RAIN – Risk Analysis of Infrastructure Networks in Response to Extreme Weather

Project Reference: 608166

FP7-SEC-2013-1 Impact of extreme weather on critical infrastructure

Project Duration: 1 May 2014 – 30 April 2017

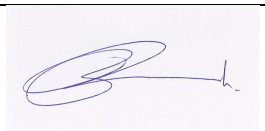
Security Sensitivity Committee Deliverable Evaluation

Deliverable Reference	**D 4.1 version 2.3**
Deliverable Name	**Electrical & Telecom Infrastructure description and identification of critical elements and threats**
Contributing Partners	**Grupo AIA**
Date of Submission	**2015-05-05**

- **The content is not related to general project management**
- **The content is not related to general outcomes as dissemination and communication**
- **The content is related to critical infrastructure vulnerability or sensitivity**
- **The content is publicly available or commonly known**
- **The content does not add new information on vulnerabilities, sensitivities or incident scenario's on specific objects or transport systems or assets in general**
- **There are no uncertainties that need to be discussed with a NSA**

Diagram path: 1-2-3-4-5.1-5.2-9. Therefor the evaluation is: Public.

Decision of Evaluation	**Public**	~~**Confidential**~~
	~~**Restricted**~~	

Evaluator Name	**P.L. Prak, MSSM**
Evaluator Signature	
Date of Evaluation	**2015-05-22**

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608166

This project is funded by the European Union

RAIN – Risk Analysis of Infrastructure Networks in Response to Extreme Weather

Project Reference: 608166

FP7-SEC-2013-1 Impact of extreme weather on critical infrastructure

Project Duration: 1 May 2014 – 30 April 2017

Electrical & Telecom infrastructure description and identification of critical elements and threats

Authors

Milenko Halat* (Grupo AIA)

Vicens Gaitán(Grupo AIA)

***Correspondence author: Av. de la Torre Blanca, 57.**

E-08172 Sant Cugat, Barcelona, Spain. halatm@aia.es, +34 935 044 900.

Date: 19/03/2015

Dissemination level: (PU, PP, RE, CO): CO

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608166

This project is funded by the European Union

DOCUMENT HISTORY

Index	Date	Author(s)	Main modifications
1.0	March 2015	Vicens Gaitán Milenko Halat	First version
2.0	2015-03-31	Zdenek Dvorak Maria Luskova	UNIZA review
2.1	2015-04-08	Vicens Gaitán Milenko Halat	Revise after UNIZA review. Complete bibliography and figure sources.
2.2	2015-04-14	Billy Brazil	Miscellaneous comments and proof editing
2.3	2015-05-05	Nico Becker Katrin Nissen Milenko Halat	Final proof editing and review

Document Name: "Electrical & Telecom infrastructure description and identification of critical elements and threats"

Work Package: WP4

Task: 4.1

Deliverable: D4.1

Deliverable scheduled date: January 2015

Responsible Partner: Aplicaciones en Informática Avanzada, S.L. (AIA)

Executive Summary

This deliverable examines the electricity and telecom network infrastructures in the context of the RAIN Project. It is introductory in nature, and has the following goals:

1. Provide an overall description of the two Critical Infrastructures (CI) elements:
2. Identify the CI elements and their (weather related) threats:
3. Provide a first scheme of interdependencies with other CI:
4. Describe a few selected representative examples

The descriptions of these two infrastructures are necessarily somewhat technical in nature, but the basic principles governing them and their topological structure can be easily understood. A certain level of technical understanding is necessary in order to extract meaningful risk analyses concerning extreme weather events.

Power networks transport the electricity generated at power stations (from sources such as nuclear, fuel, gas, hydro, wind, solar, etc.) to consumers across very large distances and with relatively low losses (averages around 8% for transmission plus distribution). Topologically speaking, the grid is structured in two levels: (a) The transmission part, otherwise known as the bulk electric system which operates at very high voltages, carries large amounts of power over large distances, and has a meshed structure that confers it a certain level of resiliency against the loss of any one node (i.e. substation) in the network. (b) The distribution part which operates at medium and low voltages and has a "radial" structure (i.e. tree-like), and therefore less resiliency against node failures. Operational resiliency is, in general, weak, even in transmission. This is attested to by the increasing frequency of power blackouts. This is because power generation needs to be carefully coordinated in order to match the power demand at all times, with real-time response. This in turn needs human monitoring and control via SCADA[1] systems at Control Centres. The diminishing amounts of transport capacity margins in an ageing transmission grid, together with the steady growth in demand, result in a network that is operated closer to its limits and is therefore more prone to disturbances and voltage collapse.

Telecom networks transport information (voice, video, and data) across very large distances across the globe. They do so over different type of media such as: Overhead lines vs. underground/submarine cables (either copper or fibre optics) and radio links vs. satellite links. This infrastructure inherits a lot from the traditional telephone network (PSTN), which dominated the telecommunications world for most of the 20th century. However, this has been changing very rapidly in the last 20 years due to convergence with the world of computing, data networks, and the Internet. Structurally these networks also have: (a) A "transmission" section, which is composed of large switching centres interconnected by backbone lines, forming a meshed topology built for redundancy; and (b) a distribution section having a tree-like topology, reaching the end customers at each end. The routing of flows and the real-time management of margin capacities are a much

[1] Supervisory control and data acquisition. See a brief glossary of terms at the end of the document.

smaller issue here, in comparison to the power grid. Most of the operation is automated and, thanks to the hyper-convergence of all technologies towards Internet-like principles (packet-switching, TCP/IP), resiliency against partial failures is comparatively high. On the other hand, when facing natural disasters such as windstorms, lightning, extreme heat, etc., the electronics equipment found in telecom networks can be substantially less robust than power lines and transformers. Moreover, they are dependent on electric power supply for their operation. A worrying trend is the concentration of exchange nodes in the so-called *Carrier Hotels* (several Telco companies sharing the same building), presenting a serious concentration of risk that is actively counteracting the failure-tolerance benefits of IP networks.

Just like other critical infrastructures networks, electrical and telecom networks are rather expensive and require careful planned studies for their expansion and for the design of their security. However, they have some specific characteristics that are not found in other infrastructures:

- They undergo rapid technological evolution
- The operations are well described by precise formulas or algorithms
- Well-defined parameters exist for monitoring health and "service level" concepts
- A considerable degree of automation exists, but SCADA and real-time human control are still needed for some critical functions
- They are truly *networked* critical infrastructures: more tightly interconnected and therefore prone to suffer long-range interaction effects.

This last point means that when faults arise, problems can propagate far and wide, through cascading failures. A weather-related disaster in the wrong place, and at the wrong time, could spell widespread disaster. The problem is probably more acute in power networks, since it is far more expensive to build redundancy mechanisms into a transmission power grid than it is in Information and Communications Technology (ICT) networks. Telecom networks compare better in this respect as they degrade more gracefully in the event of local failures (except in the case of cyber-security events, which can quickly spread globally).

Therefore, in the case of energy & telecom, probably in contrast with transport networks, the effects of local failures have two equally important components to take into account:

1. The obvious local impacts derived from the loss of service (e.g. the loss of power by a whole neighbourhood due to a flooded substation).
2. The "self-impact" on the rest of the network. This implies an increase in the likelihood of cascading failures, not just locally, but potentially at far away distances as well. Measuring this impact is not easy, in general, as it depends on the current operational state of the network.

The deliverable also describes a few representative cases of weather-related outages, giving an overview of the causes and the impacts on both the population and the infrastructure. Some statistics about outages are also given.

Table of Contents

1. Introduction

There is no doubt that modern society has become highly dependent on Electricity and Telecommunications, to the point that we consider these as highly critical functions. Both of them are provided thanks to large and costly infrastructures (the power grid being the costlier of the two). The European Commission defines a "Critical Infrastructure" (CI) as—"An asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of a failure to maintain those functions" (European Commission 2015). In addition, "European Critical Infrastructure" (ECI) means critical infrastructure located in Member States, the disruption or destruction of which would have a significant impact on at least two Member States[2].

This deliverable is of an introductory nature and examines the Electricity and Telecom network infrastructures in the context of the RAIN Project, with the following goals in mind:

1. **Provide an overall description of the two CI.** This is intended to be a primer for non-experts, in order to provide an adequate level of understanding for the rest of risk-management modellers in the RAIN consortium. The operation of power and telecom grids is highly specialised and technical, but the basic principles can be easily understood.
2. **Identify the CI elements and their (weather related) threats.** We focus only on understanding what the threats are, and how they affect the operation. Subsequent deliverables in WP4 will focus on the protection mechanisms and procedures (D4.2), and on the ultimate social impacts (D4.3).
3. **Provide a first scheme of interdependencies with other CI.** This will be a qualitative overview analysis of how the failures in electrical grids and telecom networks affect each other, as well as other infrastructures under study in the RAIN project.
4. **Describe a few selected representative examples** of weather-related failures in these infrastructures, trying to cover the whole gamut of incidents that may take place (extreme heat, extreme cold, flooding, extreme wind, etc.).

The descriptions of the two infrastructures given in this document are somewhat technical in nature. We firmly believe that, in order to carry out any meaningful risk modelling, it is absolutely necessary to acquire at least a cursory understanding of how Electricity and Telecom networks work. This is most evident in the case of the power grid, where local risks can easily turn into widespread disturbance. Additionally, risks in a power grid are highly context-dependent, that is, they should take into account the *electrical state* of the network at a particular point in time. You may view this as the complete operational picture of the "levels of utilization" of the network: generation inputs, network voltages and flows, and loads. To understand why this is needed, we will explain the

[2] Council Directive 2008/114/EC on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection, Brussels, 08.12.2008, COM(2006) 787 final.

essentials of how the grid works. However, we will try to keep the technical discussion focused only on those aspects relevant to abstract risk modelling.

Common themes that characterize the Electricity and ICT infrastructures, in contrast to those in Transport[3], are:

- Operations are well-described by precise formulas or algorithms
- Well-defined parameters exist for monitoring health and "service level" concepts
- A considerable degree of automation exists, but SCADA and real-time human control are still needed for some critical functions
- Higher interconnectedness means it is potentially easier to bring down the whole grid (although, in the case of ICT, convergence towards TCP/IP has mitigated this).

Compared to transportation infrastructures, it may be argued that the power grid and telecom networks appear to be more resistant to extreme weather events, but on the other hand, as a network, they lack a good "graceful degradation" behaviour. When faults arise, problems can propagate far and wide, through cascading failures (Lewis 2015). A weather-related disaster in the wrong place, at the wrong time, can spell widespread disaster. The problem is more acute in power, since it is far more expensive to build redundancy mechanisms in a transmission power grid than it is in ICT networks. We all have experienced this in the form of large-scale blackouts that sometimes have spanned across several countries in Europe (Silvast and Kaplinsky 2007).

We hope that by focusing the descriptions of these two infrastructures on their behaviour as *networks*, we will better support the joint work on modelling risks and interdependencies with the rest of the infrastructures studied in the RAIN Project.

About the impacts of failures in Electricity & Telecom networks: local vs. global

Since power and telecom infrastructures are tightly networked, local failures have the potential to cause significant effects in the network at **far away locations**, and with **nearly instant propagation**. Telecom networks compare better in this respect as they degrade more gracefully in the event of local failures (except in the case of *cyber-security* events, which can quickly spread globally). Power grids, on the other hand, degrade more abruptly, and are more likely to end up in widespread blackout. However, in both cases the key idea is that a single failure has the potential to immediately change the physical state of large parts or even the whole network (e.g. increasing flows at stressed paths, or rerouting traffic and overflowing routers) and, as a consequence, immediately increase the likelihood of further network failures both locally and globally.

Therefore, in the case of Energy & Telecom, in contrast with Transport, the effects of local failures have two equally important components:

[3] Please see RAIN Deliverable 3.1, which is the counterpart of this D4.1 focused on the Transport Infrastructure.

a) Obviously, the local impacts derived from the single-mode failure (e.g. the loss of power by a whole neighbourhood due to a flooded substation).
b) The impact on the rest of the network. It is true that some failures in transport (e.g. a critical junction) may impact the rest of the network, but this does not happen with the degree of pervasiveness, long range, and instantaneous effects that we encounter in Energy & Telecom. This implies an increase in the likelihood of cascading failures, not just locally but potentially at far away distances. Measuring this impact is not easy in general, because it depends on the current operational state of the network.

Although it would be tempting to analyse only impacts of type (a), there is a case to be made for assessing this second type of impact as well. The risk of cascading failures spreading to distant locations is probably the best reason. In this respect, we note that the mindset of network operators of these two infrastructures is heavily biased in favour of the health of the whole networked infrastructure, to the detriment of local supply. In the event of failures, operating procedures and automatic protections are designed first and foremost to protect the network, and then deal with the restoration of local service afterwards. This is simple economics, as permanent damage to lines, transformers, or switchgear would incur in a very high cost *and* risk a loss of service for a much longer time. The topological structure of these networks has also been designed with this in mind, with a transport-level part having a graph-like structure for redundancy, and a distribution-level part having a tree-like structure, since problems get more easily isolated at this level.

Some final comments about another difference between Energy & Telecom networks and the Transport infrastructure, with the only exception of nuclear power, failures in these two networked infrastructures never put human lives in danger; at least not among the general public, in a direct way[4]. The impacts are almost always indirect, deriving from the loss of service. These impacts could be rather serious, but there is at least some response time in order to avoid human casualties. This is why outage time is an important measure of the impact of failures in these two infrastructures (the other one is just the amount of service lost, be it power or subscriber lines).

[4] Proper observance of rights-of-way regulations should in principle avoid high-voltage lines falling on people.

2. Electrical Power Networks

2.1 General description and architecture

The power grid has been hailed by the US National Academy of Engineering as the most influential engineering innovation of the 20th century (Constable and Somerville 2003). According to the Academy, the power grid surpassed the invention of the automobile, the airplane, spacecraft, the atomic bomb, the delivery of safe and abundant water, and electronics as the most important engineering accomplishment. Indeed, electrical power is what makes modern society tick. We have become so dependent on grid power that a power blackout lasting more than a few days could send us temporarily back to the dark ages. Recent high-profile blackouts have raised a new level of awareness to this problem, but despite all talk about distributed micro-grids and generation, the power grid will remain a critical infrastructure of modern society, for a long time.

Electric power transmission is the bulk transfer of electricity from one place to another. Typically, power transmission occurs between a power generation facility and a substation located in close proximity to consumers. Power distribution refers to the delivery of electricity from a substation to consumers located in residential, commercial, and industrial areas.

The science and technology necessary to produce electric power and transport it over long distances was developed a long time ago. In the late 1880s, Edison and Tesla engaged in what is now known as the "War of Currents", a bitter dispute over the superiority of AC (alternating current) versus DC (direct current). By the mid 1890s, Tesla won the argument with AC, because back then it was far more energy-efficient than DC technology. The main reason is that it is far easier to step voltages up or down in AC, using transformers. By contrast, energy-efficient DC "transformers" (actually called DC-DC converters) were not possible until the advent of power semiconductor electronics. Another reason was that AC electric motors were also more efficient than DC ones at the time (again, efficient DC motors for high power applications became available much later, thanks to electronics and strong rare-earth permanent magnets).

Due to the physics of power losses, high voltages are essential for the efficient transport of power over long distances. Power is the product of current and voltage, therefore, for a given amount of delivered power, the higher the voltage, the lower the current. Since the power losses on transmission lines are proportional to the square of the current, high voltages achieve very low losses. Thanks to the relative simplicity of voltage transformation in AC power (a transformer is basically a huge pair of coils around a massive chunk of iron), it is possible to transport gigawatts of power over distances of 500 Km and more, with overall energy losses of 8% or less. This is quite an achievement, especially when we compare it against any other energy-delivery mechanism devised by human civilization[5].

[5] Here we are referring only to the efficiency in the transport of electrical power. Large inefficiencies exist when producing electricity from primary energy sources such as fossil fuels, of course.

On the other hand, electrical energy storage is an unsolved problem. Notwithstanding pumped-storage hydro reservoirs, there is currently no way to store electrical energy at the scale that is needed by power utilities. As a consequence, electricity has to be generated precisely in synch with the real-time demand. This imposes a great deal of burden on the operation of power grids, as the production has to be carefully scheduled in advance (according to forecasts of aggregate demand) and then carefully monitored and regulated to account for real-time deviations (Brown and Sedano 2004).

Figure 1 shows a schematic view of the whole power grid infrastructure, from generation (power stations), transmission lines, distribution lines, to the final customers, commonly referred as *loads*. Transmission-level voltages are generally considered those above 110 kV. Voltages between 110 kV and 33 kV are typically considered sub-transmission voltages, but are occasionally used for long transmission systems with light loads. Voltages of less than 33 kV are representative of distribution projects. The so-called *substations* are the nodes of the network, where several lines join and where voltage transformation takes place.

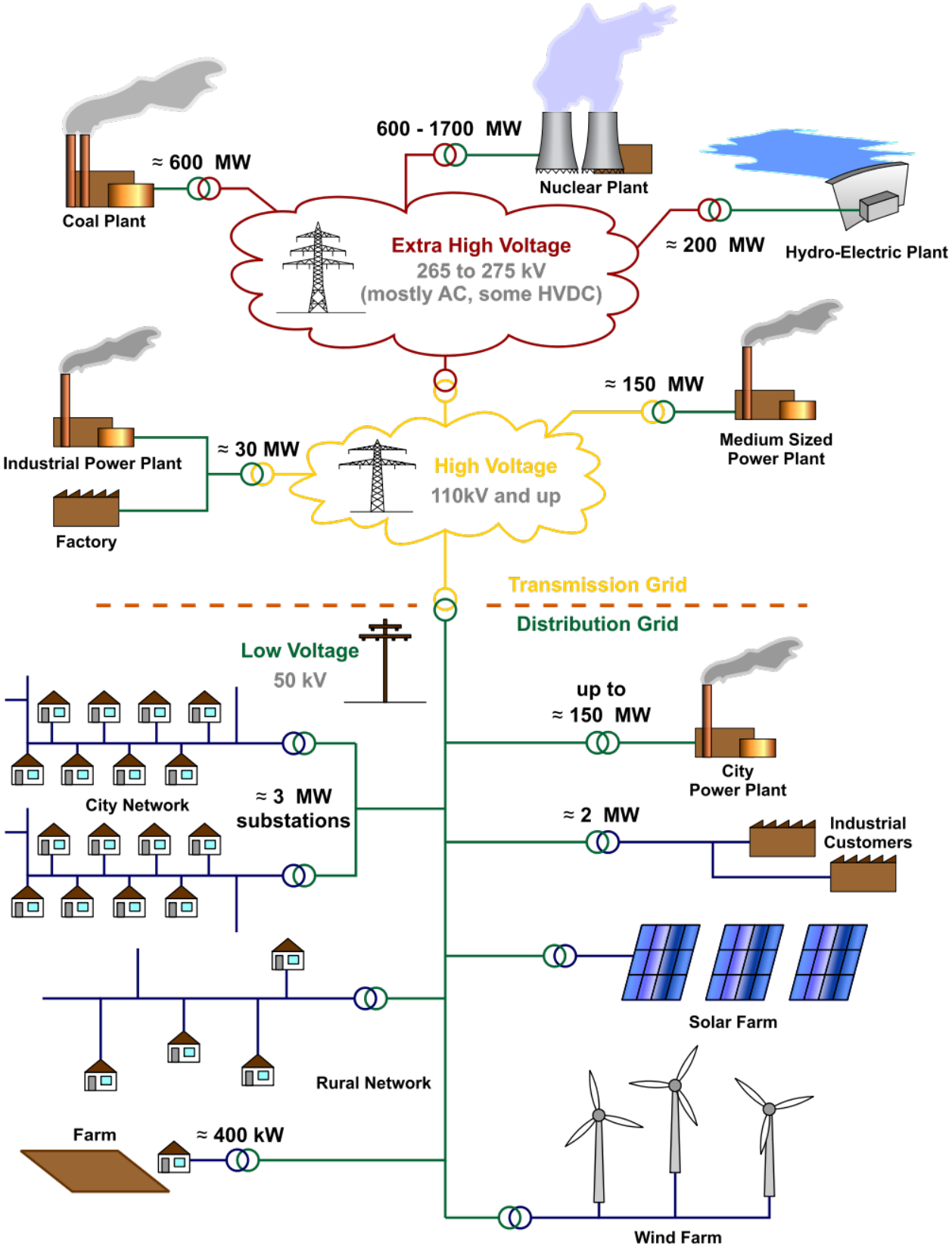


Figure 1. View of the electric power network infrastructure (source: Wikipedia). The two "clouds" depicting transmission are really a meshed network, which gives the power *grid* its name.

We now describe each of the main components of the electrical power infrastructure.

Generation

Generators convert some primary energy source into electricity, which gets injected into the transmission grid via step-up voltage transformers. Generator units are housed in a facility called *power station*, also referred to as a generating station, power plant, powerhouse, or generating plant. In the past, power plants were located as close as possible to the consumers. Nowadays, they try to be located close to a high-voltage transmission substation, where they can inject the power into the grid.

Generators are key to the stability and health of the power grid. Because of the way AC power works, generators need to be coordinated in several aspects. First of all, they need to be synchronized to the common frequency of the grid (50 Hz in Europe). If, for whatever reason, their rotation slipped out of step with the rest of the grid, protective devices would kick in and quickly disconnect the generator from the grid in order to avoid permanent damages to the alternator. Secondly, they need to respond quickly to the varying power demands of consumers. A net shortage of generation would translate in the frequency decreasing, while a net generation surplus would increase it. Many electrical loads such, as motors, need the frequency to remain at 50Hz or very close, otherwise they would be damaged. Thirdly, they all have to contribute to the support of voltage levels across the transmission grid, which they achieve by providing *reactive* power. We will not go deeply into the technicalities of reactive vs. real power, something that would require delving into the mathematics of AC electrical circuits. Suffice it to say that reactive power can be viewed as power that is reflected back to the generator, and thus produces no net delivery of real energy. However, it is something unavoidable due to the intrinsic physical properties of transmission lines and loads (reactance and capacitance). Due to the way AC power networks are designed, generators should provide enough reactive power, otherwise voltages could not be kept near their nominal values and the whole grid would collapse.

Generators can be classified according to the type of primary energy they use:

- Nuclear: they provide very cheap electricity[6], but their shut-down/start-up costs are high and they can take longer than a day or two to come back online. Therefore they are always operated at or near 100% output, trying to avoid maintenance stops since they are costly (ideally, they only stop for refuelling).
- Fossil-fuels:
    - Coal: they also provide very cheap electricity. Start-up times are also slow and costly, although not as much as nuclear.
    - Oil: more expensive than coal, but faster operation and cheaper start-up costs.
    - Gas: fastest operation of the three, and rather cheap start-up costs. Gas-fuelled generation may be cheaper than oil in some countries now. Modern plants implement the so-called *combined cycle*, where the heat recovered from the gas turbines is used to power a steam power generator (resulting in higher efficiency).

[6] We do not wish to enter the debate about externalities of nuclear and coal power, which would take us far from the discussion. Here we mostly concerned about the *operational characteristics* of different sources.

- Renewables:
    - Hydro: this is probably the cheapest and most convenient source (provided there are good reserves), with the fastest rates of operation. In some special locations, it is possible to construct a *pumped-storage* plant using two reservoirs. This provides large quantities of energy storage, at an efficiency that varies from 70% to 80%.
    - Wind: wind farms have now a great penetration in many EU countries (for instance, wind generation in Spain achieved a 20.9% share in 2013). The downside is that this type of generation cannot be scheduled or tapped at will. In the parlance of the field, it is *non-dispatchable*.
    - Solar: most commonly photovoltaic, but also thermal solar. Also non-dispatchable.
    - Biomass / biofuel / waste: similar in operation to oil-fuelled plants, but the fuel comes from renewable sources.
    - Geo-thermal: these are steam turbine-based plants that use the heat from the earth's magma by injecting water or some other fluid and recovering it. They are feasible only in places where the tectonic plates are close to the surface. Italy has some non-negligible geo-thermal generation.

Our aim here is not focusing on the economics of different electrical power sources. Rather, we want to stress how the type of source influences strongly the *operational characteristics*, most importantly the cold start-up times (i.e. how fast can a generator be switched on), and the ramping up/down rates (i.e. how fast can a generator increase or decrease its power output). Start-up costs are also a big concern for some technologies. Let us remember that, since electrical energy cannot be stored in very large batteries (at least not of the size needed for utility operation), generators should track the demand closely, in real time. Therefore, in the context of emergencies and disasters, it is quite important to understand this classification of generators attending to their *duty*:

- Base load power plants: they run all the time, typically near 100% of their rated output. Nuclear and large coal-fired plants. They provide cheap and reliable "base support" for the demand.
- Load-following power plants: they complement the base load until the forecasted demand is met. Lower costs than peaking plants, but more flexible than base load plants. Most of the generating technologies except nuclear are in this case.
- Peaking power plants: designed to be flexible in order to meet daily peaks in demand, thus running only for a few hours a day. Their electricity costs may be higher, but the start-up costs are lower. Simple-cycle gas and some hydro plants are designed to be peakers.
- Non-dispatchable power plants: wind and solar.

Finally, we should also mention the concept of auxiliary services. All types of generators, with the exception of wind and solar, need auxiliary power to get started. The key point is that not all of these generators have autonomous auxiliary generators to self-start without the need of grid power. The ones that have this are said to have "Black Start" capability. In the event of a blackout, Black Start power plants are highly critical, since they are the "seeds" from which the power grid can be restored.

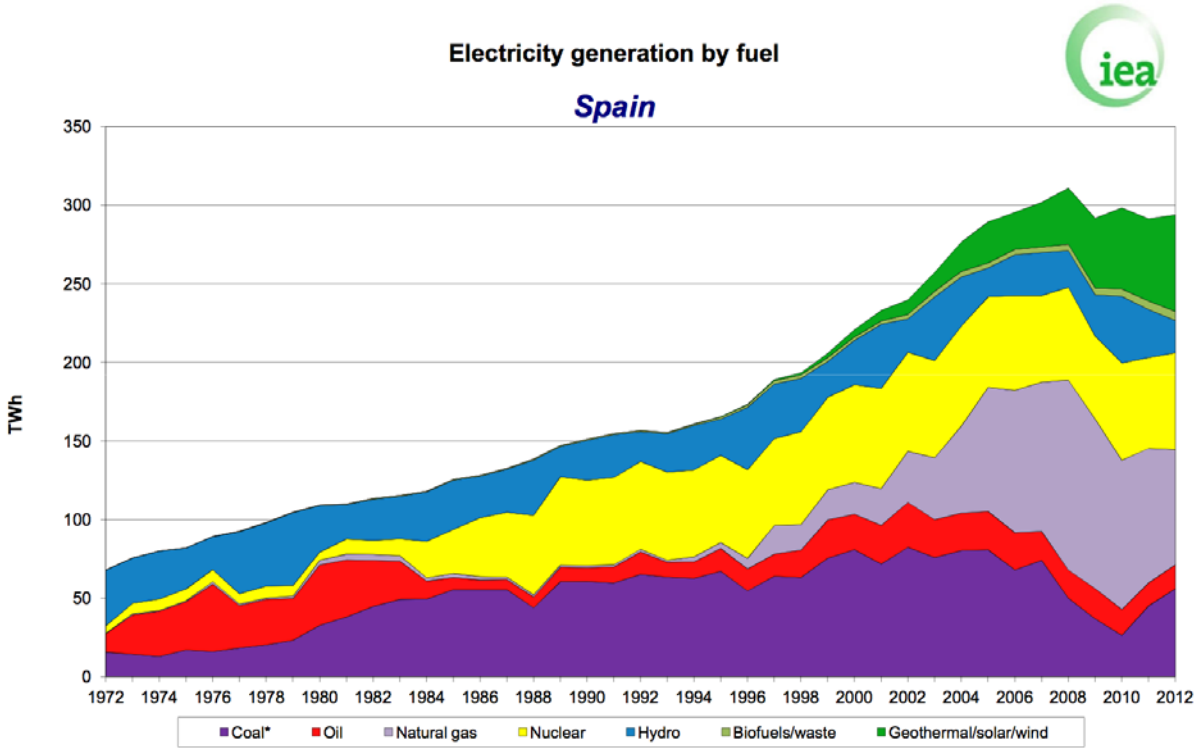


Figure 2. Evolution of the so-called "energy mix" for Spain, from 1972 to 2012 (source: IEA)

Power Transmission Systems

The electric power transmission system is often referred to as a grid. Redundant paths and lines are provided so that power can be routed from any generation facility to any customer area through a variety of routes, based on the economics of the transmission path and the cost of power. The redundant paths and lines also allow power flow to be rerouted during planned maintenance and outages due to weather or accidents. However, as we discuss below when touching on the physics of electrical circuits, this routing cannot be freely controlled at will.

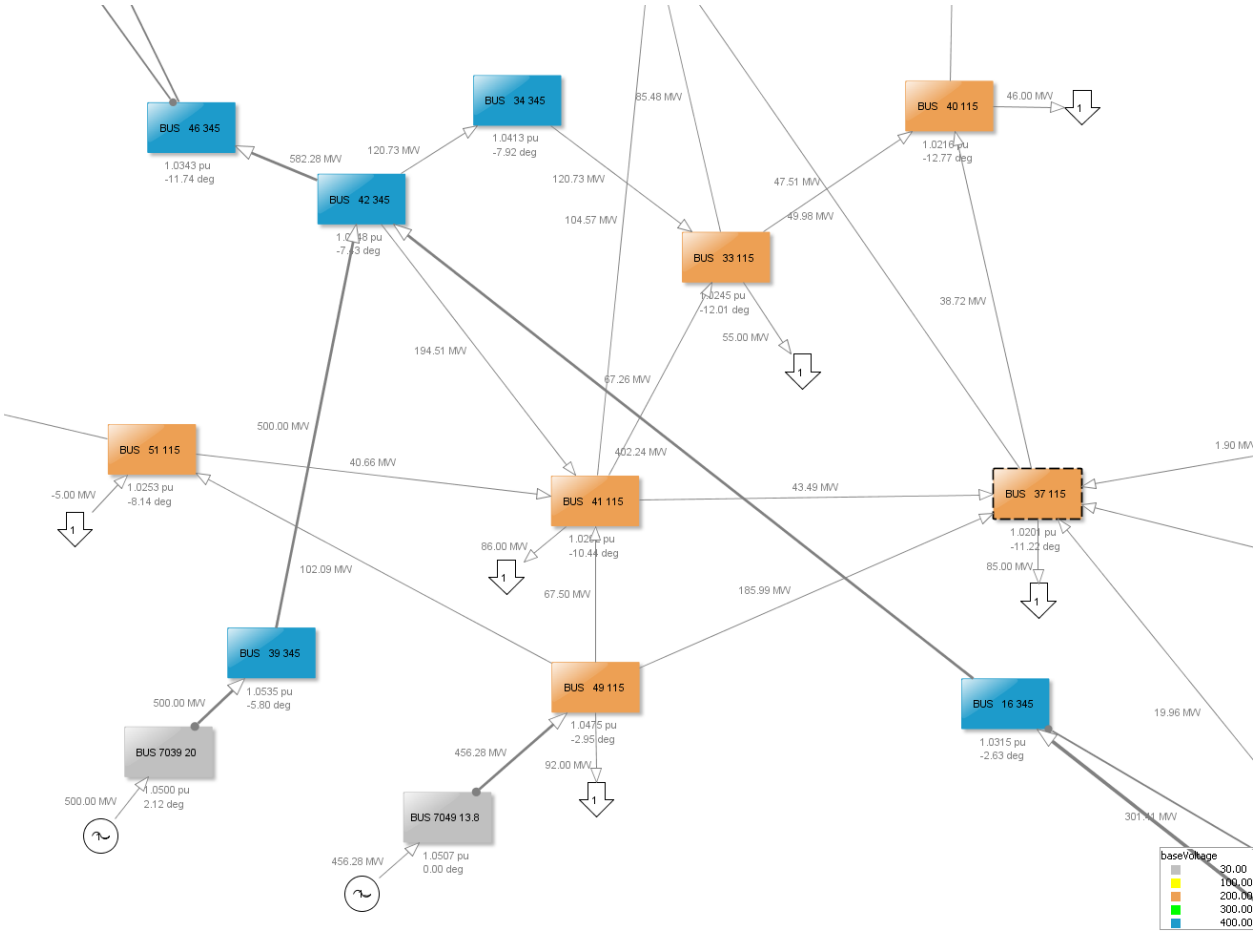


Figure 3. Portion of a transmission network. Notice how the topology is meshed, i.e. it contains multiple redundant paths (source: Grupo AIA).

Power transmission occurs via a system of overhead power lines and towers located between a power plant and a substation. When crossing a dense residential area is necessary, transmission and distribution systems can also be buried within underground conduits. Though the transmission efficiency is typically lower for underground lines and installation and maintenance are costly (about 5 to 10 times as much), locating the transmission system underground reduces impacts on land values, visual aesthetics, and vegetation loss. Submarine cables placed on the ocean floor by cable-laying boats are also occasionally used to transmit high-voltage power across long stretches of water to islands and other locations that are inaccessible by conventional techniques. Submarine cables are typically self-contained and fluid-filled to provide insulation over long distances.

Regional transmission grids consist of several large transmission systems connected by substations that are designed to transport electricity as efficiently as possible. Transmission networks can cover thousands of kilometres and encompass tens of thousands of towers. Energy is typically transmitted using a three-phase alternating current (AC) that is more efficient than a single phase. Energy is generally produced at generators at low voltage (up to 30 kV) and then stepped up by a power station transformer to a higher voltage in order to reduce resistance and reduce the percentage of energy lost during transmission over a long distance. For long distance transmission, electricity is usually transmitted at voltages between 110 and 1200 kV. At extremely high voltages, such as those

over 2000 kV, the so-called “corona discharge” effect produces energy losses that offset the benefits of reductions in energy losses from higher voltage. Over long distances, energy can also be transmitted via High Voltage Direct Current (HVDC) links. In these instances, smaller losses in energy and lower construction costs offset the need to construct conversion stations at each end of the transmission line to convert from AC to DC and back.

Transmission towers or pylons are utilized to suspend high-voltage overhead power lines. These systems usually transmit three-phase electric power (the common method for transmission of high-voltage lines of over 33 kV) and, therefore, are designed to carry three (or multiples of three) conductors. One or two ground conductors are often added at the top of each tower for lightning protection. Transmission towers can be constructed from steel, concrete, aluminium, wood and reinforced plastic. The wire conductors on high-voltage lines are generally constructed of aluminium, or aluminium reinforced with steel strands. Each transmission tower or support structure must be constructed to support the load imposed on it by the conductors. As a result, foundations for transmission towers can be large and costly, particularly in areas where ground conditions are poor such as in wetlands. Guy wires can be utilized to stabilize transmission towers and resist some of the force of the conductors.

There are three main types of transmission powers or pylons used in a transmission system. Suspension towers support straight stretches of a transmission line. Deviation towers are located at points where a transmission line changes direction. Terminal towers are located at the end of overhead transmission lines where they connect with substations or underground cables.

The most common type of transmission tower or pylon used for high-voltage power lines is a steel lattice structure. Tubular steel monopoles are also used to support high or medium voltage transmission lines, usually in urban areas. Transmission towers constructed of a steel framework can be used to support lines of all voltages, but they are most often used for voltages over 50 kV. Lattice towers can be assembled on the ground and erected by cable (which uses a large laydown area), erected by crane, or, in inaccessible areas, by helicopter. Transmission towers typically range from approximately 15 to 55 meters (m) in height.

Wooden transmission towers consisting of single poles, H-frames, or shapes resembling A’s or V’s are also commonly used to support high-voltage transmission lines. Wooden transmission towers are limited by the height of available trees (approximately 30m), and generally carry voltages of between 23 kV and 230 kV, lower than those carried by steel lattice transmission towers. Aluminium towers are often used in remote areas where they can be transported in and installed by helicopter. Towers of reinforced plastic are now available, but high costs currently restrict their use.

For underground transmission lines, the three wires used to transmit the three-phase power must be located in individual pipes or conduits. These pipes are covered in thermal concrete and surrounded in thermal backfill materials. Underground cable conduit systems typically require trenches of at least 1.5m in depth and width. Due to difficulties in dissipating heat, underground conduits are typically not used for high-voltage transmission lines over 350 kV.

Power Distribution Systems

Prior to consumer use, high-voltage energy is stepped down to a lower voltage overhead line for use in sub-transmission or distribution systems. Distribution lines typically vary from 2.5 to 25 kV. Finally, the energy is transformed to low voltage at the point of residential or commercial use. The mains voltage ranges between 100 and 600 volts (V) depending on country and customer requirements (the current European standard, EN50160, is 230V). Power distribution poles (or utility or telephone poles) are typically constructed of wood, but steel, concrete, aluminium, and fiberglass are also used. Distribution poles are typically spaced no further than 60m apart and are at least 12m in height. Wooden distribution poles are limited by the height of available trees (approximately 30m).

More than voltage levels, the defining characteristic of distribution networks, setting them apart from transmission, is actually their topology. Distribution networks are no longer meshed; rather, they have a tree-like topology. At the top of each distribution tree is the so-called *feeder*, which is just one or more transformers connecting to the transmission or sub-transmission grid. In many instances distribution networks do have redundant paths (more so at the higher voltage levels), but they are only activated on-demand, when faults take place, so that the network topology gets "reconfigured", but still operated as a tree and not a mesh. Figure 4 below illustrates this concept.

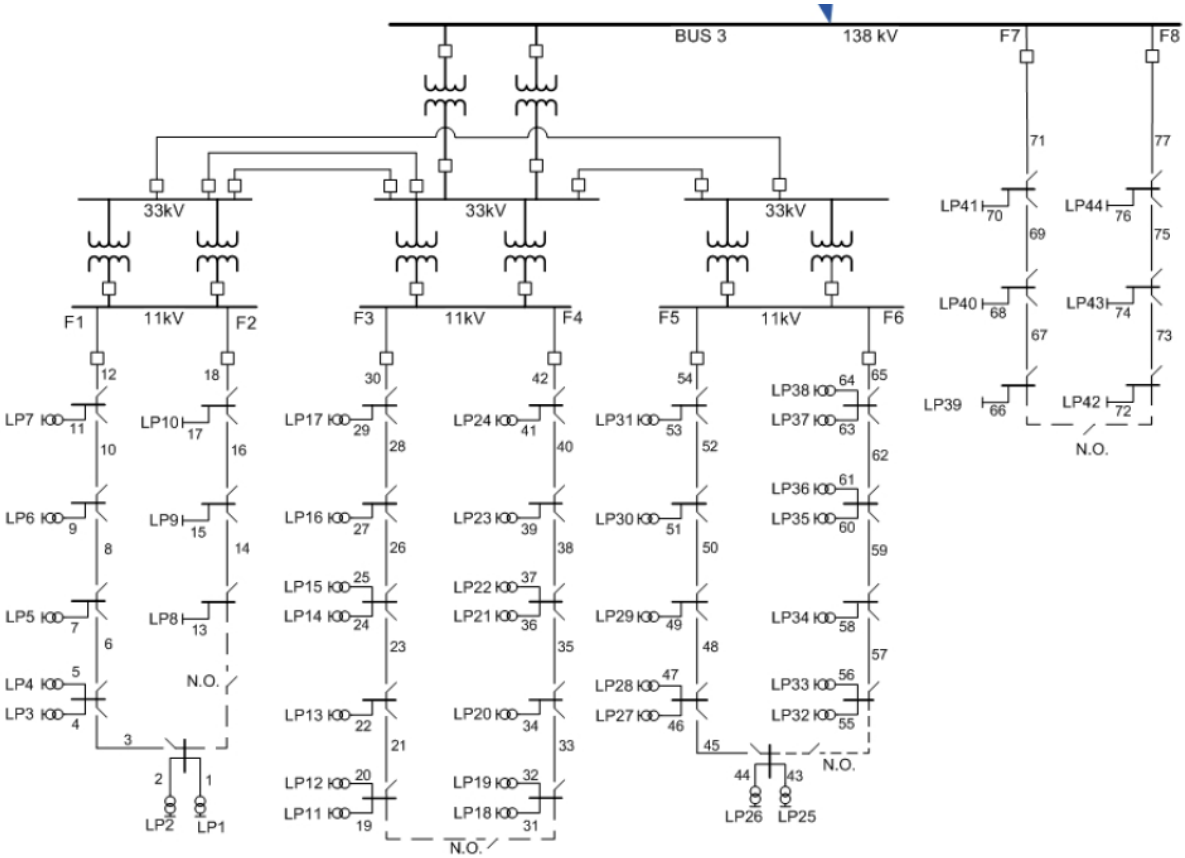


Figure 4. Schematic view of a distribution network, showing the tree-like topology. Dashed lines are normally open, and they are used only to reconfigure the network when needed (source: Helmut Simonis blog).

Electrical Substations

Electrical substations are facilities along the electricity transmission and distribution system that house transformers and switchgear to transform power from low to high or high to low voltage levels. Step-up transformers are used to increase voltage while decreasing current, while step-down transformers are used to decrease voltage while increasing current. Substations not only contain transformers and switches/breakers, but also control, and protection equipment. Substations can be located in fenced enclosures, underground, or inside buildings.

There are two main types of electrical substations. Transmission substations contain high-voltage switches used to connect together high-voltage transmission lines or to allow specific systems to be isolated for maintenance. Distribution substations are used to transfer power from the transmission system to the distribution system. Typically at least two transmission or sub-transmission lines enter a distribution substation, for redundancy. Distribution substations can also be used to isolate faults in either the transmission or distribution systems. Complicated distribution substations containing high-voltage switching, switching, and backup systems are often located within large urban centres.

The role of physics in the operation of electrical networks

It is out of the scope of this document, and indeed out of the scope of the RAIN Project, to analyse the technicalities of power transmission. But there are at least a couple of insights that are worth mentioning, and they should be definitely a take-away points for anybody engaged in risk modelling for power networks.

The first one is that, even though the transmission grid is a network (and therefore allows redundant paths), *electric power is not routable at will* (Brown and Sedano 2004). It follows the laws of physics, going down the paths of least impedance. In fact, operators and planners need to solve the *power flow equations* in order to find out how the flows will distribute. The point is that, even though a given network path may have the capacity to transfer the power we want, the particular *electrical state* of the network may not allow us to use that capacity to the fullest. Controlling the route of flows is even more complicated in the presence of markets, because operators lose most of the control on the generation schedules. The design of transmission networks takes all of this into account and tries to build enough capacity and safety margins to ensure that the redundancy meshing is effective. However, transmission lines are a very expensive investment, so the redundancy is somewhat limited. Topological network analysis shows in many cases that just a handful of lines are extremely more critical than the rest.

Another insight is that *the grid does not run on autopilot* (Brown and Sedano 2004). It needs human control, just as much (and in a similar vein) as air traffic control. Transmission operators monitor and operate the grid in real time, using SCADA systems and other tools for on-line analysis and simulation. At a very basic level, they need at least to command some generators to increase or decrease their output (following real-time demand), and respond to events with switching and other control actions.

In connection to the two points above, notice how the power grid does not have mechanisms for graceful and gradual degradation of service, compared to other networks, such as telecom, that have some rate-limiting defences built in. An AC power network may hit its limits either because there is a shortage of power or because the transmission capacity is reached, but the end result in both cases is *load shedding*, that is, a total disconnection of customer loads. In extreme cases, disturbances spread and the disconnections (triggered by protection devices) affect large portions of the transmission network, resulting in a blackout. Restoring from a blackout is a slow and difficult process that may take hours or even days, because operators have to "rebuild" the grid by keeping a delicate balance between generation, load, and adequate voltages, at a time where everything is very dynamic and unstable.

Planning and Operations

Running a power grid relies on two key functions: planning and operations.

Long term planning deals with *expansion plans* for the infrastructure such as where to build more generators and which type, and where to construct more substations and lines. These studies need projections of future demand and its geographical location. Short term planning deals with power-flow calculations for simulating near term conditions, in order to prepare operations. For instance, day-ahead planning consists in taking the forecasted demand, the production schedules, and the maintenance statuses of the grid elements, and performing the necessary power-flow studies to prepare for real-time operation the next day. Special care is taken to assess the level of security of the resulting scenarios (i.e. how sensitive they are to failures), and to ensure security margins (e.g. leave enough room in transfer capacity for demand fluctuations or forecast error). In countries where there is a free energy market, the planning studies may impose corrections on the production schedules coming out of the market bids (remember: electrons obey physics, not markets).

Real-time operation takes place at Control Centres. The system is monitored and controlled using SCADA systems, supplemented by analysis and simulation tools. In transmission, the collection of all these tools is typically referred to as an EMS, Energy Management System; in Distribution, it is called DMS, Distribution Management System. Monitoring data (voltages, currents, power flows, breaker statuses, alarm data) are collected at the substations using so-called Remote Terminal Units (RTU), and sent to the SCADA at the Control Centre through telecommunications (normally, but not always, using dedicated telecom lines owned by the utilities).

Rights-of-Way Management

We briefly mention this issue because of its importance in weather-related threats to the power grid, particularly to transmission and distribution lines. Both aboveground transmission and distribution projects require rights-of-way to protect the system from windfall, contact with trees and branches, and other potential hazards that may result in damage to the system, power failures, or forest fires.

Electric power transmission and distribution lines are often located in conjunction with highway, road, and other rights-of-way to minimize both costs and disturbance to ecological, socio-economic and cultural resources. Other factors, including land value, archaeological resources, geotechnical hazards, accessibility, parks and other important features also contribute to the locating of transmission and distribution line right-of-way alignments.

Operational activities may include maintenance of access to the transmission lines, towers and substations (e.g. low-impact trails or new / improved access roads) and vegetation management. Upgrades and maintenance for existing infrastructure are a consideration throughout the life cycle of the project. Power transmission and distribution facilities are decommissioned when they are obsolete, damaged (e.g. by corrosion) or replaced due to increased power demand. Many power facilities are replaced with new or updated equipment at the same site or right-of-way.

Rights-of-way are also utilized to access, service, and inspect transmission and distribution systems. Underground distribution lines also require rights-of-way where excavation is prohibited or strictly monitored, construction activity is limited, and access to lines can be achieved if necessary. Being larger systems transmitting higher voltages, transmission rights-of-way are typically much larger than those for distribution systems and, consequently, require more extensive management.

Rights-of-way widths for transmission lines range from 15 to 100m depending on voltage and proximity to other rights-of-way (typical range is between 15 and 30m). For overhead distribution power lines up to 35 kV, 12 to 24m corridors (6 to 12m on each side) are recommended. Access roads are often constructed in conjunction, or within, transmission line rights-of-way to provide access for maintenance and upkeep of the system.

To avoid disruption to overhead power lines and towers, regular maintenance of vegetation within the rights-of-way is required. Unchecked growth of tall trees and accumulation of vegetation within rights-of-way can result in a number of impacts including power outages through contact of branches and trees with transmission lines and towers, ignition of forest and brush fires, corrosion of steel equipment, blocking of equipment access, and interference with critical grounding equipment.

Regular maintenance and clearing of rights-of-way prevents natural forest succession and the establishment and growth of tall trees. Typically, tall trees of approximately 4.5m or more are not permitted within aboveground rights-of-way. Underground rights-of-way have far fewer vegetation restrictions, though trees with deep roots that may interfere with duct banks are usually prohibited from being grown within the right-of-way. Vegetation maintenance of rights-of-way can be accomplished with the following measures:

- Mowing with heavy-duty power equipment is used to control growth of ground covers and prevent the establishment of trees and shrubs in the right-of-way.

- Herbicides, in combination with mowing, control fast-growing weedy species that have a potential to mature to heights over those permitted within the right-of-way.

- Trimming and pruning is utilized at the boundaries of rights-of-way to maintain corridor breadth and prevent the encroachment of tree branches.

- Hand removal or removal of vegetation is costly and time-consuming but is often used in the vicinity of structures, streams, fences, and other obstructions making the use of machinery difficult or dangerous.

2.2 Identification of critical elements. Rationale

After having seen an overview of the whole electrical grid, we now focus on the specific purpose of identifying the critical components of the infrastructure, each with a short rationale on why they are deemed critical and how. Shortly after we will enumerate the weather-related threats that may affect them.

As for the actual rationale for identifying which elements are critical and which are not, please note that in electrical networks all elements are critical, in the sense that their malfunction always implies a loss of service to a certain extent. Actually, the question is one of model granularity: for instance, should we consider a generation plant as one whole entity, or consider instead the detailed modelling of its constituents? In enumerating these components, we necessarily need to make simplifications, in other words, some modelling assumptions. The power grid is quite large and some of its components may be extremely complex, but it is neither necessary nor useful to include all of their technical details, since the final purpose is to achieve a high-level modelling of infrastructure risks. For instance, a nuclear power plant is an incredibly complex facility in itself, but here in the context of the health and safety of the bulk power grid, it is best to consider it as simply two "components": the generator unit (with its characteristic start-up/shut-down times and ramp rates) and the auxiliary power units (which enable it to function, and crucially, to start-up).

Figure 5 below shows the essential elements in this type of simplified modelling, following the IEC Smart Grid Standards Map (IEC n.d.). This is also the type of modelling that underlies the so-called Common Information Model (CIM), which has been promoted by the IEC as a unified model for all software related to operations, analysis, maintenance, etc., in the power utilities sector.

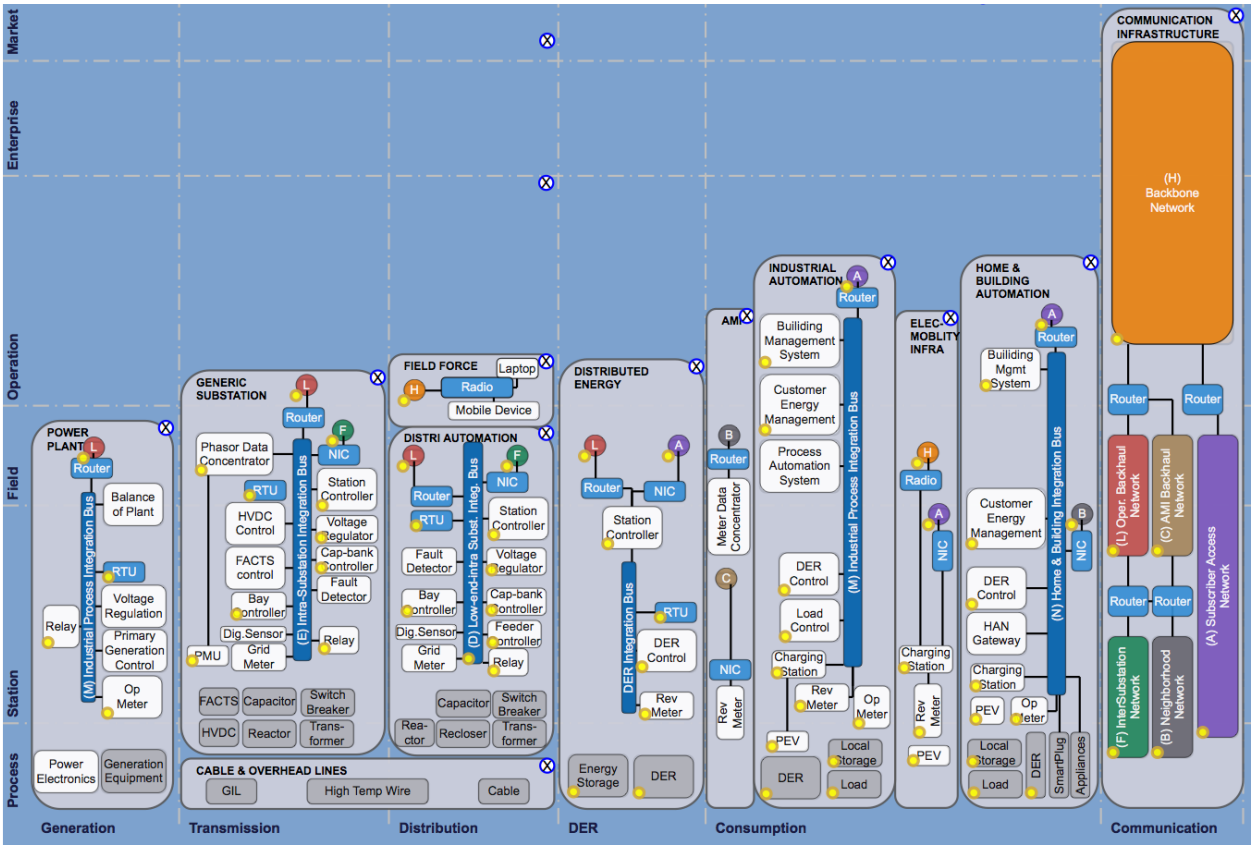


Figure 5. a partial view of the IEC Smart Grid Standards Map, focused on operational elements (source: IEC).

Here is then the list of critical elements:

- **Generators and their auxiliary power systems:** generators are the sources of power, and they should follow the demand in real time. They also sustain the voltage levels of the grid by injecting or absorbing reactive power. They are extremely critical: if there is a shortage of either real or reactive power, the whole transmission grid can collapse (blackout). That's why there should always be a sufficient amount of installed capacity, with reserve generation ready to be called on with more or less response time, depending on the case. For instance, "spinning reserve" generators are already started up but running on empty, waiting to be called when the demand surges.
- **Transmission lines (incl. HVDC links):** the lines carry the power, but even though the network is laid out with certain degrees of redundancy (i.e. meshing), the electrical behaviour of the system can be quite sensitive to the loss of a given line. Also, the re-arrangement of power flows after a line loss is not entirely obvious to operators, so they need to calculate it using power-flow analysis software.
- **Transmission transformers (including feeders to distribution):** transformers play a very similar role as lines, and they are critical for the system for the same reasons. Perhaps the only difference, besides their obvious role in transforming voltage levels, is that they also contribute to the control of voltage, through the manual or automatic setting of their tap changer. This ability to control is not, in itself, a critical feature (and in fact, under some emergencies automatic tap changers are sometimes locked, as a protective measure to the transmission grid).

- **Switches and breakers:** these devices allow operators to connect and disconnect lines, transformers, and other equipment, for maintenance or any other operational purposes. They are just as critical as lines and transformers. A switch is a relatively simple mechanical contact device, but a high-voltage breaker is rather more complex, typically a large gas-filled device fitted with electromechanical actuators.
- **Protection relays:** closely related to power breakers, protective relays are the devices that detect faults (short-circuits), or more generally any type of dangerous abnormal behaviour, and trigger the opening of breakers accordingly. They are essential to the long-term health of the system. Since generators, transformers, and lines are very costly infrastructures and they all would need a long time to replace, the whole network is engineered and architected with plenty of protective measures. The design always errs on the safe side and disconnects equipment to avoid permanent damage. Historically, protections have been very local to the protected device. More recently, with the advent of modern telecommunications, some protections are now designed for wide-area coordination and actuation (the so-called SPS, System Protection Schemes).
- **SCADA and associated Telecoms:** except in very light demand scenarios, the grid cannot run without central monitoring and control for more than about 5 to 15 minutes. In the times when there were no SCADA technology, the grid would work thanks to larger built-in margins in transmission and generation capacity, which makes the system more forgiving of slower and less precise operation (it was performed through telephone calls). Nowadays, margins are much tighter and the SCADA is essential for the operators. Additional EMS tools like the State Estimator and other analytical applications are also becoming essential for enhanced situational awareness.
- **Other Voltage-management devices:** shunt/series capacitors and reactors and FACTS devices. These devices are essential for controlling voltages, which becomes a critical task whenever the system is pushed to stressful limits, or in abnormal situations such as when the grid is being restored from a blackout. These devices generate or absorb reactive power as needed, thus contributing to maintaining voltage levels within established limits. FACTS devices are modern devices based on power electronics, rather more complex (and expensive) than capacitors and reactors, but they are more dynamic and therefore allow a certain degree of control over the “routing” of power flows.

Note that we have opted for not considering loads as a critical component of the infrastructure. A load is a modelling abstraction representing thousands or more customer endpoints, in other words, aggregate demand. Therefore it is usually just the expression of the active and reactive power demand (P, Q) at the output end of a “feeder” transformer. In this view, the actual critical components sitting at the end of the infrastructure are therefore said transformers, and the loads that they serve provide us with a measure of the amount of “service” that could get lost. As to the question of granularity in this modelling, it is of course necessary to decide at which level of the distribution network hierarchy one wants to stop.

Again, it is important to remark that the impact caused by the failure of any of these particular elements listed above is potentially much higher than simply losing the loads that were being directly supplied by them. Depending on the operating conditions, the rest of the network could be

impacted. This way, purely local weather events could have the potential to disrupt the whole bulk electric system.

2.3 Weather-related threats

For the purposes of identifying weather threats to the electric infrastructure, we will adopt the point of view of differentiating between weather threats vs. climate change threats. Our concern will clearly focus on the former, not the latter. By this we mean that we will focus on extreme weather *events*, and not so much on the long-term effects of changes in the average values of weather variables such as average rainfall, average temperatures, rising sea levels, etc. Preparedness for long-term climate change is obviously extremely important (European Environment Agency 2012), but it plays on a longer time scale compared to preparedness for extreme weather events. It can be argued that it is now more urgent to be prepared for extreme events, more so in the case of a networked infrastructure such as the power grid, in which local problems can easily spread far and wide.

The EU Commission, as part of its climate action plans, has drafted an EU Adaptation Strategy Package[7], a set of studies and recommendations for shaping high-level policies addressing adaptation of society to climate change. Of all these plans, the document "An EU Strategy on adaptation to climate change" (EU Commission 2013) contains the most current policy recommendations. In the accompanying communication "Adapting infrastructure to climate change" (EU Commission 2013), the following table of threats on energy sources is shown:

[7] http://ec.europa.eu/clima/policies/adaptation/what/documentation_en.htm

Technology	Δ air temp.	Δ water temp.	Δ precip.	Δ wind speeds	Δ sea level	flood	heat waves	storms
Nuclear	1	2				3	1	
Hydro			2			3		1
Wind onshore				1				1
Wind offshore				1	3			1
Biomass	1	2				3	1	
PV							1	1
CSP						1		1
Geothermal						1		
Natural gas	1	2				3	1	
Coal	1	2				3	1	
Oil	1	2				3	1	
Grids	3					1	1	3

Figure 6. Impacts of changing climate change parameters on different energy supplies (3 = severe impact, 2 = medium impact, 1 = small impact). Source: (EU Commission 2013).

However, as mentioned above, this table focuses on long-term changes, whereas we will emphasize extreme weather events (moreover, it focuses on production and does not consider transmission). Such events are, of course, a consequence of climate change. They are considered extreme events precisely because the weather parameters are significantly out of the historical high/low limits typical of the particular country or region (for instance, an extreme heat wave in northern countries).

To make our position even more clear, we could cite the key recommendations of the 2014 report "Climate Change Impacts in the US: The Third National Climate Assessment"[8] (Melillo, Richmond and Yohe 2014), and point out that our focus is on Key Message #1:

1. *Extreme weather events* are affecting energy production and delivery facilities, causing supply disruptions of varying lengths and magnitudes and affecting other infrastructure that depends on energy supply. The frequency and intensity of certain types of extreme weather events are expected to change.
2. Higher summer temperatures will increase electricity use, causing higher summer peak loads, while warmer winters will decrease energy demands for heating. Net electricity use is projected to increase.
3. Changes in water availability, both episodic and long lasting, will constrain different forms of energy production.
4. In the longer term, sea level rise, extreme storm surge events, and high tides will affect coastal facilities and infrastructure on which many energy systems, markets, and consumers depend.

[8] http://nca2014.globalchange.gov

5. As new investments in energy technologies occur, future energy systems will differ from todays in uncertain ways. Depending on the character of changes in the energy mix, climate change will introduce new risks as well as opportunities.

With these considerations in mind, we enumerate now the extreme weather threats to the electrical elements we described in the previous section:

- **Lightning:** it affects mainly overhead lines and unsheltered transformers. Proper grounding techniques, protection relays, and automatic reclosers minimize the risk. A high concentration and concurrence with simultaneous faults increase it.
- **Wind storms:** they affect mainly overhead lines and unsheltered transformers, typically bending or toppling power line towers and causing electrical faults. The damage to towers (pylons), either directly or indirectly by fallen trees, can be permanent. (Note: we include here hurricanes, tornadoes, and tropical cyclones; actually, the term *European windstorm* is now commonly used to refer to extratropical cyclones which occur across the continent of Europe.)
- **Ice/snow storms:** they affect mainly overhead lines and unsheltered transformers. Ice storms can cause ice to grow on power lines, which may crumble under its weight, or whip violently when the wind blows large chunks of ice off the line.
- **Flash floods:** we include here coastal and river floods. They mainly affect generator plants. It could also affect ground-level and underground transformers, many times causing permanent damage. If they are accompanied by mudslides, they can also affect power pylons.
- **Extreme cold:** extreme cold waves not only strain the grid due to peak loads, but because many generator plants can get affected. Two big problems are inadequate winterization of the power plant equipment on the one hand, and also curtailments of the primary energy supply on the other (for instance, gas supply), also due to extreme cold weather.
- **Extreme heat:** nowadays extreme heat waves cause more strain on the grid than cold waves in terms of peak demand, because in contrast to heating, almost all cooling systems run on electricity. Aside from peak demand, extreme heat is a risk to congested transmission lines, due to the reduction in capacity (lower thermal limits due to less thermal dissipation) and to line sagging (dilated lines may cause faults by short circuiting to vegetation below).
- **Wild fires:** these may affect mainly unsheltered transformers, sitting on ground level. Proper maintenance of vegetation in rights-of-way for lines and around substations should lower this risk.
- **Sand storms:** not a likely event in the EU countries, but a sandstorm can affect power transmission lines severely, directly or indirectly by fallen trees.
- **Sudden seasonal drought:** for a country with a significant proportion of hydro in its energy mix, a sudden seasonal drought puts a stress on the grid due to generation shortage. This is probably not a weather “event” in the sense of having little time to react, but nevertheless we decided to include it here because providing extra generation capacity in a time-frame of 6 to 12 months is not possible.

The table below lists our threat assessment (low/mid/high) for each of the weather threats listed above, as applied to each of the critical components of the power grid: generators, lines, transformers, breakers, etc.

	Generators (housed)	Generators (wind / PV)	Lines	Trans-formers	Sw / Breakers	Relays	SCADA & telecom	Voltage control devs
Lightning	Low	Mid	High	High	High	High	High	High
Windstorms	Low	High	High	High	Mid	Mid	Mid	Mid
Ice/snow storms	Low	High	High	High	Mid	Mid	Mid	Mid
Flash floods	High	Mid	Mid	High	High	Mid	Mid	Mid
Extreme cold	High	Low	High	High	Mid	Low	Low	Low
Extreme heat	Mid	Low	High	High	Low	Mid	Mid	Mid
Wild fires	Low	Mid	Mid	High	Mid	Mid	Mid	Mid
Sand storms	Low	High	Mid	Low	Low	Low	Low	Low
Seasonal drought	Mid	Low	Low	Low	Low	Low	Low	Low

Other natural threats

Other threats not related to weather and therefore not considered here are: earthquakes, tsunamis, and space weather (geomagnetic storms produced by coronal mass ejections from the sun, i.e. solar flares). Solar superstorms in particular have attracted more attention recently, as in 2012 there was a large flare that luckily missed the earth but had the potential to knock down large portions of the grid all around the world (Krausmann, et al. 2013). A geomagnetic storm induces currents in the power grid, causing damages via overvoltages or overloads. A real incident of this type took place in Quebec in 1989. The solar superstorm of 1859 (dubbed “the Carrington event”) was much stronger, but it only affected telegraph infrastructures since there was no power grid at the time.

2.4 The impact of weather-related power outages

We close this section on the electric power infrastructure by giving an overall idea about the impacts of blackouts and smaller power outages caused by extreme weather, particularly from the point of view of social economics.

All the threats described above, with the exception of drought, extreme heat, and extreme cold, have the potential to destroy equipment. Replacement of equipment is in general very costly, both

in terms of time and money. For instance, laying down an emergency service 66 kV line can take at least 3 to 5 days. In the worst case, a large transmission transformer with no spare replacement could face a lead-time at the production factory of about 5 months. At the distribution end, the situation is obviously different, but even when the utility has an adequate number of spares, repair works typically take a few days in case of natural disasters, because the number of repair crews is limited.

The impacts in terms of loss of service depend a lot on the section of the network being affected. If the assets belong to the transmission part and the incidents are not very widespread geographically, chances are the service can continue uninterrupted, since the transmission network is built with some degree of redundancy (topologically meshed network). If the incidents affect distribution equipment, the impact will depend on how far down the distribution this happens. Higher upstream, distribution networks typically have some degree of "reconfiguration" in order to isolate faulted sections. But as we go down the distribution levels and we approach the consumer end, supply becomes purely radial (i.e. tree-like). There, a loss of a transformer or a line means that all the associated customers become disconnected.

We know that power outages shut down businesses, close schools, and impede emergency services, disrupting the lives and causing huge economic losses. It is hard to quantify exactly the losses in monetary terms, but it is useful and necessary to attempt to, in order to estimate the resources and efforts that should be dedicated to strengthen the power grid.

In a 2013 report prepared jointly by the US President's Council of Economic Advisers, US Department of Energy, and US White House Office of Science and Technology, estimates were given for the annual costs of outages caused by severe weather between 2003 and 2012. Various strategies to increase the resilience of the electric grid were also provided, based on the economic benefits (Executive Office of the US President 2013). These are the highlights from the report:

- Severe weather was found the leading cause of power outages in the US. Between 2003 and 2012, an estimated 679 widespread power outages occurred due to severe weather.
- Weather-related outages were estimated to have cost the U.S. economy an inflation-adjusted annual average of $18 billion to $33 billion (this is 0.13% to 0.25% of the 2012 real GDP). Annual costs fluctuate significantly and are greatest in the years of major storms such as Hurricane Ike in 2008, a year in which cost estimates range from $40 billion to $75 billion (0.3% to 0.56% of the 2012 real GDP), and Superstorm Sandy in 2012, a year in which cost estimates range from $27 billion to $52 billion (0.2% to 0.39% of the 2012 real GDP).

Another recent Congressional Research Service study (Campbell 2012) estimated the inflation-adjusted cost of weather-related outages at $25 to $70 billion annually (0.18% to 0.52% of the 2012 real GDP). The variation in estimates reflects different assumptions and data used in the estimation process. The costs of outages take various forms including lost output and wages, spoiled inventory, delayed production, inconvenience and damage to the electric grid. In any case, these estimated figures provide a very good picture about the magnitude of the problem. They are also very useful for researchers and policy makers trying to decide what should be the amount of continued investment in grid modernization and resilience that will mitigate these costs over time – saving the

economy billions of euros and reducing the hardship experienced by millions of citizens when extreme weather strikes.

2.5 Interdependencies of the Electrical Power Infrastructure with other CI

The power grid has enjoyed for a long time quite a low direct dependence on any other critical infrastructure, other than the obvious one on the supply of primary sources (mainly oil and gas—nuclear plants refuel at 1-2 year intervals). Dependency on the transport infrastructure is quite low, and is mainly limited to having access for the maintenance crews to distribution equipment. Utilities have their own special transportation means to reach very remote substations and lines. And regarding telecoms, we should remark that the grid developed in the early 20th century without the benefit of extensive telecommunication networks.

This last point is less true nowadays. Before the 1980s, transmission networks had plenty of transmission capacity margins built in, so that the operation of the system could rely on basic automatic coordination. In essence, the common frequency of the grid (50Hz in Europe, 60Hz in North America) provided the synchronization and regulation mechanism for all generators, and operators had the time to coordinate further control actions by means of simply telephone calls to the power plants. The safety margins for operation are now much tighter, and these control decisions must be taken must faster. The operators need to receive their SCADA telemetry via data communications, and their SCADA commands need to actuate immediately. All SCADA systems rely critically on telecommunications. Luckily, the power utilities have always been rather conservative and always preferred to build their own ad-hoc communications lines, in order to be independent of external telecom providers. Many high-voltage lines carry one or more so-called optical ground wire (OPGW) at the top of the pylon, which carries a fibre optic communications line and doubles as grounding wire. Many utilities actually lease these lines to the big telecom companies.

However, it is uncertain whether all SCADA systems at power utilities are truly independent from external Telecom providers. It is generally true for transmission-level networks, at least in the highest voltage levels. But as one descends downwards to distribution sections, it becomes more likely to find utilities that lease lines from Telcos for SCADA use. Such lines may have guaranteed traffic capacities, but they could be affected by network outages just like the rest of telecom lines.

3. Telecom networks

This chapter describes the telecommunications infrastructure, identifying its critical elements and the threats arising from extreme weather events. Although telecommunications have undergone tremendous advances and very rapid changes in the last 20 to 30 years, we have tried to capture the essential aspects of this networked infrastructure that are relevant to reliability and resiliency under weather-related threats (Snow, Hoag and Weckman 2009). This means we have stayed away from complexities such as protocols, routing, security, etc., all of which would only be relevant in the context of cyber-security, for instance. For a gentle introduction to telecom networks and their technology, see for instance (Nassar 2001).

3.1 General description and architecture

Telecommunications have revolutionized our modern daily lives. Analogue telephone and radio communications changed our lives in the 20th century, but the transition to digital communications and the *convergence* with computer technology and the Internet are shaping a second revolution with far larger consequences, many of which we are still unable to fully comprehend (Singh and Raja 2010). In any case, it is clear that telecommunication infrastructures are highly critical for the wellbeing of modern society, as we have grown highly dependent on them.

The first commercial electrical telegraphs were introduced in 1837 (the Cook and Wheatstone telegraph, London). Telegraphy had one major drawback: it required a trained operator to translate the digital data into words and the reverse, words into digital code. This limited its usefulness as a consumer product. In 1876, the great Scottish inventor Alexander Graham Bell (1847–1922) demonstrated the first operating telephone, also the first one to obtain a US patent. Bell, his father-in-law Gardiner Hubbard, and Thomas Sanders formed the Bell Telephone Company in 1877. They established their first telephone exchange in New Haven, CT (21 telephones and 8 lines). Growth was rapid because Bell Telephone licensed its patents to others, thus attracting investments in local exchanges and “telephone companies.” Revenues from licensing and equipment manufacturing soon led to network system building. American Telephone and Telegraph Company (AT&T) was incorporated as a subsidiary of American Bell Company in 1885, for the sole purpose of building long-distance networks. Expansion quickly reached San Francisco, and in 1915 the first coast-to-coast long distance call was made. The first transatlantic telephone service for commercial service (3500 miles) was inaugurated in 1927. In 1935 the first telephone call around the world by wire and radio took place. By the early 1950s most of the advanced nations had universal coverage and international connections. In 1965 the first geosynchronous communications satellite was put in orbit, providing both telephone circuits and TV signals. Finally, during the 1970s, advances in semiconductor electronics and computing would kick-start the technological changes of the digital revolution we have witnessed in the last years.

Although the underlying technologies and equipment have changed tremendously, the overall structure of current telecom networks still resembles the one laid down during the last century for the voice telephone system. The main differences are that everything is now digital and, wireless technology is ubiquitous, and all types of services (voice, video, data) have converged onto the same

network infrastructure and they are inextricably married to computing technology. These developments are significant in terms of infrastructure risk and we will revisit them later on.

The figure below (Figure 7) shows schematically the structure of the telecom infrastructure. It is a networked structure with a topology that resembles very much that of electrical networks, in that there is a long-distance transmission core having a meshed topology (i.e. redundant connectivity, alternative routes), and local distribution leafs having a tree-like topology:

- The distribution section: this is operated by a telecom company that is commonly termed the Local Exchange Carrier (LEC). In this section we have the following elements:
    - The **Headends**, typically cabinets that aggregate several end-customer lines (the so-called local loop pairs). In the terminology of telecoms, these are commonly termed the "Outside Plant" (see below), to distinguish them from the "Inside Plant" which represents all other equipment at the customer premises.
    - The **End Offices**, where cables from the Headend points are collected. This is the first point where calls get switched and the signals are multiplexed in order to reach other customers. These are also called telephone exchanges (technically, Class 5 Telephone Exchanges).
    - The **Central Offices**, larger telephone exchanges aggregating the traffic from End Offices. They contain so-called Tandem Switches (Class 4 Telephone Switch), used to interconnect local exchange carrier offices to the long distance transmission networks. Note that sometimes "Central Office" is used to refer to both Class 5 and Class 4 switches.
    - **Trunk lines**: lines interconnecting End Offices and Central Offices, as well connections to the Interexchange carriers are generically termed trunk lines because they provide access to many clients by sharing a limited set of lines or frequencies instead of providing all of them individually (the assumption is that customers are not calling all at the same time).
- The transmission section: operated by the Interexchange Carrier (IEC). In this section we have the following elements:
    - **Points of Presence:** telephone exchanges connecting the interexchange carrier companies to the local exchange ones.
    - **Class 1, 2, and 3 centres:** in the Bell System nomenclature, these are the three levels of telephone exchanges in the long-distance network. Class 3 are "Primary Centres" (and typically points of presence), Class 2 are "Sectional Centres", and Class 1 are "Regional Centres".
    - **Backbone lines:** the transmission lines joining all of these switching centres.

Note that the terminology used here is heavily borrowed from the traditional telephone network (PSTN, public switched telephone network). The actual terminology used in today's hyper-converged networks, which marry voice, video, and data may vary considerably and it is still in a state of flux. However, in this document we are more concerned about the essential structure, and less about the precise terminology *du jour*.

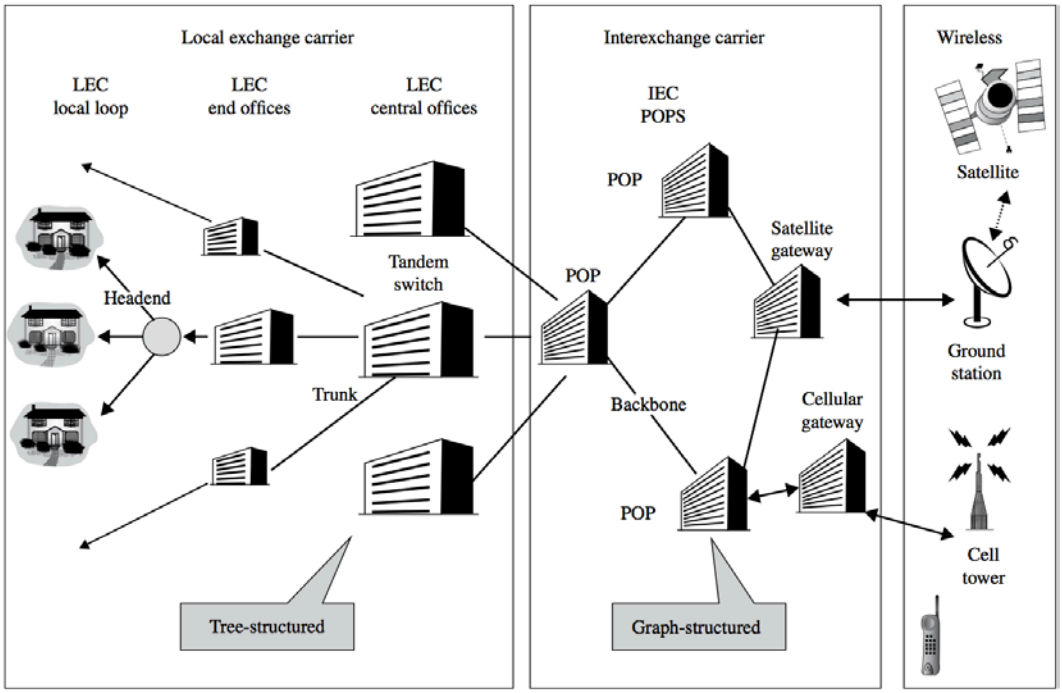


Figure 7. Structure of the telecom infrastructure. Source: (Lewis 2015).

Trunk lines and backbone lines can be implemented in various physical forms:

- Copper cables, either twisted pair or coaxial type; aerial, underground, or submarine.
- Fibre optic cables, having much higher capacity than copper ones. Also aerial, underground, or submarine.
- Terrestrial microwave links, operating in frequency ranges of 1 GHz to 50 GHz. Used for distances of about 40 Km, in cases where the terrain is very difficult to lay wire. Longer distances can be achieved by using repeaters.
- Satellite connections, which can bridge the distance between any points on earth. These links are connected to so-called **Satellite Gateways**, an exchange point to the landline network.

The picture below shows the site of a large Satellite Gateway facility hosting several satellite communication dishes, the famous Goonhilly Satellite Earth Station in the UK (near Helston, Cornwall). It was at one time the largest satellite earth station in the world, with more than 25 communications dishes in use and over 60 in total. The site also linked into undersea cable lines. In 2008 it was replaced by the Madley Communications Centre (between Madley and Kingstone, Herefordshire), which claims to be the largest earth station in the world, having 65 dishes, with three main dishes each having a diameter of 32 metres and weighing 290 tonnes.

Figure 8. Goonhilly Satellite Earth Station in Cornwall, UK (Source: Wikimedia Commons).

Mobile telephone networks are also linked to the landline PSTN network through **Cellular Gateway** exchanges. The topological structure of mobile networks is quite similar to that of local exchange carriers, but with the added complexity involved in handling the mobility of end-users hopping along exchanges and networks. The figure below (Figure 9) shows a schematic view of mobile networks.

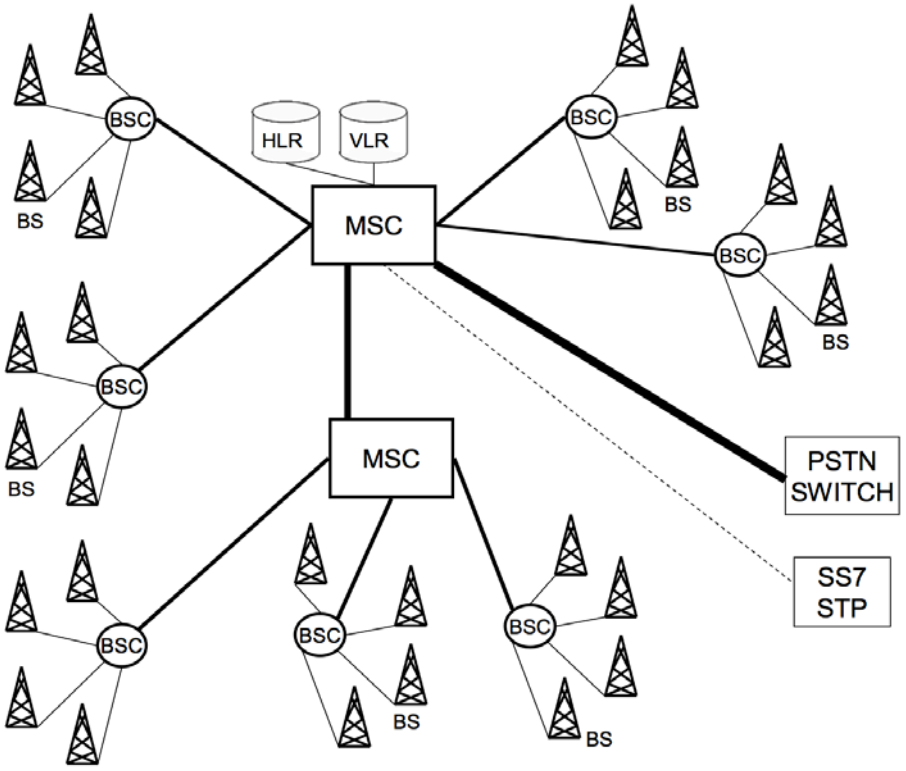


Figure 9. Schematic view of (cellular) mobile networks (Source: (Snow and Weckman 2013).

Here is a brief description of each element in mobile networks:

- **Base Stations (BS):** these are the antenna towers at the endpoints of the service. As their range is limited to just few kilometres, they are located so that their radio coverage conforms a tapestry of contiguous “cells”, in order to provide full coverage. Therefore the name *cellular* network. In Global System for Mobile Communications (GSM) networks, the correct term is Base Transceiver Station (BTS). Other colloquial synonyms are "mobile phone masts", “cell sites” or “cell towers”.
- **Base Station Controllers (BSC):** the BSC act as concentrators, controlling one or more Base Stations. BSC provide the intelligence behind BS, with functions that include radio network management (such as radio frequency control), BS handover management, and call setup.
- **Mobile Switching Centre (MSC):** the MSC is the primary switching centre, responsible for routing voice calls, SMS, and data. The MSC sets up and releases the end-to-end connection, handles mobility and hand-over requirements during the call, and takes care of charging and real time pre-paid account monitoring.
- **Home Location Register (HLR):** a central database handled by all MSC belonging to the same carrier, containing information about each of its mobile phone customers, such as phone number, SIM card identifiers, cell tower location, subscribed services, and other user configurations.
- **Visitor Location Register (VLR):** a database of subscribers belonging to other carriers, who have roamed into the jurisdiction of the MSC that it serves. The HLR and VLR databases provide the mechanisms to allow users to roam freely from network to network.
- **Gateway MSC:** an MSC that interfaces to the PSTN (i.e. the landline network).

Typically a BSC has tens or even hundreds of BS under its control, and they are housed in buildings in urban areas, or in sheds in rural areas. An MSC is typically a larger facility, handling a larger number of calls, and it is housed in better-protected buildings. The BS, i.e. the cell towers, are the element that is most exposed to weather threats.

Figure 10. A solar-powered GSM base station on top of a mountain (Source: Wikimedia Commons).

Figure 11. Cell towers are sometimes concealed for reasons of safety or appearance (Source: Wikimedia Commons).

In passing, let us mention that since commercial mobile networks are prone to local saturation of the radio-frequency spectrum (that is, the Base Stations can only serve a limited number of simultaneous calls), most emergency and police services use private mobile networks operating at different frequencies. That way the communications of police, search and rescue teams, etc. are guaranteed even in the event of massive overuse of mobile phones, which is common during emergencies and disasters. An example of such technology is the TETRA system (Terrestrial Trunked Radio), widely used across EU countries and also introduced in the US in 2012. In the US and Canada, similar competing systems are P25 and DMR.

To conclude this overall description of the telecom infrastructure, we will briefly discuss some topics and trends that we think are relevant in understanding reliability and risk assessment in this sector.

The transition from analogue to digital

The modern advances of the telecom sector started with the crucial step of transitioning from analogue to all-digital signals. This transition took place during the 1980s and 1990s. Originally the reasons driving this transition were the clear superiority of digital communications in terms of avoiding and recovering from the effects of noise. The rapid availability and low cost of digital components did the rest.

The convergence with video, TV, and other communication services

The next logical step for traditional telcos was to integrate services other than voice: fax, video, TV. This was an era of transition, where the telecom sector and the computing sector were still going their own separate ways. Telcos were pushing their idea of the Integrated Services Digital Network (ISDN), as a way to bring integrated voice, video, and data to the customer over telephone lines. For instance in the 1990s the Videotext service, of which the French Minitel is the best example, provided users with text information through a small video terminal, in what many consider a precursor of the World-Wide-Web.

Hyper-convergence with data networks: the rise of ICT

Then by the second half of the 1990s the Internet revolution took off rapidly, at such speed that it caught most telcos by surprise. Computer networks had developed a lot earlier, but for the most part as Local Area Networks (LANs). Wide Area Networks (WANs) were mostly private, used for corporate IT in large businesses, with one exception: the Internet. Originally a project of the US Defence Department, it began interconnecting Universities all around the world during the second half of the 1980s. Companies such as CompuServe, America Online, or Prodigy had tried to build their own private versions of the Internet, but the openness and international connectedness of the Internet quickly displaced those efforts, and they were forced to transform into Internet Service Providers (ISP). The Internet's takeover of the global communication landscape was almost instant in historical terms: it only communicated 1% of the data flowing through two-way telecommunications networks in the year 1993, already 51% by 2000, and more than 97% by 2007 (Hilbert and Lopez 2011).

For telcos this revolution meant a huge increase of data communications, while voice traffic remained the same. Now they were no longer in control of many of the aspects of data networks, such as transport and routing protocols. Traditional voice traffic runs on the SS7 protocol (Signalling System No. 7), while the Internet runs on TCP/IP. For some time telcos had been merely carrying Internet data traffic piggybacked (so to speak) on their traditional circuit-switched technology, but they were now accepting and integrating many of the ideas of TCP/IP networks (packet-switched technology) into their core network. In fact, just when the telecom industry was trying to standardize their "broadband ISDN" technology (B-ISDN, based on ATM, Asynchronous Transfer Mode), which was their vision for the future of integrated packet-switched networks, the Internet revolution quickly made IP the dominant protocol. Today, new carrier networks are "all IP" (also termed *New Generation Network*, NGN). This reflects the fact that all types of communications, whether voice or video, are quickly converging onto "just data", on the Internet. A consequence of this is the marriage between the telecom and the computing world, giving rise to the term *Information and Communications Technology* (ICT).

However, the difference between the two cultures can still be perceived in many aspects. Telecom engineers are biased towards communications that ensure *maximum guaranteed latencies*, which are needed for voice and video without lag or breaks. Circuit-switched technology guaranteed this, because essentially it set up a dedicated circuit between the two ends. On the other hand, computer people are more biased towards *data throughput*, and are more forgiving of latency. Packet-switched technology maximizes this and, moreover, it is resilient against node failures (the connection does not break, thanks to the dynamic rerouting of individual packets). We can clearly witness the trade-offs represented by these two approaches in our everyday experience with Voice-over-IP calls (VoIP). The connection may suffer lags and temporary break-ups but it is able to recover itself, whereas a traditional call would break up and need redialling.

Overreliance on IT and Cyber-risk

The convergence towards packet-switched, all-IP networks has many technological benefits but it also has disadvantages: the overreliance on computer software. This problem has two aspects to it:

- A cultural/technological one, derived from the intrinsic difficulty of software engineering. Software is extremely flexible, but also extremely complex. Compared to other engineering fields, designing software programs without defects (bugs) is virtually impossible. Disciplined design and rigorous testing minimizes the risk, but all quality-conscious software engineers know that achieving zero-defects is an impossible task. Take for instance what happened to the Ariane 5 rocket flight 501[9] or, closer to the topic at hand, the crash of the AT&T network in 1990[10].
- An economic one, driven by the trend towards software monocultures. The same exact version of a given software program may be used across all routers around the globe. This exacerbates the problem because, once a bug or security flaw is found, very large portions of the network are affected.

A word about capacities, the Internet, and regulation

One of the advantages of the dot-com boom at the end of the 1990s is that there was a huge overinvestment in backbone capacity in most countries, the EU included. This was also partly helped by the great advances in fibre optics technology. Ever since, telecom networks have been bottlenecked only on "the last mile", that is, the customer end of the network, where most lines are still low-bandwidth copper wire.

However, things are slowly changing. The dot-com crash, deregulation of long-distance telecoms, and some aspects of net-neutrality may conspire to generate a new "Tragedy of the Commons", ending up in capacity shortage. For instance, sometimes long-distance carriers are forced by regulation to share (getting paid a regulated tariff) their backbone infrastructure with smaller carriers. Net-neutrality legislation may also impact the business plans of large Telcos, depending on how it is done. Whatever the case, if Telcos do not find a compelling business case for the expansion of their backbone infrastructure, everybody loses. The situation is starting to look not entirely unlike what has happened to the transmission power grid in most advanced countries, after partial (and arguably clumsy) deregulation (Griffin and Puller 2005).

The "carrier hotel" trend

As highlighted by Ted Lewis in his book on Critical Infrastructure Protection (Lewis 2015), there is currently a trend towards the concentration of switching nodes belonging to different carriers into one common building, in order to share the facility, and also interchange traffic more efficiently. These are the so-called *carrier hotels*. In essence, it is like several Central Offices concentrated in the same building. The problem with this is the high concentration of risk that it entails. For instance, if the power supply fails for a carrier hotel, it brings down the nodes for all of the companies housed there. The weakening of the network is evident, but Lewis goes further and carries out some quantitative analysis of the network resilience due to this factor, based on mathematical models of general network dynamics (namely, Bak, Tang and Wiesenfeld's theory of self-organized criticality, together with concepts from graph theory).

[9] See for instance http://archive.wired.com/software/coolapps/news/2005/11/69355
[10] See http://www.phworld.org/history/attcrash.htm

3.2 Identification of critical elements. Rationale

According to the exposition above, and using that terminology, here is the list of critical elements in Telecom network infrastructure.

At the distribution level, operated by Local Exchange Carriers (LEC):

- **Inside Plant** equipment: typically housed in outdoors cabinets that aggregate several end-customer lines (the so-called local loop pairs). Also referred to as *headends*.
- The **End Offices**, where cables from the Headend points are collected (technically, Class 5 Telephone Exchanges). Normally housed under more robust sheds or buildings.
- The **Central Offices**, larger telephone exchanges (Class 4 Telephone Switches), used to interconnect local exchange carrier offices to the long distance transmission networks. Normally housed under more robust sheds or buildings.
- **Aerial trunk lines**: lines interconnecting End Offices and Central Offices, as well connections to the Interexchange carriers (aerial cables).
- **Underground trunk lines**: lines interconnecting End Offices and Central Offices, as well connections to the Interexchange carriers (underground cables).
- **RF link trunk lines**: lines interconnecting End Offices and Central Offices, as well connections to the Interexchange carriers (microwave links).

At the transmission section: operated by the Interexchange Carrier (IEC). In this section we have the following elements:

- **Class 1, 2, and 3 centres:** in the Bell System nomenclature, these are the three levels of telephone exchanges in the long-distance network. Class 3 are "Primary Centres" (and typically points of presence), Class 2 are "Sectional Centres", and Class 1 are "Regional Centres". All of them are normally networked under some kind of redundant, graph-like topology. Some are called "Points of Presence" when they connect the interexchange carrier companies to the local exchange ones.
- **Aerial backbone lines:** the transmission lines joining transmission-level switching centres (aerial cables).
- **Underground and submarine backbone lines:** the transmission lines joining transmission-level switching centres (underground and submarine cables).
- **RF and Satellite Backbone lines:** the transmission lines joining transmission-level switching centres (terrestrial microwave links and satellite links).

Additionally, we should also consider the following key elements of the mobile network world (we omit trunk lines, as they are the same as above):

- **Base Stations (BS):** also called Base Transceiver Stations (BTS), these are the antenna towers for cellular telephony (see the discussion in the preceding subsection).
- **Base Station Controllers (BSC):** the BSC act as concentrators, controlling one or more Base Stations.
- **Mobile Switching Centre (MSC):** the MSC is the primary switching centre, responsible for routing voice calls, SMS, and data.
- **Gateway MSC:** an MSC that interfaces to the PSTN (i.e. the landline network).

- **Home Location Register (HLR):** the central database that manages the carrier's own subscribers (see the discussion in the preceding subsection).
- **Visitor Location Register (VLR):** the database that manages roaming users (see the discussion in the preceding subsection).

Note how in this view we have not singled out any specific router/switch component. We consider them to be integral part of the abstract elements "Central Office", "Primary Centre", etc., as that is the main role that these nodes play in the networked infrastructure, i.e. switching traffic. Given the level of risk analysis needed in the RAIN project, we do not think it is necessary or useful to make these fine-grained distinctions.

3.3 Weather-related threats

We enumerate now the extreme weather threats to the telecom elements we described in the previous section:

- **Lightning:** telecom equipment is based on electronics, and electronics are quite sensitive to lightning and the power surges produced by lightning. Proper grounding and surge-protection techniques minimize the risk to a certain degree. All types of telecom equipment, with the exception of those under well-grounded Central Office buildings, are prone to this risk.
- **Wind storms:** affect mainly aerial, RF, and satellite trunk lines, as well as outside plants and cell towers. (Note: as mentioned before, we include here hurricanes, tornadoes, and tropical cyclones.)
- **Ice/snow storms:** affect mainly aerial lines and RF links. Ice storms can cause ice to grow on aerial lines, which may crumble under its weight, or whip violently when the wind blows large chunks of ice off the line.
- **Flash floods:** affect mainly outside plants. If they are accompanied by mudslides, they can also affect cell towers (Base Stations).
- **Extreme cold:** only affects indirectly, via the batteries and the auxiliary generator facilities, to Outside Plant equipment, RF link stations, and in general any switching centre without reliable access to the power grid.
- **Extreme heat:** affects the electronics of outside plants, RF link stations, cell towers, and Base Station Controllers.
- **Wild fires:** may affect aerial trunk lines and RF links; also the Outside Plant equipment in residential areas close to forests or dense vegetation.
- **Sand storms:** not a likely event in the EU countries, but a sandstorm can affect aerial trunk and backbone lines, directly or indirectly by fallen trees.

The table below lists our threat assessment (low/mid/high) for each of the weather threats listed above, as applied to each of the critical components of the power grid: generators, lines, transformers, breakers, etc.

	Outside Plants	End Offices	Central Offices	Aerial lines	Underground lines	RF/Sat links	Base Stations	MSC	BSC

Lightning	High	Mid	Low	Mid	Low	High	High	Mid	Low
Windstorms	High	Mid	Low	High	Low	High	High	Mid	Low
Ice/snow storms	High	Mid	Low	High	Low	High	High	Mid	Low
Flash floods	High	Mid	Low	Mid	Low	Mid	High	Mid	Low
Extreme cold	Low	Low	Low	Low	Low	Low	Low	Low	Low
Extreme heat	Mid	Low	Low	Low	Low	Mid	Mid	Low	Low
Wild fires	High	Mid	Low	High	Low	High	High	Mid	Low
Sand storms	High	Mid	Low	Mid	Low	High	High	Mid	Low

All of these threats (with the exception of extreme cold) have the potential to destroy equipment. Replacement of equipment is, in general, costly, but much less so than their analogous counterparts in the power network. One exception may be a severed backbone cable, such as a long-distance submarine line. In such a case, replacement could take many days.

The impacts in terms of loss of service depend a lot on the section of the network being affected. If the assets belong to the transmission section, and the incidents are not very widespread geographically, it is quite likely that the service remains largely unaffected. This is because the telecom network has a high grade of redundancy and also excess backbone capacity, at least for now (government regulation heavily affects future investments in this area). A worrying trend, however, is the concentration of several switching centres belonging to different carriers in so-called *Carrier Hotels*, which poses a concentration of risk. Still, if we compare the situation with the power infrastructure, impacts on the transmission network are more likely to remain local.

If the incidents affect the distribution section, the impact will depend on how far down the network this happens. Obviously, the higher is the concentration level of the Switching Centre, the higher the number of affected customers.

3.4 The impacts of weather-related outages in Telecom networks

In contrast to power grid outages, most studies about Telecom network outages focus strongly on characterizing the loss of service (extent and duration, essentially), and do very little in terms of quantifying business or societal losses in monetary terms. These kinds of secondary losses are increasingly difficult to assess, as telecom networks become enmeshed in all aspects of our daily life. Additionally, hyper-convergence with the world of IT complicates matters even further. The assessment of secondary losses should at least contemplate monetary losses, threats to public safety, and loss of lives. These last two are somewhat addressed by watchdogs and regulatory bodies by closely examining what happens to *emergency services* during network disruptions (the ENISA reports discussed in Section 5 measure this aspect). Monetary losses on the other hand are modelled crudely by means of simple calculations based on average revenues and labour costs. For instance:

LOST REVENUE = (GR/TH) x I x H	LABOUR COST = P x E x R x H
Where: GR = gross yearly revenue TH = total yearly business hours I = percentage impact on business operations H = number of hours of outage	Where: P = number of people affected E = average percentage they are affected R = average employee cost per hour H = number of hours of outage

In any case, these models contain crucial parameters that cannot be easily measured. In the above table, parameters *I* (percentage impact on business operations) and *E* (average percentage of people's work affected) embody this difficulty. It is quite evident that measuring the impact of loss of information inputs is harder than measuring loss of energy inputs in our production processes. Consequently, and in contrast to the electrical power infrastructure, there are no serious studies quantifying these monetary losses.

3.5 Interdependencies of the Telecom Infrastructure with other CI

The telecommunications infrastructure has an intrinsic dependency on the supply of power. All equipment devices consist of electronics, and these need electric power to run. Therefore all switching centres, base stations, satellite downlinks, etc., are retrofitted with backup power. The figure below (Figure 12) shows how this backup power typically consists of batteries, and sometimes also includes a backup generator (typically a diesel one).

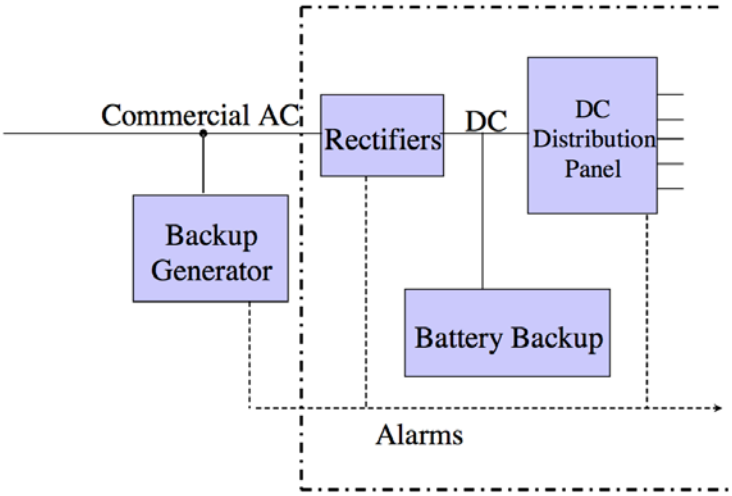


Figure 12. General scheme of power supply to telecom equipment / facility (Snow and Weckman 2013).

In case the power from the grid goes out, the batteries supply backup power first, with a duration that may go from 30 minutes to 8 hours, or even a full day. For long power outages, the diesel backup generator kicks in. Equipment with lower power consumption requirements may be made more independent by using PV panels to recharge the batteries during the day; however, this is not the most common case.

It is interesting to note how, in the event of a long power blackout, the Telecom network then becomes interdependent with the Transportation infrastructure, as the diesel generators need to be refuelled.

Having said all this, power grid cuts are a dominant cause of severe network and service outages in the EU's electronic communications sector, as can be seen in the ENISA annual reports about major incidents. A special report by ENISA on power supply dependencies (ENISA 2013) points out that actual resiliency against power cuts was not sufficient in many cases, and details a series of recommendations for Telco providers and National Regulatory Authorities. They also suggest that power utilities should consider including preferential treatment schemes for Telco loads, in the context of blackout restoration.

4. Case studies of past weather-related failures

4.1 Case studies in electricity networks

We will select a few representative cases of weather-related blackouts or widespread disturbances in transmission systems (sometimes the difference between a large disturbance with lots of load-shedding and a blackout is not so clear). We will try to extract cases from the EU area (EURELECTRIC 2006), but we will also briefly mention some in North America because they have been extensively studied and the reports have been made public.

4.1.1 Windstorms Lothar & Martin (France, 26-28 Dec. 1999)

Overall description

Extra-tropical cyclones Lothar and Martin affected Western Europe on December 26-28, 1999. The wind fields from the two storms covered more than half of France and extended into Switzerland and Germany. The storms caught Europe by surprise. Meteorological forecasts failed to predict Lothar's dramatic inland intensification. Modern infrastructure such as electrical distribution systems, transportation, and communication lines were hit particularly hard, leading to several very large insured and uninsured losses throughout the industrial and public sectors. Observed damage to residential structures was in line with previous experience, however, the total damage from Lothar and Martin covered an exceptionally large area, leading to higher overall losses.

Lothar was the first storm, arriving with hail and rain crossing the northern part of France during the night of December 25 to 26. The gusts of wind started on the Brittany Coast around 3.00am. Wind speeds of 170 km/h were recorded in Brest. The storm gained speed and power as soon as it crossed France. At Orly airport, 173 km/h was recorded, 216 km/h on the top of the Eiffel Tower, 150 km/h in Paris streets, and 180 km/h in the Vosges Mountains. There are no data in Meteo France archives of such fierce weather ever being recorded.

Martin was the second storm, hitting the southern part of France on December 27 around 5 pm. There, wind speeds of 150 km/h were recorded.

Damage caused

Between them, these windstorms produced over €14.2 billion in economic damage, approximately €7.7 billion of which was insured. This ranks as the third largest insurance loss ever, after Hurricane Andrew in 1992 and the 1994 Northridge Earthquake. Windstorm Lothar alone represents the largest monetary insurance loss in European history. The global insurance industry was not prepared for losses of this magnitude in France. Common risk transfer practice in France was for insurers to buy cover based on the level of losses in the 1990 storms Daria and Herta. These covers proved inadequate, because wind speeds in the 1990 storms were almost 20% lower than those

experienced in Lothar and Martin. In addition, the occurrence of two storms within the typical 72-hour interval for reinsured events tested reinsurance contract definitions and previous assumptions.

During the first storm, 30 people were killed. Damage was substantial with several houses and other buildings partially or totally destroyed. Many roads, motorways, and railways were blocked. The electrical grid also suffered severe damages with flooded substations, broken or tangled wires, flattened poles, twisted pylons and so forth. The interconnection grid was also badly affected with lines to Germany temporary out of order. 5,500 medium and low voltage poles needed to be replaced.

The storm also caused huge damage to forests. Some of them were completely ruined. Thousands of trees fell on MV and phone overhead lines. Air and railways traffic was severely disturbed. But most damage occurred on the Electricité de France (EdF) grid. For long, EdF had been prepared for ice storms (white frost or sticking snow on lines), but such a severe situation was completely unanticipated by the company. Nearly 3.4 million household customers were left without electricity. 35 EHV lines (a quarter of the total number) tripped due to protection relays. 180 HV lines were brought to the ground and more than 100 HV/MV substations were out of order. Innumerable lengths of MV and LV lines collapsed under falling trees.

Impact on customers and civil infrastructure
On the morning of December 27, 1.4 million household customers were without electricity, mainly in the East, the North and in Paris suburbs. In these regions, the EdF grid was severely damaged: 120 EHV pylons and 67 HV lines.

After the second storm, the situation became worse. The total number of household customers without electricity on December 28 reached 3.45 million.

Repair procedures
Immediately after the first storm, 8,000 people worked in call centres to provide information to customers. EdF gave specific and regular information to the prefectures and city halls concerning the local situation. The EdF website provided regularly updated information to the public.
Exceptional measures to restore electricity in a minimum of time were set into force. Thirty helicopters examined lines in order to locate the damage precisely. About 6,000 EdF operators started repairing the grid (most of them having interrupted their holidays). They were helped by 6,000 other people from public work companies. 5,000 technical vehicles were used. In most regions, a co-ordinated plan between authorities, helping organisations, the army and EdF was deployed.

After the second storm, new reinforcements were added. Consolidated EdF teams of operators and equipment started restoring electricity in the country:

- 18,800 operators specialised in grid maintenance;
- 40,000 logistic and commercial employees;
- all operators with electrical ability working in any other company;
- 3,600 soldiers;

- operators and engineers from French overseas territories (Guadeloupe, Martinique, Guyana and Réunion);
- EdF group companies: Clemessy, London Electricity, which sent 6 drilling cranes to create foundations of new pylons;
- all the EdF staff on holidays and also “early retired” were called back to help.

1,200 foreign operators from 17 countries contributed to the restoration: e.g. Ireland (176 on Atlantic coast), Great Britain (170 in the North and Vosges Mountain), Italy (151 in Central Mountain and Savoie), Germany (140 in Dordogne, Limousin and Vosges Mountain), Spain (130 in South West), Belgium (115 in the North and East), Czech Republic (30 in Champagne) Netherlands (25 in the North), Portugal (20), Morocco (20), Hungary (15 in Paris suburb Montereau), Croatia (12). Foreign companies sent 300 portable power generators across a broad power scale from some kW to 1.25 MW, which EdF bought or rented. For example, 25 units of 850 MVA were loaded in a plane from Zagreb in Croatia to Bordeaux. German company Ets Wilson sent 22 units transported by German civil security. London Electricity sent 5 powerful units to Périgueux and Limoges. In fact, EdF used all the available portable power generators in Europe and beyond: some of them came from Canada. Altogether, 1,600 units were connected. Operational equipment was also sent to France, e.g. Hungary provided two off-road cars and two lifting trucks (12 m and 20 m).

After days of work, recovery teams concentrated on regions with significant access difficulties, such as forests, mountains or flooded zones. Just before the weekend of January 8/9, 97% of the affected household customers had recovered electricity. The last customer was reconnected on January 14.

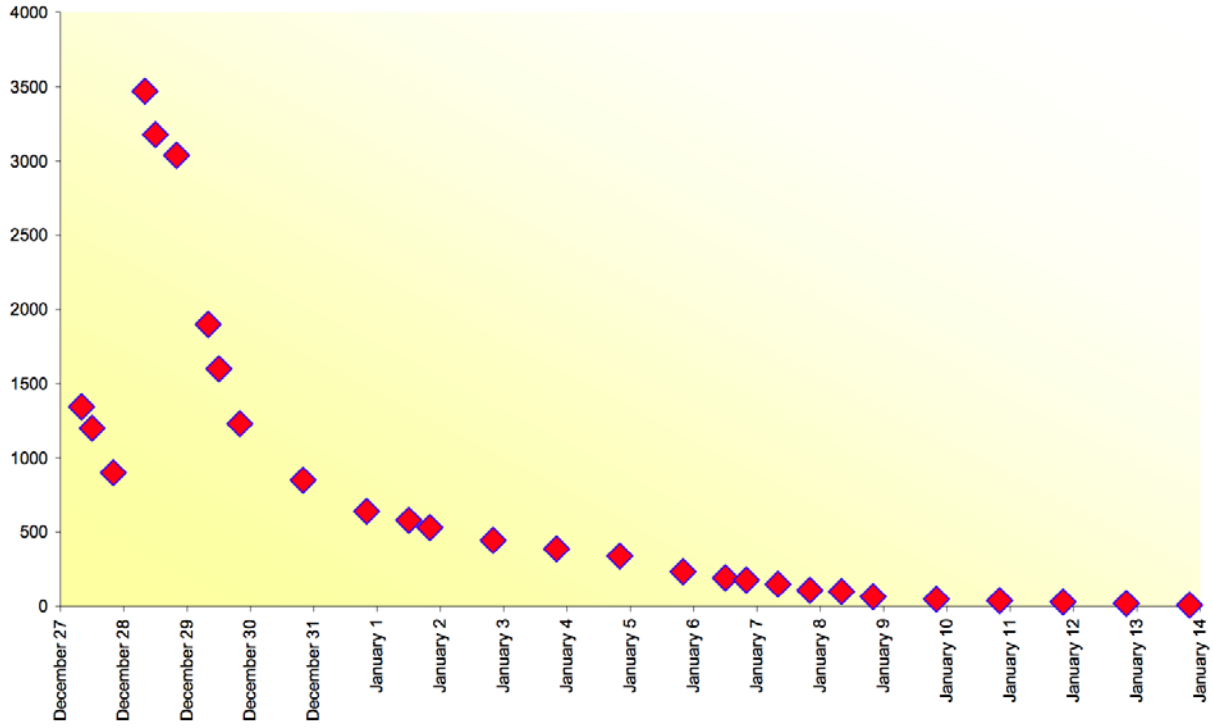


Figure 13. Number of households without electricity, in thousands (EURELECTRIC 2006).

Estimated costs

The following estimation of *direct* costs was made immediately after the storm:

- Generation: 38.9 M€
- Grid: 1240 M€
- Loss of energy sales (0.7 TWh was not supplied): 69.3 M€
- Compensations paid to customers: 60 M€

4.1.2 Heavy snow/wind storms in Poland (November 2004)

Introduction

On November 19, 3 of the 17 administrative regions in Poland, a part of Silesian and parts of the Malopolskie and Świętokrzyskie *voivodships* (provinces) were affected by a snowstorm with heavy snowfall and extremely strong wind gusts. The weather conditions caused some serious disturbances in the operation of the national electricity system, both in the transmission grid (400 and 220 kV) and in the 100 kV sub-transmission grid, bringing about many serious damages both to national and international transmission lines. As a result of these disturbances, the dispatching services of the TSO and DSOs had to conduct a series of actions in a very short time in order to minimise the danger, to eliminate the disturbances and also to restore the dispatch of electricity to customers. The storm caused serious problems in the transmission system, with the disconnection of some 1,000 MW of load in the area covered by the Katowice distribution operator.

Event description

As the result of the storm, 400 kV and 220 kV cross-border tie lines with the Czech Republic tripped. In Poland, three 400 kV lines, six 220 kV lines, and one 400/220 kV 330 MVA autotransformer also tripped, as well as four smaller 220/110 kV 160 MVA autotransformers. The disconnection of the 400 kV line between Dobrzyn and Albrechtice (permanent since November 16, due to line damage at the Albrechtice station) had a significant influence on the sequence and evolution of this disturbance.

The worst hit region was in southern Poland, where the operation of 110 kV lines is coordinated by the Katowice DSO. The main characteristics of the disturbances were:

- simultaneous intensive propagation of outages and other disturbances (undervoltages, undervoltages, overloads) in the transmission grid at 400 kV, 220 kV and 110 kV levels
- simultaneous intensive propagation of disturbances in the grids of some distribution companies at different voltage levels
- with widespread serious damage to equipment, disabling the restoration of electricity supply within a short period of time
- large number of disturbances for final customers in a short period of time, due to the tripping of the radial 110kV connection, which included several stations having low internal redundancy (sectionalized single-bus bar)
- loss of connections between the 110 kV distribution grid and the transmission 400 kV and 220 kV grids (tripping of 4 autotransformers, 3 of them being switched off permanently).

The distribution system operator (OSDE) and the local dispatching system services (ODM) undertook coordinated actions in order to accomplish the following targets:

- maintaining the connection of 110 kV grids with each other and with the bulk transmission grid
- introduction of a temporary operation system for distribution grids, in order to maintain the cohesion of the grid and power output from the operating generation units
- balancing of the 110 kV sub-transmission grid
- recovering the transmission grid that tripped, restoring the voltage after quick analysis of the security of the system, taking into account the generating units then in operation
- preventing the formation of islanded areas
- restoring supply to final customers disconnected for security reasons
- cooperation with the operation/maintenance services, in order to locate the damage and to determine the date of their readiness to switch back on.

Damage caused. Impact on customers and civil infrastructure

Świętokszyskie province: some 51 distribution lines and 434 transformer stations were destroyed. Around 13,000 customers suffered interruption of electricity supply. The failures were repaired within two days.

Silesia province: 6135 failures were recorded. As a consequence, 310,000 household and industrial customers, such as steel mills, water conditioning stations, coal mines and cooling plants, lost supply. The loss of supply to the Water Production Plant Goczałkowice and Zawada for 24 hours caused shortages in fresh water supply to the Silesian area. Disturbances in the functioning of public transport also occurred. The traction power grid of railway traffic was also affected and 25 tramway traction lines were damaged.

Małopolskie province: due to the damage to HV and MV lines, approximately 200,000 customers were left without electricity supplies. On November 20, 757 substations were out of operation and 57 MV lines were damaged. The following day, 1 HV line and 32 MV stations were still out of order. The largest number of failures was recorded in Kraków. On November 22, 1 HV line, 26 sections of MV lines and 24 MV stations remained out of service. About 4,000 customers were still without electricity. The faults in the MV network were repaired by November 23, and the HV line was put back into operation on the following day.

Estimated repair costs

According to the reports, the costs resulting from these events are estimated at around €20 M. The repair work started immediately. It was well organised and coordinated by local crisis centres, the TSO, DSOs, Polish State Forests, and other bodies involved. Actions were executed in an efficient manner. Customers were partly supplied by emergency equipment where possible. Administration bodies were informed about the availability of preferential loans for reconstruction of the damaged infrastructure, and insurance companies compensated damage and losses.

Political consequences

The situation showed weaknesses in the flow of information between the distribution companies and the administration bodies at province level. During subsequent meetings between representatives of local administration and distribution companies, new procedures were developed to facilitate information exchange.

Summary

The November 19 storm was one of the most serious disturbances in the recent history of the Polish national electricity system. Having parallel impacts at all levels of the national grid, it clearly showed how important the cooperation between system operators is for the safe operation of the national system. At the transmission level, data analysis shows that it took only a few minutes for the operation services to make decisions on the necessary switching, steering and regulating actions. It should be noted that dispatching services were effectively maintained due to the correct information flow, hierarchical system of decision-making and reliable operation of data communication appliances, plus appropriate cooperation with operation services.

Recent developments in the grid configuration and effective regulatory actions limited the impact of grid disturbances on the operation of generating units. During the disturbances, two generating units were tripped by the automatic safeguard equipment, one generating unit was disconnected on the dispatcher's orders, in order to ensure the safety of equipment, two generating units were disconnected in order to balance the system; and output from one generating unit was limited.

However, the location of disconnected and severely damaged lines in the 110 kV grid made it necessary to make a temporary set of distribution line arrangements in the following hours and even days. At that time, some parts of the grid were 'emergency supplied', with lower reliability, which created a real risk of repeated disconnection of customers. A great problem was the relatively large number of stations without permanent operation personnel and a lack of remote connector-control in many places.

4.1.3 Gudrun/Erwin windstorm (Sweden, 8 Feb. 2005)

Overall description

This storm was named Gudrun in Norway and Sweden, and Erwin in Germany. It hit southern Sweden on January 8, with devastating effects. The entire infrastructure was hit. Roads and railways in large parts of southern Sweden were obstructed by large numbers of trees; for instance there were no trains between Stockholm and Malmö for 12 days. Electricity outages were extensive and a large part of both the landline and mobile telephone traffic in the affected area was hit for a long period.

The storm gathered northwest of Ireland and followed a path usual for intense low-pressure systems passing over Sweden. It was not exceptional from a meteorological point of view, although it hit a larger area than usual. During the storm, there were hurricane-force winds (more than 117.7km/h) over large areas and the most powerful gusts reached 151km/h. That had happened several times before during the last 100 years, but had never led to such damage. 70 million cubic meters of wood (150 million trees) were uprooted, corresponding to almost one normal year of woodcutting for the

whole of Sweden (the second most severe storm in 1969 uprooted 25 million m3 of wood). The severe consequences can be explained by a number of contributing circumstances. Among other things, there was no ground frost at the time and the planted spruce trees may have been biotopically unsuitable for the area. It was primarily in spruce woods that electric lines were cut, causing outages.

Damage caused

The storm caused widespread outages that lasted for a long time. The generation system was also affected. Due to network problems, two nuclear power plants, amounting to 25% of Sweden's generation, were shut down for a short period (the Barsebäck plant because of "line dancing", and Ringhals due to salt problems in the switch yard).

Sub-transmission networks were proportionally less badly hit than distribution networks, because rights-of-way are normally wider or "tree secure". It was only Sydkraft's sub- transmission network that was affected to a large extent, and it also took longer for Sydkraft to restore the network – seven days compared to less than 24 hours for other network companies.

Impacts on customers and civil infrastructure

Immediately after the storm, there were 663,000 network customers without electricity supply. Of these, 295,000 belonged to Sydkraft's network. There were some other network companies with many affected customers: Vattenfall with 260,000 customers facing power outages, and Fortum with 50,000. In relative terms, the local distribution company KREAB Öst was hit the hardest, with 100% of its 7,200 customers without electricity supply, mainly due to problems at sub-transmission levels (Sydkraft's 50kV line feeding KREAB was out of service). Sydkraft's customers had to wait the longest time before the electricity supply was resumed, due to extensive damage to the sub-transmission network and many poles that had collapsed. 354,000 network customers (out of a total 663,000) had their electricity supply restored within 24 hours; 159,000 customers had to wait between one and three days; 82,000 network customers got their electricity back 4 to 7 days after the storm; 56,000 customers were without electricity between 8 and 20 days; and finally, 12,000 customers had to wait for more than 20 days before supply returned. In general, Sydkraft had the worst problems restoring supply, some of their customers being without supply for 34 days. The graph below gives some figures for how long customers of different network companies had to wait before the electricity supply returned.

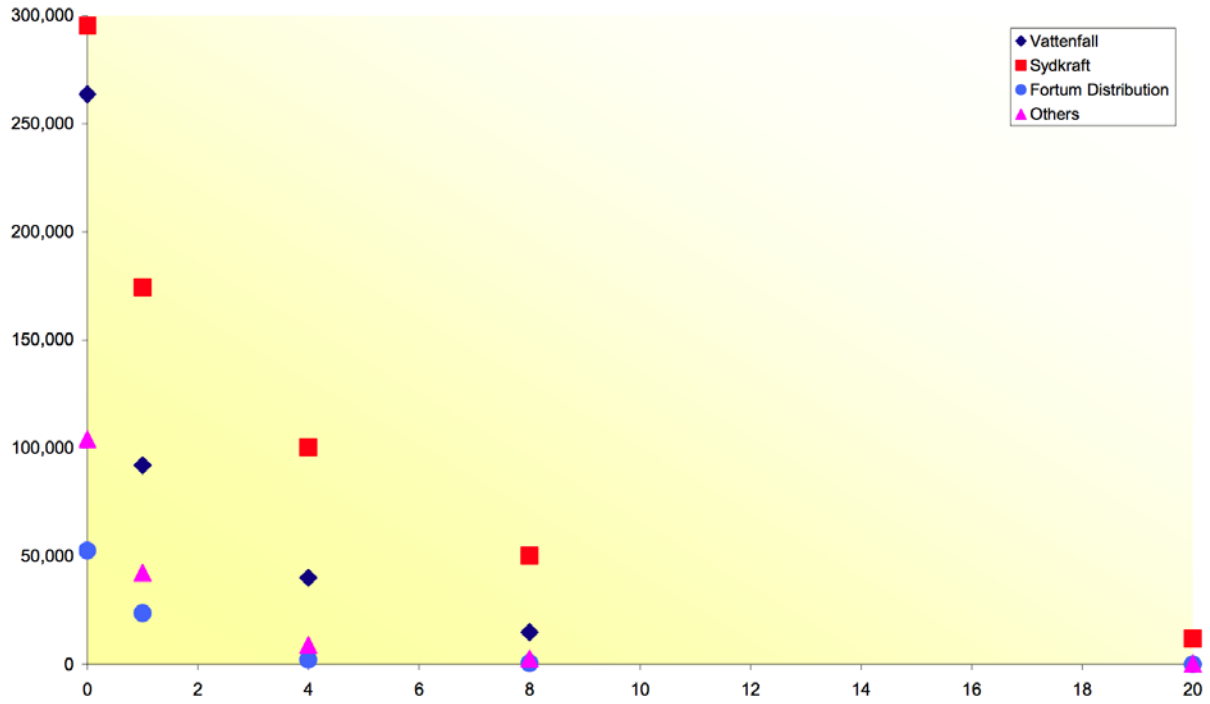


Figure 14. Customers of distribution companies without electricity by number of days (EURELECTRIC 2006).

Besides affecting the lights and in most cases the heat supply, there were major problems with communicating and receiving information. Not only did mobile phone batteries run out and computers stop working, but the landline telephone network was also damaged and mobile stations had insufficient battery capacity to stay in operation for more than 1-2 days. Receiving information therefore became a critical issue for many households. Transportation by car was almost impossible due to the large number of trees fallen across the roads. Many households had a rough time just trying to keep their houses warm, to prepare food and to receive information as to when the electricity supply could be expected to be restored. The quality of life was drastically reduced for many families, despite the great efforts of authorities, network companies, the army, municipalities and local companies in attempting to help as many people as possible.

Repair procedures

The repair work started very quickly. However, due to the extent of the damage, Sydkraft soon faced problems with lack of spare parts and people. Vattenfall and Fortum, having fixed their own networks, lent some resources to Sydkraft. In order to provide customers with electricity as soon as possible, more than 1,000 small mobile generation units were used and connected to the network at strategically important points. The repair procedures for some of the network companies are summarised below.

- **Sydkraft.** Around 20,000 km of network lines were damaged in Sydkraft's network and around 2,000 km had to be completely rebuilt. On January 10, almost 1,400 people were working on the repairs and on the next day, 600 people were added. At the end of that week (January 15), around 2,400 people were working on the repairs following the arrival of

personnel from Germany, Poland and the Swedish army. Hercules aircraft were used for transporting spare parts from the northern part of Sweden. A special project organisation was set up for the administration of the repair works. In order to facilitate communication, around 100 satellite telephones were bought from abroad. Spare parts were sent from Sydkraft's mother company E.ON in Europe and other parts of the world.

- **Vattenfall.** Vattenfall's special force for large disturbances, consisting of around 200 people, was put into operation already on January 8. For safety reasons, the repair work could not get started during the on-going storm, but only as soon as it was considered safe to start. Up to 1,300 people were active in the repair work. In addition, around 15 helicopters were used. Special resources from northern Sweden were brought to the scenes of the damage. Massive resources were used to get information out to customers, which was difficult due to problems with the telephone network.

- **Fortum**. Fortum created a special organisation for dealing with the repair work. Around 300 to 400 people were engaged in restoring the electricity supply. Fortum also used 4-5 helicopters in the works. Fortum experienced no major problems finding spare parts.

- **Other network companies**. The 8 smaller network companies affected by the storm had around 600 staff involved in the repair works, some of them borrowed from other network companies and the Swedish army. Some of these people came from other parts of the country. Some 40-50 mobile generation units were used.

Emergency procedures and cooperation

Approximately 5,000 people were engaged in the restoration of the network. In the international company groups, employees from neighbouring countries were also assigned to the restoration work. In Sweden, cooperation between network companies is formed under the aegis of SwedEnergy, the Swedish association of electricity companies. This cooperation was severely tested during the storm. A cooperation procedure had been established after earlier storms and, according to the companies involved, it worked very well during the storm.

An important role in the cooperation was played by the Federation of Swedish Farmers. They assisted in clearing roads, transporting food and water, helping sick and old people and so on.

The cooperation with municipalities and county administrative boards seems to have worked well in most cases. The military helped with transportation, local forestry helped with clearance work and other local organisations and individuals assisted in locating faults. Also, many network operators have agreements with external contractors in case of emergency. During the storm Gudrun, the network operators reported that contributions from these had been of great importance.

Estimated costs (repair, compensation, investments)

The overall cost to the network operators was calculated at about 2,350 MSEK (€257 M). About two thirds of this (€168 M) was spent on clearance, reparation and re-building the network. Compensation to customers, paid voluntarily based on the companies' own rules, amounted to €67 M (an average of about €280/customer). The various companies reported costs ranging from about €33/customer to €1,300/customer.

4.1.4 Tropical Storm Delta (Canary Islands, 28-29 Nov. 2005)

Tropical Storm Delta was a late-forming tropical storm that affected the Canary Islands and Morocco as a strong extratropical storm. It began as a subtropical storm in the central Atlantic Ocean, which at first evolved to just below hurricane strength but then appeared to weaken. However, after showing some erratic movement, and against all predictions, it headed northeast towards the Canary Islands, picking up strength again. It hit the Canary Islands on the 28—29 of November 2005, causing a significant amount of devastation.

Since the islands generally enjoy mild weather all year round, most infrastructures were not prepared for windstorms of this level. However, the power grid was particularly affected, comparatively more than other infrastructures.

Some key data points about the blackout, collected from the official report by the Canary Islands Government Commission set up after the incident, and from various web sources:

- About 300,000 customers were affected by power cuts (and 12,000 lost telephone service)
- Four days after the event, 20,000 customers in the metropolitan area of Tenerife were still without power. In some areas of Tenerife and La Palma the power grid was not restored until seven days later.
- The blackout also affected during one day the water supply (electric pumps) in several neighbourhoods in La Laguna (population 150,000).
- The cost of the damages to the grid infrastructure was estimated at some €12 million.
- Total overall costs of the incident were estimated at €300 million.

Thousands of homes were left without electricity as rusted pylons were blown down. Some homes and businesses had to wait the best part of a week for normal supply to be re-established. The wind toppled or wrecked 39 high voltage pylons and no less than 103 medium voltage ones. The corroded condition in which the structures were found to be in provoked little short of a major scandal. Various institutions, including the Santa Cruz city council, initiated legal proceedings against Unelco-Endesa, the island utility. Business leaders were shocked to discover that the company did not possess a basic support and back-up system in Tenerife, such as a warehouse to store equipment and replacements for use in the case of a major incident of this kind.

With the Canary Islands' power grid substantially disrupted, the Unelco-Endesa power company was forced to use temporary generators to boost power at sub-stations far from the main grid. In La Corujera in Santa Úrsula, these generators were poorly received and over 1,000 local residents claimed to be affected by the noise and pollution.

Four high-voltage towers toppled very near a main motorway, a few kilometres away from a large generating station (las Caletillas-Candelaria). This was the main supply line to the capital and its metropolitan area (San Cristóbal de La Laguna, Tegueste, El Rosario). Therefore, an emergency

underground line was quickly laid down alongside the motorway, covered by concrete. It was in July 2007, one and a half years after the incident, that all high-voltage towers were rebuilt and the emergency line could be finally removed.

Figure 15. Effects of tropical storm Delta in the Canary Islands, 2005 (source: Foro contra la incineración de Tenerife).

Figure 16. Effects of tropical storm Delta in the Canary Islands, 2005 (source: Foro contra la incineración de Tenerife).

4.1.5 Some case studies in North-America

We offer below a short description of a few selected blackout events that have taken place recently in the USA and Canada. They are interesting because they are all relatively recent and, given the heightened awareness to this problem, they have been subject to extensive analysis and public scrutiny by regulatory bodies such as FERC and NERC.

The great August 2003 blackout in northeast USA-Canada

On August 14, 2003, large portions of the Midwest and Northeast United States and Ontario, Canada, experienced an electric power blackout. The outage affected an area with an estimated 50 million people and 61,800 megawatts (MW) of electric load in the states of Ohio, Michigan, Pennsylvania, New York, Vermont, Massachusetts, Connecticut, and New Jersey and the Canadian province of Ontario. The blackout began a few minutes after 4:00 pm and power was not restored for 2 days in some parts of the United States. Parts of Ontario suffered rolling blackouts for more than a week before full power was restored (US-Canada Power System Outage Task Force 2004).

This case is not really related to extreme weather; however, the root cause of this high-profile incident was traced back to trees tripping an important line, which then triggered an ensuing series of cascading failures. This highlights how important the issue of vegetation management in right-of-ways can be. More generally, the case contributed to raise awareness of the problems of the aging power grid. It is interesting because it showed how delicate transmission operations are, as this blackout could have been largely avoided if the control operators could have had better and timelier situational awareness.

February 1-4 2011, Southwest USA disturbances

This case is quite important, as it resulted in new NERC rules making mandatory to prepare for winter at critical generator plants (“winterization” rules). 67% of the generator failure was directly attributed to cold weather in this case.

During the first week of February of 2011, the Southwest states of Texas, New Mexico, and Arizona experienced an extreme cold weather event. There were a recurrence of rolling blackouts and extensive natural gas curtailments. Concluding a six-month inquiry, the task force found that a majority of the electric outages and gas shortages were due to weather-related causes. In total, approximately 1.3 million electric customers did not have service at the peak of the event on February 2, and a total of 4.4 million were affected over the course of the event from February 2 through February 4. Natural gas customers also experienced extensive curtailments of service during the event. These curtailments were longer in duration than the electric outages, because relighting customers’ equipment has to be accomplished manually at each customer’s location. Analysis reports of this event point out to interdependencies between gas supply and electricity generation that had been previously unnoticed.

October 2011 Northeast Snowstorm Event

On May 31, 2012, FERC and NERC issued a joint report on the October 29–30, 2011 Northeast Snowstorm. The unprecedented fall snowstorm hit the north-eastern United States, blanketing the region with up to two and a half feet of heavy, wet snow. Snowfall amounts broke all previous October records throughout the Mid-Atlantic and New England regions. The snowfall totals were most significant in New England, but parts of New York, New Jersey, and Pennsylvania also received well over a foot of snow. On the morning of October 30, near the end of the storm, more than 3.2 million homes and businesses were without power. Thousands were without power for more than a week, some for as long as 11 days. Estimates put storm costs between approximately $1 billion and $3 billion.

The joint inquiry focused on determining the causes of the transmission facility outages and on the steps utilities could take to improve their performance in maintaining grid reliability during the next large snowstorm or similar weather event. In this case the transmission system was responsible only for 5% of the outages (95% was due to distribution failures). Nevertheless, the inquiry stressed the need for improved vegetation management for the transmission infrastructure.

4.2 Case studies in telecom networks

In contrast with the power sector, network outages in the Telecoms sector are not audited in the open or with the same level of detail released to the public (this is probably a reflection on the fact that the telecoms sector is more deregulated). Another defining characteristic is that most risk studies are heavily biased towards *cyber-security* risks.

It has been therefore impossible to obtain good examples of study cases for weather-related network outages. However, the reports by ENISA (The European Union Agency for Network and Information Security[11]) provide since 2011 annual statistics about major events (ENISA 2014). ENISA now requires each National Regulatory Authority to report incidents affecting the following communication services and networks:

- Fixed telephony (e.g. PSTN, VoIP over DSL, Cable, Fibre, etc.),
- Mobile telephony (e.g. GSM, UMTS, LTE, etc.),
- Fixed Internet access (e.g. DSL, Fibre, Cable, etc.),
- Mobile Internet access (e.g. GPRS/EDGE, UMTS, LTE, etc.)

In their yearly reports, ENISA details the thresholds for the extent and duration of an incident to be considered of enough significance to be reported. The reports distinguish four categories of root causes:

- **Natural phenomena** – This category includes incidents caused by severe weather, earthquakes, floods, pandemic diseases, wildfires, wildlife, and so on.

[11] See the ENISA website at: www.enisa.europa.eu

- **Human errors** - This category includes incidents caused by errors committed by employees of the provider or outside the provider, during the operation of equipment or facilities, the use of tools, the execution of procedures, etc. (e.g. an excavator cutting off a cable.)
- **Malicious attacks** - This category includes incidents caused by a deliberate act by someone or some organisation, e.g. a cyber-attack or a cable theft.
- **System failures** – This category includes incidents caused by failures of a system, for example hardware failures, software failures (bugs) or flaws in manuals, procedures or policies.
- **Third party failures** – This category includes incidents caused by a failure or incident at a third party. This category is used in conjunctions with one of the other root cause categories.

From the 2013 report (ENISA 2014), we will extract the following interesting conclusions and data points:

- 90 major incidents reported: This year, in total 19 countries reported 90 significant incidents and 9 countries reported no significant incidents.
- Mobile networks most affected: Approximately half of the major incidents had an impact on mobile Internet and mobile telephony.
- Mobile network outages also affect many users: Incidents affecting mobile Internet or mobile telephony affected most users (around 1.4 million users and 700 000 users respectively per incident). This is consistent with the high penetration rates of mobile telephony and Internet.
- Impact on emergency calls: A fifth of the major incidents had an impact on the emergency calls (aka 112 access).
- System failures are the most common root cause: Most major incidents were caused by “System failures” (61 % of the incidents). Most common detailed causes were “software bugs” and “hardware failures”.
- System failures affect the most user connections: around 1.5 million user connections on average per incident. Interestingly, the detailed causes affecting most user connections were “software misconfiguration”, “software bugs”, and “power surges”.
- **Natural phenomena (heavy snowfall, storms, etc.) and malicious actions (arson, cable theft, etc.)** cause the longest lasting incidents: more than 50 hours per incident, on average.
- **Natural phenomena and system failures have most impact:** Multiplying the number of user connections and duration, one obtains a measure for total impact, or ‘total user-hours lost’. **Natural phenomena had on average most impact, followed by system failures.** Looking more in detail, power cuts, heavy snowfall, cable cuts and storms, respectively, impacted most user hours.
- Base stations and switches were most affected: Overall, base stations, switches and mobile switching were the assets most affected by incidents.

It is therefore quite interesting to remark that, according to total user-hours lost, which is arguably the best measure of the direct impact of loss of service, natural phenomena is the root cause having the highest impact on the telecom infrastructure. System failures provoke a higher number of

incidents and even affect a higher number of customers, but they are quickly recovered from. So when the product of user connections and outage duration is taken into account, natural phenomena become the cause with the largest overall impact.

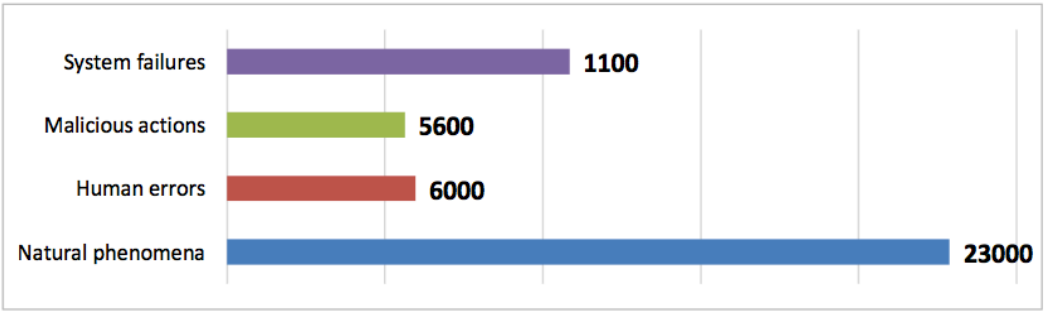


Figure 17. Average user hours lost per incident per root cause category (source: ENISA 2014).

We quote the 2014 report:

> *Severe storm affecting power supply and mobile networks causing large scale mobile outage (duration: days, connections: thousands, cause: natural phenomena and third party failure): A deep low-pressure with storms and hurricane winds caused power outages, damaged transmission lines to mobile sites, and damaged access networks. Hundreds of GSM and LTE sites and thousands of UMTS sites were affected, with some lasting longer than 72 hours.*

It is also interesting to have a look at the detailed causes of the lost user-hours:

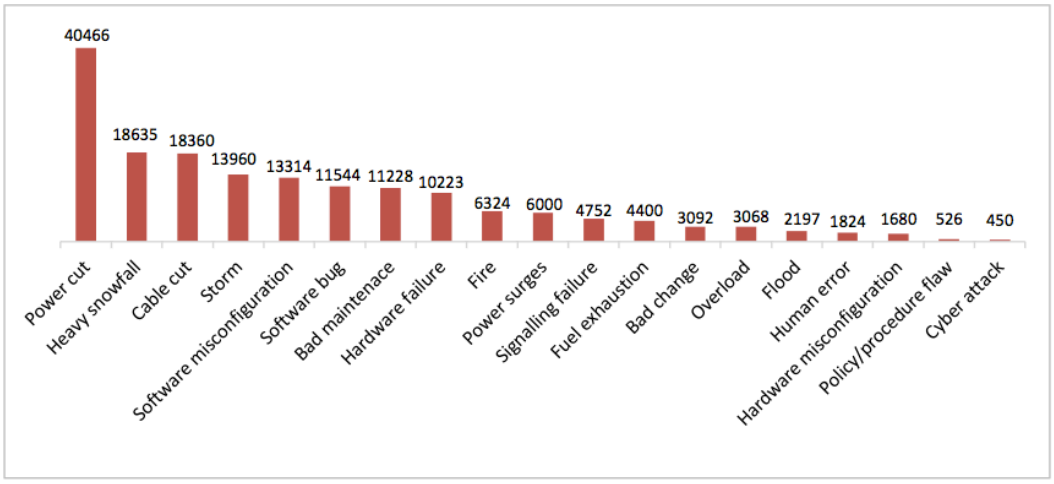


Figure 18. Average user hours lost per incident per detailed cause (source: ENISA 2014).

Power failure was higher this year (2013) because an important Mobile Virtual Network Operator lost primary and secondary power in its data centre, causing loss of voice and data connections for thousands of customers for several hours.

5. Glossary

ISO - Independent system operator. In countries with a deregulated sector, sometimes the main transmission operator is independent from transmission utilities.

TSO - Transmission system operator, i.e. transmission utilities that also operate (part of) the transmission network.

DSO - Distribution system operator, i.e. distribution utilities that operate a distribution network.

SCADA - Supervisory Control And Data Acquisition, a system that collects data inputs from sensors and displays them for monitoring at the control room, and at the same time transmits the operators' tele-command orders to actuator devices on the field. In other words, it is the telecoms+computer system for remote monitoring and control.

HV / MV / LV - High, Medium, and Low voltage. Sometimes, the term EHV (*Extra High Voltage*) is used for 400 kV levels and above.

6. Bibliography

Brown, Matthew H., and Richard P. Sedano. *Electricity Transmission: A Primer.* Washington DC: National Council on Electric Policy, 2004.

Campbell, Richard J. "Weather-Related Power Outages and Electric System Resiliency." US Congressional Research Service, 2012.

Constable, George, and Bob Somerville. *A Century of Innovation: Twenty Engineering Achievements that Transformed Our Lives.* Joseph Henry Press, 2003.

ENISA. " Power Supply Dependencies in the Electronic Communications Sector." 2013.

ENISA. "Annual Incident Reports 2013: Analysis of Article 13a annual incident reports." 2014.

EU Commission. "Adapting infrastructure to climate change." 2013.

EU Commission. "An EU Strategy on adaptation to climate change." 2013.

EURELECTRIC. "Impacts of Severe Storms on Electric Grids." Task Force on Power Outages, 2006.

European Commission. *Protection of Critical Infrastructure.* 2015. http://ec.europa.eu/energy/en/topics/infrastructure/protection-critical-infrastructure (accessed March 2015).

European Environment Agency. "Climate change, impacts and vulnerability in Europe 2012." Report, Copenhagen, 2012.

Executive Office of the US President. ""Economic benefits of increasing electric grid resilience to weather outages"." President's Council of Economic Advisers; U.S. Department of Energy; The White House Office of Science and Technology , 2013.

Griffin, James M., and Steven L. Puller. *Electricity Deregulation: Choices and Challenges.* University Of Chicago Press, 2005.

Hilbert, Martin, and Priscila Lopez. "The World's Technological Capacity to Store, Communicate, and Compute Information." *Science* 332, no. 6025 (2011): 60-65.

IEC. *Smart Grids Standard Map.* http://smartgridstandardsmap.com/ (accessed March 2015).

Krausmann, E., E. Andersson, W. Murtagh, and N. Mitchison. "Space Weather and Power Grids: Findings and Outcome." Joint Research Center, 2013.

Lewis, Ted G. *Critical Infrastructure Protection in Homeland Security.* 2nd edition. Hoboken, New Jersey: Wiley, 2015.

Melillo, Jerry M, Terese C Richmond, and Gary W Yohe. "Climate Change Impacts in the United States: The Third National Climate Assessment." US Global Change Research Program, 2014.

Nassar, Carl. *Telecommunications Demystified.* Eagle Rock, Virginia: LLH Technology Publishing, 2001.

Silvast, Antti, and Joe Kaplinsky. *White Paper on Security of European Electricity Distribution.* Project UNDERSTAND, 2007.

Singh, Rajendra, and Siddhartha Raja. *Convergence in Information and Communication Technology: Strategic and Regulatory Considerations.* World Bank Publications, 2010.

Snow, A., J. Hoag, and G. Weckman. "Understanding Danger to Critical Telecom Infrastructure: A Risky Business." *Eighth International Conference on Networks, 2009. ICN '09.* IEEE, 2009. 451-454.

Snow, Andy, and Gary Weckman. "Protecting Critical Telecommunications and Networking Infrastructure." Tutorial, The Twelfth International Conference on Networking ICN 2013, 2013.

US-Canada Power System Outage Task Force. "Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations." 2004.