

# RAIN

## PROJECT

### Security Sensitivity Committee Deliverable Evaluation

Deliverable Reference	D 4.2
Deliverable Name	Protection elements and methods in Energy and Telecom infrastructure
Contributing Partners	AIA
Date of Submission	October 2015

- The content is not related to general project management (SSC item 1)
- The content is not related to general outcomes such as dissemination & communication (SSC item 2)
- The content is related to critical infrastructure vulnerability
- However, the content is publicly available and generally known
- The content does not disclose new information about vulnerabilities of specific infrastructures or scenarios, or on assets in general
- We do not see any uncertainties about this assessment that would warrant contacting the National Security Authority for an independent assessment.

Diagram path: 1-2-3-4-5.1-5.2-9. Therefore our assessment is: clearance level Public.

Decision of Evaluation	Public	<del>Confidential</del>
	Restricted	

Evaluator Name	P.L. Prak, MSSM
Evaluator Signature	Signed by the chairman
Date of Evaluation	2015-10-30





# Protection elements and methods in Energy and Telecom infrastructure

## Authors

**\*Milenko Halat (Grupo AIA), Xavier Clotet, Vicens Gaitán (Grupo AIA),**

**\*\*Dimitrios Bechrakis (IPTO)**

**\* Corresponding author: Aplicaciones en Informática Avanzada SL, Av. De la Torre Blanca 57, Edificio ESADECREAPOLIS, 08172 Sant Cugat del Vallès, Spain. E-mail: [halatm@aia.es](mailto:halatm@aia.es). Phone: +34 935 044 900.**

**\*\* Corresponding author: IPTO, Dyrachiou 89 & Kifisou 10443, Athens, Greece. Email: [dmpexrak@admie.gr](mailto:dmpexrak@admie.gr). Phone: +30 210 5192669.**

**Date:** 30/10/2015

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

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

## Table of Contents

1. Executive Summary.....	3
2. Introduction .....	4
3. Protection measures .....	7
3.1 Protection: Prevention and mitigation .....	7
4. Telecommunication infrastructure .....	9
4.1 Review of architecture .....	9
4.2 Threats and Vulnerabilities .....	11
4.3 Protection .....	12
4.4 Industry Best Practices, Standards, Protocols and recommendations .....	13
4.5 Preventive Protection Measures .....	16
4.6 Mitigation Protection Measures .....	23
5. Electric Network.....	25
5.1 Power lines.....	26
5.2 Pylons.....	27
5.3 Protection Measures matrix: Prevention.....	29
5.4 Protection Measures Matrix: Mitigation .....	39
6. Protection protocols .....	41
6.1 Software tools aiding in protection .....	42
7. The role of protection methods in the Bayesian Network-based risk assessment framework....	43
7.1 Root Cause Analyses: sample outages.....	44
8. Summary and Conclusions .....	48
9. Bibliography .....	49

## 1. Executive Summary

RAIN project aims to provide a risk analysis framework that minimises the impact of extreme weather events on critical components of EU infrastructures. The Work Package 4 of the project is dedicated to the study of electrical power and telecommunication networks. This deliverable presents a review of the methods and procedures used in these two industries to protect critical equipment against damage from extreme weather disasters. This includes physical measures as well as security protocols for preparedness. Additionally we also include a description of some software tools that operators use in order to monitor the behaviour of equipment and detect anomalies in the context of disturbances and service disruptions caused by weather events.

The methods and protocols are listed, classified by scope and type of equipment over which they act. The technical descriptions of these methods are kept brief, since it is not our objective here to explain how they work. Our main goal is to analyse them in terms of their effectiveness and their flaws, in protecting critical elements as well as the overall functionality of the network during extreme weather events. The outcomes from this analysis about effectiveness become an important input to the Bayesian Network-based risk assessment methods that will be developed in WP6 and WP7 (“preventive measures” and “mitigation actions”).

### **EXTRACTS FROM THE DoW:**

**Task description (Task 4.3):** This task will focus on the methods found in industry to protect equipment in E & TC infrastructure. This task will review software elements that help to protect the system from anomalies, SCADA capabilities that help operators to detect anomalies in the network and hardware security capabilities that protect equipment in the open field. This task will review also security protocols that E & TC companies follows in order to check their equipment behaviour.

**D4.2 description:** Report where the methods and protocols used in the industry are listed and analysed, especially their effectiveness and flaws, classified by scope and system over which it acts.

## 2. Introduction

Electrical and telecommunication infrastructures are both extended geographically over vast distances, just like transport, roads, & bridges. Therefore they are very exposed to extreme weather threats. The only exceptions where the exposure is lower are the wireless links in telecoms (only the link stations are exposed, but not the wire) and underground power lines (unless there are affected by landslides, but these are far less common because most underground lines are located in city areas).

In this report, we analyze the protection measures adopted to minimise the effects of extreme weather threats relating them to specific critical components of each infrastructure identified in the deliverable D4.1, *Electrical & Telecom infrastructure description and identification of critical elements and threats*. General scope protection measures (for any other type of threats) are not covered in this analysis. For instance, in power grids, all protection relays are just “operational” protections, which work only on electrical-based concepts and parameters: they are there to protect the network against “electric threats”, such as overcurrents, overvoltages, undervoltages, and frequency deviations. Such relays will of course act during disturbances caused by a meteorological cause, but it is clear that they are not weather-related protection measures. Similarly, our focus is on *atmospheric* weather phenomena: space weather is interesting as it affects electric equipment (solar flares may cause large disruptions through induced EMF effects), but they are out of scope of the RAIN project. On the other hand, some of the weather-protection measures (e.g. walls, elevations) are at the same time designed to protect against other threats such as vandalism and terrorism.

It worth mentioning that in the last decade the focus on the protection of these infrastructures (particularly in Telco) has progressively displaced to cyber threats, in detriment of weather preparedness. This trend is a bit worrying, considering the statistics on the causes of large Telco outages (Dekker & Karsberg, 2011 - 2012) which show that, after technical failures, weather is a major root cause of severe outages (many years surpassing malicious actions). And in terms of the average *duration* of the incident, weather-related outages have the longest duration by a large difference, compared to all the other causes.

The interrelation between the infrastructures cannot be neglected when assessing the protection systems. Electricity affects strongly other CI, since most of them depend strongly on grid power supply (Telco is clear; land transport: trains, illumination, traffic lights, etc.). This dependence causes that the telecoms infrastructures have be prepared not only for the temporary lack of energy supply (through backup batteries), but also to variations in the quality of the service. For instance, a lightning that hit some component of the power grid may lead to voltage instabilities that produce over- (or under-) voltages that can damage some devices in the communication network. The dependence in the opposite direction is weaker: the main dependence that the power grid has on telecommunications are the services for monitoring and control (SCADA), but usually electrical utilities have their own private channels, at least for the high-voltage transmission network, which is the one requiring constant oversight and control (the distribution end operates in a more automated fashion).

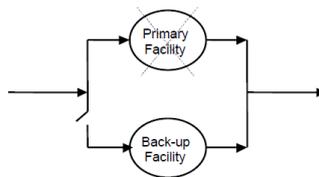
One common theme among protection measures for extreme weather events is that, since they are rare and it is very difficult to estimate their frequency, it is difficult to estimate the overall risk and therefore estimate the amount of investment that makes economic sense. It is interesting to find that some protection measures are not overly expensive (e.g. some easy winterization measures, such as coverings at generation stations), so in this cases like this it may be sensible to prescribe them as preparedness measures, even for cases in which the “black swan” event is judged to have very low probability.

The protection measures can be of different nature: special protection devices, protocols (including maintenance programs), procedures, or physical protection (like walls, elevation platforms, etc.)

The main output of this work are the protection measure matrices (mitigation / prevention ) in both infrastructures, which are a fundamental input for the approach of the Risk Analysis Framework that is being developed in WP5.

We focus now on measures and methods for protecting individual elements that are critical for the functionality of the network. We should mention redundancy as a global mitigation measure:

### Pre 9-11 IT Redundancy



Scenario	Single IT Facility Reliability	Redundant IT Facility Reliability
1	0.90	0.9900
2	0.95	0.9950
3	0.99	0.9999

Figure 1. Example of simple redundancy.

This is an example from the September 11 attacks to the World Trade Centre in New York, where the simple redundancy didn't work since the backup system was placed in the second tower (Snow & Weckman, 2010). Therefore the importance of the idea of “distributed redundancy”.

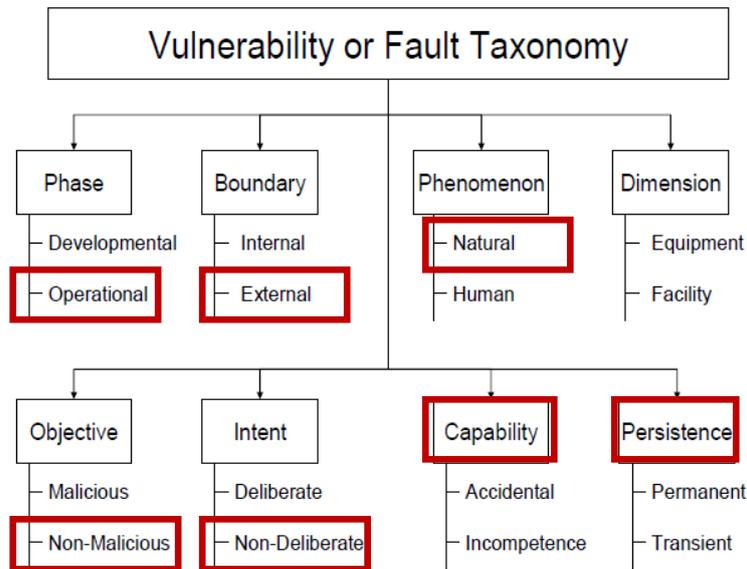


Figure 2. Avizienis, et al, “Basic Concepts & Taxonomy of Dependable & Secure Computing”, IEEE Transactions on Dependable & Secure Computing, 2004.

In Figure 2, we can observe a general taxonomy of vulnerabilities. In red frames, the types of vulnerabilities we focus in this report:

- **Operational:** The system (the infrastructure) is in operational phase, not in development
- **External and Natural:** The system boundary is the common frontier between the system and its environment. We are dealing with meteorological triggering events.
- **Non-Malicious and non-Deliberated:** No intention nor objective is assigned to the triggering cause.
- **Capability.** Since the human factor is not considered here as part of triggering event, it is not applicable.
- **Persistence.** Even if the meteorological framework is climate change, we consider only specific events, not trends. The trends are considered only as determining factor on how frequently these events happen.

The work is organized in the following way. There are two main chapters (4 and 5) where the specific protection systems for each infrastructure are analyzed: **chapter 3** is devoted to telecommunications and **chapter 4** to electric network. In each of them, a quick review of the architecture and general vulnerabilities is presented. Then, the protection measures are classified according the scope (prevention or mitigation) and explained to some extent. Then, in **chapter 6** some of the most relevant protection protocols are described. Finally, **chapter 7** explains the relation of this work with the Risk Analysis framework being developed within the RAIN project. The last chapter gather the conclusions, highlighting the most relevant aspect on protection of these infrastructures.

### 3. Protection measures

Optimum protection of plant and equipment involves striking a balance between the initial cost of the protection measures, the cost of maintenance, the value of uninterrupted service and the cost of system repairs. Electrical protection should be considered early in the development and planning of plant facilities, because most protection measures cost more to introduce at a later time. Where service continuity is the dominant factor, there is no alternative other than to initially provide a high level of protection.

#### 3.1 Protection: Prevention and mitigation

In the description of the protection measures, we make the distinction between prevention measures and mitigation measures based on the moment they are applied respect to the event.

Since in some cases this distinction could be not totally clear, we provide a concise definition:

- **Preventive** protection: prevent or minimize the extent and/or strength of the impact of events, **before** the event takes place. Some authors refer to this as “mitigating risk”, but we will reserve the word mitigation to refer to all those measures.
- **Mitigation** protection: minimize the impact and prevent the propagation of events, **after** the event has taken place.

As an example, redundancy of equipment is a preventive protection measure, since the installation of redundant systems is made before an event occurs. On the other hand, overcurrent relays in the power grid are considered as a mitigation measure because its objective is to minimise the spreading of an electrical contingency.

The reason for this classification of protection measures is the logical structure needed for the application of the methodology of the risk assessment framework developed in Work Package 5 which is based on Bayesian Networks. There, the probabilities of occurrence of specific events in the infrastructure (like failures in specific components) will be computed depending on the context. See chapter 7 for details, in particular figure 14.

Tables 1-4 gather and summarise the protection measures according to this criteria (prevention / mitigation) for each infrastructure. They relate specific extreme weather causes to each critical element. The colour represent the level of impact that a failure in that element could cause (red= high, yellow= medium, green= low) as shown in D4.1.

### Proactive Fault Management

According to (Snow & Weckman, 2010), the management of faults (in Telco, but it applies also to power systems) can be grouped by four concepts:

- Fault **Prevention** by using design, implementation, and operations rules such as standards and industry best practices. In this report we describe the standards and some protocols chapter 6.
- Fault-**Tolerance** techniques are employed, wherein equipment/process failures do not result in service outages. In the case of Telco's, because of fast switchover to equipment/process redundancy.
- Fault **Removal** through identifying faults introduced during design, implementation or operations, and taking remediation action.
- Fault **Forecasting** where the telecommunication system fault behaviour is monitored from a quantitative and qualitative perspective and the impact on service continuity assessed.

The first and the fourth correspond to preventive measures, while the second and third are mitigations measures.

## 4. Telecommunication infrastructure

### 4.1 Review of architecture

A more complete description of the architecture of telecommunication systems can be found in public deliverable RAIN D4.1 *Electrical & Telecom infrastructure description and identification of critical elements and threats*

Figure 3 below 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**: 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.

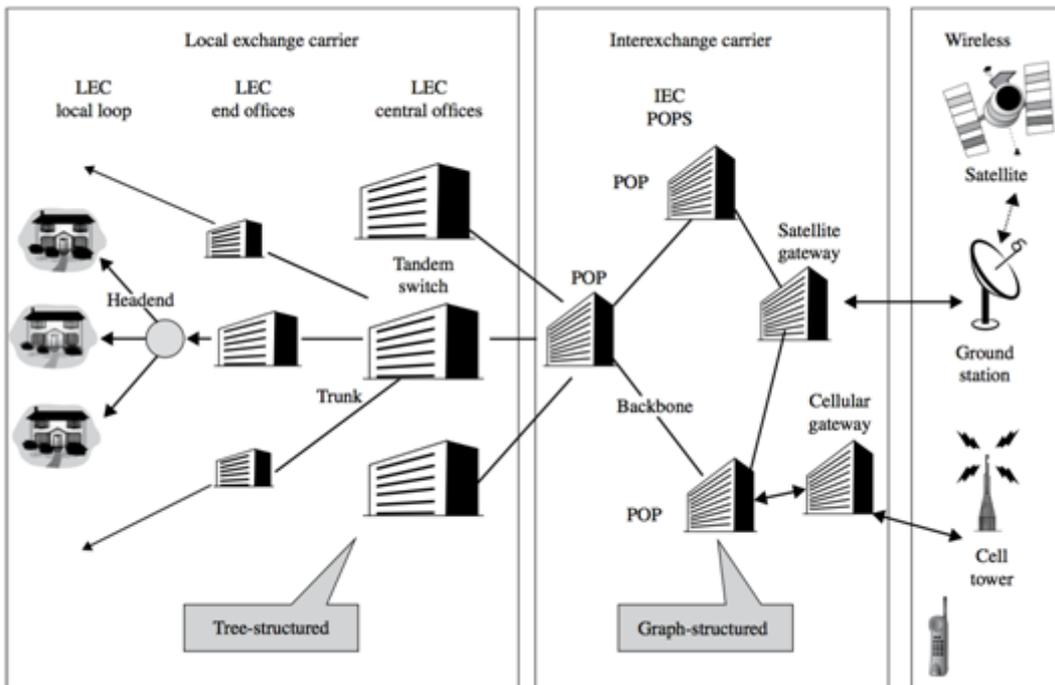


Figure 3 Structure of the telecom infrastructure. Source: (Lewis 2015)

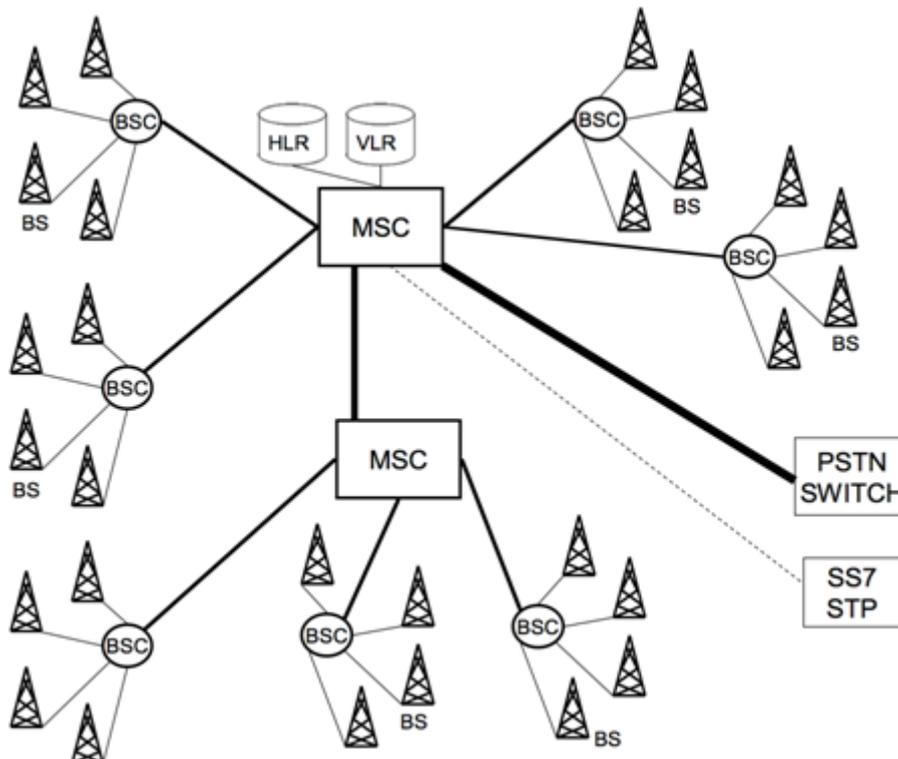


Figure 4 Schematic view of (cellular) mobile networks Source: (Snow and Weckman 2013)

## Mobile networks

The main elements of the mobile networks are:

- **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).

## 4.2 Threats and Vulnerabilities

The following are the main concerns in protecting this infrastructure. Notably, in recent years the efforts are focused more in targeted intentional threats than natural ones, specifically on those related to cyber attacks.

- Natural Threats
  - Water damage
  - Fire damage
  - Wind damage
  - Lightning
  - Power Loss
  - Earthquake damage
  - Volcanic eruption damage
- Human Threats
  - Introducing or triggering vulnerabilities
  - Exploiting vulnerabilities (hackers/crackers, malware introduction)
  - Physical Vandalism
  - Terrorism and Acts of War

Telecommunication infrastructure is particularly sensible to 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 (Elisabeth Krausmann, 2013) However, within the scope of RAIN project we will analyze only the protection against natural threats related to atmospheric meteorological events.

### 4.3 Protection

The focus of general protection is often on More Reliable and Maintainable Components. One way to obtain more reliability is avoiding single points of failure (e.g. over concentration for economical reasons). Another way to increase reliability is through *diversity*: creating redundancy on in-line equipment spares, transmission paths or power sources. Minimizing times of fault detection, equipment isolation, repairing replacement and testing of equipment also contributes to have a more reliable infrastructure. Other standard measures involve spare and test equipment, best practices guides, personnel training programs and alarm systems. The telecommunication system poses very particular challenges that are directly related to the technology behind it: how fast it evolves and how different channels converge. In this sense, outages that previously could affect only one channel nowadays could have much greater impact affecting voice, data and video simultaneously. Other important challenge comes from the management part. It is very frequent to find cases in which Telecommunication companies merge or acquire other telecommunication companies. In those cases, much effort, and resources has to be invested in order to harmonize all kind of procedures, including those of maintenance and protection.

In the case of telecommunication infrastructure it is not easy to list the protective measures aimed to minimize effect of weather event since it is strongly dependent of the electricity supply. We can separate measures aiming to face “direct” weather effects (i.e. lightning rods) from those aiming to act when the power supply is interrupted or its quality has been affected, even if the cause is meteorological. For instance, the protection devices that protect components sensible to voltages instabilities.

One relevant question is where to invest to improve reliability: on prevention or in mitigation measures. Preventing outages requires both capital and operational expenses. The capital expenditures for such items as backup AC generators, batteries, redundant transmission paths, etc. can be very large. Moreover, the capital expenses to remove some vulnerabilities might be cost prohibitive, wherein the risk is deemed as acceptable. For instance, duct space in metropolitan areas might present significant constraints to offering true path diversity of fibre cables or rural local switches might present considerable challenges for designers to offer two separate SS7 access links. As rule of thumb, there should be an adequate balance between preventing outages and reacting to outages once they have occurred. This is a delicate economic equilibrium point which service providers struggle with.

Finally, as it is extremely complex to compute the rate-of-return of investments on protection against rare or extreme weather events, companies may tend to take only the measures to comply national regulations. Indeed regulator and the service provider might have significant disagreements

as to what is an acceptable risk. In this analysis, the comprehensive costs of preventive and mitigation (or restoration) measures are compared probabilistically.

#### 4.4 Industry Best Practices, Standards, Protocols and recommendations

Industry best practices deal with the architecture, design, installation, operations and maintenance activities. Deviations from best practices should never be accidental, as an inadvertent or unknown deviation represents a latent vulnerability that can be triggered or exploited.

- In the U.S. Wireline best practices were initially developed as a Network Reliability & Interoperability Council (NRIC) initiative<sup>1</sup>.
- The scope of best practices has been expanded to cover the major network types and there are over 700 common best practices.
- A website can be queried by network type, industry role, and keyword

The Study Groups of ITU's Telecommunication Standardization Sector (ITU-T) is the body responsible of the development of international standards for telecommunication. It is part of ITU, which is the United Nations specialized agency for information and communication technologies – ICTs. They are responsible of allocation of global radio spectrum and satellite orbits, develop the technical standards that ensure networks and technologies seamlessly interconnect, and strive to improve access to ICTs to underserved communities worldwide. ITU-T has published a series of recommendations (Recommendations ITU-T (Study Groups ITU)) that include protocols to face climate change effects. The most relevant related to extreme weather effects are the **L** and **K** series:

- **L series:** Environment and ICTs, **climate change**, e-waste, energy efficiency; construction, installation and protection of cables and other elements of Outside Plant.
- **K series:** Protection against interference.

Below, the most relevant reports are listed (relevant for the scope of RAIN), Within the L series, these are the reports that contain recommendation for protection:

- **L.1:** Construction, installation and **protection** of telecommunication cables in public networks
- **L.92:** Disaster management for outside plant facilities
- **L.1500:** Framework for information and communication technologies and adaptation to the effects of climate change
- **L.1501:** Best practices on how countries can utilize ICTs to adapt to the effects of climate change

---

<sup>1</sup> NRIC is a federal advisory council to the Federal Communications Commission, which has been continuously re-chartered since 1992.

The main weather concerns are lightnings, and indirects effect of the power grid instabilities: over/under voltages and over currents.

#### 4.4.1 Lightning

- K.39: Risk assessment of damages to telecommunication sites due to lightning discharges. This Recommendation gives support to protection engineers in evaluating the risk for severe damages caused by lightning. It comprises a risk analysis that includes the effect from direct and nearby lightning strikes as well as overvoltages originating from incoming services, mainly power and communication networks. The analysis also indicates the most efficient additional protective measures for sites with insufficient basic protection. Part of this Recommendation deals with the risk of injuries to people being present at the site during thunderstorms. This Recommendation is based on a concept from IEC TC 81 and modified to be applicable to practical cases in telecommunication systems.
- K.40: Protection against LEMP in telecommunications centres
- K.46: Protection of telecommunication lines using metallic symmetric conductors against lightning-induced surges
- K.47: Protection of telecommunication lines against direct lightning flashes. Recommendation ITU-T K.47 gives a procedure in order to protect telecommunication lines using metallic components (symmetric pair, coaxial or optical fibre cables) against direct lightning flashes to the line itself or to structures that the line enters. In particular, it presents a rationale for the protective effect of guard-wires.
- K.56: Protection of radio base stations against lightning discharges. The protection techniques for the external area cover the lightning protection system (LPS), bonding procedures, earthing and the installation of surge protective devices (SPDs) at the power meter station. The protection techniques for the equipment building cover the feeder and lighting cables, the electric power conductors, the telecommunication cabling and the earthing/bonding procedures applied to cable trays and equipment frames. This Recommendation also provides guidelines in order to achieve adequate protection of the telecommunication equipment based on the coordination between equipment resistibility, SPD protection level and installation characteristics.
- K.67: Expected surges on telecommunications and signalling networks due to lightning
- K.85: Requirements for the mitigation of lightning effects on home networks installed in customer premises
- K.89: Protection of persons inside a structure using telecommunication services provided by metallic conductors against lightning - Risk management. Gives the methodology for evaluating the need to protect users of telecommunication equipment in structures and that of building occupants related to the telecommunication installation. This method is based on a risk assessment: protection measures are necessary when the risk is greater than the tolerable risk. A maximum value of the tolerable risk is suggested. The risk is evaluated using the lightning risk components which can be a source of injury to telecommunication service

users and building occupants (lightning flashes direct to the line or to the structures connected at the ends of the line).

- **K.97: Lightning protection of distributed base stations.** Protection of these interfaces is achieved by installing a protection module. Possible protection schemes for such installations are also described. This Recommendation indicates when these protection modules should be used, and provides indication of their withstand current. The surge protective device (SPD) needed on the feeder cable is also indicated.
- **K.101: Shielding factors for lightning protection**
- **K.105: Lightning protection of photovoltaic power supply systems feeding radio base stations**

#### 4.4.2 Over/under voltage and OverCurrent

- **K.11: Principles of protection against overvoltages and overcurrents.** It deals with protection principles, e.g., risk management, safety and reliability, surge protective devices and surge protective components. It gives guidance for the protection of telecommunication equipment, installations and cable plants exposed to the results of external sources of interference such as overvoltages and overcurrents due to lightning or effects related to power lines and electric traction systems. It gives general information about:- the origin of overvoltages and overcurrents (lightning, power induction, power contacts, earth potential rises);- types of protective devices (voltage-limiting and current-limiting devices) and their residual effects;- risk assessment;- protection of telecommunication lines;- protection of exchange and transmission equipment;- protection in access networks.
- **K.20: Resistibility of telecommunication equipment installed in a telecommunication centre to overvoltages and overcurrents**
- **K.21: Resistibility of telecommunication equipment installed in customer premises to overvoltages and overcurrents**
- **K.44: Resistibility tests for telecommunication equipment exposed to overvoltages and overcurrents – Basic Recommendation**
- **K.45: Resistibility of telecommunication equipment installed in the access and trunk networks to overvoltages and overcurrents**
- **K.65: Overvoltage and overcurrent requirements for termination modules with contacts for test ports or surge protective devices**
- **K.66: Protection of customer premises from overvoltages.** It provides recommendations for bonding and earthing of telecommunication equipment in residential and commercial customer premises.
- **K.82: Characteristics and ratings of solid-state, self-restoring overcurrent protectors for the protection of telecommunications installations**
- **K.98: Overvoltage protection guide for telecommunication equipment installed in customer premises**

- **K.102: Parameters of fixed-voltage thyristor overvoltage protector components used for the protection of telecommunication installations**

#### 4.4.3 Protection

- **K.36: Selection of protective devices.** Information about the application of new devices in the different parts of a telecommunication network. It is intended to guide protection engineers and manufacturers of equipment to select appropriate protection devices for a telecommunication system. It should be noted that the implementation of protective devices in a communication system is only one of several methods to mitigate transient overvoltages.
- **K.57: Protection measures for radio base stations sited on power line towers**
- **K.69: Maintenance of protective measures.** Guidance on the maintenance of protective measures (protective devices and assemblies and their earthing) in telecommunication installations. It deals with the maintenance of the protection of telecommunication equipment, installations and cable plants exposed to the results of external sources of interference such as overvoltages and overcurrents due to lightning discharges or power induction.
- **K.71: Protection of customer antenna installations**
- **K.72: Protection of telecommunication lines using metallic conductors against lightning – Risk management.** Methodology for evaluating the need for protection measures against lightning of telecommunication lines using metallic conductors. This method is based on the risk assessment: protection measures are necessary when the risk is greater than the tolerable risk. Maximum value of the tolerable risks is suggested
- **K.96: Surge protective components: Overview of surge mitigation functions and technologies**

Environmental factors: If an outage is triggered by an earthquake, storm, vegetation, water ingress or HVAC failure, then they are categorized under environmental factors.

#### 4.5 Preventive Protection Measures

In the following, the effect of the different extreme weather events are evaluated per each element of the telecommunications structure, (for the meteorologic events described in WP2 and critical components listed and described in D4.1) and preventive protection measures are proposed. Unless the threat is particularly important for a specific telecommunication element, problems derived from power outages due to extreme weather (described in detail in chapter 5) are not listed in this section.

The information is also summarized in the following Table 1.

PREVENTION								
	Lightning	Windstorms	Ice/snow storms	Flash floods	Extreme cold	Extreme heat	Wild fires	Sand storms
<b>Outside Plants</b>	<ul style="list-style-type: none"> <li>Evaluate exposure</li> <li>Bonding and grounding.</li> <li>Protector units and heat coils</li> <li>Fuse cable and fuse links</li> </ul>	<ul style="list-style-type: none"> <li>Street side cabinets</li> </ul>	<ul style="list-style-type: none"> <li>Street side cabinets</li> </ul>	<ul style="list-style-type: none"> <li>Street side cabinets</li> <li>Air pressure systems</li> </ul>				<ul style="list-style-type: none"> <li>Street side cabinet</li> </ul>
<b>End Offices</b>								
<b>Central Offices</b>								
<b>Aerial lines</b>								
<b>Underground lines</b>								
<b>RF/Sat links</b>	<ul style="list-style-type: none"> <li>Consider PIM</li> </ul>	<b>Antennas</b> <ul style="list-style-type: none"> <li>Shrouding (Radomes)</li> <li>Flexure</li> </ul> <b>Towers</b> <ul style="list-style-type: none"> <li>Welded towers</li> </ul>	<b>Antennas</b> <ul style="list-style-type: none"> <li>Shrouding (Radomes)</li> <li>Flexure</li> <li>Low-adhesion coatings</li> <li>Heating</li> </ul> <b>Towers</b> <ul style="list-style-type: none"> <li>No buildings in "fall zone"</li> <li>Welded towers</li> <li>Black anodized</li> </ul>					<b>Antennas</b> <ul style="list-style-type: none"> <li>Shrouding (Radomes)</li> </ul> <b>Towers</b> <ul style="list-style-type: none"> <li>Welded towers</li> </ul>
<b>Base Stations</b>	<ul style="list-style-type: none"> <li>Lightning rods</li> <li>Circuit protection: <ul style="list-style-type: none"> <li>earthing</li> <li>bonding (mesh-BN, mesh-IBN)</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>Wind Survival: <ul style="list-style-type: none"> <li>Recommended 200 km/h</li> <li>Heavy duty antennas 240 km/h</li> </ul> </li> <li>Guyed masts</li> </ul>	<b>Antennas</b> <ul style="list-style-type: none"> <li>Shrouding (Radomes)</li> <li>Flexure</li> <li>Low-adhesion coatings (specific regions)</li> <li>Heating (specific regions)</li> </ul> <b>Towers</b> <ul style="list-style-type: none"> <li>No buildings in "fall zone"</li> <li>Welded towers</li> <li>Black anodized</li> </ul>	<ul style="list-style-type: none"> <li>Water Ingress <ul style="list-style-type: none"> <li>RF path interconnections protected</li> <li>Enclosure rating IPX6</li> </ul> </li> <li>Rain <ul style="list-style-type: none"> <li>10 mm/minutes for 30 min</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>Temperature Survival: <ul style="list-style-type: none"> <li>16 hours at -33 °C or -40 °C</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>Temperature Survival: <ul style="list-style-type: none"> <li>16 hours at +40/55 °C or +60 °C</li> </ul> </li> </ul>		<ul style="list-style-type: none"> <li>Dust and sand ingress: <ul style="list-style-type: none"> <li>Enclosure rating IP5X</li> </ul> </li> </ul>
<b>MSC</b>								
<b>BSC</b>								

Table 1. Protection preventives measures in telecommunication infrastructure.

**Outside plants**

Outside plants can be located in very different environments that will affect their exposure to extreme weather conditions. Then, implementation of preventive protection measures will depend on a previous evaluation of the actual weather risks in each geographic position. In addition, the initial cost of implementation of such measures, the cost of maintenance, the value of uninterrupted service, and the cost of system repairs will have to be assessed and balanced.

These plants are especially exposed to lightning. Exceptions are found when the plants are located on soil with resistivity smaller than 100 meter ohms and there is low incidence of thunderstorm (less than 5 per year), in metropolitan areas where buildings are close and high (cone of protection shielding), or underground. However, even in cases where the plant is not particularly exposed to lightning, it may be at risk by lightning because some branch or extension connected to the plant are exposed. A diagram summarizing these conditions is shown in Figure 5.

Regarding preventive protection measures, bonding of the various metallic elements and proper grounding of the elements should be the first priorities. Favouring low impedance paths to ground by, for instance, establishing and maintaining continuity of metallic cable components, installing protector units and heat coils, and fuse cables and fuse links are other recommended measures regarding exposure to lightning.

Outside plants consisting of street side cabinets are also particularly susceptible to other extreme weather conditions such as windstorms, ice/snow storms, flash floods, wild fires, or sand storms. Some protection measures implemented in older large cable facilities consists of air pressure systems designed to prevent water infiltration.

In a lower level, extreme heat may affect telecommunication plants mostly related with problems related with power outages.

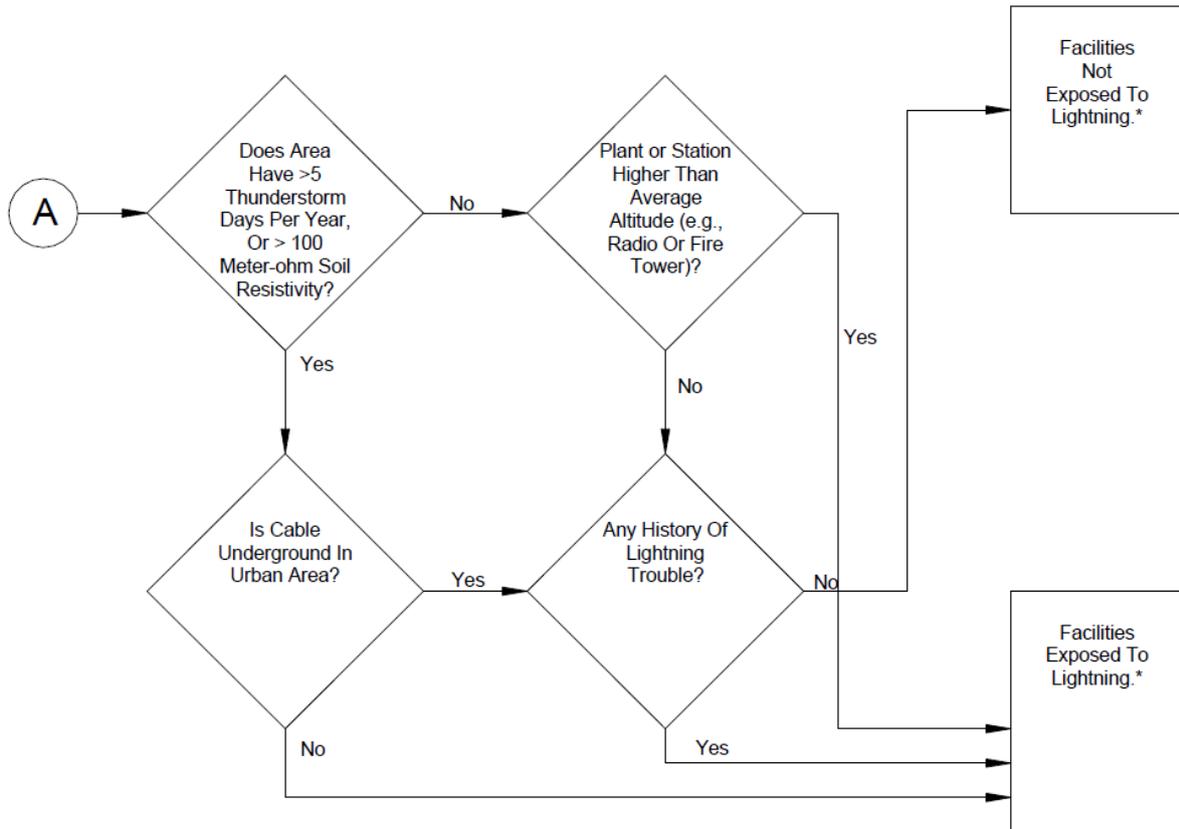


Figure 5 Determination of plant lightning exposure. Diagram from (Electrical Protection of the Subscriber Outside Plant, 2013)

### End Offices

Extreme weather conditions affecting End Offices are the same as those described affecting Outside Plants. However, given that End Offices are located in buildings, the exposure to risks is lower.

### Central Offices

Central Offices exposure to extreme weather risks is low for all extreme conditions considered.

### Aerial Lines

Similarly to the exposure of Power Lines (see chapter 5), Aerial Lines are especially susceptible to windstorms and ice and snow storms. Due to strong wind or accumulation of snow trees may fall over the lines, disrupting the connection. Damage of the supporting pylons can also affect communication. Wild fires are another important threat to aerial lines. Lightning, flash floods or sand storms can also disturb the telecommunication system.

### Underground Lines

Opposite to Aerial Lines, extreme weather conditions do not pose a threat on Underground Lines.

### Radio Frequency and Satellite Links

These stations have antennas usually build on towers. Then, one of the most threatening extreme weather conditions that can affect Radio Frequency and Satellite Links are lightnings. These stations are also particularly exposed to ice/snow storms and windstorms. To a lower level, flash floods and extreme heat can also have negative effects on these facilities.

To decrease the effect of these extreme conditions, a number of measures should be considered. In relation to lightning, different elements are recommended like lightning rods and proper bonding and grounding (mesh Bonding Network and mesh Isolated Bonding Network). However, special attention must be paid to Passive InterModulation distortion (PIM). This distortion is generated when two or more RF signals pass through a non-linear junction. Several in-line RF lightning protection devices contribute to these interferences. Therefore, if the service provided by the station is sensitive to PIM, additional tests must be performed to check the effects of the preventive protection measures on the actual operation of the facility.



Figure 6 Antenna protected with radome (source: commons wikimedia)

Regarding ice and snow storms, antennas are recommended to be shrouded in, e.g. with a radome. Radomes, blend word from radar and dome, are structures that surround the antenna built with materials that are electromagnetically transparent. Using building materials with flexural properties (so that ice cannot settle), low-adhesion coatings, and, in particular regions, heating systems should be considered also. As for the towers, first of all those should not be built in *fall zones*. Then, depending on the geographical specifications, welded (with all mechanical junctions are welded to increase loading strength), or black anodized towers (with electrically-charged protective coating that are particularly good for heavy icing and corrosive environments) may be advised.

Some of the preventive measures for ice and snow storms are also useful to protect the facility against wind and sand storms.



*Figure 7 A tower with a heavy copper grounding (Wireless Networking in the Developing World)*

### **Base Stations**

Base Stations (BS) consist of two elements: tower with antennas and a small building to house the equipment. These facilities are widely distributed geographically. These facts make them especially prone to being affected by a large number of different extreme weather conditions. Then, each case should be reviewed individually, and solutions adapted to its particular environment.

One of the most common meteorological threat for Base Stations is lightning. Oftentimes, these facilities are placed in elevated locations to maximize their coverage area. This also maximizes their exposure to lightning, that can result in voltages differences of 250 kV from top to bottom of the antenna mast during a direct lightning strike. Ground Potential Rise poses an additional threat; in particular in facilities where the distance between the tower and the transmitters is large (it can be up to 30 meters). Therefore, lightning rods and proper bonding and grounding (mesh-BN and mesh-IBN, i.e. mesh (Isolated) Bonding Network) are essential (Protection against lightning, 2010).

Base Stations are also exposed to windstorms, in concrete their antenna. According to EN 1991-1-4 and/or EIA/TIA 222-G, antennas should survive exposure to strong winds up to 180 km/h without damage. However, BASTA team (NGMN, 2013), recommends resistance to 200 km/h for standard duty, and 240 km/h for heavy duty antennas. In windy areas, the use of guyed masts is strongly recommended in order to protect the facility, as well as welded towers.

As for ice/snow storms, recommendations are similar to those for RF/Sat links: shrouding the antenna, using flexural materials, and low-adhesion coatings. These methods, however, are not applied to the whole facility but only to tower sections immediately surrounding antennas due to their cost-effectivity.

Base Stations design must be concern about flash floods also. Water ingress in such facilities should comply with enclosure rating IPX6 as defined by IEC 60529 (Degrees of protection provided by enclosures, 2013) that states how antenna electronics and RF path interconnections potentially exposed to water should be protected against splashed, sprayed or windblown ingress of water.

Recommendations regarding rain are also provided by IEC (test methods in IEC 60068-2-18 (Environmental testing - Test R and guidance: Water , 2000)): 6 or 15 mm/minute for 30 minutes for baseline or extended test, respectively. BASTA team recommendation is 10 mm/minute for 30 minutes.

Extreme cold conditions pose a low risk to these facilities. The International Electrotechnical Commission (IEC) proposes two tests, a baseline and an extended (Environmental testing - Test A: Cold, 2007), that these station should pass. According to IEC, antennas should operate within specifications after exposure to cold air for 16 hour at temperature -33°C or -40°C for the baseline or extended case respectively. Then, only few BS will be affected by extreme cold conditions within the region considered in project RAIN.

Extreme heat poses a higher threat than extreme cold in relation to BS although lower than the other threats described. According to IEC 60068-2-2 (Environmental testing - Test A: Cold, 2007) antennas should operate correctly 16 hours at +40/55°C or +60°C (baseline or extended). Thus, in the area considered in this project, only a few regions will have to pay special attention to this threat.

Like other facilities that may be located in remote areas, wildfires pose a high risk for Base Stations.

Sand storms are of concern in relation to Base Stations. However, dust and sand ingress are usually not considered to be a direct problem. Following IEC 60529 (Degrees of protection provided by enclosures, 2013) and its definition of enclosures, antenna components potentially affected by dust or sand exposure should be protected from ingress to a rating of IP5X. Also, protection against sand is rarely tested.

As a final remark regarding Base Stations, it is worth noting that these facilities may be installed in remote areas with difficult access. Thus, preventive protection measures are particularly indicated since application of mitigation measures can take longer times than in other kind of stations.

Other relevant references can be found at (ESTI, 2014).

### **Mobile Switching Centre**

The number of Mobile Switching Centres is lower than that of Base Stations. That allows building them in better locations regarding natural weather threats. Therefore, extreme conditions risks are similar to those of BS, but with a lower impact level.

### **Base Station Controllers**

Base Station Controllers exposure to extreme weather risks is low for all extreme conditions considered.

## 4.6 Mitigation Protection Measures

It is not always possible to completely avoid failures that lead to outages. Proactive steps can be taken to minimize their size and duration as avoiding single points of failure that can affect large numbers of users, and having recovery assets optimally deployed to minimize the duration of outages. Generally, this can be accomplished by ensuring there is not too much over-concentration of assets in single buildings or complexes and properly deploying and operating fault tolerant telecommunication architectures. Some measures are oriented to obtain tolerance to equipment failure (what is call N-1 tests in power systems) or power faults; other, to guarantee the existence of physical and logical diverse transmission systems or paths. The human factor is highly relevant in the post contingency situation, so the company should ensure that there is adequate trained staff and dispersal of maintenance capabilities and assets. Regarding training of employees, apart from CI company documentation, some regulatory authorities provide training material aimed to deal with specific risks.

To assess the reliability of an infrastructure, it should be quantified to what extent the Industry Best Practices and Standards are adopted, how often the disaster recovery plans are reviewed, and how much is learnt from past event, through a systematic outage data collection and analysis. Thus, mitigation is extremely case-dependent.

Outage data is the bellwether of infrastructure vulnerability. The faults which manifest themselves because of vulnerabilities are a good indicator of the reliability and survivability of critical telecommunications infrastructure. It is equally important to track reliability and survivability in order to assess whether the protection level is increasing, constant, or decreasing.

MITIGATION								
	Lightning	Windstorms	Ice/snow storms	Flash floods	Extreme cold	Extreme heat	Wild fires	Sand storms
Outside Plants								
End Offices								
Central Offices								
Aerial lines			<ul style="list-style-type: none"> <li>• Insulated rods</li> <li>• Helicopter rotor blow away</li> <li>• Helicopter with attached risk of damage of fibre optic conductors</li> </ul>					
Underground lines								
RF/Sat links			<ul style="list-style-type: none"> <li>• De-icing only on antennas, not towers</li> </ul>					
Base Stations								
MSC								
BSC								

Table 2. Protective (Mitigation) measured in telecommunication infrastructures.

## 5. Electric Network

The architecture of the electric network was described in some detail in deliverable D4.1. The most common measures taken on the power grid against meteorological causes are:

- Overhead Transmission Lines: (High Voltage and Extra High Voltage transmission lines)
  - Tower: a lattice steel tower or steel tubular tower. Towers face problems in the presence of a force that is beyond the mechanical tolerance of the construction.
  - Insulators: A common problem is when dust (or any kind of dirt) overlays on the surface of the insulator. The combination of contamination and wetting (or icing) of insulator surfaces initiate the flow of leakage current. The leakage current leads to flashover and has distinctive stages of development. This may result in dry-band arcing and extension of the arc to bridge the insulator. For that reason overhead transmission lines installed in islands or near to the coastline require particular maintenance procedures to remove the salt deposition in insulators.
  - Conductors: Each conductor is stranded, steel reinforced aluminium cable. The designer of the transmission line, apart from the electrical specifications of the circuit, should take notice of all factors that affect the distance of the conductor to any obstacle. Icing has an effect on the weight of the conductors. High temperatures increase the line sag and decrease the thermal limit (and the transfer capacity) of the lines.
  - Shield conductors: Two grounded shield conductors protect the phase conductors from lightning.
  - Foundation: Steel-reinforced concrete foundation placed in the ground. This is an element with high probability of failure.
  - Grounding: Grounding electrodes, placed in the ground at specific depth. This element is the least prone to non-electrical cause failure (only under severe circumstances such as landslides, earthquakes, etc).
- Transformers:
  - Walls and covers
  - Elevation platforms to avoid floods
- Generators
  - Winterization procedures. These are probably the most important ones among newly developed measures. See NERC Winterization studies, which have made it into an official Recommendation (Reliability Guideline. Generating Unit Winter Weather Readiness ), and standard EOP-001-2.1b within the NERC Reliability Standards (North American Electric Reliability Corporation) (whose compliance is mandatory by US regulations) now explicitly mentions that generators should have winterization plans in place. (This was triggered by the February 2011 blackouts that took place in the South West.)

- Buses and the rest of switchgear at the substation (maybe including the local control infrastructure, i.e. RTUs, etc.)

## 5.1 Power lines

Among all the different components of the electrical power grid infrastructure, power lines are always hit the hardest in extreme weather events. This is not surprising, as lines cover extensive lengths across both urban and country areas, and are quite exposed to weather. Comparatively, other components such as transformers and switchgear (breakers, protection relays, etc.) are more protected, being fenced at substations and sometimes housed under sheds. This reflects the fact that transformer and switchgear are more critical to the operation of the grid: the transmission network may typically afford to lose some redundant lines, but not so much the loss of substation functionality (substations are the nodes or “hubs” of the transmission grid). This is even more evident with generators: generating plants are comparatively more resilient under extreme weather threats, but when they do get affected, the impacts on the grid are still more serious than those created by lines or substation failures. For instance, in the US the “February 2011 Southwest Cold Weather Event” highlighted the problem of inadequate preparedness for extreme low temperatures in gas and fuel power plants: the generation shortfall was so serious that it endangered the stability of the whole grid. The incident proved so serious that NERC ended up amending their reliability standards to include mandatory “winterization procedures” in the Emergency Operations Planning standards.

Most high and medium voltage lines are not shielded, again because of the economic trade-offs involved. They are simply isolated by maintaining a minimum separation between the different phases. If, for whatever reason, the phases touch each other or the ground, this produces a short circuit, which triggers (“trips”) the protection relays and the line gets disconnected. Actually, the cables do not need to touch in order to produce the short circuit: given enough proximity, the short can be produced by electric arc (arc discharge). The higher the voltage, the higher the minimum distance needed to prevent arcing.

Rusting of the unshielded conductors is not in general a big concern, as most cables are made of aluminium (with a steel core). However, rusting of the pylon is a big problem, since most of them are made of steel.

As discussed in D7.1 *Analysis of Practical Remediation Strategies for discrete Infrastructure systems*, the impacts that the various weather threats may have on transmission and distribution lines. They are listed approximately in order of likelihood:

- **Wind storms and tornados:** they affect overhead lines typically by bending or toppling power line towers, bending or toppling trees over lines, or swinging lines violently 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:** ice storms and wet snow storms can cause ice to grow on power lines, which may make the line crumble under its weight, or whip violently when the wind blows large chunks of ice off the line.
- **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).
- **Lightning:** it affects mainly overhead lines and unsheltered transformers. Proper grounding techniques of pylons, protection relays, and automatic reclosers minimize this risk. But a high concentration and concurrence of lightning-triggered tripping may put the grid at risk.
- **Flash floods:** they are a very high risk mainly for generator plants, but it could also affect pylons with weak foundations, causing permanent damage to the line.
- **Wildfires:** these may affect mainly unsheltered transformers sitting on ground level or on poles, and overhead lines. 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, just like windstorms.
- **Rain dust:** is a variety of rain (or any other form of precipitation) which contains enough desert dust, visible without using a microscope. This dust comes to Europe from the Sahara desert and causes problems in transmission line insulators.

## 5.2 Pylons

Transmission towers, commonly known as pylons, are used to support overhead power lines. The most common type is the steel lattice tower, but they come in a wide variety of shapes and sizes. Typical height ranges from 15 to 55 metres, though the tallest are the 370 m towers of a 2,700-metre-long span of the tie line connecting Zhoushan Island with mainland China. In addition to steel, other materials may be used, including concrete and wood.

Together with lines, pylons suffer the most varied types of weather threats. Transmission and distribution lines carry electrical power over long distances. The most common types are overhead lines, especially in high-voltage transmission. Underground cables are much less common, except when considering last-mile sections in distribution networks, or some special high-voltage tie lines such as submarine power cables used to connect islands. Underground cables are virtually immune to most weather threats (except maybe mudslides triggered by heavy rainfall), but they are not used very often because their price is 7 to 15 times that of overhead lines.

An integrated approach to vegetation management may indicate that use of herbicides is the preferred approach to control fast-growing vegetation within transmission and distribution rights-of-way. In such case, they should be used observing environmental regulations (e.g. avoid their migration into off-site land or water environments).

PREVENTION									
	Lightning	Windstorms	Ice/snow storms	Flash floods	Extreme cold	Extreme heat	Wild fires	Sand storms	Seasonal drought
<b>Generators (housed)</b>									
<b>Generators (wind / PV)</b>	<ul style="list-style-type: none"> <li>Graded lightning protection</li> <li>Lightning rods</li> <li>Grounding</li> </ul>	<b>Wind Brakes:</b> <ul style="list-style-type: none"> <li>Tip brakes (aerodynamic)</li> <li>Mechanical braking system</li> </ul>	<ul style="list-style-type: none"> <li>Winterization procedures.</li> </ul> <b>Wind</b> <ul style="list-style-type: none"> <li>Blade anti icing systems: blade active heating, passive hydrophobic coating</li> </ul>		<b>Wind</b> <ul style="list-style-type: none"> <li>Overproduction: breaking systems</li> </ul>			<b>PV</b> <ul style="list-style-type: none"> <li>Minimize effects of exposure</li> <li>Polymer Encapsulation</li> <li>Forced air flow</li> </ul>	
<b>Lines and Pylons</b>		<ul style="list-style-type: none"> <li>Right-of-way maintenance</li> <li>Tower inspections and maintenance</li> <li>Wind-induced oscillations (gallop, flutter)</li> <li>Stockbridge damper:</li> </ul>	<ul style="list-style-type: none"> <li>Line monitoring (LMO)</li> <li>Protection against ice:               <ul style="list-style-type: none"> <li>Passive</li> <li>Active coatings</li> <li>Mechanical</li> <li>Thermal</li> </ul> </li> </ul>		<ul style="list-style-type: none"> <li>Tower inspections</li> <li>Maintenance</li> </ul>	<ul style="list-style-type: none"> <li>Line sagging:               <ul style="list-style-type: none"> <li>Static and dynamic re-rating</li> <li>Real time monitoring</li> <li>SLiM</li> </ul> </li> </ul>			
<b>Xformers</b>	<ul style="list-style-type: none"> <li>Walls and covers</li> </ul>	<ul style="list-style-type: none"> <li>Walls and covers</li> </ul>	<ul style="list-style-type: none"> <li>Walls and covers</li> </ul>	<ul style="list-style-type: none"> <li>Elevation platforms</li> </ul>	<ul style="list-style-type: none"> <li>Walls and covers</li> </ul>	<ul style="list-style-type: none"> <li>Walls and covers</li> </ul>	<ul style="list-style-type: none"> <li>Walls and covers</li> </ul>		
<b>Sw / Breakers</b>									
<b>Relays</b>									
<b>SCADA &amp; telecom</b>									
<b>Voltage control devs</b>									

Table 3. Preventive protection measures in electric infrastructures.

## 5.3 Protection Measures matrix: Prevention

### 5.3.1 Wind /PV generators

#### Wind generators

Wind turbines are placed on towers or pylons usually on hilltops, thus making them prone to be hit by lightning. **Lightning** and overvoltages can cause significant damage and may even result in the complete loss of the wind turbine. For instance, in 2013, 11 out of 15 cases of turbine failures in the USA were caused by lightning strikes or other ignition source causing blazes that began hundreds of meters in the air. Lightning protection of such facilities follows the international standard IEC 61400-24 (Wind turbines - Part 24: Lightning protection, 2010) and IEC 62305 (Protection against lightning - ALL PARTS, 2013) that establish that all possible lightning paths have to be considered, e.g. from the rotor blade to the base via the nacelle. Blades, for instance, are protected against currents of up to 200 kA via a lightning rod fitted close to its tip. The nacelle canopy, being a Faraday cage, is protected against lightning, as well as the equipment that contains. The other components of the wind turbine system have to be properly bonded and grounded.

**Wind storms** have a high impact on these facilities. One of the consequences could be overspeed of the rotor. In these cases, automatic overspeed protection systems take over. The primary of these systems are tip brakes. This is an aerodynamic braking system that turns the rotor blades (in the case of pitch controlled or active stall controlled turbines) or the rotor blade tips (in the case of stall controlled turbines) 90 degrees. This system can also be automatically activated when a problem occurs, e.g. loss of normal operational hydraulic pressure. Turbines are also provided with a mechanical braking system as a backup. Over the years turbine have become larger and a new risk related to wind appeared: aeroelastic instabilities (aeroelasticity is the combination of elastic deformations with the aerodynamic loading). As a preventive protection measure against such threat, better aeroelastic analysis assessment has to be performed.

Additional references can be found at (Ragheb, 2013).

Regarding **snow** and **ice storms**, the latter specially affect wind turbine operation. Icing (precipitation, atmospheric, and in-cloud) affects wind turbine operation in a number of ways, including

- measurement and control errors,
- power losses,
- mechanical and electrical failures, and
- safety hazard.

Regarding icing safety hazards, wind turbines can cause problems up to hundreds of meters from them: since turbine blades rotate at high speeds at their tips (up to 145-290 km/h), there is a possibility of ejection of ice chunks in large turbines or blade ejection in small turbines.



Figure 8. Ice accretion on a wind turbine blade. (Photo by Erik Pederson obtained from WKSU Exploradio - Outwitting ice).

Ice prevention system results from two main approaches: Anti-icing and De-Icing Systems (ADIS). In the former, the system prevents ice to accrete on the elements of the turbine, while the latter is used to remove ice layers from the surfaces. These systems can be divided in passive (that do not require extra energy supply) and active systems. Passive systems take advantage of the physico-chemical properties of the materials involved. They include special coatings (like hydrophobic, dark coatings) or flexible blades. Among active systems blade active heating is one of the most tested systems. Other options include ejection of a layer of heated air around the blade or flexible pneumatic boots. Up-to-date techniques are reviewed by Parent and Ilinca in (Parent & Ilinca, 2011). Some manufacturers provide guides to protect wind generators using their commercial solutions (i.e. (SIEMENS AG, 2012).

Icing is a permanent concern in countries that combine wind and cold weather. Indeed in 2015 took place the 1st international conference on anti-icing for wind turbines in Germany (Anti-icing for Wind Turbines).

### **PV generators**

Photovoltaic panels are especially susceptible to **sandstorms**. Some photovoltaic panels arrays has been designed to minimize effects of exposure to such weather conditions. Roughly speaking, the “soft” arrays are arrays polymer encapsulated with a higher abrasion resistance (much higher probability of surviving a severe sand environment). (Thornton, 1992)

Another effect of sandstorms is the accumulated dust that shades sunlight and induces overheating of the cells resulting in lower production. Different approaches are proposed depending on the specific geographical conditions, including forced air flow. (Assi, Hassan, Al-Shamisi, & Hejase, 2012)

### Transmission Lines

As mentioned at the beginning of the section, power lines are the most affected element in electricity networks in an event of extreme weather. Therefore, a more thorough description of the various preventive protection elements is provided in the following.

Proper maintenance of right-of-ways helps to address most of the weather threats, except maybe extreme heat. In simple terms, the right-of-way is the strip of land immediately below and adjacent to a transmission line. The width of a right-of-way varies by the type of line: the higher voltage line, the wider the right-of-way. The typical corridor widths, unless otherwise specified in the right-of-way agreement, are as follows:

- 44 to 100 kV lines require a corridor of about 21 m or more,
- 110 to 250 kV lines require a corridor of about 46 m or more,
- 400 to 500 kV lines require a corridor of about 60 m or more.

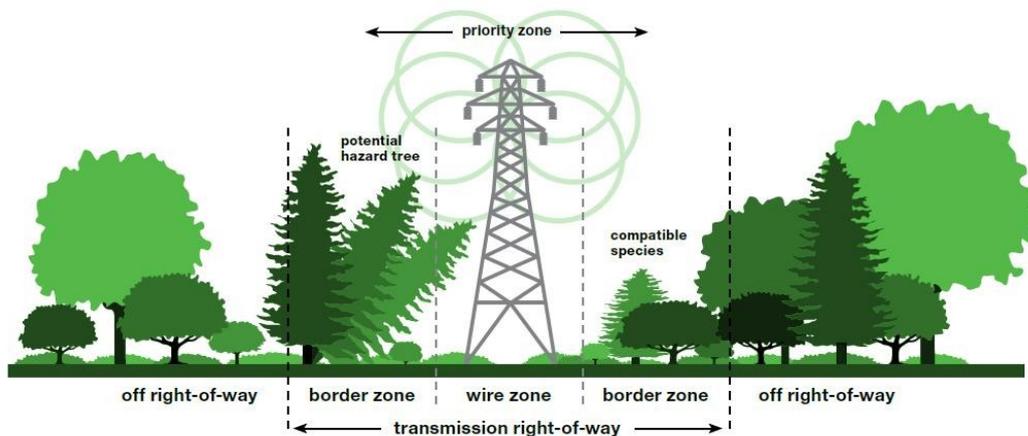


Figure 9. Schematic view of a transmission right-of-way (ConEdison)

Regular maintenance of vegetation within the rights-of-way is necessary to avoid disruption to overhead power lines and towers. Unchecked growth of tall trees and accumulation of vegetation within right-of-way may 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. The maintenance of right-of-way to control vegetation may involve the use of mechanical methods, such as mowing or pruning machinery, in addition to manual hand clearing and herbicide use. Vegetation management does not eradicate all vegetation, but instead aims to maintain trees and plant growth that may negatively affect infrastructure at a safe threshold. These thresholds depend on the voltage level of the line, as explained above, and also on the typical swings and sags of the line depending on the expected wind and temperature extremes.

Some concrete measures for maintaining the rights-of-way are:

- Implementation of an Integrated Vegetation Management approach (IVM). The selective removal of tall-growing tree species and the encouragement of low-growing grasses and shrubs is the common approach to vegetation management in transmission line rights-of-way. Alternative vegetation management techniques should be selected based on environmental and site considerations.

- Mowing with heavy-duty power equipment may be 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, may control fast-growing weedy species that have a potential to mature to heights over those permitted within the right-of-way. Trimming and pruning may be utilized at the boundaries of rights-of-way to maintain corridor breadth and prevent the encroachment of tree branches. Hand removal of vegetation, while labor intensive, may be used in the vicinity of structures, streams, fences, and other obstructions which make the use of machinery difficult or dangerous.
- Removal of invasive plant species, whenever possible, cultivating native plant species.

### **Wildfires**

Regarding forest fires, if line underlying vegetation growth is left unchecked, or slashing (wood debris) from routine maintenance is left to accumulate within right-of-way boundaries, sufficient fuel can accumulate that may promote forest fires. Recommended measures to prevent and control risk of forest fire include:

- Monitoring right-of-way vegetation according to fire risk;
- Removing blowdown and other high-hazard fuel accumulations;
- Time thinning, slashing, and other maintenance activities to avoid forest fire seasons;
- Disposal of maintenance slash by truck or controlled burning (observing the local requirements regarding burning, such as fire suppression equipment requirements, fire watcher monitoring, etc.);
- Planting and managing fire resistant species (e.g. hardwoods) within, and adjacent to, rights-of-way;
- Establishing a network of fuel breaks of less flammable materials or cleared land to slow progress of fires and allow fire fighting access.

### **Ice and snow storms**

One of the main effects of ice and snow storms is icing formation on structures and power lines. This is an important natural hazard that causes damage in many countries. Accumulated ice can weigh the lines down and cause ground faults. Also, ice suddenly breaking off the line can make the line whip and snap. On lattice towers with weakened structures, accumulated ice can add a considerable amount of weight and make the tower crumble.

Power lines are usually built following climatic hardiness rules (Design criteria of overhead transmission lines , 2003). But in many countries, rules are only based on rough climatic evaluation by altitude and latitude of the terrain where the power line will be built.



Figure 10. Nano-particle coating prevents ice buildup on roads and power lines (Cao, Jones, Sikka, Wu, & Gao, 2009).

In many countries where power line icing is a relevant problem, some strategies are taken into account in order to mitigate or avoid the effect of this phenomenon on the reliability of the power supply service. A wide presentation of these techniques can be found in the specific Cigré Report (Cigré 2009). The strategies can be classified in four groups:

- **Passive methods:** they do not require an external source of energy but use only natural forces such as wind, gravity or solar radiation. Consequently, they can function on both energized and non-energized phase conductors as well as ground wires. This group includes most of the anti-icing methods used to prevent or reduce the accretion of wet snow and ice on conductors. For instance, a well-known method among these consists in using counterweights to increase the torsional stiffness of conductor spans. Field observations in Japan, Iceland and France on wet snow have shown that this device can limit the formation of cylindrical deposits of wet snow by limiting the rotation of a conductor resulting from eccentric snow loading on its windward side. With highly eccentric snow loadings, shedding caused by gravity and wind forces is facilitated.
- **Active coatings and devices:** methods based on active coatings are active methods requiring some electrical energy to be effective. For instance, one method is based on the use of a ferromagnetic coating for the purpose of sustaining a positive temperature of the energized conductor surface. This method, known as LC-Spiral Rod method, has been implemented successfully in Japan. These spiral rods have been manufactured and installed for more than 20 years to prevent accidents caused by the sudden fall of large chunks of snow.
- **Mechanical methods:** in most cases, mechanical methods can be considered as de-icing methods as they are used to speed the shedding process after snow packs or ice have formed on conductors and ground wires. It has been demonstrated that mechanical methods require around 100,000 times less energy than thermal methods to force ice shedding. Generally, most of the mechanical methods are based on two strategies. One strategy consists in breaking the ice by scraping it, and the second in releasing energy from

shock waves, vibrations or ground wire/conductor twisting to break and pull off the ice. One of the main advantages of mechanical methods is their relative ease of application compared to thermal methods. In fact, mechanical methods are those preferred for timely and fast intervention to de-ice short critical sections of a power network. However, in general, these methods are to be avoided with ground wires carrying communications, as the bending can damage the optical fibers.

- **Thermal methods:** heating of line conductors or ground wires to prevent ice accretion or for de-icing purposes is more expensive, but it is recognized worldwide as the most efficient engineering approach to minimize the consequences of severe ice storms on overhead lines. Thermal methods include all methods causing the ice to melt in order to force shedding. Some of these methods can be used for anti-icing purposes in order to prevent supercooled water droplets from freezing during their impact on the conductor surface. In that case, less energy is required for anti-icing than for de-icing. Thermal methods can be divided in two categories: (i) methods based on pure Joule effect, and (ii) methods based on dielectric losses, radiative waves and external heat sources. An example of the first case, Line Impedance Modulation (LIM) (Couture, 2011) allows line power flow and stability to be controlled by individually switching in and out subconductors of bundled-conductor lines, thus modifying the net line impedance directly and dynamically. Another example is the Levis De-Icer technique, designed in Canada. It is aimed to de-icing AC power lines through High voltage direct current. The DC current of the conductor needs to be just high enough to melt the ice on it without actually going above the thermal limit of the conductor. (Wikipedia - Levis De-Icer).

In addition, a real-time line monitoring system (like LMO proposed in (Couture, 2011)) can provide data related to electrical, mechanical or climatic events needed for line de-icing, power flow or stability control.

### **Line sagging prevention/mitigation**

Line sagging prevention/mitigation addresses mainly extreme heat. When lines carry electric power, they heat up due to the Joule effect, since they have some non-negligible resistance. The cables then dilate, causing sagging. Under extreme heat weather, particularly with low wind speeds, the line exchanges a lot less heat with the air around it, and the dilation could reach dangerous levels.

Short of re-fitting the line with new cables (reconductoring), there exist some mitigation measures:

- **Static re-rating of the line:** it basically consists in measuring again the actual physical parameters of the line, in order to measure the real thermal capacity limits (*ampacity*). This could be useful for very old lines whose properties may have changed with aging.
- **Dynamic re-rating:** this is a more useful technique. It measures the effective line rating in real time, by electrical methods, thus taking into account the dynamic thermal properties (i.e. the level of heat dissipation at a particular point in time, which depends on the wind and solar irradiation).

- Real time monitoring: install devices to monitor and measure line sagging in real time. This is of course more expensive and cannot be deployed extensively.
- Sagging Line Mitigator (SLiM): a novel mechanical device that is purely passive. It automatically decreases the effective length of conductor in the span, counteracting the thermal expansion of the conductor.

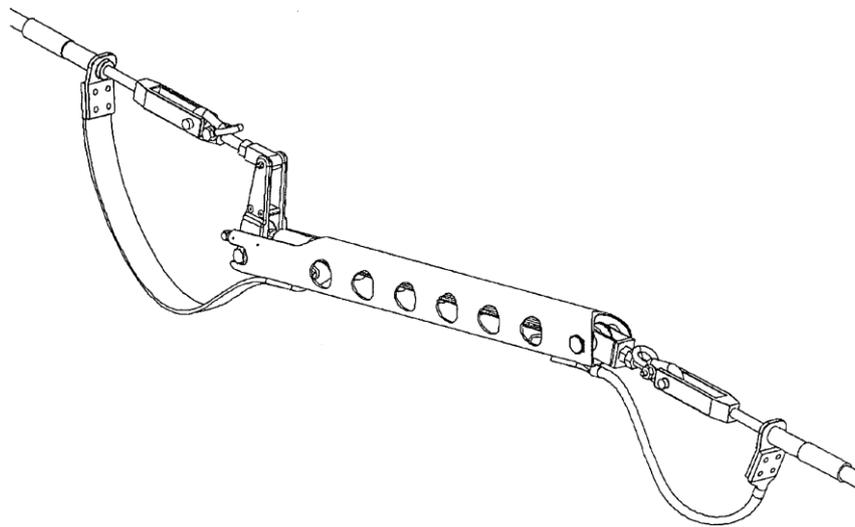


Figure 11. Line sagging mitigator. Image from Patent US6864421 B1. [37]

### Tower inspection and maintenance

The same way maintenance of the right-of-use is important to address most of the weather threats discussed, proper maintenance of towers is also a crucial to reduce the risks associated to extreme weather events.

Towers are designed to withstand quite severe weather; in fact they should always be designed to withstand the expected extreme values at the location where they are built. However, these investments typically last more than 40 years, and they need periodic maintenance.

Maintenance should check at least for:

- Rusting: towers are built with high quality steel and they may have anti-rust coating, but nevertheless they should be checked for rusting, especially near coastal areas.
- Grounding: the grounding cables should be checked in order to ensure proper protection against lightning.
- Check for damaged or weak foundations. This includes checking for possible permafrost melting in Nordic countries.
- Check and clear birds nests: big birds such as storks have quite long wingspans and they can easily cause short-circuits.
- Washing insulators

### 5.3.2 Reliability and security levels of OverHead Transmission Lines (OHTL) (Snow & Weckman, 2010)

Present line design practice views the support structure as an isolated element supporting half span of conductors and OverHead Ground Wires (OHGWs) on either side of the structure. A 3D simulation study about investigating line failures with the approach of the following Figure 12 took place. After the designing of a structure, loading events of increasing magnitude were analytically applied from different directions until the actual critical capacity for each key member of interest is reached. The probability of occurrence for those specific loading events can then be predicted for the specific location of that structure by micrometeorology experts. A few of the key conclusions for that specific case are:

- The legs had a probability of failure in that location of once in 115 years;
- Tension cords in the conductor arm and OHGW arm had probabilities of failure of 110 and 35 years respectively;
- A certain wind condition at an angle was found to be critical for the foundation design with a probability of occurrence at that location of once in 25 years.

Some interesting observations can be drawn:

- The legs were conservatively designed under the NESC (National Electrical Safety Code) “heavy”<sup>2</sup> specifications.
- The loss of an OHGW is a more likely event than the loss of a conductor.
- The foundation was found to be the weak link.

---

<sup>2</sup> Loading condition for wire wind pressure of 4 psf (pounds per square foot of wind equivalent to a 40 MPH or 18 m/s), pole Structure Wind Pressure of 5 psf (eq. to 20 m/s) and 0.5 in. of ice

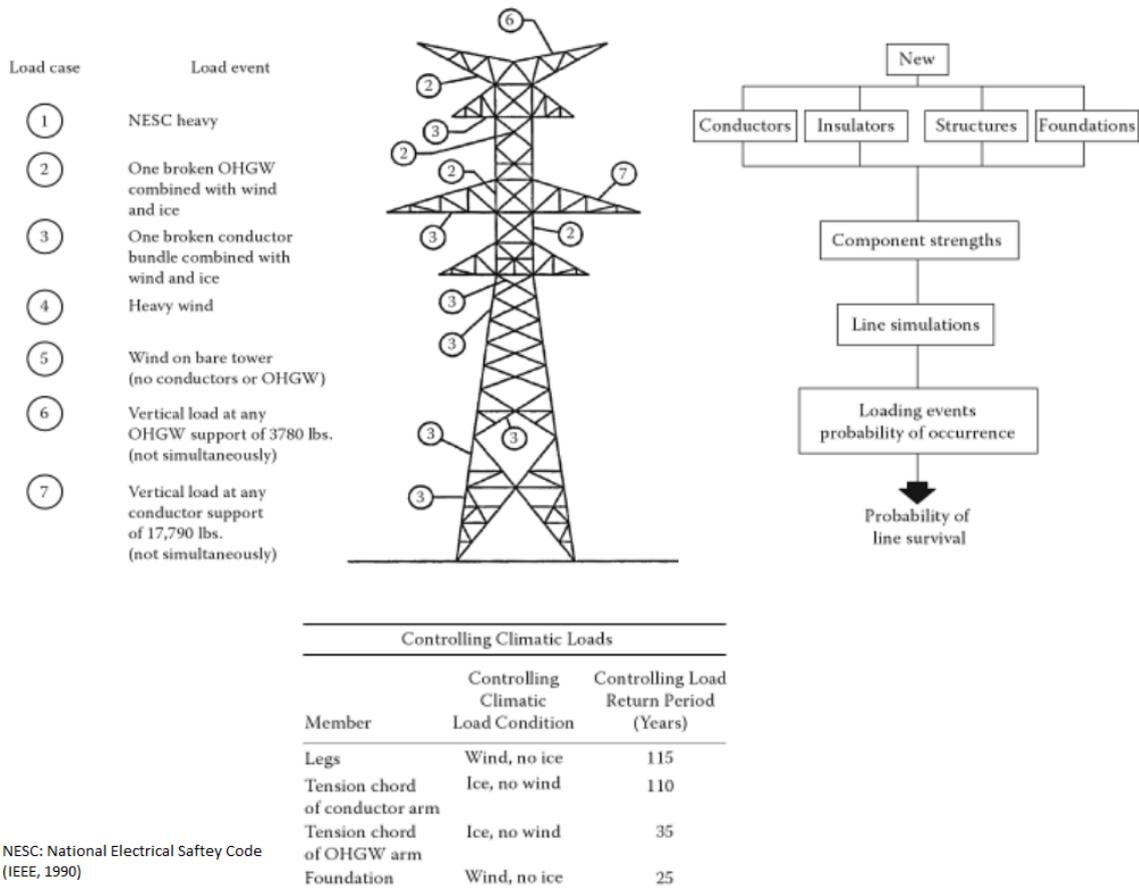


Figure 12. Typical High Voltage transmission line tower and the results of a reliability testing [15b]

Then, in order to estimate the probability of survival ( $P_s$ ) of an element it is sufficient to know the annual probability of failure ( $P_f$ ), that is

$$P_s = 1 - P_f.$$

If it is desired to know the probability of survival over an extended length of time, i.e.  $n$  years of service life (a 50-year service life as expected by the designers) (Grisby, 2006), the year survival probabilities are multiplied:

$$[P_{s1} \times P_{s2} \times P_{s3} \times \dots \times P_{sn}] = (P_s)^n.$$

It should be noted that the failure of every component does not necessarily progress into extensive damage. Since the OHTL is a contiguous mechanical system, the forces from the conductors and the OHGWs on one side of each tangent structure are balanced and restrained by those on the other side. When a critical component fails, energy stored within the conductor system is released suddenly and sets up unbalanced transients that can cause failure of critical components at the next structure. This can set off a cascading effect that will continue to travel downline until it encounters a point in the line strong enough to withstand the unbalance.

A good estimate of failure correlation (probability of failure of multiple elements at once) can be also obtained. These correlations are usually quite high since the dominant loading on all elements is wind. Failure of other elements usually implies the presence of a weakest element failure. For instance, for towers it is observed that the foundation, followed by the legs in lower panels govern failure.

It is also observed statistically that the effect of simultaneous extreme wind and wire break can effectively be neglected for reliability-based design of tangent suspension transmission line towers, where conductor icing is not observed [16]. A recent study of BPA (Bonneville Power Administration, USA) shows the strength criterion that combines both wind and ice loading Figure 13. In developing the reliability model, it is observed in full scale tower tests that, on average, wind velocity  $V$  when a collapse occurs is about 12% higher than strength capacity  $U$  of the tower. In other words, if a tower can bear winds  $U = 44.7$  m/s, then 50% of similarly-designed and installed towers should fail at  $V = 50.1$  m/s. This implies that the average tower fails at 125% of the design load. This extra 25% is a combination of the conservatism built into the elastically-based design, coupled with some post-yield capacity of a typical tower to accept more load before it actually collapses.

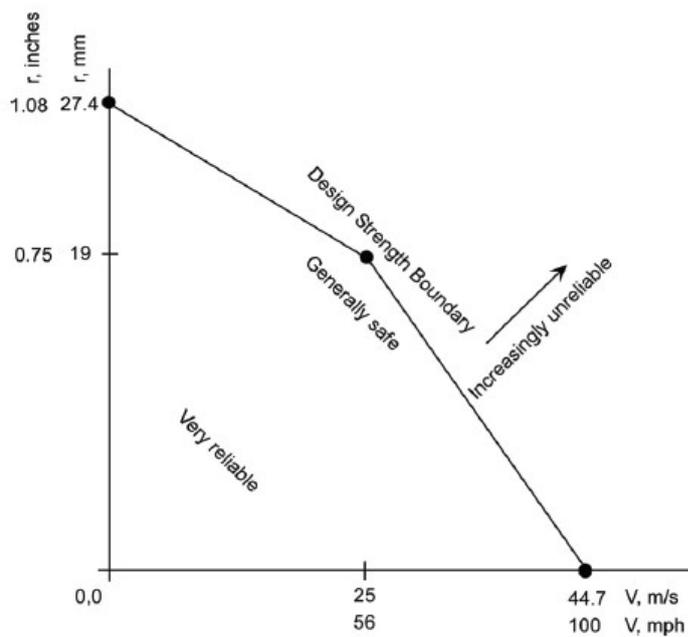


Figure 13. Strength criterion for HV line towers (reliability boundaries in combined icing and windy conditions) (Krishnan, Kalyanaraman, & Menon, 2006)

The BPA evidence over 50 years shows that an average long term failure rate of 0.00005 per year (5 tower failures per 100,000 towers, per year), appears reasonably cost effective and to have no serious long term impact to society. On the contrary, a failure of 1,000 steel lattice-type transmission towers in one storm event does not appear acceptable to society, as evidenced in the Montreal ice storm of 1998 (Edinger & Kempner, 2012).

## 5.4 Protection Measures Matrix: Mitigation

Like in the case of telecommunication infrastructures, mitigation measures strongly depend on the specific case considered.

Some mitigation procedures are equivalent to prevention measures already presented, i.e. active de-icing of power lines.

In the case of Photovoltaic generators, however, as mitigation procedure, it is possible to correct the defects caused by sandstorms on the glass used as protective sheets of solar panels. The relative photovoltaic efficiency can sensitively improved: In laboratory tests it passes from 0.88% for the sandblasted state to 0.97% for the coated samples.

MITIGATION									
	Lightning	Windstorms	Ice/snow storms	Flash floods	Extreme cold	Extreme heat	Wild fires	Sand storms	Seasonal drought
Generators (housed)									
Generators (wind / PV)			<ul style="list-style-type: none"> <li>• Anti-Icing and De-Icing Systems (ADIS).</li> </ul>					<b>PV</b> <ul style="list-style-type: none"> <li>• Correct defects caused by sandstorms</li> </ul>	
Lines			<ul style="list-style-type: none"> <li>• Passive</li> <li>• Thermal</li> <li>• Mechanical</li> </ul>			<ul style="list-style-type: none"> <li>• Line sagging mitigator SLiM</li> </ul>			
Xformers									
Sw / Breakers									
Relays									
SCADA & telecom									
Voltage control devs									

Table 4. Mitigation protection measures in electric infrastructures.

## 6. Protection protocols

In this Chapter, a quick overview of the standards and regulations regarding protection critical infrastructures is provided.

Within the European Union, concerns about security of Critical Infrastructures (CI) like the electric power network have resulted in a series of programmes for their protection, like the European programme for Critical Infrastructure Protection (EPCIP), accepted by the European Council on December 2004 (European Programme for Critical Infrastructure Protection). This programme aims to respond to natural hazards, apart from human threats including criminal activities or terrorism, and to increase the resilience of CI to limit the detrimental effects of disruptions of such infrastructures on the society and citizens. The Critical Infrastructure Warning Information Network (CIWIN) was created to facilitate the implementation of EPCIP. The European Commission also created an European Reference Network for Critical Infrastructure Protection (ERN-CIP) to foster security solutions related to CI.

The European Organisation for Security (EOS) coordinated the FP7 project European Risk Assessment and Contingency Planning Methodologies for Interconnected Energy Networks (EURACOM). This project addressed risk assessment and contingency planning in all energy sectors, and in particular the issue of protection and resilience of energy supply for European interconnected energy networks. (European Organisation for Security)

Other countries are also developing their protection systems. In the USA, the National Infrastructure Simulation and Analysis Centre (at Los Alamos National Laboratory) developed the Critical Infrastructure Protection Decision Support System (CIPDSS) tool. It provides information and decision support for the protection of CI based on an assessment of risks including natural disasters (Bush, Dauelsberg, LeClaire, Powell, Deland, & Samsa, 2005)The North American Electric Reliability Corporation (NERC) provides reliability guidelines in relation to bulk power system in North America. It is particularly interesting for project RAIN their (Reliability Guideline. Generating Unit Winter Weather Readiness)]. These guidelines were developed as a result of an unusual cold weather event in the southwest of the USA in 2011, not normally exposed to freezing temperatures. The same institution offers cold weather training modules to improve preparedness for such extreme weather events. At the governmental side, the department of homeland security set the National Infrastructure Protection Plan (NIPP) (Department of Homeland Security). It is a risk management framework to coordinate government and private sector participants in the CI community.

Australia also has its own Critical Infrastructure Program for Modelling and Analysis (CIPMA). It offers modelling and analysis to government and critical infrastructure owners. This information aims to *help prevent, prepare for, respond to, or recover from, a natural or human-caused disruption to CI.* (Critical Infrastructure Program for Modelling and Analysis)]

For a review of different schemes of behaviour analysis and modelling of critical infrastructure systems see (Ghorbani & Bagheri, 2008).

## 6.1 Software tools aiding in protection

Some software tools provide monitoring and/or analysis of the networks in real time. They are the “eyes and ears” of operators, i.e. they provide *situational awareness*; crucial in dealing with critical events and crises.

At the Network Operations Centres (NOC) network monitoring, incident response, and communications management take place. These facilities are equipped with software tools like

- Supervisory Control And Data Acquisition (SCADA), for monitoring and actuation on the network;
- Energy Management Software (EMS), a real-time analytical software, that also allows contingency analysis, or assessment of reliability by analysing PV/QV Curves (i.e. Power-Voltage and Reactive Power Q - Receiving end Voltage V curves) in the case of electric networks;
- Geographic Information Systems (GIS), software tools that allows spatio-temporal location of events.

An in-depth analysis of extreme events and planning of infrastructure protection investments can be facilitated by decision support systems like the American CIPDSS developed at Los Alamos National Laboratory, or the Australian CIPMA commented earlier.

## 7. The role of protection methods in the Bayesian Network-based risk assessment framework

The role of the protections in the framework for risk assessment is schematically shown in Figure 14. Preventive measures affect the probabilities of occurrence of an event, which is triggered by meteorological causes. The event is also determined by the context and the condition. The condition is related to the physical state (age, maintenance, quality of materials) of the assets

The idea is to analyze in detail the sequences of cause-effect relationships in outages. One secondary objective is to unify all preventive measures in a holistic view of the problem. Then, the next step is to assess their relative effectiveness (which will most likely depend on context). Finally, to try to wrap it all up in a Bayesian-Network approach, linking to risk analysis framework being developed in WP5.

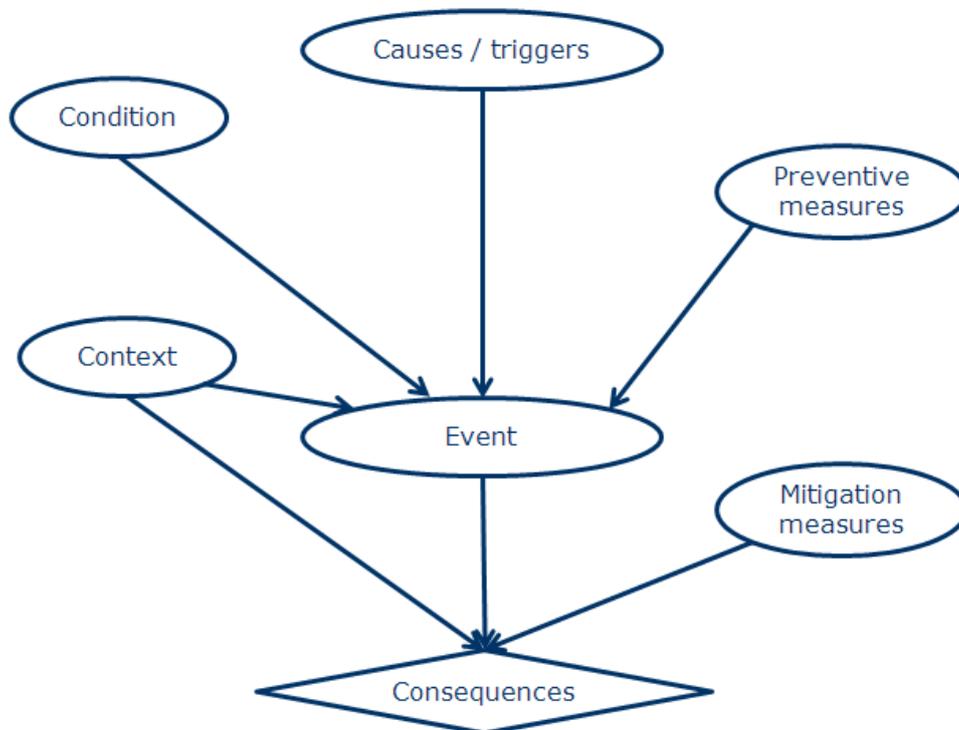


Figure 14. Following the initial work WP6, and complemented with ideas from Fenton & Neil

**Preventive measures.** “Preparedness”, e.g. winterization procedures, line sagging prevention, de-icing, etc.

- **Mitigation measures.** E.g. System Protection Schemes and “Defence Plans”
- **Consequences.** There are two broad types:
  - For the customers & businesses. These are local.
  - For the grid itself. These may spread globally (cascading effects leading to a blackout)
- **Condition.** E.g. rights-of-way condition; steel tower rusting. Any other intrinsic properties such as: age, model/make, technology type.
- **Context.** Two broad types:

- a. Operational: electric scenario of the grid
- b. External context (e.g. day of week, special events...)

## 7.1 Root Cause Analyses: sample outages

Root cause analysis (RCA) a technique designed to identifying root causes of fault. It can help to understand and prioritize the vulnerabilities in order to design protection schemes (Wilson, Dell, & Anderson, 1993).

It fits perfectly with Bayesian approach because, as seen in Figure 14, it follows the same sequence causes / events / consequences.

It define three types of events,

- **Trigger cause**, that is the event that initiates the sequence that finally resulted in the outage. In the context of RAIN, they are of meteorological nature.
- **Direct cause**, the final event in the sequence of events that lead to the outage.
- **Root cause**, that gives an insight of why the outage occurred, and how to avoid such outages in the future. In this sense, the analysis of the root cause.

Below we present a couple the examples (Grisby, 2006) of identification of these elements in events of meteorological in a telecommunication infrastructure.

### Example 1:

A lightning strike resulted in a commercial AC power surge, causing the rectifier AC circuit breakers to trip open. This means that AC from either the primary or backup source cannot be converted to DC. As a consequence, the batteries must supply power until the rectifiers are manually switched back on line. The alarm system does not work properly. After some time the batteries are exhausted and the communications equipment loses power, and an outage occurs.

- **Trigger Cause:** Lightning strike.
- **Direct Cause:** Battery Depletion.
- **Root Cause:** Maintenance -- Failure to test alarm system.

### Example 2:

Torrential rains and flooding due to a tropical storm causes commercial AC power failure. The generators in the communication complexes are supplied with fuel from supply pumps that are located in the basement of the building. Due to the flooding, water entered the basement causing supply pump failure. Hence, the generators ran out of fuel, and the facility goes on battery power. After some time, the batteries stopped supplying power to the equipment thus resulting in an outage.

- **Trigger Cause:** Storms (Flooding).
- **Direct Cause:** Battery depletion.

- **Root Cause:** Engineering failure (The fuel pump system was placed in the basement in an area prone to flooding).

In the following tables (Grisby, 2006) see that Natural disasters are the main trigger cause of High Impact events (the impact has been measured in terms of the Lost Consumer Hours indicator. The trigger, root cause, and equipment most associated with the root cause, have been examined by outage impact for telecommunications power outages over an eight year period.

Trigger Cause	Total Outages	Low	Medium	High
Natural Disasters	14%	8%	16%	35%
Power Surges	18%	23%	10%	10%
Comm.AC Loss	38%	39%	37%	23%
Human Errors	30%	30%	37%	23%
Total	100%	100%	100%	100%

Table 5. Trigger causes of outages according to impact.

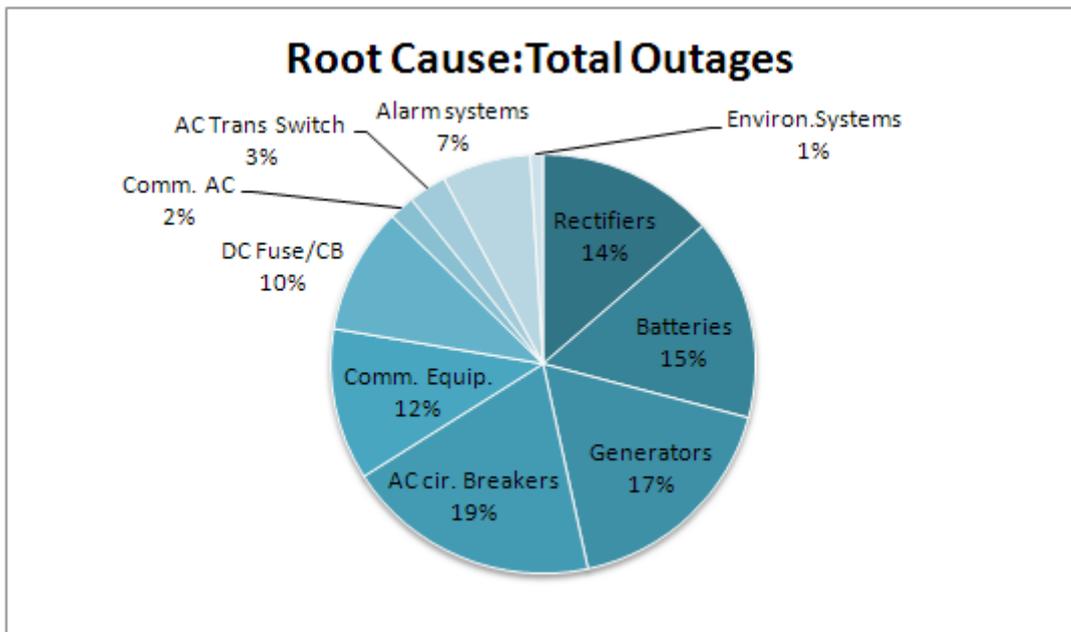


Figure 15. Number of outages produced by each cause

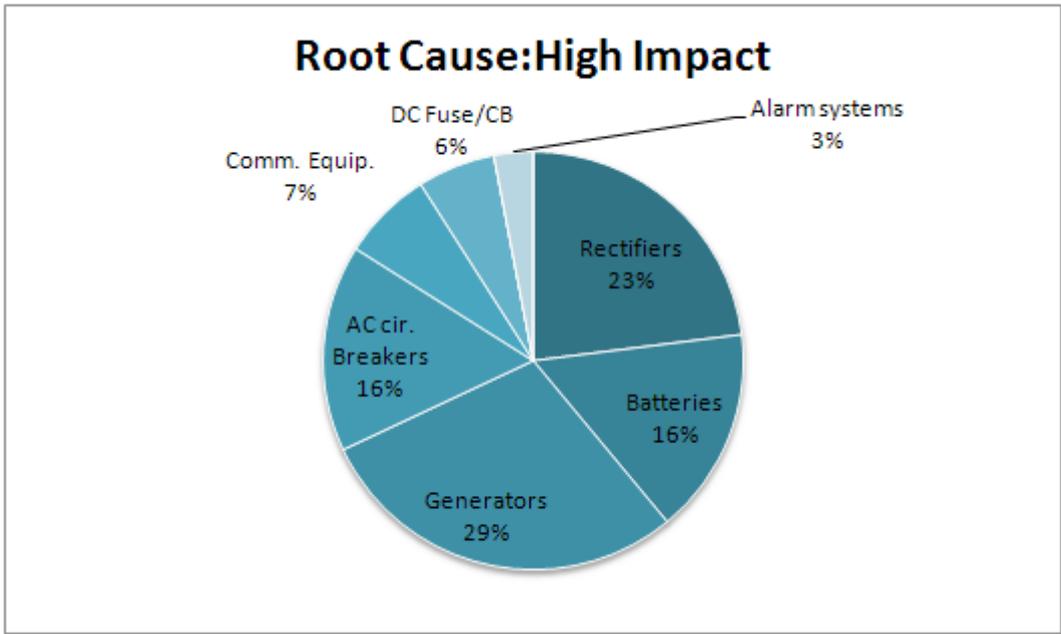


Figure 16. Number of event of high impact due to different root causes

As shown in figures 15 and 16, the root causes of electrical outages are mainly circuit breakers, generators, batteries and rectifiers. Moreover, these devices are the responsible of the events of higher impact. Therefore, the protection should be focused on them.

Component	Example
Rectifiers	1. Power surge, due to lightning strike.
	2. Rectifiers damaged, batteries not charged.
	3. Batteries eventually exhausted.
Batteries	1. Loss of commercial AC.
	2. Batteries failed because of loose battery cell strings.
Environmental Systems	1. Loss of commercial AC.
	2. Generator started running.
	3. Failure of Air Conditioning system.
	4. Generator overheated and stopped.
Circuit Breakers	1. Loss of commercial AC.
	2. Main Circuit breaker opens due to an AC power surge.
	3. Site is supplied power from batteries.
	4. Batteries eventually exhausted.
Generators	1. Loss of commercial AC.
	2. Generator started but stopped after some time due to piston seizure, contaminated fuel, or runs out of fuel.
	3. Batteries supply power until finally exhausted.
Alarm System	1. Loss of commercial AC.
	2. Generator started to run but stopped due to overheating.
	3. Alarm system failed to generate an alarm at NOC.
	4. Site runs on batteries until exhausted.
AC Transfer Switch	1. Loss of commercial AC.
	2. Failure of AC transfer switch.
	3. Site is left on batteries until exhausted.
Communications Equip.	1. Technician working on the communications equipment drops tool shorting DC bus on equipment.
	2. Equipment shutdown.
DC Fuse/CB	1. Fuses to telecommunications equipment blow since they were drawing more current than their rated specifications.
	2. Equipment Shutdown.
Commercial AC	1. Some outages occurred due to the loss of Commercial AC.
	2. No information given about the series of events in report.

Table 6. Examples of failures in telecom components due to failures in the power system

## 8. Summary and Conclusions

In general, it is very difficult to choose or design protections against rare and severe events. In one hand the costs of implementation are high, but also the resources to maintain the protection system must be considered. Usually the decision of investment in protection (for the type of threat described) is taken when some threshold in some indicator of severity is surpassed, but even if the estimation of impact on different scenarios can be done reasonably, the estimation of probability of occurrence is highly imprecise by nature.

In both infrastructures, Telecommunications and Electricity, exposed cables suffer mainly due to icing, lightning and heat. There several techniques used are prevention measure and as mitigation. Some of them are in an early stage of research.

The utilities are in general prepared for the typical weather they have (in other words, they're adapted to the climate they live in). The problem is that, as climate changes (slowly or not, it does change) then weather phenomena that is considered "extreme" in a given climate may start to become more common. The good news is that protection methods and protocols can then be copied from utilities in other climates where those phenomena are more common. This is what happened for instance with the "Winterization Procedures" that NERC now imposes to Southern states in the US.

This is more of an opinion point but it is substantiated in the statistics: in Telecoms there is too much hype regarding cyber-security, to the detriment of weather-related preparedness. The latest ENISA reports confirm that about 50% of large outages originate in weather problems, not cyber threats. Another large percentage is just malfunction of electronic equipment. There's certainly a danger of overlooking or understating the importance of weather preparedness.

Finally, in Telco, an important part of mitigation strategies are related to backup power. This means having batteries and those auxiliary diesel gens in good shape.

## 9. Bibliography

- Anti-icing for Wind Turbines*. (n.d.). Retrieved from <http://www.anti-icing-wind-turbines.com/>
- Assi, A., Hassan, A., Al-Shamisi, M., & Hejase, H. (2012). {Removal of air blown dust from photovoltaic arrays using forced air flow of return air from air conditioning systems}. *2012 International Conference on Renewable Energies for Developing Countries (REDEC)* (October 2015), 1-5.
- Bush, B., Dauelsberg, L., LeClaire, R., Powell, D., Deland, S., & Samsa, M. (2005). *Critical infrastructure protection decision support system (CIP/DSS) project overview*. Boston.
- Cao, L., Jones, A. K., Sikka, V. K., Wu, J., & Gao, D. (2009). Anti-Icing Superhydrophobic Coatings. *Langmuir* , 12444–12448.
- ConEdison*. (n.d.). Retrieved from [http://www.coned.com/publicissues/vm\\_transmission.asp](http://www.coned.com/publicissues/vm_transmission.asp)
- Couture, P. (2011). Smart Power Line and photonic de-icer concepts for transmission-line capacity and reliability improvement. *Cold Regions Science and Technology* , 65 (1), 13-22.
- Critical Infrastructure Program for Modelling and Analysis*. (n.d.). Retrieved from <https://www.ag.gov.au/NationalSecurity/InfrastructureResilience/Pages/CriticalInfrastructureProgramforModellingandAnalysisCIPMA.aspx>
- Degrees of protection provided by enclosures. (2013). *International Electrotechnical Commission* .
- Dekker, D. M., & Karsberg, C. (2011 - 2012). *ENISA Annual Incident Report*. Greece.
- Department of Homeland Security*. (n.d.). Retrieved from <http://www.dhs.gov/national-infrastructure-protection-plan>
- Design criteria of overhead transmission lines . (2003). *International Electrotechnical Commission* , 243.
- Edinger, M., & Kempner, J. (2012). Reliability of Transmission Towers under Extreme Wind and Ice Loading. *G&E Engineering Systems and Bonneville Power Administration US* .
- Electrical Protection of the Subscriber Outside Plant* . (2013).
- Elisabeth Krausmann, E. A. (2013). *Space Weather and Power Grids: Findings and Outlook*. Ispra, Italy.
- Environmental testing - Test R and guidance: Water* . (2000).
- Environmental testing - Test A: Cold. (2007). *International Electrotechnical Commission* .
- ESTI. (2014). *Environmental conditions and environmental tests*.

*European Organisation for Security.* (n.d.). Retrieved from <http://www.eos-eu.com/Middle.aspx?Page=euracom>

*European Programme for Critical Infrastructure Protection.* (n.d.). Retrieved from <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV:I33260>

Ghorbani, A. A., & Bagheri, E. (2008). The state of the art in critical infrastructure protection: a framework for convergence. *International Journal of Critical Infrastructures* , 4 (3).

Grisby, L. L. (2006). *The Electric Power Engineering Handbook*. CRC Press.

Krishnan, J., Kalyanaraman, V., & Menon, D. (2006). Estimating the Reliability of Transmission Line Towers. *3rd International ASRANet Colloquium*. Glasgow.

NGMN. (2013). *Recommendation on Base Station Antenna Standards*. Frankfurt.

*North American Electric Reliability Corporation.* (n.d.). Retrieved from <http://www.nerc.com/pa/Stand/Pages/ReliabilityStandards.aspx>

Parent, O., & Ilinca, A. (2011). Anti-icing and de-icing techniques for wind turbines: Critical review. *Cold Regions Science and Technology* , 88-96.

Protection against lightning - ALL PARTS. (2013). *International Electrotechnical Commission* , 799.

Protection against lightning. (2010). *International Electrotechnical Commission* .

Ragheb, M. (2013). *Safety and protection for wind turbines perfectly coordinated components for low-voltage power distribution*.

*Recommendations ITU-T (Study Groups ITU).* (n.d.). Retrieved from <http://www.itu.int/ITU-T/recommendations/>

*Reliability Guideline. Generating Unit Winter Weather Readiness* .

SIEMENS AG. (2012). *Safety and protection for wind turbines*.

Snow, A., & Weckman, G. (2010). *Protecting Criminal Telecommunications and Networking Infrastructure*. ICN.

Thornton, J. (1992). The effect of sandstorms on PV arrays and components. *National Renewable Energy Lab* .

*Wikipedia - Levis De-Icer.* (n.d.). Retrieved from [https://en.wikipedia.org/wiki/Levis\\_De-Icer](https://en.wikipedia.org/wiki/Levis_De-Icer)

Wilson, P. F., Dell, L. D., & Anderson, G. F. (1993). *Root Cause Analysis : A Tool for Total Quality Management*. American Society for Quality.

Wind turbines - Part 24: Lightning protection . (2010). *International Electrotechnical Commission* , 153.

*Wireless Networking in the Developing World.* (n.d.). Retrieved from  
[http://www.vias.org/wirelessnetw/wndw\\_07\\_05b.html](http://www.vias.org/wirelessnetw/wndw_07_05b.html)