is very sophisticated.

In Smart Grids, the so–called *attack surface* is growing: both the quantity of Internet connections and the number of vulnerabilities in the connected systems is going to increase. There are 53 million smart meters in the United Kingdom, and in Spain, there are currently about 28 million energy consumers that will receive smart meters between now and 2018. Very often, the users' devices that are utilised for smart measurement are connected between themselves via wireless networks and with the energy supplier. The wireless networks are often easy for an attacker to access. He will be able to intercept, capture, record, repeat and handle the information in two directions, altering both the billing and consumption massages sent to the supplier, such as commands, the prognoses and supply prices in the energy market. In certain smart devices it is possible to extract the secrets from the memory, enabling the manipulation of the communication with all of the meters of the particular supplier that use these same factory pre-set secrets. The attacker could remotely disconnect homes, offices, and large-scale buildings by wired or wireless (GSM) connections. The current security of smart meters and of other equipment for the users and consumers leaves a lot to be desired, the protection of these devices does not have preventative security measures and there is no system for responding to eventualities in the case of attacks.

### *Other attacks on the infrastructure of the ICT environment*

There are more indirect ways –which are no less effective– of attacking the energy supply infrastructures. If infrastructures are infected, which systems' production or the global communication or the sources of trust in Internet depend on, and then the doors will be open to very serious attacks on the energy supply.

One scenario would be to infect an equipment manufacturer, breaking its production systems and introducing Trojans into the machines that are used in order to design, develop or fit out the equipment used in security systems or the control of critical infrastructures. If an attacker manages to get in there, the software patches, the files and the producers' compilers would be the perfect mechanism for dismantling an installation. In the eighties of the XX century, an already-classic article from the ACM (Association for Computing Machinery) written by Ken Thomson, the winner of the re-named Turing prize, demonstrated how it is possible to maliciously modify a fundamental compiler in such a way that the operating system's authentication and authorisation systems are completely open to the attacker.

A second scenario is provided by attacks on the sources of Internet trust (trust anchors). If it is possible to attack those that distribute codes, passwords, certificates and equipment used to identify, authenticate or authorise equipment or people, it is then easy to enter into any part that depends on the relevant security services. One example of these attacks was the intrusion of the RSA company in 2011, which began with e-mails to employees with a relatively low-profile, with a malicious Excel file. In the end, the attack was successful in extracting information related to the authentication products of two SecurID factors of the company's servers. These attacks seem to be connected to at least 64 infiltrations that have invaded approximately 100 identified victims, remaining stealthy for many months, stealing secret information that may probably be used for attacks on critical infrastructures.

These attacks are massive, but not impossible to counteract. One example has been a reaction of Lockheed Martin in this emergency. The security team of this company has invested a large amount of time in setting up a methodology to recognise the attacks, monitor its activities and prevent the theft of important information.

A year later on, a team of experts in cryptography found another attack on RSA SecurID, due to some subtle cryptographic faults, managing to compromise existing cryptographic devices, including smart cards and an information credential issued by Estonia. Similarly, faults were found in a large number of smart cards of different companies.

Other attacks on credentials suppliers and certifying authorities, such as the cases of Comodo and Diginotar, have received a great deal of attention in the media.

A third type of scenario is attacking communications networks (such as the GSM system) or the Internet pillars, such as path tables, domain name servers, etc.

## The role of icts in smart grid

### *The characteristics of Smart Grid*

Figure 1 depicted many characteristics of the grid:

I. Automated billing with a unidirectional grid. This system offers relatively detailed billing by time slots, making it possible for consumers to watch and understand their consumption patterns and choose the most favourable hours of these. This is a rudimentary demand response mechanism, which, as we shall see in a memento, ensure the provision of the best use of the grid's capacity, meaning that end consumers lower their demand in response to the price differences of the different time slots. In order to offer users the information, it is necessary to have the information storage and processing at the customer's premises or, in the absence of this, the communication channels that make it possible to pass the consumption data in the server's desired granularity.

II. Demand response with a bi-directional grid. A reliable operation of the electronic systems requires a suitable balance between supply and demand in real time. "Demand response" can be defined as a set of actions and measures, that aim to influence the electricity consumption habits of the end users. More specifically, raising the energy prices at times when there is usually more demand, or even modifying them in real time, depending on the supply and demand, will allow to have an influence on the time at which a well-informed user, or one fitted with smart equipment, consumes energy, helping to balance the system. Demand response will help to save energy in its entirety, but the importance of this lies in "moving" demand from certain times to other less critical ones, thus levelling out the difference between the curves of available reserves and the consumption that is demanded. It is usually expected that a user will reduce his consumption when the prices are high, switching off lights or equipment when they are not functioning, or transferring some of their peak-demand hour operations to times of low demand. In the future moreover, consumers will be able to opt to generate their own energy or to buy it to store, supplying it to the local or global network. For example, the local or global grid can be supplied in electric vehicles so it can later be used or sold. In any event, it is necessary to provide consumers with interfaces with information and communication systems so as to notify it in real time about current and forecast prices, consumption amounts, etc. However, it will not be possible to force consumers to be present in every energy consumption decision. The users must set rules (also known as their "preferences" or "policies") that will have to determine the actions of a smart decision-making system. This automation works, with no human intervention, controlling the smart equipment or domestic appliance in accordance with the users' preferences. The demand response measures are not limited to managing the quantity and the time of consumption, they also include for example, subsidies for re-integrating locally generated energy into households, etc. The mechanisms require the continuous compiling of data, as well as the processing and the communication of large quantities of information, both that relate to consumption by the different pieces of equipment in their homes, such as expected prices, etc.

III. Detection of faults and restoring of equipment using smart sensors. The distribution grid today is "blind" in many cases. The energy operators and companies have got very scarce information about the state of the grid, and in many cases they are unaware of the existence of supply problems, untill a client calls to complain about a lack of service. Using the Advanced Measurement Infrastructure system (AMI), the distribution companies will quickly know about any fault in the system. In addition, the network will be fitted with a larger number of smart electric devices that are capable of directing and resolving problems locally and of communicating with the highest supervision and control units in the hierarchy.

IV. Information systems for users and portals for consumers. Users will be able to supervise and administer the electrical apparatus both locally, from their homes, and remotely. This presupposes the availability of detailed information about the status and the activities of domestic appliances. Furthermore, it is necessary to have a systems so that users can define their policies (rules) that represent their necessities or preferences, and according to which, the service of a piece of apparatus is turned on or turned off, or its parameters are changed. They key will be the development of intuitive information systems for users which, in order to be broadly accepted, must comply with the personal information security and protection requirements.

V. Distribution automation. The infrastructure of the future will be capable of identifying and dynamically integrating new energy sources, regardless of the form of generation or of localisation in the grid. In the cases of excess charge it will be possible to recharge reserves, ensuring that the grid maintains an efficient and trustworthy supply level.

VI. Self-healing. Self-healing is a topic of investigation that may be considered one of the critical branches for the undertaking of the Smart Grid. The concept is really a euphemism, under which techniques are grouped together, which seek to provide the grid with the autonomous capacity to detect, analyse and isolate faults, and to find compensatory measures in order to recover the service immediately. The implementation would imply increasing the maintaining of the system's stability and reliability, even if the missing number of components rises.

## ICT Security in the Smart Grid of the future

One global trend for information and communication systems in critical infrastructures and very much in particular, for those that are pertinent to the electrical supply system, is that these are opening up, being connected to the outside world and to the global Internet.

Going back a decade or two, the general model was –and in many cases is still– that of medieval castles or fortresses; with deep moats, high walls, secure gates that are constantly under guard surveillance, and secret passageways that are only known to a small set of very select and reliable people. Specifically, the electrical supply supervision and control systems in this model are practically isolated from external systems. They have control centres where only completely-trusted individuals can enter, and where very communication with the outside world is subject to highly-scrutinised. But it is notable that it is impossible for the systems to really be isolated from everything. This is because it is necessary to update programmes put new computers in, connect external data banks, or to coordinate the production or distribution of energy with of the control centres. The security depends on the so-called perimeter protection. It is not vital, within the control centre's internal system, that the computers do not have vulnerabilities. What is important is that nobody authorised can access them.

This model is gradually disappearing and, with Smart Grids, the model will have substantially changed. It is now just the energy companies that are the ones interested in protecting their own information, but also that the general public is also the owner of sensitive information, not only its consumption data but also its energy consumption policies, its commands to the equipment of their private residences, etc. There will still be multiple players involved that provide and read information of all types and rely on their integrity, confidentiality and/or availability.

The model of medieval fortresses has become a group of residents in an apartment building of a modern city. Soon –with Smart Grids– this model will be mutate into that of a shared flat: the different participants have certain common security interests and other different one and they are compelled to reach agreements that determine in which way which objects value are going to be protected. In the case of Smart Distribution Grids, the different participants have a clear common interest: the integrity of the global system. Besides, each one needs its own personal or commercial information to be protected. Although the participants' different requirements do not contradict each other, they do, in any case, compete with the system's efficiency and they are costly to install and supervise. Even more so: in order for a server to offer a participant, it is often necessary to have personal information about this and the better, more accurate and more abundant that information the better the service that it can offer is. Thus, in addition to the tension between security, on the one hand, and efficiency and cost on the other hand, there is also tension between privacy and functionality.

Thus, as the people who share a flat have to agree on certain basic rules, which objects are kept under lock and key and who can enter it, with a future electrical network it will be necessary to negotiate the security rules that the system has to impose. Owing to the large number of participants and the system's dynamics, this leads us to the need for every party to write down its security or privacy *policies* in a language that can be automatically processed. Thus, a smart system can analyse the preferences of the participants and find suitable compromises.

It is important to remember that it is impossible to build a complex system, based upon information technologies, which are completely secure. What we need is for it to be reliable enough, that we have credible evidence that a set of requirements is going to be complied with. Security is not a static subject. If we find method today to protect us from attacks such as the Stuxnet one or another particular one, using programmes that verify certain conditions in the memory or in the programmes that can be run, it is possible to think that the future versions of the Trojan first attack our defence security systems, the detection and monitoring programmes, and they then attack the system of interest. In such a case, it will be equally possible to build defences against that attack and so on, successively. The security risks that organisations confront are being sorted out but new ones are equally appearing, which are very often more complex. Security requires continuous processes of making it secure, monitoring, scrutiny, verification and much more. In an open system in particular, such as Smart Grids will be, it is necessary to involve all of the participants, including the general public, in the security processes. So as to protect it against intruders and thieves, it is not enough to duly close all of the gates with all types of padlocks, but no window can be left open either. Like a thief that comes in through a bathroom window, he could go through to the living room or the bedrooms, a cybernetic intruder can come in through a computer, search there for passwords or codes, and move on to another more important one and then to another one that is perhaps vital.

## *Security Measures in Smart Grids*

The security of an information processing system is implemented with a set of *preventative* measures that try to shield and protect both the particular information, and the information processing services, as well as *reactive* measures that help to recover the correct state in the case of a critical event. For all of the protection that we take, is important to take account of the fact it is impossible to avoid all of the security defects or faults, which is the vulnerabilities. If an attacker finds ways of accessing these, the attacks are going to be inevitable and it is necessary to take measures to make the risks manageable.

The security cycle can be separated into four tasks: first, to facilitate the security process that involves defining a security strategy, policies and rules, roles and responsibilities, processes, education and training; second to build secure systems, use adequate protection technology, define a security architecture, implement and configure this with a secure coding and good practices; thirdly, evaluate both the security processes and the individual security of the systems and, in particular, the presence of vulnerabilities and faults, for example by using penetration tests (pen-tests); and fourth, to respond, detecting and analysing security incidents and reacting quickly so as to establish the usual functioning and minimise the impact of the incidents.

### Facilitate the security processes

The first task, that of facilitating security processes, corresponds to the bodies and the functions of business (or corporate) governance. Within each company that takes part in the electrical supply, there must be one unit that has the commitment of the company management and its financial support. This unit, and its head in particular, a top level executive, the CISO (chief information security officer) is responsible for following tasks:

I. Define control roles and responsibilities. It is necessary to define who is the person responsible for the information and for the company's relevant processes.

II. Define the internal policies. The policies outline the conduct of all of the players that have direct or indirect access to the system and, in particular, the critical data or processes. Those people in charge of the running and management have to take part in treating the security checks that must be applied to its systems.

III. Provide feasible and proven action plans and resources. The security policies and processes defined must be crystallised in the form of specific plans where the administrators, system proprietors, the security staff in the organisation and, in particular, the emergency response team all participate. The physical and economic resources, as well as the teams of experts and the support services, have to be properly confirmed by the risks analysis, and once these have been justified, they must be furnished.

IV. Establish a continuous analysis and risks management process. As well as establishing the process, the security governance also has to decide what is the right way of handling the risks. In order to determine the risks, it is necessary to conduct a detailed study of the system's facilities, the consequences that the attacks may have on the physical processes and the integrity of the elements, functions and services of the system, as well as the information flows, that is to say, how the relevant information is identified, captured or measured, and the data that need to be protected. In addition, it is necessary to determine realistic attacker models, and it is necessary to decide what is the right reaction, e.g. avoid, mitigate or accept the risk. In very general terms (when the organisation dispenses with the possibility of exposure to the risk, avoiding the reason that gives rise to it), mitigate (the consequences of the risks can be lessened to some degree by security measures), can be transferred (for example, the costs resulting from a risk acceptable to insurance companies are transferred), or these are responded to (in the case of an incident, the resulting risk may be minimal, if the response to the incident is adequate). The decision has to be characterised by the recognition of the existence of the risk, and the agreement to assume the losses involved.

V. Determine the methods to evaluate the effectiveness of the checks and of the monitoring. It is necessary to know how adequate are the existing security checks and tools, the intrusion detection processes, regarding vulnerabilities and incidents. We should recall that we have seen malware that has spent several years undetected.

VI. Guarantee the reporting of each step in every general security process. In order to be able to learn from the security events, whether these are findings of violations of policies or the presence of vulnerabilities or of incidents, it is necessary to protocolise in detail not just the corresponding situation, but also the analyses that were attained during and after the event, the measures that were taken, etc. Also it is regularly necessary –with no particular reasons– to describe the processes used and the results obtained.

VII. Continuously identify opportunities to improve security. The regular reports, discussion via security groups such as the Computer Security Emergency Response Team (CSERT), must be scrutinised in the search for improvements to security or the evaluation.

VIII. Define a revised and approved legal strategy. Security incidents may have various consequences, and even criminal ones on many occasions. Security planning has to be developed with members of the legal consultancy team. The legal consultancy has to have knowledge about the legal consequences of a violation, the value and the hazards of a client's personal information, medical or financial procedures. The local state or federal regulations will at least partly dictate the methodology to carry out the post-mortem analysis.

### Build secure systems

Organisations have to adopt a comprehensive set of security checks so as to protect their information and information systems. The purpose of the security architecture is a holistic vision of the system's security requirements, of the mechanisms that make them secure and how they are integrated into the global architecture.

### Evaluate the security and the processes

In order to comprehend the effectiveness the evaluation methods, it is convenient to use profound and far-reaching tests in controlled laboratories for systems that are highly important, intrusion tests (penetration test) and white box tests, both automatic and systematic reviews of the source code, using so-called honeypots, software or hardware that is meticulously monitored, whose intention is to attract attackers, simulating being productive systems, and comparing the risks calculated with the actual incidents observed. It is important to compare these with external evaluation methods so as to help the local team, participate at laboratories that work together in studying vulnerabilities.

### Respond

The impossibility of avoiding all types of security defects or faults makes it essential to create a computer emergency response team, as well as draft an incidents response plan. This will not only minimise the effects of an intrusion or attack, but the same applies for adverse publicity. An incidents response plan must have the support of and participation of the entire organisation and it must be frequently tested. The response plan has to recognise security incidents, that is, those unexpected or undesirable situations as compared to the system protection targets. However, its priority aim is to be detecting the incident, immediately restoring the expected state and the resources affected and limiting the damage throughout the organisation. Given that, in the case of an incident, there is very little space for errors; emergency actions have to be quickly and swiftly taken. One important element is the forensic analysis that facilitates the recognition of the attack or intrusion process and of the vulnerabilities, faults or neglect that led to the incident. This analysis is increasing the experience of the security team and of its capacity to respond to adverse conditions in a swift, formal and opportune manner, on the basis of the experience acquired. Lastly, it is necessary to give appropriate instructions for treating the causes and reporting the incident via suitable channels.

## *Challenges*

There are many challenges related to the protection of future energy networks, and there are a lot of steps to be taken by the different parties that are involved or interested: the equipment manufacturers or vendors, the energy production and distribution infrastructures operators, the companies that provide information services and other ancillary or additional services, the security system vendors, the security investigators, the standardisation organisations, the state organisations, etc.

We divide these challenges into seven different groups: the technical operation and infrastructure aspects, the operating aspects of the infrastructure and its related processes, the education, dissemination and awareness raising, the exchange of information, the creation of standards, guides and regulation, the research and development of new solutions and the protection of the privacy of personal data.

### Technical aspects of operation and of infrastructure

The equipment manufacturers and the operators must work together so as to find and define technical incidents prevention solutions. This has to result in a collection of security mechanisms that are to be implemented and integrated during the production of the equipment, and additional mechanisms and the configuration of parameters, passwords, etc. during the deployment of the systems.

I. Definition of a security architecture. The operators, together with the vendors of security services and equipment, will analyse in detail all of the risks, and accordingly design a "security architecture" that is suitable for the operating systems.

II. The implementation of security programmes for industrial control systems that are open to Internet networks could be very costly. Many operators make use of controls that compensate for the lack of intrinsic control mechanisms, so as to prevent the investment of large sums of money in renewing equipment, old devices, operating systems and general software. The two requirements for facilitating this route are: on the one hand, it is necessary to create versions of products with limited functionality and that offer few but sufficient options for some specific SCADA systems. On the other hand, it is necessary to design a deep defence architecture, that is, the inclusion of multiple layers of protection and overlapping security mechanisms, which act as various barriers against attackers. This focus constitutes a good route for protecting industrial control systems.

III. A fundamental aspect of the security architecture is provided by the systems' remote access protection mechanisms. Remote access for control systems by the vendors or management staff for maintenance tasks exposes some aspects of the architecture to external manipulation.

IV. Secure programming. The hardware and software manufacturers of industrial control systems must apply the right methodologies and rules of secure programming during the system's development cycle.

V. Analysis of the security requirements throughout the entire life cycle of the systems. Security requirements must be included from the outset, in the specifying and analysis of the system. In other words, security must accompany the development of the system and not become a set of additional mechanisms for compensating for the security defects found that are due to a lack of foresight.

VI. Consideration of the system's lifecycle. The software and hardware for offices has a lifecycle of between three to five years. In industrial control systems, which are designed for a very specific purpose, the lifecycle could last much longer. This is why it is hard to ensure the components of the industrial control systems continuously throughout the lifecycle against new security attacks. Thus, it is necessary to have detailed plans so as to be able to modify the systems being produced.

### Operating aspects of the infrastructure and related processes

We include the systems operators' activities here. This includes the provision of physical security, the governance of security (in particular: definition and application of roles and responsibilities), crisis management and risks management. The education of rising of awareness of the employees and users is considered to be a separate issue here. This is because it is an activity that is not the operators' responsibility, but also the system's protagonists.

I. Establishing of comprehensive security programmes. The operations of transmission and distribution networks have to set up comprehensive security programmes, which include all of the processes and equipment, of both the desktop and commercial and control computing of the industrial systems. Many organisations have designed cyber security programmes for commercial computing systems, but the security management practices are not properly adapted for the industrial control systems.

II. Hardening. During the installation of equipment, it is necessary to eliminate the modules and services that are unnecessary, select the most secure configuration of parameters and SW versions that are best suited. This is fundamental for reducing the surface area of attacks and, hence, the risks.

III. Changes control management. As internal or external incidents reports appear, as well as the vulnerabilities discovered, or SW patches, it is necessary to review the system configuration, the parameters of SCADA systems and programmable logic controllers (PLC), the versions of firmware, properties, files or any other programme or application. Adequate management is especially important with the aim of preventing interruptions or serious problems in industrial control systems.

### Education, dissemination and awareness rising

All of the protagonists at all levels have to take part in the work on education and raising awareness, including the top ranks of the companies involved.

I. Education awareness raising and conscientiousness campaigns. It is imperative to create a culture that is conscious of the topics pertinent to security, above all achieving a certain level of profundization of the necessary knowledge, above all concerning the risks, the recognised procedures that encourage security, as well as the practices that endanger it. With this aim in mind it is necessary to define and implement education programmes for the staff of industrial control systems, and campaigns of raising awareness and conscientiousness for end users and the services providers.

As we have seen, many attacks could be avoided if the staff and other protagonists in the system act by imposing rules of conduct that are not always evident. For example, spear-phishing tries to mislead the victim with a piece of information (a link to a web site or an attachment in an electronic message) that is apparently interesting to him. It is not just that the company has to have policies on the reactions in such cases, but also the employee who has to know about such rules and understand their value in protecting the system.

### Information exchange

It is not easy for critical infrastructures operators to cooperate in detecting attacks and to share information about incidents. The European Community is looking for new ways of incentivizing this form of cooperation, studying the possibility of creating test banks and a *Computer Emergency Response Team* for industrial control systems (CERT) for coordination, going beyond the diversity of capacities that the different countries and organisations of the community have, as well as legal, strategic and private interest problems.

I. Creation of evaluation groups. Industrial control systems incidents have to be used as the basis for updated evaluations of risk, of possible corrective measures and those of re-assigning resources. Both manufacturers and operators need to tackle the challenge of creating analysis committees that meet up regularly so as to discuss security risks and re-evaluate the risks. Those teams also have the requirement –in addition to the expert security staff and the procedural engineers– of people in middle management posts and must have the unconditional support of the senior management.

II. Information exchange. New vulnerabilities are discovered every day in the software of industrial control systems. The operators need to be ready to face up to these new problems. At the same time, the manufacturers of industrial control systems have to offer swift and effective responses for the need to create and distribute patches and vulnerability reports. Business, and academic and independent research need to work together, making it possible for the manufacturers to correct their systems before making the information public.

### Standards, guides and regulation

I. Incentives, rules, legislation and regulations. The European Community studies ways of compelling or at least of motivating operators to adjust themselves to inspections of industrial control systems and risk analysis. The North American regulation is led by the organisations FERC and NERC.

II. Auxiliary guides**.** In addition to the previous rules, it is necessary to define auxiliary guides, which include a set of security and good practices controls, which are compensatory alternatives and supplementary processes. Examples of the topics included in these guides may be: account management, separation of functions, the principle of minimum privilege, concurrent control sessions, remote access, contingency tests and plans, changes of control, maintenance instruments, remote maintenance, protection against malicious codes, tests methods, etc.

III. Standardisation. It is necessary to define and standardise flexible and elegant solutions for the specific purposes of Smart Grids and to analyse whether it is necessary to define a set of basic secure communication protocols, adapting a suitable cryptographic system for the requirements, but allowing for the introduction of new algorithms when necessary.

IV. Certification. The three preceding points can –and in many cases they ought to- be accompanied by certification processes, either mandatory or optional, which confirm the conformity with the corresponding guides.

### Research and development of new solutions

I. New solutions. Security investigators have to develop new techniques and solutions for control and supervision systems and other elements of Smart Grids. This has to include forensic methods, automatic techniques that are non-intrusive and provide for real time monitoring that makes best use of the unique type of systems used. It will also be convenient to define communication and cryptographic protocols, as well as compensatory controls that are adapted to the needs of future energy distribution, for both large pieces of equipment that are specific and for devices with few computing, storage or battery resources.

### Protection of the privacy of personal data

I. Privacy. In today's world, it has already been demonstrated in medical or commercial systems that ensuring user privacy is an immense difficulty. One particularly relevant challenge in Smart Grids will be that of having to administer an unprecedentedly huge amount of data, and at the same time to ensure the anonymity and the privacy of many of these.

## Conclusions

Electrical supply Smart Grids will become a reality. There is heavy pressure in the modern world that force us to follow this technological development, which has been described as humanity's largest engineering endeavour. The use of information and communications technologies (ICT) is essential but this will entail new security risks. It is practically impossible to calculate the actual likelihood of a serious attack taking place today, now or in the future, on the electrical supply system of a developed country, or know what the equipment or functions are that will be targeted for attacks. The most important thing is not to try to build completely secure systems. This would be an unattainable ideal and a futile enterprise. Instead, it would be better to have a holistic concept of security that determines which processes to follow in order to prevent the attacks or make them difficult, which tools to use in order to swiftly recognise them, and which actions to take in order to respond to and recover normal functioning in the shortest possible time, and before wreaking havoc. The security challenges are great but possible to manage. They are a call of coordinated and determined action by our society.

## Bibliography

Akyildiz, I.F; Weilian, Su; Sankarasubramaniam, Y. & Cayirci, E., A survey on sensor networks., SISS Communications Magazine, 40, 8, August, 102 -114, 2002

Anagnostakis, K.G.; Sidiroglou, S.; Akritidis, P.; Xinidis, K.; Markatos, E. & Keromytis, AD, Detecting targeted attacks using shadow honeypots, 9, 2005, Proceedings of the 14th conference on USENIX Security Symposium-Volume 14

Anderson, Ross, Why Information Security is Hard-An Economic Perspective, Computer Security Applications Conference, Annual, 0, 358, 2001, Los Alamitos, CA, USA, SISS Computer Society

Anderson, Ross & Fuloria, Shailendra, Who controls the off switch?, October, 2010, SISS International Conference on Smart Grid Communications

Anderson, Ross & Kuhn, Markus, Low cost attacks on tamper resistant devices, Security Protocols, 1361/1998, 125--136, 1998, http://dx.doi.org/10.1007/BFb0028165

Anderson, Ross J., Security Engineering: A Guide to Building Dependable Distributed Systems, 2008, http://www.cl.cam.ac.uk/~rja14/book.html, Second, Wiley Publishing

Aycock, J., A design for an anti-spear-phishing system, 2007, 7th Virus Bulletin International Conference

Barnes, Ken & Johnson, Briam, Introduction To SCADA Protection And Vulnerabilities, INEEL/EXT-04-01710, March, 2004, http://www.inl.gov/technicalpublications/Documents/3310860.pdf, Idaho National Engineering and Environmental Laboratory

Bishop, Matt, Computer Security: Art and Science, 2003, Addison-Wesley

Carl, Glenn; Kesidis, George; Brooks, Richard R. & Rai, Suresh, Denial-of-Service Attack-Detection Techniques, SISS Internet Computing, 10, 1, 82-89, 2006, Los Alamitos, CA, USA, SISS Computer Society

Cohen, F, The smarter grid, 8, 60-63, 2010, Proceedings of SISS Symposium on Security and Privacy

Cohen, Fred, Simulating cyber attacks, defences, and consequences, Computers \& Security, 18, 6, 479 - 518, 1999, http://www.sciencedirect.com/science/article/pii/S0167404899801151

European Council Directive 2008/114/EC of the Council on the Identification and Deisgnation of Critical European Infrastructures and the Evaluation of the Need to Improve ther Protection, http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/jl0013_es.htm

Creese, Sadie; Goldsmith, Michael H. & Adetoye, Adedayo O., A Logical High-Level Framework for Critical Infrastructure Resilience and Risk Assessment, September, 2011, Milan, Italy, The 3rd International Workshop on Cyberspace Safety and Security (CSS 2011), To appear

ENISA, CERT cooperation and its further facilitation by relevant stakeholders, Deliverable WP2006/5.1(CERT-D3), http://www.enisa.europa.eu/act/cert/background/coop/files/cert-cooperation-and-its-further-facilitation-by-relevant-stakeholders/at_download/fullReport

ENISA, ENISA Smart Grid Security Recommendations, https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/smart-grids-and-smart-metering/ENISA-smart-grid-security-recommendations/at_download/fullReport

Ericsson, G.N., Cyber Security and Power System Communication 2014;Essential Parts of a Smart Grid Infrastructure, Power Delivery, SISS Transactions on, 25, 3, 1501-1507, 2010

Igure, Vinay M.; Laughter, Sean A. & Williams, Ronald D., Security issues in SCADA networks, Computers \& Security, 25, 498--506, 2006

Inger Anne Tøndel, Martin Gilje Jaatun, Maria Bartnes Line, Security Threats in Demo Steinkjer - Report from the Telenor-SINTEF collaboration project on Smart Grids, http://www.demosteinkjer.no/attachment.ap?id=2

Kalogridis, G.; Efthymiou, C.; Denic, S.Z.; Lewis, T.A. & Cepeda, R., Privacy for Smart Meters: Towards Undetectable Appliance Load Signatures, 232-237, 2010, Smart Grid Communications (SmartGridComm), 2010 First SISS International Conference on

Khurana, H.; Hadley, M.; Lu, Ning & Frincke, D.A., Smart-grid security issues, Security Privacy, SISS, 8, 1, 81-85, 2010

Koepsell, Stefan; Wendolsky, Rolf & Federrath, Hannes, Revocable Anonymity, Emerging Trends in Information and Communication Security, 206-220, 2006, http://dx.doi.org/10.1007/11766155_15

Liu, Yao; Ning, Peng & Reiter, Michael K., False Data Injection Attacks against State Estimation in Electric Power Grids, 2009

Lu, Zhuo; Lu, Xiang; Wang, Wenye & Wang, C., Review and evaluation of security threats on the communication networks in the Smart Grid, 1830-1835, 2010, MILITARY COMMUNICATIONS CONFERENCE, 2010 - MILCOM 2010

McDaniel, P. & McLaughlin, S., Security and Privacy Challenges in the Smart Grid, Security Privacy, SISS, 7, 3, 75-77, 2009

McGraw, Gary, Software Security, SISS Security and Privacy, 2, 2, 80-83, 2004

Metke, A.R. & Ekl, R.L., Security Technology for Smart Grid Networks, Smart Grid, SISS Transactions on, 1, 1, 99-107, 2010

Microsoft, Spear phishing: Highly targeted phishing scams, http://www.microsoft.com/protect/yourself/phishing/spear.mspx

Minghan, Zou & Yun, Miao, Summary of Smart Grid Technology and Research on Smart Grid Security Mechanism, 01.Apr, 2011, Wireless Communications, Networking and Mobile Computing (WiCOM), 2011 7th International Conference on

Ministry of Defence, Cyber security. Challenges and Threats to National Security in Cyber Space, Strategy Journals Nr. 149, http://bibliotecavirtualdefensa.es/BVMDefensa/i18n/catalogo_IMAGEes/grupo.cmd?path=17029

Ministry of the Interior, 8/2011 Act, of April 28, whereby measures are established for the protection of critical infrastructures, http://www.boe.es/diario_boe/txt.php?id=BOE-A-2011-7630

Ministry of the Interior, Royal Decree 704/2011 whereby the Regulation for the Protection of Critical Infrastructures is passed into law, http://www.boe.es/diario_boe/txt.php?id=BOE-A-2011-8849

Mo, Yilin; Kim, T.H.-H.; Brancik, K.; Dickinson, D.; Lee, Heejo; Perrig, A. & Sinopoli, B., Cyber-Physical Security of a Smart Grid Infrastructure, Proceedings of the SISS, 100, 1, 195-209, 2012

NERC, CIP-009-4: Cyber Security — Recovery Plans for Critical Cyber Assets. North American Electric Reliability Corporation (NERC), http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

Ogwu, Francis Joseph; Talib, Mohammad; Aderounmu, Ganiyu & Adetoye, Adedayo, A Framework for Quality of Service in Mobile Ad Hoc Networks, Int. Arab J. Inf. Technol., 4, 1, 33-40, 2007

Paar, Christof & Weimerskirch, Andre, Embedded Security in a Pervasive world, Information Security Technical Report, 12, 155--161, 2007

Palmer, Graham, De-Perimeterisation: Benefits and limitations, Information Security Technical Report, 10, 4, 189--203, 2005, http://www.sciencedirect.com/science/article/B6VJC-4HNF68X-3/2/65c03ea72fa1ff3c61a53447fc8dd9ca

Rifkin, Jeremy, The Third Industrial Revolution: How Lateral Power is Transforming Energy, the Economy, and the World, 304, 2013, Palgrave Macmillan

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

Symantec, W32.Stuxnet Variants, http://www.symantec.com/connect/blogs/w32stuxnet-variants

Wack, John; Tracy, Miles & Souppaya, Murugiah, Guideline on Network Security Testing, {NIST} Special Publication, 800, October, 42, 2003, http://csrc.nist.gov/publications/nistpubs/800-42/NIST-SP800-42.pdf

Wang, Wenye & Lu, Zhuo, Survey Cyber Security in the Smart Grid: Survey and Challenges, Comput. Netw., 57, 5, April, 1344-1371, 2013, New York, NY, USA, http://dx.doi.org/10.1016/j.comnet.2012.12.017, Elsevier North-Holland, Inc.

Wang, Yong; Ruan, Da; Gu, Dawu; Gao, J.; Liu, Daming; Xu, Jianping; Chen, Fang; Dai, Fei & Yang, Jinshi, Analysis of Smart Grid security standards, 4, 697-701, 2011, SISS International Conference on Computer Science and Automation Engineering (CSAE), 2011

Yang, Y.; Littler, T.; Sezer, S.; McLaughlin, K. & Wang, H.F., Impact of cyber-security issues on Smart Grid, 01.Jul, 2011, 2nd SISS PES International Conference and Exhibition on Innovative Smart Grid Technologies (ISGT Europe),2011.