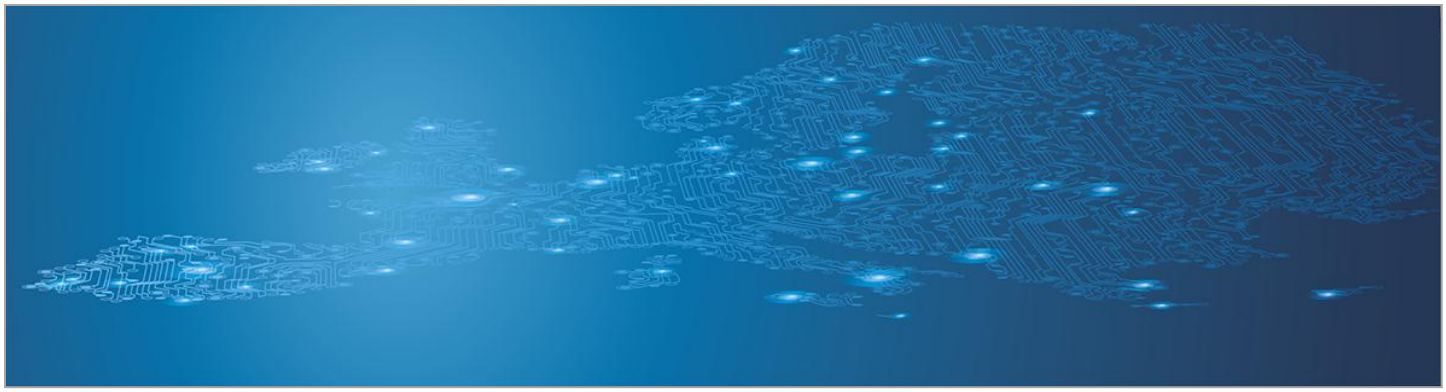

Power Supply Dependencies in the Electronic Communications Sector

Survey, analysis and recommendations for resilience against power supply failures

December 2013

European Union Agency for Network and Information Security

www.enisa.europa.eu

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Authors

Christoffer Karsberg, Dr Konstantinos Moulinos, Dr Marnix Dekker

Contact

For contacting the editors please use resilience@enisa.europa.eu.

For media enquires about this paper, please use press@enisa.europa.eu.

Acknowledgements

This study has been carried out in collaboration with Saab AB, in particular Mr Hans Åkermark.

ENISA would like to thank the service providers and National Regulatory Authorities within the electronic communications sector and power supply sector respectively, that have provided information underlying the findings and recommendations made in this report.

We have also received valuable reviews from industry experts in the ENISA Electronic Communications Reference Group. Listing the organisations (in non-particular order): Zon Optimus, Deutsche Telekom, Allegro Networks, OniTelecom, BT, HEAnet, Vodafone, AVEA, OTE Group – Cosmote, Telecom Italia, Fastweb, TeliaSonera, Magyar Telekom, Telekom Austria, TDC, Netnod, Telefonica, Colt, Telekom Austria, Magyar Telekom.

Finally we thank the experts at National Regulatory Authorities across EU and EFTA countries who work with us as members of the Article 13a Expert Group, in providing us useful feedback during discussions, interviews and reviews of drafts of this document. Listing the organisations (in non-particular order): OEC (PL), Centre for Cyber Security - CFCS (DK), ANACOM (PT), PTS (SE), Ministry of Economic Affairs (NL), FICORA (FI), Ofcom (UK), ComReg (IE), EETT (GR), ADAE (GR), RTR (AT), ANCOM (RO), CRC (BG), Ministry of Economics, Finance and Industry (FR), Bundesnetzagentur (DE), BIPT (BE), MITYC (ES), MPO (CZ), CTO (CZ), CERT LT (LT), TRASR (SK), ILR (LU), PECSRS (SI), MCA (MT), Ministry of Economic Development (IT), OCECPR (CY), NPT (NO), ETSA (EE), NMIAIAD (HU), ITSIRI (LV), APEK (SI), Teleoff (SK), OFCOM (CH), HAKOM (HR).

Legal notice

Copyright Notice

ISBN 978-92-9204-081-9 doi: 10.2824/29209

Executive summary

Electronic communications are the backbone of the EU's digital society. The electronic communications networks and services allow citizens, businesses, governments and organisations to communicate and exchange information and to offer and consume online services. Article 13a of the EU's electronic communications Framework directive, which was implemented across the EU in 2011, asks EU Member States to ensure the security and resilience of public electronic communications networks and services.

As part of the implementation of Article 13a, National Regulatory Authorities (NRAs) in the EU collect reports about incidents with a significant impact on the electronic communications networks and services. Yearly, ENISA publishes an annual report which summarizes these incident reports and provides an aggregate analysis of major outages. As can be seen in the ENISA annual report about major incidents, power cuts are a dominant cause of severe network and service outages in the EU's electronic communications sector.

In this report, we study these incidents in more detail and we make recommendations to NRAs and electronic communications service providers (providers) and to some extent also to actors in the energy sector as well as civil protection authorities. Our recommendations are not about preventing power failures in the power supply sector, but they are aimed at improving the electronic communications sector's ability to withstand and act efficiently after power cuts.

ENISA conducted an online survey and interviews about how power cuts are handled in the electronic communications sector. We found that:

- A majority of EU Member States have implemented more general resilience policies through legislation, whereas a minority of the Member States have implemented policies that are directly linked to resilience against power cuts.
- A majority of the NRAs do not and may even lack suitable input to perform risk assessments that include power cuts. It is also noted that the national use of state funding and public-private partnerships to address power cut resilience are exceptions rather than the norm within the EU.
- Resilience against power cuts is lower in access networks closer to customers than for network elements that carry traffic for a large number of customers. Mobile networks tend to be more vulnerable to power cuts compared to fixed networks.
- A majority of NRAs believe that current protection levels are not adequate and they would like to see power cut resilience to become a market differentiating factor for network and providers.
- A review of incident reports from 2011 and 2012 shows that a significant number of power cuts led to more severe service disruptions than what would have been the case had existing protection measures worked as intended.
- A large number of energy sector regulators within Europe have adopted regulatory instruments to maintain or improve continuity of supply in the energy sector, balancing other regulations aiming at increasing competition and market efficiency.
- In some countries, the energy sector has taken significant steps in defining socio-economically acceptable quality of service levels, whereas in some countries the providers face the fact that there are no special contractual agreements with the power companies containing SLA-based requirements.

- Cooperation and information exchange can be improved within the electronic communications sector and with the energy sector and civil protection authorities, and the room for improvement is even more significant for cross-sector restoration efforts.
- Prioritization schemes to give assets within the electronic communications sector preferential treatment in the event of more significant power cuts, are not yet widespread in the EU.

We also make 8 recommendations mainly to NRAs and providers within the electronic communications sector, and in some recommendations we also address the energy sector and civil protection authorities. The recommendations describe steps which could be taken to reduce the risk of network and service outages caused by power failures, and in this way improve the electronic communications sector's ability to handle disruptions and outages caused by power supply failures. Summarizing the recommendations:

1. NRAs should analyse the frequency and impact of network and service outages caused by power cuts.
2. NRAs should liaise with providers, energy regulators and other NRAs to collect good practices that could be used to increase resilience against power cuts. These good practices should be considered as part of a cost-benefit analysis (recommendation 3).
3. NRAs should perform, in cooperation with energy regulators and civil protection authorities, a cost-benefit analysis, where societal costs and benefits are evaluated, to determine what is reasonable to expect from different actors regarding power cut resilience measures.
4. Providers should regularly perform checks of existing protection measures, such as checks of UPS systems and batteries, and running facilities with fixed and transportable power generators at full load, to avoid and mitigate the impact of network and service outages from shorter and medium duration power cuts.
5. NRAs should in their follow up of major network and service outages caused by power cuts ensure that affected providers, based on lessons learned, systematically develop their protection measures to avoid and mitigate the impact of network and service outages from shorter and medium duration power cuts.
6. NRAs should act to establish a strategy to promote cooperation and mutual aid agreements on joint service restoration after severe power cuts which can include cross-sector exercises.
7. NRAs should consider a priority scheme that would give preferential treatment within the electronic communications sector and decrease service restoration times under exceptional circumstances.
8. NRAs, providers, actors in the energy sector, civil protection authorities and other societal functions should cooperate to establish information exchange mechanisms. These mechanisms should enable an efficient exchange of situational awareness information, forecasts of restoration times and other information that is essential for the efficient restoration after severe power cuts.

More details can be found in the body of this report. We look forward to working with the NRAs and providers to mitigate the impact of network and security incidents caused by power supply failures. We encourage the different actors to find ways to improve information-sharing about failures and outages, particularly between the energy sector and the electronic communications sector.

Table of Contents

1 Introduction

The reform of the EU legal framework for electronic communications which was adopted in 2009 and came into effect in May 2011, adds Article 13a to the Framework directive (2009/140/EC). Article 13a addresses security and integrity of public electronic communications networks and services. The legislation concerns National Regulatory Authorities (NRAs) and providers of public electronic communications networks and services (providers).

Among other things, Article 13a states that:

- Providers of public electronic communications networks and services should take measures to guarantee security and integrity of their networks
- Providers must report to competent national authorities about significant breaches of security or integrity that have had a significant impact on the operation of networks or services
- National Regulatory Authorities (NRAs) should notify ENISA and national authorities abroad when necessary, for example in case of incidents with cross-border impact
- Annually, NRAs should submit a summary report to ENISA and the European Commission (EC) about the incidents

ENISA started in 2010 an expert group with NRAs from all the Member States, to implement Article 13a and to address security and resilience of electronic communications in general.

Background

ENISA has, based on incident reports sent from NRAs to ENISA and the European Commission under Article 13a of the Framework Directive (2009/140/EC), analysed incidents on an aggregated level and published two reports, Annual Incident Reports 2011 and Annual Incident Reports 2012. In these reports, ENISA provides an analysis of the received incident reports, dealing with severe disruptions in public electronic communications networks or services in the EU. Examples of public electronic communications services are fixed and mobile telephony and fixed and mobile internet access. The diagram below shows the causes of the reported incidents in falling order:

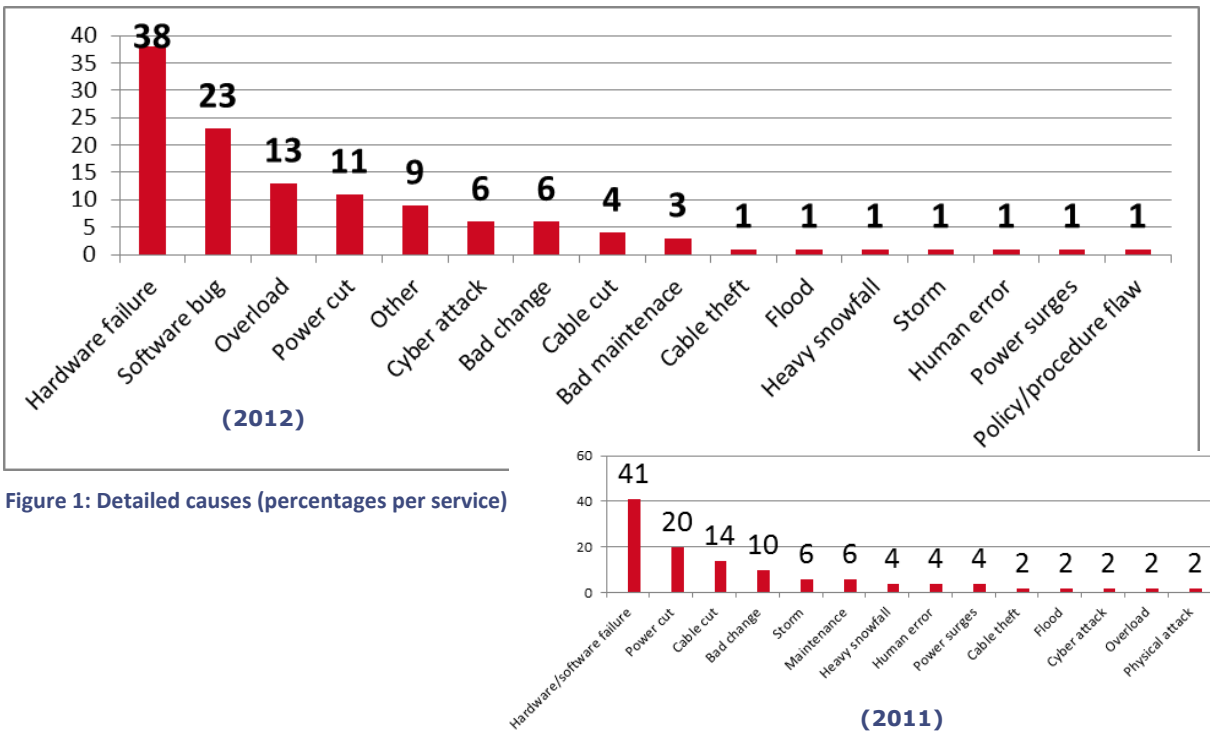

Figure 1: Detailed causes (percentages per service)

The diagram below shows the average impact per cause per reported incident from 2012. The impact is calculated as affected user connections times the duration of the incidents in hours.

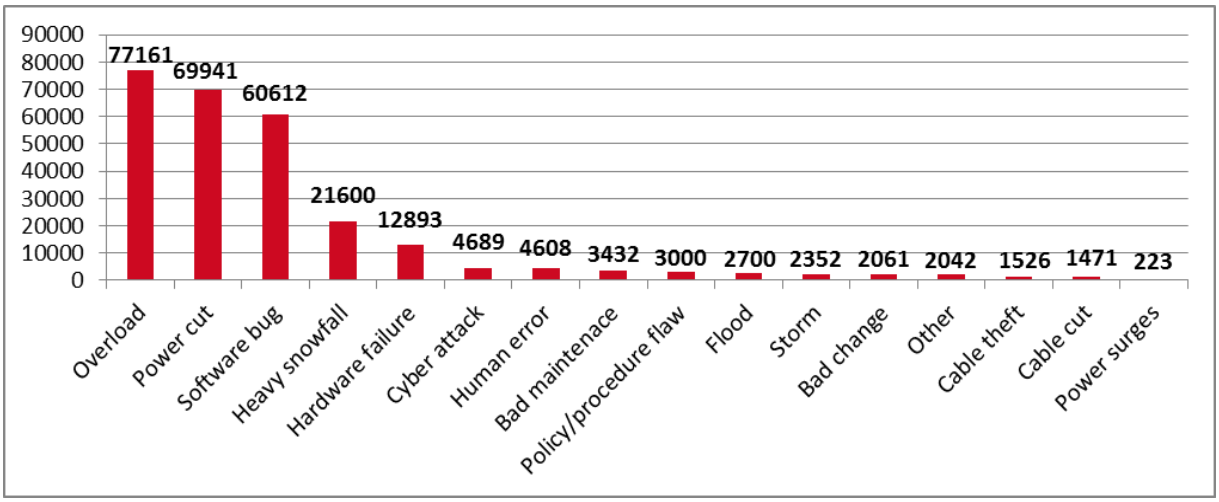

Figure 2: Average impact in user-hours (in thousands) from causes per incident.

From the analysis, ENISA has drawn the following conclusions, which have a direct or indirect link to power supply dependencies within the electronic communications sector:

- Power cuts were in 2011 identified as the second most common cause of incidents.
- During 2012, power cuts were the fourth most common cause.
- Power cuts caused major impact in 2012 in terms of user-hours lost per incident.
- During 2012, incidents caused by natural phenomena, mainly storms and heavy snowfall, were the two root causes that produced the longest incidents averaging to 36 hours.
- During 2011, natural phenomena gave rise to incidents that lasted 45 hours on average.
- Natural phenomena have a major impact on the power supply to providers within the electronic communications sector.

Goal

The goal of this report is to

- analyse the dependency of the electronic communications sector on power supply, and to
- issue recommendations on:
    - measures to reduce the frequency of network disruptions and outages caused by disruptions in the power supply sector, and
    - measures that improve the ability for the electronic communications sector to handle disruptions caused by power supply failures.

The analysis and findings cover three major perspectives:

- regulatory requirements in both the electronic communications and utilities domain,
- commercial drivers and
- public sector initiatives.

Target audience

The target for this report are mainly experts working at NRAs and ministries, who are dealing with security and resilience within the electronic communications sector, as well as experts working at

providers of public electronic communications networks and services, particularly experts involved with security, resilience, business continuity and disaster recovery. Also energy regulators, energy distributors, fuel providers, transport companies and civil protection authorities are addressed in this report.

Methodology

The primary sources of information are results from desk top research activities, a web survey among experts from NRAs across the EU[1], and interviews with experts from six providers and two NRAs. Specific information on national conditions is derived from desk top research activities and should not be attributed to statements made by individual NRAs or providers.

Structure of this document

The rest of this document is structured as follows. Sections 2 to 5 collect information covering four principal domains:

- the electronic communications policy domain that through legislation, procedures, state funding or public-private partnerships influences how well the sector can withstand and act to minimise the negative impact of power cuts;
- the electronic communications domain grouping together providers, that are directly responsible for the choice and implementation of resilience and recovery mechanisms and procedures, and their customers;
- the utility domain in which energy distributors, field technicians, fuel providers and transport companies act to provide vital services to assets and actors within the electronic communications sector;
- the utilities policy domain that groups together actors that through legislation, procedures or other means excerpt influence over the utility domain.

Section 6 collects proposals from providers and NRAs on possible measures to improve resilience against power cuts.

In section 2 to 6, 16 findings are extracted. Each finding, in the form of an observation of an existing condition that has, or can have a positive or negative impact on the electronic communications sector's ability to withstand and/or respond to power cuts, is presented in tabular format:

Short description of the finding
Further text that gives background information or added perspective to the finding.

Section 7 couples the findings made in sections 2 to 6 to a description of the activities that can be used to improve matters together with the parties that are or would be affected by establishing an improvement. The report concludes in section 8 with a set of recommendations to identified actors that individually and collectively can improve the electronic communications sector's ability to withstand and respond to power supply failures.

[1] The 23 NRAs who responded to the survey are listed in annex A to this document.

2 The electronic communications policy domain

Actors within the electronic communications domain are influenced by policies that bind them to uphold a certain level of reliability in the provision and maintenance of networks and services. At the EU level, article 13a states that providers of public electronic communications networks and services should take measures to guarantee security and integrity of their networks. This article is then complemented by national legislation that may provide further clarifications of this obligation and possibly also national additions. In addition, the policy domain can also influence the electronic communications sector through state investments and public-private partnerships.

This section couples legislation, state investments and public-private partnerships to how well electronic communications networks can withstand and recover from power cuts.

2.1 Legislation regarding resilience against power cuts

We have asked NRAs to provide information about national policies for electronic communications providers regarding resilience against power cuts, hereafter called power cut resilience[2]. The responses, shown in table 1 below, indicate that while a clear majority have implemented general resilience policies, less than half of these Member States have adopted policies that are directly linked to power cut resilience.

	Yes	No	Other[3]
Existence of general resilience policies	17[4]	5	1
Existence of power cut resilience policies	6	13	4

Table 1: Overview of the existence of general and specific power cut resilience policies among the 23 NRAs that have responded to ENISA's web survey.

One of the NRAs pointed to the existence of a general legal requirement obliging providers to supply a security concept to the NRA, which should include provisions taken to withstand or recover from power supply failures. The law does not specify detailed requirements regarding emergency power supply.

Another NRA pointed to the existence of a national electronic communications act that was recently modified to contain provisions that providers are obliged to provide electronic communications services with appropriate security for end users in times of peace, during crises and even in times of war. The NRA may decide that a service provider should take action to provide an appropriate level of security and preparedness. Detailed secondary legislation classifies sites into four classes

[2] The term power cut resilience measures is used as a term for measures to reduce the risk for disruptions and outages caused by disruptions in the power supply, and measures that improves the ability for the electronic communications sector to handle disruptions caused by power supply failures. The level of protection that these measures give is denoted as the electronic communications sector's resilience against power cuts.

[3] The term Other is here and throughout the report used to indicate the number of respondents that have either refrained from providing an answer or have answered Unknown. In cases where the number of respondents is less than the 23 NRAs that have provided some form of information to ENISA, the remaining respondents occupy this Other category. If the number of replies that are provided sum up to less than 23, the remaining answers were in the Other category.

[4] The number represents here and throughout the report the number of answers for this particular option in the web survey to the NRAs.

depending on the network equipment that is stored on the site. For class A and B sites, backup power must be sufficient for a minimum of three days. Two days of backup power is needed for class C sites and there are no requirements for class D sites. There must also be documented operating and maintenance routines which include routines for handling transport of fuel.

A third example is an EU Member State where a proposition for a specific decision on minimum requirements for power backup on mobile networks has been issued to all four mobile network providers in the Member State. The proposed decision states that the mobile networks should still provide services (both speech and data) at least six hours after a cut in primary power. The network should provide services with outdoor coverage in the areas where people live and work as well as all main roads in the Member State. The network owners would not receive any compensation for this resilience measure. The decision is meant to give the public some hours to communicate to prepare for a major and long-lasting loss of power.

Example 1) Resilience related legislation in Finland

The Finnish Communication Market Act contains general provisions that are related to resilience aspects but do not point to a set of resilience increasing measures that each operator has to take, instead pointing to clarifications in secondary legislation, in ordinances. At present, there are three principal ordinances that have a direct link to resilience:

- *Regulation 47 on information security management of telecommunications operators that principally concerns the need for information security control documentation, risk management practices and information security measures.*
- *Regulation 54 on resilience of communications networks and services designed to ensure the reliability of communications networks and services, protection of privacy and information security under normal circumstances, in fault situations in normal circumstances and in a state of emergency.*
- *Regulation 57 on the maintenance of communications networks and communications services, procedures and notifications in the event of faults and disturbances.*

Of these three regulations, Regulation 54 has the most direct link to power cut resilience. Within the regulation, components within electronic communications networks are assigned a priority based on a rating where the geographical area and the number of end users are the two principal factors that determine the rating. The regulation then assigns a set of resilience increasing measures based on the rating in a number of areas:

- *hardware redundancy, reserve routes and cooling systems,*
- *power supply including planning and monitoring aspects,*
- *physical protection measures.*

As one example, the regulation stipulates that GSM base stations must have a back-up time of the emergency power supply of at least three hours, a time that is extended to six hours due to remote location, difficult terrain conditions and expected weather conditions.

Few NRAs have implemented legislation related to power cut resilience

The motivation to include or not include specific power cut resilience measures can vary between Member States as the threat environment, in the form of likelihood for and characteristics of power cuts can be expected to vary. The survey does not provide specific information that can couple the existence of such policies to results from risk assessments. Many Member States consider power cut resilience to be a market rather than a regulatory issue (cf. section 2.3).

2.2 Risk assessments by NRAs

We asked if NRAs have a structured risk assessment process to analyse to which extent certain events and conditions can impact electronic communications networks and services. A large majority, as indicated in table 2, of the NRAs do not perform, compile or distribute risk assessments that cover power cut resilience aspects.

	Yes	No	Other
NRAs performing risk assessments including power cut resilience	5	17	1

Table 2: The total number of NRAs that perform risk assessment over the electronic communications sector and has a direct bearing on power cut resilience.

One NRA performing risk assessments regarding power cuts looks back on the previous 14 months and ranks power cuts just below hardware and software issues as the main cause for incidents.

One NRA subdivides power cuts into categories depending on the geographical area and duration of the power cut. Storms and other weather related incidents that cause power cuts are treated as part of one such category. Both regional power cuts of medium duration, with part of a day as an example, and weather related power cuts are considered as medium risks which is the third highest level. Several other threats are assigned to the same risk level and software induced errors are assigned to a higher risk level.

One NRA mentioned they have no access to statistics on power cuts.

Most NRAs do not perform risk assessments which include the risks for network and service outages due to power cuts

Risk assessments that include risks for network and service outages due to power cuts, where different types of power cuts and their potential technical and societal consequences are assessed, can be regarded as a platform from which various actions, for example the introduction of policies or state funding of resilience increasing measures, can be evaluated.

2.3 State funding and public-private partnerships

Most NRAs indicate that resilience related legislation is in place. Any form of measures that goes beyond this legally mandated level of resilience can be complemented by market driven investments, by state funding or through public-private partnerships[5]. Of the 23 NRAs that responded to the survey, only four reported that state funding or public-private partnerships had been used to introduce power cut resilience increasing measures. Examples of the measures that have been taken in this regard are principally state funded procurements of both stationary and transportable, fuel-powered generators.

Other NRAs motivate the general lack of state funding activities or public-private partnerships with statements that reflect a general lack of need or that market forces should be sufficient motivation for providers to make necessary investments.

[5] Market driven aspects related to resilience against power cuts is discussed in section 3.4.

Example 2) State funding – a national example

State funding, in the order of 2.5 million Euros annually over the last decade, has been used in one EU Member State to improve network resilience. Using this funding, providers have invested in transportable power generators, stationary power generators and also batteries for spare telecom exchanges for fixed networks.[6]

State funding and public-private partnerships that concern power cut resilience are rare

The use of state funding and public-private partnerships to address power cut resilience is the exception rather than the norm within the EU. There can be several reasons for this disparity, for example differences in policies, national market conditions and threat environment with respect to the frequency and duration of power cuts.

[6] Government funding has for example paid for some spare parts that service providers keep in stock, for example a fixed telephony exchange.

3 The electronic communications domain

This section focuses on the measures for resilience taken by providers. We give an overview of:

- current risk assessments and protection measures that have been implemented to increase power cut resilience,
- aspects that influence the restoration process after a power cut building on operational experiences and exercises,
- commercial aspects regarding power cut resilience including both the service provider and customer perspectives, and
- a characterisation of power cuts based on incident reports from 2011 and 2012.

The major findings in the section are carried over to (a) section 6.2, where possible actions to address some of the challenges within the electronic communications sector are analysed, and (b) to the recommendations that conclude the report in section 8.

3.1 Risk assessments by service providers

The interviews with providers indicate that risk assessment is a well-established practice. The following three examples give an overview of these practices based on interviews with selected providers.

Example 3) Risk assessment – a service provider perspective

The service provider performs regular risk management activities based on established routines. These activities are coordinated by a risk management steering committee that influences all aspects of the provider's operations. As part of risk management practices, identified risks are associated with actions. Power cuts have not been identified as an individual threat: most power cuts are said to have only minor impact on services and more significant power disruptions are often associated with natural disasters (for example storms and earthquakes). Risk assessments for such extraordinary events do not treat power cuts as an individual threat.

The provider considers several other threats as coupled to risk levels greater than what is considered for power cuts. Examples of such more severe threats are natural disasters, cyber-attacks, civil works and copper thefts.

Example 4) Risk assessments and business continuity planning – a service provider perspective

The provider has an active risk management process accompanied by business continuity and disaster recovery plans. As part of this risk management process, different types of threats are evaluated, which influence the provider's risk mitigation activities. The risk level that has been associated with power cuts is coupled to two factors: likelihood and consequence. Power cuts are here deemed to the one of the most common causes of service disruptions so the threat is associated with a high probability. The loss of client side connections is here regarded as the most common source of service disruptions.

However, consequences are often local (single site or limited number of customer sites) so that the overall risk that has been assigned is lower than for several other threats. Two examples of more severe threats are equipment failures and damage to cables (road works, diggers, etc.). The probability for power cuts varies within the nation. A majority of the provider's key assets are placed in a part that is rarely affected by power cuts compared to other, more exposed areas.

Example 5) Risk assessment – a service provider perspective

The provider has established procedures for performing risk assessments that have been in place for several years. These cover individual network components, sites and geographical areas. The risk assessments that are performed are tailored so that the variability of threats governs the interval between assessments. For example, in areas where there is generally more variability (over time) in power cuts, risk assessments regarding this aspect would be performed more regularly than in areas where there is more stability.

Power cuts is in many regions are not considered as a major threat, and is often associated with a risk level outside the top 5 risks. In some regions, principally regions undergoing changes and with more frequent power cuts, the risk level can conceivably motivate a top 5-ranking.

Example 6) Risk assessment – a service provider perspective

The service provider has an established Business Continuity Management program (BCM). Within this BCM program, there is a phase devoted to business impact analysis and risk assessment where assets and respective risks are identified and categorized, and associated with appropriate protection strategies/measures. The provider differentiates between different types of power cuts:

- *external power cuts or disturbances (from the external supplier) or*
- *internal power cuts that might be caused by maintenance activities, upgrades or similar.*

The risk level that is assigned to power cuts is different for the two types and also depends on the network component (access network or core network). In general, the risk is considered as low in the core network as protection mechanisms will give adequate protection for a wide range of external power cuts. The main issues are failures to UPS systems and -48V systems, fuel powered generators and other backup systems. Such issues are very important from an operational viewpoint as the consequences can be significant.

In access networks, the probability that a power cut leads to service disruptions is higher (more network elements with a lower protection level than core network elements) but the effects are also smaller.

Risks associated with power cuts is not always considered a significant threat by providers

Even though the interviews that have been performed as part of this study do not constitute a sufficiently broad selection of providers, it can be noted that power cuts are typically not considered as a major threat by the interviewed providers.

3.2 Protection measures taken by service providers

One important aspect regarding the sectors ability to withstand power cuts is the protection levels that have been implemented in order to overcome shorter or longer power cuts without undue effects on networks and services. In the web survey, NRAs were asked for information regarding the time before a power disruption would lead to service disruption within the electronic communications sector for different network types.[7] Table 3 summarizes the results and indicates

[7] Results for satellite networks and terrestrial mass communications networks have been omitted as the number of responses covering these network types is too low to draw any significant conclusions.

that fixed circuit-switched and broadband networks can be expected to exhibit a higher level of resilience than mobile networks.

Network type	< 1 hour	1-2 hours	2-4 hours	4-8 hours	> 8 hours
Fixed circuit switched	1	1	2	3	8
Fixed broadband networks	1	2	2	2	7
Mobile networks	2	3	3	3	3

Table 3: Estimation of the time before a power cut leads to service disruptions within the electronic communications sector based on responses from 23 NRAs.

As stated in section 3.1, vulnerabilities to power cuts tend to be higher in access networks compared to core components of the networks. As core platforms and backbone circuits serve both mobile and fixed networks and are usually located in the same core sites, they have similar levels of resilience and protection equipment against power cuts at least in the core parts of the networks.

Power cuts may affect more the access component of the mobile network due to the locations of mobile sites and the difficulty of transporting power supply to them.

Besides that, the mobile network nodes (e.g. base stations) are more exposed to natural phenomena and other outdoor risks that may impact power supply.

Another reason why fixed networks could have a greater level of resilience can be explained due to the type of network architecture that is typically more granular in mobile networks than in fixed networks, thus having more energy dependent components.

NRAs have provided additional clarification and information to this overview through comments.[8] One example of such additional information is that certain providers give priority to voice services over data services and may also prioritize coverage over capacity in mobile networks in order to prolong network life after a power cut. Another NRA remarks that first priority is always given to emergency calls, and second priority is given to restore services to customers with service level agreements. It is also pointed out that the network type, for example the use of 2G or 3G networks to support a specific service, and how power is supplied in a distributed fashion or from central offices also lead to variability. Some base stations may only have battery power that is sufficient for some ten minutes, but where key sites will have reserves that cover several hours.

Mobile networks tend to be more vulnerable to power cuts than fixed networks

While there is considerable variability in resilience against power cuts, between network types and within networks, mobile networks can be expected to offer less resilience than fixed network types. This is most likely due to natural consequence of the costs that would come from improving protection to the large number of network components including base stations that are used.

Providers can implement several different protection measures in order to reach the levels of resilience that are reported in table 3. One component is the deployment of fixed, fuel-powered

[8] Most comments are related to the expected variability within the national sector that was difficult to include as part of the responses to the web survey.

power generators which typically provide protection during a period that approaches or exceeds 24 hours. Based on the web survey, stationary power generators are principally used in core network segments more or less independent of the network type (i.e. fixed circuit-switched, broadband and mobile networks). Uninterruptible power supply with batteries is another protection measure that is commonly deployed either throughout a network or limited to core network segments. A third protection measure is the use of transportable power generators that can be moved to a specific site where there is an ongoing power disruption. In most cases, the deployment of these transportable power generators is limited with some exceptions. The use of solar cells and similar technologies for own-generated power supply is rare with some EU Member States reporting some limited deployment.

In the web survey, NRAs were asked to provide an overall rating of providers' abilities to cope with power cuts through existing physical protection measures in relationship to a reasonable balance between incurred costs and associated risk levels. Table 4 gives an overview of this assessment for both fixed and mobile networks.

Network type	Unsatisfactory	Poor	Adequate	Good
Fixed circuit switched	1	3	12	4
Fixed broadband networks	1	3	12	4
Mobile networks	2	2,5	16,5	—

Table 4: Overall qualitative assessment of protection measures, balancing costs against risk, per network type based on responses from 23 NRAs.

In general, NRAs consider current protection measures against power cuts as a reasonable balance between risk and cost

Even though power cuts are a significant cause of incidents within the electronic communications sector, most NRAs see current protection measures as an adequate balance between the risks associated with power cuts and the costs of establishing and maintaining protection measures. Only for mobile networks NRAs consider the current level of protection less than adequate.

The provider view of security measures is naturally broader than the high-level information that NRAs have at hand. The following examples show some of the considerations that providers make before establishing a set of resilience measures.

Example 7) Protection measures – a service provider perspective

Protection mechanisms are not applied to individual network elements per se but as part of an operational risk management methodology. In this methodology, assets are classified in one category based on technological, societal and commercial aspects. Protection measures are applied to assets in relationship to this classification rather than only identifying network element types (for example, base stations) and applying protection measures to them (for example, batteries).

In general, access networks have some form of protection through batteries. Core network elements are protected through fixed power generators. The provider also has fuel supplies stored in underground facilities that can be used during extraordinary circumstances for transportation and to drive fixed power generators.

The provider has introduced specialized vehicles that have shelter, fuel and communications infrastructure (Wi-Fi and mobile network infrastructure) that can be transported and quickly re-establish coverage in an area without any other infrastructure in place. The vehicles have been funded by the provider.

Example 8) Protection measures – a service provider perspective

The provider has four principal protection levels. On level one, assets are placed in facilities with mains connections as well as UPS solutions and fixed power generators with fuel tanks sufficient for days of sustained operation even in the absence of mains power. The second level contains the same protection mechanisms but with smaller fuel generator tanks. On the third level, there will only be a UPS resource. The fourth level consists of UPS protection but with quite limited protection time.

In general, the provider prefers to apply protection according to levels 1 and 2 in facilities where it can exert control (either through direct ownership of the facility or through commercial agreements with the provider of the data centre or co-location facility). Protection principles are also applied to be proportionate with site protection mechanisms: A customer that lacks power protection can make no use of any connectivity as computers and routers will cease to operate due to a power cut. The provider tries to advise customers to procure protection mechanisms where it is deemed to be advisable.

Normal redundancy principles will also affect the provider's ability to withstand power cuts. The provider does not have access to any transportable power generators.

Example 9) Protection measures – a service provider perspective

The deployment of fixed power backup solutions varies between network segments and geographical areas. A general rule is that base stations and local exchanges have some form of UPS system in place. In rural areas, where only a few customers would be affected by a service disruption due to a power cut, there may not be any UPS system in place at all. In more populated areas, protection may provide a minimum of 4-6 hours of continued operation.

One motivation for differentiating spare power supply is that many users would also be negatively impacted by the power cut as they are generally not equipped with own-generated power supplies. The situation is different for many enterprise customers.

Core network elements are typically protected by fixed power generators. For some sites, 2 or even 3 power generators can be used to create redundancy. The provider also has the option to activate the use of transportable power generators.

The provider does evaluate resilience against power cuts as an individual cost driver. A first step is to establish targets that determine the overall resilience levels that the provider aims to fulfil followed by the determination of the most cost effective way to achieve these goals.

Example 10) Protection measures – a service provider perspective

Core sites are protected with UPS and batteries (with autonomy between 1 and 2 hours for AC systems and up to 4 hours for DC systems) and also with stationary power generators (with own diesel tanks) that will supply the site with sufficient power to continue operation indefinitely as long as external refuelling can occur at regular intervals. External power generators can also be used for power supply. If an internal protection measure fails (for example, the fixed power generator), the provider will attach an external power generator to maintain the same level of resilience.

In access networks, individual base stations have batteries that give protection of at least two hours in the event of a power cut. Critical sites in transmission and aggregation network have battery protection around 8 hours. Assets in these non-core network segments allow them to be supplied by external power generators.

The provider has a contractor that will transport and deploy mobile power generators. The time between a decision to initiate a deployment and when a mobile power generator has started providing power to a network element is subject to geographical variations but is typically between 2 and 4 hours.

Batteries incur a high cost to procure and maintain but are deemed to be cost effective in the sense that they ensure that services can be maintained with zero interruption, even in the event of short duration power cuts or temporary disturbances from the external power supplier.

Example 11) Protection measures – a service provider perspective

Power is remotely supervised by an entity within the provider's organization which provides continuous every day, all day alarm monitoring and technical measurements from all power elements including electrical line connections, DC batteries, UPS systems, generators and cetera. Approximately 8 000 network sites are supervised by this entity and all power cut incidents are remotely managed in coordination with local field technicians, external contractors and power suppliers.

- *All network sites are protected with DC batteries and UPS systems.*
- *Medium network sites are also protected with fixed power generators*
- *Strategic network sites are also protected with redundant fixed power generators and electrical line connections.*
- *The provider has geographically deployed mobile power generators to attend to local power outages*
- *The provider has five Emergency Logistical Bases with large number of mobile power generators for attend severe and extensive power outages with regional or national implications.*

These protection mechanisms are a relevant cost driver. However, they are considered to be the best solution in order to guarantee the availability and quality of services to customers.

3.3 Restoration after power cuts – sector internal cooperation and lessons learned

The potential negative impact to society of power cuts causing service disruptions within the electronic communications sector is principally determined by two factors. The first factor is the security measures described in the previous section. The second factor is the ability of providers to act efficiently to restore services and networks. Such actions will typically involve contacts with a number of parties:

- an internal or external (to the provider) field service organization that is responsible for the transport and provisioning of transportable power generators or other temporary solutions,
- other providers where the sharing of information and resources can lower service restoration times,
- various actors, such as private customers, other providers and authorities, that require information from the providers about the service disruption, and

- the energy supplier for information regarding the power cut and forecast regarding restoration times.

Table 5 provides an overview of an assessment of providers' individual abilities and the providers' abilities to cooperate with other providers within the electronic communications sector to respond to power cuts and act efficiently to minimize service disruptions and restore services after power cuts.

Response and Cooperation	Unsatisfactory	Poor	Adequate	Good
Individual abilities	—	3,5	12,5	2
Intra-sector cooperation	—	8	9	1

Table 5: Overall qualitative evaluation of service provider's response and cooperation capabilities after power cuts

Cooperation within the electronic communications sector can be improved

The NRA's assessment point to a problem where intra-sector cooperation between providers are deemed to range from poor to adequate which is less than ideal as cooperation becomes increasingly important as the severity of the power cuts and challenges of the restoration effort grows.

Information sharing is a critical enabler to the successful cooperation between providers but also to inform authorities and the general public regarding the impact and forecast for restorations after a service disruption has started. Table 6 shows that information exchange between providers, such as web-based solutions or contact paths to NOCs, which enable providers to share information regarding impact and forecast for restorations are to be considered as limited to a few actors and or with limited functionality. Information exchange to the authorities and the general public is better or slightly better.

Information exchange	Limited to few actors and with limited func.	Limited to a few actors or with lim. func.	Widespread but with limited func.	Widespread and with desired func.
Between providers	3	10	1	2
To authorities	4	3	7	2
To the general public	1	7	3	5

Table 6: Overall qualitative evaluation of information exchange mechanisms

Information exchange mechanisms between providers can be improved

A majority of NRAs state that information sharing mechanisms between providers are either limited to a few actors, or with limited functionality. The situation is better for the information that goes to authorities and to the general public.

3.4 Power cut resilience – commercial aspects

Improvements to resilience measures for power cuts do not have to come through legislation. One alternative is commercial drivers rewarding a service provider, who places a higher emphasis on power cut resilience measures compared to its competitors, with increased market share and profitability. Another alternative is that the overall level of resilience is the value rather than its individual components, where power cut resilience would be one of these components. It is also likely that different market segments make these evaluations differently.

NRAs were asked to assess how different customer segments evaluate resilience against power cuts as a differentiating factor in their choice of service provider. The same question was also asked taking the provider perspective, with combined results shown in table 7.

Customer segment (Service provider view)	Little individual value	Some individual value	Some collective value with other measures	Significant value with other measures
Ordinary customers	13 (10)	3 (2)	1 (5)	— (—)
Private companies	5 (4)	2 (5)	9 (6)	1 (2)
Authorities	5 (3)	1 (4)	5 (7)	6 (3)

Table 7: Overall qualitative assessment on how different customer segments place value on power cut resilience based on two different perspectives: the customer perspective and the service provider perspective (in parentheses).

A further commercial aspect is if private companies, authorities and other organisations that require a higher degree of resilience against power cuts, can and will act to seek assurances from their respective providers of this increased resilience level. This would typically mean that providers deploy a mix of fixed power generators and UPS systems with batteries in all network segments that serve this specific customer. Whilst this may be realistic in some circumstances, in particular where the need is coupled to a single or a few geographical locations, it is perhaps not realistic that this type of agreement would lead to a higher general, network wide level of resilience.

Example 12) Commercial aspects – a service provider perspective

According to the provider, resilience against power cuts is not regarded as a differentiating factor, compared to factors such as geographical coverage. The provider has large commercial contracts with authorities and companies and will not be evaluated for resilience against power cuts but for resilience as a whole. However, the provider will not divest responsibility regarding a service disruption caused by third party power supply failure and place the blame on an actor within the energy sector.

This means all in all that overall resilience is the key according to the provider. Power cuts can be regarded as one threat that the provider needs to be aware of and consider as part of network and service continuity planning. But as stated before, according to the interviewed provider, power cuts are not considered to be the most important issue to consider in this regard.

Example 13) Commercial aspects – a service provider perspective

According to the provider, reliability of electronic communications services as a whole is an important factor rather than resilience to power cuts. One reason for this statement is that power supply in the country in question is relatively reliable and there is only one major power distributor without effective alternatives, although there may be several power retailers. Other

providers also depend on the same power supplier and are likely to have implemented similar protection mechanisms. Power supply is understood as a utility and not as a differentiating factor, therefore resilience against power cuts would not be a point of concern if SLAs were properly defined in terms of continuity and quality of supply.

Special customers, like customers in the corporate segment and public administration, that seek additional information regarding reliability never ask specific questions regarding power supply issues but may ask for information regarding the resilience of telecommunications equipment and transmission lines (circuits).

Market forces are not deemed to be a significant contributor to the direct improvement to power cut resilience

NRAs make the assessment that ordinary customers place little value on the extent to which providers are resilient to power cuts. In the same manner, private companies or authorities are unlikely to place value on power cut resilience measures specifically but are more likely to place some value on resilience measures as a whole. Depending on the distribution between the revenue bases for private customers and other customer segments, an increased market demand that specifically addresses power cut resilience and leads to increased power cut resilience levels may be regarded as an unlikely development.

3.5 Power cut resilience – 2011 and 2012 incident reports

As part of this study, ENISA has analysed 12 incidents from 2011 and 10 incidents from 2012 that were reported to ENISA and the European Commission and that involved power supply failure causing the incident, either as initial cause or subsequent cause.

In 2011 the four longest lasting incidents were caused by natural phenomena in the form of three storms and one instance of heavy snowfall. In several cases, the power cut on its own did not determine the duration of the service outage as five of the incidents had hardware or software failures as secondary cause. The two incidents with the largest number of affected users were both due to power surges (rather than power cuts) combined with hardware and software failures.

In 2012 the two longest lasting incidents were caused by natural phenomena, one storm and one instance of heavy snowfall. Power cut was not the only cause. In one case there was a combined power cut and a failure in the provider's emergency power supply which led to an outage that lasted 7 hours and affected more than one million subscribers.

We distinguish two types of events:

- Power cuts where existing protection measures work as intended but do not give the necessary protection resulting in service disruptions
- Power cuts where existing protection measures do not work as intended adding to the length of the service disruption[9]

Applying this classification to the incidents reports from 2011 and 2012 shows that around half of all reported incidents that were caused by power cuts can be attributed to this second category.

[9] The addition to the length of a service disruption is made in reference to a situation where the protection measures would have worked as intended by their design and implementation.

	2011	2012
Security measures worked as intended	A total of six events affecting from a few tens of thousands subscribers up to a million subscribers	A total of four events affecting from more than 10 000 up to a few hundred thousand subscribers ranging from a number of hours to several days
Security measures failed	Six incidents affecting hundreds of thousands of subscribers up to and over a million subscribers.	Six incidents affecting a few thousand subscribers up to several hundred thousand subscribers during a few hours up to and over 24 hours

Table 8: Categorization of incident reports based on incident reports from 2011 and 2012 depending on whether or not existing protection measures worked as intended.

This leads to the following finding.

In half of the reported incidents involving power cuts, security measures did not work as intended, which contributed to the impact on networks and services.

The incident reports show that incidents where existing protection measures did not work as intended were as frequent and severe as incidents where protection measures did work as intended.

4 The utilities domain

In the previous section, the focus was on the electronic communications sector describing current protection measures as well as sector internal information exchange mechanisms without including information that describes more specific details on the interactions between the energy and electronic communications sectors. In this section we look at how resilience of power supply is addressed in the energy sector and cooperation mechanisms between the two sectors.

4.1 Continuity of supply – national statistics and variability

Power supply is a critical dependency for the electronic communications sector. This dependency is shared between EU nations. However, there may be national and even regional differences between the continuity of power supply. Continuity of supply concerns interruptions in power supply and focuses on events where the voltage at the supply terminals of a network user drops to zero or nearly (practically) zero. Continuity of supply can be described by various quality dimensions, for example the number of interruptions per year.

A large majority of EU Member States monitor continuity of supply[10] even though Member States may apply different definitions of an interruption[11]. This monitoring enables regulatory authorities to follow how the continuity of supply evolves over time, and is not confined to specific incidents where a specific number of users are affected over a more extended period of time as follows from the incident reporting practices introduced in the electronic communications sector from Article 13a in the Framework directive.

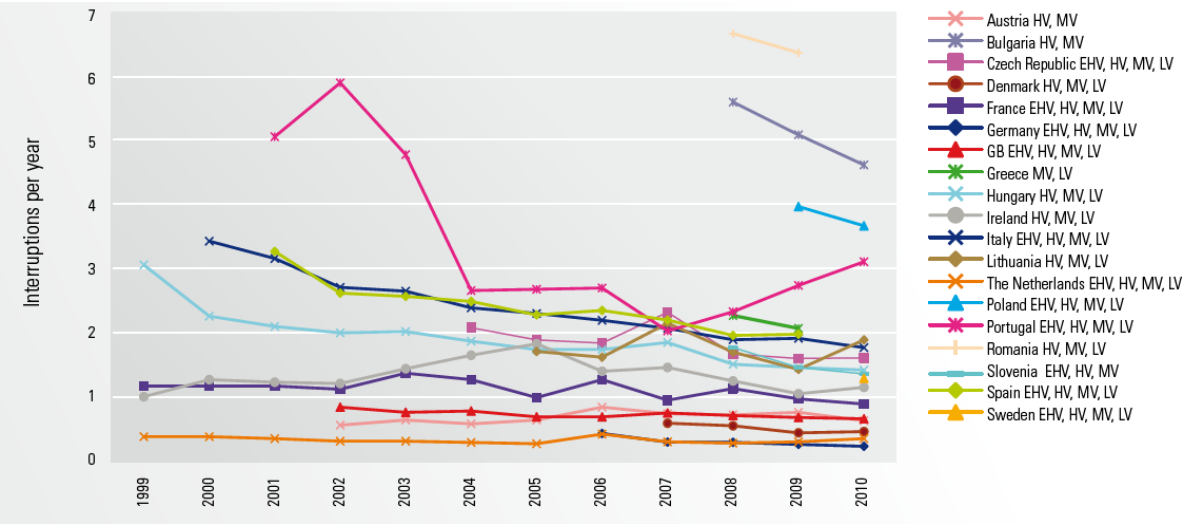

Figure 3: The number of unplanned, long interruptions per year excluding exceptional events. The voltage level (EHV, HV, MV and LV) relates to where the incidents occur.

Figure 3 indicates that the number of long interruptions per year varies both between Member States and over time. Most Member States show stability or improvements in this regard. Storms and heavy snowfall will typically affect energy networks that utilize a large number of overhead

[10] All 26 countries that have contributed to the CEER benchmarking report.

[11] For example, most countries define interruptions longer than three minutes as a long interruption but there are exceptions. The Netherlands do not distinguish between transient, short or long interruptions. All interruptions longer than at least 5 seconds are monitored.

circuits compared to networks that mostly use underground low voltage cables. Figure 4 shows that there are considerable variations between EU Member States in this regard.

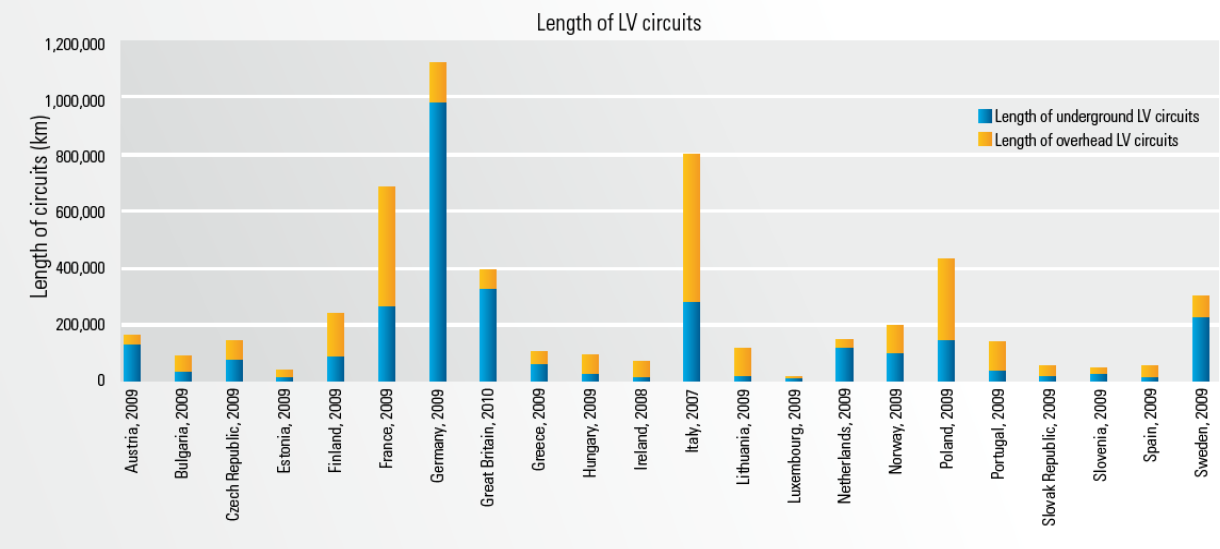

Figure 4: The length of low voltage circuits differentiating between underground and overhead circuits

Example 14) Continuity of supply in Sweden

The Swedish Energy Markets Inspectorate (Ei) is responsible for the supervision of electricity grid operators to ensure that they fulfil their obligations in accordance with the Swedish Electricity Act. One such aspect is the supply of electricity of good quality, where power failures are used as one indicator to monitor this quality. Figure 5 below shows that the frequency of power failures varies between years and also depending on the type of electricity network (rural, municipal and mixed networks).

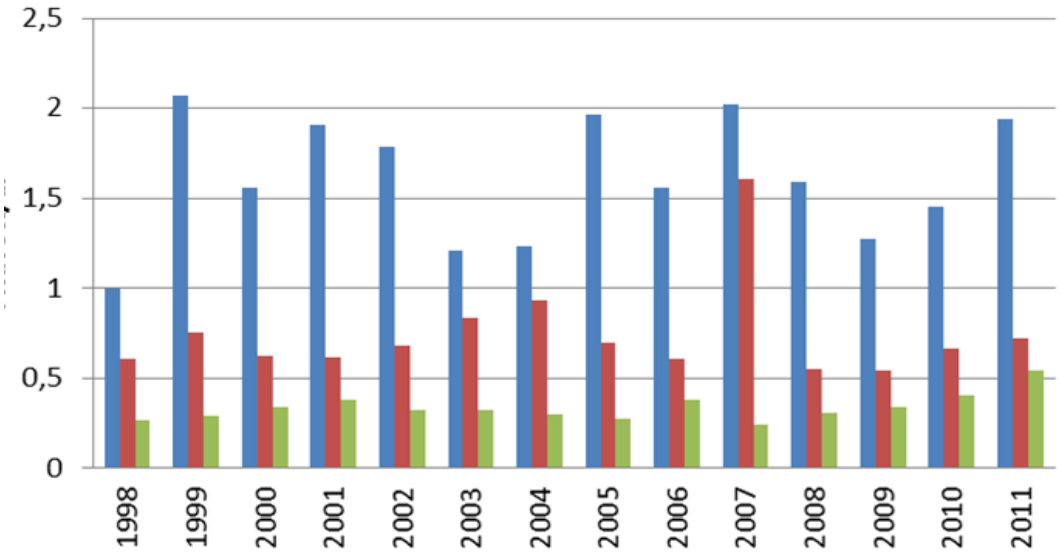

Figure 5: The average number of power failures per customer and year in local networks in Sweden with a subdivision between rural (blue), municipal (green) and mixed (red) networks

Similar statistics also point to variations between power grid operators leading to the conclusions that the continuity of power supply can be expected to exhibit regional and also local variability. The same trend can be expected in other EU Member States.

Variations in the continuity of power supply are to be expected

Indicators that characterize power cuts can be expected to exhibit both national, regional and to some extent also local variation. This means that resilience measures within the electronic communications sector could exhibit the same type of variability while still preserving the same level of protection. A level of resilience that is appropriate in one Member State, as a suitable balance between cost and risk, may not be appropriate for another Member State.

4.2 Specialized protection measures

Providers in the electronic communications sector can complement spare power systems, in the form of batteries, fixed and transportable power generators, with other protection measures. One such protection measure is to feed a high-value site via two independent energy distribution paths with as much diversity as possible.[12] Another possible option is to seek commercial agreements where the energy network owner agrees to provide increased reliability as regulated by service level agreements.

Table 9 indicates that such additional resilience increasing measures are not rare but also not common practice.

	Yes	No	Other
Specialized protection measures	9	8	6
Commercial agreements	5	9	9

Table 9: NRA assessment of specialized protection measures and their application within the electronic communications sector

Example 15) Specialized protection measures – a service provider perspective

Contracts with suppliers within the energy sector contain texts which are related to availability and business continuity based on ISO-standards. These texts do not describe specific service levels but oblige the energy supplier to implement practices to monitor and manage availability as well as develop business continuity plans.

SLAs are deemed to be less suitable to provide guarantees in case of natural disasters and similar events of an extraordinary nature as few providers will accept such stipulations without force majeure clauses.

[12] Low-voltage energy distribution networks are often monopolies within a given geographic area, which means that the level of resilience that can be achieved may be limited.

4.3 Restoration after power cuts – cross-sector cooperation and lessons learned

The previous sections, section 4.1 and 4.2, have described the variability regarding power cuts that can be expected and specialized protection measures that principally govern how often service disruptions can occur. A broader view is provided if cross-sector cooperation aspects are also included. Such cooperation is of particular importance under more severe power cuts where information exchange and coordination is essential.[13]

The number of power cuts that have required or could have benefited from coordinated restoration efforts involving actors from the electronic communications sector and the energy sector varies between EU member states. Some EU member states point to two to three such events where others report a lower number or even that no such event has occurred during the last ten years. One NRA points to three major storms during the period in which between 48 000 and 115 000 subscribers of fixed telephony were affected. In a similar manner, mobile networks were also affected over regional areas that over time decreased to local areas. Another reported instance was a massive explosion which destroyed a large part of the power producing capability in the member state.

There is significant commonality between the lessons learned which can collectively be summarized as follows:

- there is a general need for improved cooperation and information exchange between the electronic communications and energy sectors,
- information exchange regarding prioritization can bring significant benefits during the aftermath of an energy shortage situation,
- each situation is different during major emergencies and the useful pre-planning that can be done is limited, and
- in case of more significant outages, information about power outages from electric distribution companies should be quickly distributed to providers and be of high quality. E-mail or other means of communication may be useful here.

An overall assessment of providers' abilities to cooperate with actors within the energy sector to respond to power cuts and act efficiently to minimize service disruptions and restore services after power cuts, indicate a variability ranging from poor to adequate showing that there is room for improvement regarding cross-sector cooperation.

Cooperation	Unsatisfactory	Poor	Adequate	Good
Cross-sector cooperation	1	7,5	6,5	2

Table 10: Overall qualitative NRA evaluation of provider's cooperation capabilities with the energy sector after power cuts

In the same manner, information exchange mechanisms that can be used to distribute information regarding ongoing service disruptions typically are not widespread and with desired functionality.

[13] It should be noted that there is a mutual dependency as the energy sector will, to a large extent, rely on electronic communications both during normal operation and during restoration efforts.

Information exchange	Limited to few actors and with limited func.	Limited to a few actors or with lim. func.	Widespread but with limited func.	Widespread and with desired func.
Energy sector	4	6	4	1

Table 11: Overall qualitative NRA evaluation of intra sector and cross-sector information exchange mechanisms

Exercises can be regarded as a complimentary tool to resilience increasing measures, and can be expected to improve cooperation. Overall, the number of exercises that have been held varies between EU Member States, from none to five or six and even more. Examples of lessons learned from Member States is that whilst providers are used to handling power outage, there is still some room for improvements when it comes to further strengthening cooperation and information exchange.

Example 16) Cooperation, exercises and operational experiences – a service provider perspective

Power cuts is the single most common cause of service disruptions according to the provider, and the provider is indeed used to dealing with the consequences of power cuts. This experience is for example used in contacts with clients so that customer service representatives ask the customer if they have power on-site and if it can be confirmed that relevant equipment has power.

The provider can also contact the energy company but this contact does not give any form of priority compared to ordinary home owners. It is assumed that functions that have a more central function to society have more direct contact paths to energy suppliers.

Example 17) Cooperation, exercises and operational experiences – a service provider perspective

A working group (WG) has been established under the Ministry for the Interior. This WG collects actors from the electronic communications, energy and transportation sectors that fulfil some vital function to society and may need to collaborate during the restoration effort after an extraordinary event such as an earthquake or heavy storm. The WG collects between 20 and 25 actors. Personal relationships have been formed between key people in the electronic communications and energy sectors as part of the WG. These relationships are of critical importance to facilitate efficient cooperation during a crisis.

It has been found that the cooperation that is established through the WG, associated training and exercises, together form a good basis for larger restoration efforts, as no plan can account for the multitude of variations that can exist between different events. For example, two recent severe natural events occurred in regions that had been assigned to a low risk with respect to the specific threat. Exercises are held at least annually on national level, collecting actors from several sectors. On a regional level, the same type of exercises is held at least twice annually.

Example 18) Cooperation, exercises and operational experiences – a service provider perspective

Several elements of cooperation are lacking. Information sharing is one component here where providers within the electronic communications sector would like to have information regarding planned maintenance and power cuts in advance and they would also like to have notifications regarding ongoing power cuts or disturbances. Another aspect here is that providers are treated no different than a domestic customer, who is referred to general customer support, when reporting or requesting information regarding an ongoing power cut from the power company.

Example 19) Cooperation, exercises and operational experiences – a service provider perspective

The provider states that about two to three power cuts annually during the last ten years have required or could have benefited from coordinated restoration efforts involving actors from the

electronic communications sector and the energy sectors to minimize service disruption after power outages with national or regional impact. The provider also points to a daily need of coordinated restoration efforts with the owners of the energy networks in order to minimize service disruption after power outages with local impact.

Lessons learned are:

- *There is a need to know, in real time, actions and estimations with respect to restoration in energy networks in order to prioritize and mobilize our human and material protection resources for communications network sites.*
- *Energy network owners must prioritize repair of power supply to important communications network sites. This prioritization should be coordinated with communications service providers.*

Cross-sector cooperation and information exchange can be improved

Efficient service restoration requires cooperation and information exchange between the energy sector and the electronic communications sector, and improvements in this domain can decrease the negative impact of power cuts in general and more severe power cuts in particular. Exercises can be a useful tool to practice and maintain an established collaboration.

5 The utilities policy domain

Actors within the utilities domain are subject to legislation which will affect power cut restoration efforts. The primary such influence is through prioritization schemes where assets within the communications sector are given preferential treatment, and through regulation that affect the quality of power supply as is described in this section.

5.1 Prioritization schemes

The service restoration time (in the electronic communications sector) after a power cut will vary depending on a number of factors, ranging from meteorological conditions to access to transportable power generators that can be used to continue network operation. There are basically three principal policy areas that will influence the severity of service disruptions, in the case of more severe power cuts, in order to deploy transportable power generators and maintain their operation together with that of fixed power generators:[14]

- a preference scheme where power supply would be restored to assets in the electronic communications sector with priority,
- preference schemes that would give providers priority access to transportation resources, and
- preference schemes that would give providers priority access to fuel.

The parties that would participate in preference schemes, outside the providers and power grid operators, would vary depending on national conditions.

As indicated in table 12, only a few NRAs report the existence of such preference schemes.

	Yes	No	Other
Priority restoration	2	7	14
Priority transport	—	9	14
Priority to fuel	2	8	13

Table 12: Existence of preference schemes that could decrease the negative impact of more severe power cuts

Example 20) A national example of a priority restoration scheme

One NRA in an interview points to a preference scheme that builds on national regulations within the energy sector requiring energy distribution companies to have a list of priority customers and also the reason behind the prioritization. Power would here be restored to customers respecting this priority order even though the order would not always be preserved, as power companies resolve problems in the high-voltage network first and then low-voltage network to which assets in the electronic communications sector is typically connected. Some base stations and other telecommunications installations are on this national list. In the low-voltage network there are many prioritized customers like hospitals that will be higher up on the list.

[14] These three areas are complemented by general regulation, as described in section 5.2. A further policy domain is priority schemes where, during a general energy shortage situation, assets within the electronic communications sector would not be disconnected while other customers that do not fulfil an equally important function to society would be. This situation may not be caused by a power cut and is not treated here even though the electronic communications sector would certainly benefit from this type of policy.

The NRA does not have enough working experience or statistics to state that the priority restoration schemes have led to a quicker restoration of electronic communications services.

Example 21) Prioritization – a service provider perspective

Prioritization is one of the issues that can be said to be within the realm of the WG (cf. example 17). During an extraordinary event, members within the WG could interact to determine suitable actions to minimize the effects of the event on society. The prioritization scheme could therefore be regarded as an informal arrangement rather than a set of pre-established rules. The prioritization scheme has been used operationally.

Example 22) Prioritization – a service provider perspective

The provider has no special contractual agreement with the power company that contains SLA-based requirements. The provider has tried to establish a priority communication channel with the power company and also to provide a list of critical sites/assets of the access network but, considering the few past experience, the provider does not know if this mechanism is effective when needed in critical situations.

There seem to be few national examples of priority schemes within the utilities domain

Of those intyerviewed, only two member states point to the existence of national preference schemes even though such schemes can be expected to lead to some improvements in certain, more severe situations.

5.2 Regulation of quality of power supply within the European energy sector

European energy regulators work to promote well-functioning and competitive EU energy markets so that consumers get fair prices, the widest choice of supplier and the best quality of supply possible[15]. To achieve the third goal, ensuring that consumers are given the best quality of supply possible, regulatory oversight and control within the European energy sector is principally exercised in three areas:

- the continuity of supply which relates to the number and duration of power cuts,
- voltage quality that relates to the power surges or dips that affect electronic equipment, and
- commercial quality that concerns the timeliness and efficiency of the customer service provided by electricity companies.

The three areas influence the electronic communications sector's ability to withstand and react to power cuts in different ways. The first area, continuity of supply, is principally linked to protection measures in the form of UPS systems, fixed and transportable power generators that are applied to network elements in order to avoid or suitably minimize service interruptions after power cuts. In the same manner, network elements need to be equipped with protection measures against power surges and dips. The third area will primarily influence, indirectly rather than directly, the electronic communications sector's ability to react to various forms of power cuts and act efficiently to maintain and restore services to consumers.

A large number of energy regulators within Europe have adopted regulatory instruments to maintain or improve continuity of supply, as a balance to other regulation that aims to increase market

[15] CEER 5th Benchmarking Report, page iii.

efficiency[16]. Quality incentive schemes, through reward or penalty schemes or incentives, have evolved within parts of the European energy sector as a means to optimise continuity of supply levels. The use of rewards, penalties and a combination of the two varies between Member States and is also applied differently to different energy network levels[17]. The main intention of these schemes is to keep quality levels at an efficient socio-economic level.

Example 23) Energy sector regulation in Great Britain

Incentive rates are used in Great Britain to reward or penalise distribution companies based on their performance regarding continuity standards.18 Companies must reach targets for customer interruptions and customer minutes lost which are set during the price control process, with exceptional events excluded. Each distribution company performance determines the resulting penalty or reward through a complex formula with a lag of two years.

Great Britain also employs a compensation scheme that distinguishes between domestic and business customers. Domestic customers are eligible for a 54£ compensation after the first 18 hours of interruptions. Business customers are eligible to twice that amount for the same duration.

Example 24) Energy sector regulation in Sweden

Energy distribution companies may also be subject to more direct legal obligations as is the case in Sweden. The Electricity Act (1997:857) stipulates that network concessionaires shall ensure that outages in the transmission of electrical power to an electricity consumer never exceed twenty-four hours. One exception to this rule is when a concessionaire can show that the outage results from:

- *an impediment outside the concessionaire's control,*
- *which the concessionaire could not reasonably be expected to have anticipated, and the*
- *consequences of which the concessionaire could neither have reasonably avoided or overcome.*

Storms and similar events would typically not be regarded as an exception to this obligation.

The energy sector seems to have progressed further in their assessment of obligations and socio-economic effects

The energy sector has worked for a number of years to establish different forms of incentive schemes that include limits to the number and duration of power cuts as well as other quality dimensions. The evaluation of socio-economic effects has been an integral part of this process.

[16] Examples of market efficiency regulation can be price or revenue-cap mechanisms.
[17] Ibid, page 41.
[18] Ibid, page 43.

6 Assessing the need for improvements and proposals

In this section we take stock of the need for resilience improvements and of proposals from providers and NRAs for measures that can be taken to reach these improvements. The material in this section and in section 7 (evaluation of possible actions), together form the input for recommendations presented in section 8.

6.1 Assessing the need for improvements to power cut resilience

The need for improved power cut resilience within the electronic communications sector can be evaluated from two perspectives:

- a societal perspective in which the effects of service disruptions caused by power cuts are evaluated in dimensions that can include the possible loss of lives and economic losses,
- a commercial (service provider) perspective in which the costs of introducing resilience increasing measures are evaluated against the possible monetary gains, and

As we shall see, the two perspectives can lead to different results. Taking the first perspective, as shown in table 13, shows that most NRAs consider it to be important to increase power cut resilience compared to other risk mitigation activities.

	Unimportant	Not very important	Important	Critical
Need for improvement	—	3	15	1

Table 13: Qualitative evaluation of the importance of increasing power cut resilience within the electronic communications sector from an NRA perspective

NRAs also pointed to a number of resilience aspects that are deemed to be more important, for example:

- decreasing the number of software induced errors as service disruptions caused by software issues are fairly frequent and can also give rise to national disruptions for several hours,
- implementation of priority schemes, increasing redundancy and improvements to business continuity planning,
- measures that prevent cyber-attacks and introduce disaster recovery procedures, and
- protection measures against overloads.

One NRA also identified human errors, hardware and software failures, damage through excavations and digging activities without ranking.

One NRA stated that there probably is not much that is more important than power supply aspects for electronic communications resilience but notes that it does not necessarily mean that this resilience area needs improvements. The NRA was here of the opinion that providers react and cope well so that the current level of resilience may have an optimal balance between resilience and cost already. If this optimal level has not yet been established, the NRA stated that it may be more efficient to improve the resilience of the power supply itself, rather than of the electronic communications sector, noting that the dependency between the two sectors is two-way.

A majority of NRAs consider it to be important to increase resilience against power cuts compared to other risk mitigation activities.

Even though most NRAs see current protection measures as an adequate balance between the risks associated with power cuts and the costs of establishing and maintaining protection measures, NRAs still consider it to be important to increase power cut resilience compared to other risk mitigation activities.

Whilst the NRA view points at the importance of increasing power cut resilience, the provider perspective indicates a lower evaluation as the following examples show.

Example 25) Increasing power cut resilience – a service provider perspective

The provider considers several other threats to have risk levels greater than what is considered for power cuts. Examples of such more severe threats are natural disasters with direct impact on networks, cyber-attacks, civil works and copper thefts.

It is always possible to improve the capability to withstand and respond to power cuts. At present, the provider has no immediate plans to make such improvements. However, the provider is acutely aware of the importance of electronic communications services to society as a whole.

Example 26) Increasing power cut resilience – a service provider perspective

The provider places higher emphasis on equipment resilience than resilience against power cuts and sees some, limited room for improvement with respect to their own operation's resilience against power cuts. Customer improvements are a far more important issue in this regard. One other improvement would be information provided by the energy sector regarding power disruptions which would make the provider more efficient even though resilience would not be increased.

Example 27) Increasing power cut resilience – a service provider perspective

A number of flooding incidents have occurred in the last 5 to 10 years and seem to be increasing. Physical risks would be regarded as a more significant set of threats that require more attention for the future. Logical threats however, for example if someone would break the encryption on SIM-cards, could lead to more significant commercial consequences.

An important aspect is to ensure that the power sector is as resilient as the electronic communications sector. One possible improvement is the better understanding of recovery procedures and resilience aspects between actors in the two sectors.

Example 28) Increasing power cut resilience – a service provider perspective

Current internal protection measures, including the possibility to deploy mobile power generators by an external contractor, are at a level where the provider considers itself to be well prepared to deal with external power cuts. One remark must be done given that there are only 5 to 6 big contractors that supply mobile generators in the country, which could lead to a capacity shortage in case there is a major and prolonged power failure that impact a significant part of the access network sites.

The provider regards its current protection measures for dealing with power cuts as appropriate when compared to other risks, given that it has N+1 protection in core sites and battery supply in access networks. There is currently no plan to further improve investment levels regarding

protection equipment to withstand power cuts, although there is still room for improvements regarding resilience architecture and procedural enhancements, at the internal level in the provider's and at the external level with the power suppliers.

6.2 Proposals to improve resilience against power supply failures

6.2.1 Proposals from providers

Interviewed providers have brought forward a number of proposals that could be used to improve power supply resilience:

- The establishment of an EU level round table forum where providers from different sectors participate to discuss protection mechanisms and experiences from events so that lessons learned and procedures are shared as much as possible.
- The establishment of some form of commercial incentives for providers to ensure that they consider protection mechanisms that go beyond those which are applied for commercial purposes. One possible alternative in this regard is tax relief.
- The establishment of priority and ease of access to the sites by the civil protection authorities for the emergency teams of the providers and the power suppliers, as well as giving priority in the provisioning of diesel reserves for power generators.
- The establishment of increased protection of network sites by the police authorities to ensure continuity of operations, both for access network sites (given the increased occurrence of batteries thefts) and for core sites (given the possible public disorders due to social and political instability).
- The establishment of a priority customer relationship between providers and power companies.
- Improved information exchange mechanisms that allow for continuous sharing regarding ongoing power disturbances and predictions of restoration times.
- Improved early warnings and information sharing from civil protection authorities regarding storms and fires to enable the operators to prepare for and efficiently work to minimize service disruptions.

Providers see several measures that could improve resilience against power supply failures

As part of the interviews, a number of providers have pointed to actions that could improve the resilience against power cuts. Even though the number of providers that have been interviewed is limited, the finding leads to a recommendation to NRAs to collect and evaluate different proposals before any action is taken.

6.2.2 Proposals from NRAs

In the web survey and interviews also NRAs pointed to a number of possible actions and observations that can be taken to reach improvements:

- an increased use of fixed power generators,
- well prepared crisis management in each critical infrastructure company,

- improving customer understanding of the limitations of the current communications services related to power cut resilience to allow market pressure to increase commercial incentives to improve, starting with government and big business customers,
- forcing providers to establish connections with multiple suppliers of electricity in a number of points in order to have an alternative, and
- incentives for closer collaboration between providers and the energy sector.

7 Possible actions and evaluation of actions to address identified findings

This study started from the knowledge that a significant number of the major incidents that have been reported to ENISA during 2011 and 2012 can, directly or indirectly, be attributed to power cuts. The material in sections 2 to 5 has described aspects of power supply dependencies from four different perspectives. In chapter 6, providers and NRAs have given their opinion on the need for improvements regarding resilience against power cuts, and they have given proposals to increase resilience. The discussions in section 2 to 6 have led to a total of 16 findings. These findings are in this section collected and attributed with possible actions without taking a stand, as described in table 14 below.

The material in this section and in section 6 form input to the recommendations presented in section 8.

7.1 Possible actions to address identified findings

The table below describes possible actions to address the identified findings from the previous sections.

Domain	Finding	Possible actions
Electronic communications policy domain	Few NRAs have implemented legislation related to power cut resilience	There are four principal options to decrease the negative impact of service disruptions due to power cuts: a) improve the quality of supply in the energy sector (reducing the threat) b) increasing resilience in the electronic communications sector through legislation c) increasing resilience in the electronic communications through state funding or private-public partnerships d) trust that market forces will lead to an increase in power cut resilience over time
	Most NRAs do not perform risk assessments which include the risks for network and service outages due to power cuts	Each NRA may not be obliged to perform risk assessments as part of their remit. The responsibility to perform such risk assessments may also be performed by some other government agency. ENISA's view is that NRAs should consider national risk assessments as standard practice in order to evaluate different threats and consider appropriate actions. Power cuts is one threat category that is important to consider in this regard. No other option is therefore associated with this finding.

	State funding and public-private partnerships that concern power cut resilience are rare	The practice of using state funding and public-private partnerships is one possible activity that can contribute to increasing power cut resilience.
	A majority of NRAs consider it to be important to increase resilience against power cuts compared to other risk mitigation activities	The finding is not attributed to an individual action but can be considered as important motivations for the recommendations that are given in chapter 7.
Electronic communications domain	Risks associated with power cuts is not always considered a significant threat by providers	Providers typically perform risk assessment based on a commercial perspective. The interviews indicate that most providers can be expected to have established a number of protection measures that are considered to be sufficient from commercial and current legislative perspectives. No specific action is attributed to this finding.
	Mobile networks tend to be more vulnerable to power cuts than fixed networks	This fact should be included in risk assessments where society's increased reliance on mobile services should be included.
	In general, NRAs consider current protection measures against power cuts as a reasonable balance between risk and cost	The conclusion that ENISA draws here is that it is by no means certain that additional resilience increasing measures should be mandated. Depending on national circumstances priorities between different types of existing security measures for resilience could be defined, cf. section 6.1. In the case of any new action taken, for example the introduction of specific obligations, it should be preceded by a cost-benefit analysis that includes other possible options.
	Cooperation within the electronic communications sector can be improved	The primary actions that can be taken is: a) the introduction of tools and routines for information exchange, and b) strategies and procedures that can be used to increase cooperation with exercises as one example.
	Information exchange mechanisms between providers can be improved	
	Market forces are not deemed to be a significant contributor to the direct improvement to power cut resilience	This finding is primarily an indication that improvements are to be sought elsewhere and is therefore not attributed to a specific action. The cost-benefit analysis should include this option as one alternative along with state funding or private-public partnerships.
	In half of the reported incidents	The finding is treated as part of a

	involving power cuts, security measures did not work as intended, which contributed to the impact on networks and services.	recommendation to NRAs to follow up on the power supply related incidents and take lessons learned from them to continuously work for improvements of the security measures.
	Providers see several measures that could improve resilience against power supply failures	The finding is treated as part of a recommendation to NRAs to liaise with providers and other NRAs to collect and evaluate different options to increase power cut resilience as an initial measure.
Utilities domain	Variations in the continuity of power supply are to be expected	Risk assessments and cost-benefit analyses need to include a relevant threat description that includes information regarding the characteristics and frequency of power cuts. The finding is not on its own attributed to an action.
	Cross-sector cooperation and information exchange can be improved	The possible actions are captured above adding the energy sector to the reach of tools for information exchange and improved cooperation.
Utilities policy domain	There seems to be few national examples of priority schemes within the utilities domain	As the power cut threat varies between EU member states, the most appropriate action is to make a national evaluation of the need for and components in a priority scheme.
	The energy sector seems to have progressed in their assessment of obligations and socio-economic effects	Some policies and measures in the energy sector may be interesting to learn from in the electronic communications sector, for instance incentive schemes.

Table 14: Mapping between findings and possible actions

7.2 Evaluation of actions

The findings, proposals and possible actions lead to the identification of a number of general actions to consider:

- Introducing or strengthening legislation in the electronic communications sector placing stricter requirements on providers
- Introducing or strengthening legislation in the energy sector placing stricter requirements on the frequency and duration of power cuts
- Increasing commercial incentives for providers in the electronic communications sector
- Improved routines and technical systems for collaboration and information exchange between the two sectors
- Increased number of cross-sector exercises geared towards restoration after significant power cuts
- Introduction of priority restoration schemes within the utilities domain

- Increase the number of transportable power generators that are available for use in the electronic communications sectors.

NRAs were asked to evaluate these actions in two dimensions. The first dimension describes the improvements that can come from the implementation of the action and is shown in table 15.

Action	No real improvement	Limited improvement	Substantial improvement	Very significant improvement
eComms legislation	3	10	6	1
Energy sector legislation	2	11	5	1
Commercial incentives	3	10	5	2
Tools for information exchange	–	9	10	1
Exercises	–	9	7	4
Priority restoration	3	10	5	2
Transportable power generators	–	12	6	1

Table 15: NRA evaluation of example actions that can be undertaken to improve resilience against power cuts

The second dimension that was evaluated by NRAs was how difficult the action would be to implement. This evaluation is shown in table 16.

Action	May not be possible	Very difficult	Difficult	Normal
eComms legislation	2	3	7	7
Energy sector legislation	–	3	11	4
Commercial incentives	3	2	9	5
Tools for information exchange	–	1	2	17
Exercises	–	2	5	13
Priority restoration	1	5	5	7
Transportable power generators	–	7	9	3

Table 16: NRA evaluation of the difficulty of implementing actions to increase power cut resilience

The tables indicate that no specific actions, with the possible exception of tools for information exchange and exercises, stand out as actions that can be expected to bring substantially greater benefits than any other measure. This may be a consequence of the national and regional variations to the threat environment that was reported earlier.

8 Recommendations

This study attempts to address two principal questions:

- Which measures should be implemented to reduce the frequency of disruptions and outages in the electronic communications sector caused by power supply failures?, and
- Which measures should be introduced to improve the electronic communications sector's ability to handle disruptions and outages caused by power supply failures?

To meet these two questions in our recommendations, we propose a subdivision of power cuts within one principal, the duration of the power cuts. The duration we divide in three categories, power cuts of shorter, medium and longer duration.

Power cuts of *shorter duration* range from sub-second voltage fluctuations to failures in the order of a few hours.

Power cuts of *medium duration* are failures that last from a few hours up to about 10 hours.

Power cuts of *longer duration* we categorise as extended failures lasting longer than about 10 hours. Longer power cuts are typically related to natural causes such as severe storms, heavy snowfall, floods, earthquakes et cetera, and where it is no longer reasonable to expect providers to introduce resilience measures that are sufficient to avoid network and service disruptions or outages. However, from a society perspective, the need for measures to reduce the impact from such causes is extremely high. Here, efficient joint mitigation activities within and between sectors are the principal goals.

The recommendations are mainly aimed at NRAs and providers, and some of the recommendations also address the energy sector and civil protection authorities.

Recommendation 1: NRAs should analyse the frequency and impact of network and service outages caused by power cuts.

One finding of this study is that NRAs typically do not perform risk assessments that include power cuts. We believe such risk assessments are important tools to evaluate if extra measures are needed to improve resilience of networks and services in the face of power cuts. Important input for such risk assessments would be incident reports about past disruptions and outages caused by power cuts, and statistics about the number of users affected and the duration. This characterization could then enable NRAs, aided by information from providers, to relate these statistics to electronic communications effects through dimensions such as:

- the expected number of service disruptions within the electronic communications sector within a given time frame,
- the length of these service disruptions in time,
- the impact in terms of number of users and services affected, and
- the severity of these incidents, distinguishing between degradations and full outages.

The NRA would then attempt to determine a risk level based on power cut statistics and the societal impact of the risks related to power cuts.

Recommendation 2: NRAs should liaise with providers, energy regulators and other NRAs to collect good practices that could be used to increase resilience against power cuts. These good practices should be considered as part of a cost-benefit analysis (recommendation 3).

The providers that have been interviewed as part of this study have brought forward a number of suggestions that could be used to increase resilience against power supply failures. Before any actions are taken by NRAs they should meet with providers, energy regulators, actors in the utility domain and other NRAs to collect proposals for measures to improve power cut resilience. This collection serves as important input to a cost-benefit analysis, see recommendation 3.

Recommendation 3: NRAs should perform, in cooperation with energy regulators and civil protection authorities, a cost-benefit analysis, where societal costs and benefits are evaluated, to determine what is reasonable to expect from different actors regarding power cut resilience measures.

Within a risk management framework, a risk assessment would be followed by an analysis of what measures can and should be expected from providers and energy distributors in order to reduce the impact of power cuts. This risk treatment should include a cost-benefit analysis to compare risk mitigation activities within both the electronic communications and the energy sector and should be done in cooperation with energy regulators and civil protection authorities.[19]

As noted in section 4.1, national and regional variations can be expected and may lead to different results within and between EU Member States. One outcome can be that it is not relevant to formulate specific regulatory requirements if power cuts are rare and resulting service disruptions in the electronic communications sector are rare and do not have significant negative impact. Another possible outcome here could be that incentive schemes (including market demand for increased resilience), state funding, and private-public partnerships individually or collectively could lead to more efficient increases to resilience.

Recommendation 4: Providers should regularly perform checks of existing protection measures, such as checks of UPS systems and batteries, and running facilities with fixed and transportable power generators at full load, to avoid and mitigate the impact of network and service outages from shorter and medium duration power cuts.

Recommendation 5: NRAs should in their follow up of major network and service outages caused by power cuts ensure that affected providers, based on lessons learned, systematically develop their protection measures to avoid and mitigate the impact of network and service outages from shorter and medium duration power cuts.

No matter how resilient providers build their networks and develop their security measures to avoid network and service outages, there will still be incidents. In those cases it is important to learn from the incidents to address similar types of incidents in the future. When NRAS follow up major outages caused by power cuts to see that the providers continuously develop their security measures, NRAs should consult the cost-benefit analysis (recommendation 3) in order to have a balanced approach on expectations of enhanced security measures. For instance, expecting backup diesel generators at core network elements carrying traffic for a large number of users could be considered relevant, whereas backup diesel generators for “critical” mobile base stations may require increased physical protection of the sites to prevent the generators from being stolen, which will come at a cost.

[19] Based on national conditions, it may for example be more efficient to increase the quality of service within the energy sector rather than imposing obligations on service providers within the electronic communications sector to introduce costly protection measures, or to use state funding combined with public-private partnerships to increase power cut resilience.

Recommendation 6: NRAs should act to establish a strategy to promote cooperation and mutual aid agreements on joint service restoration after severe power cuts which can include cross-sector exercises.

The goal of a strategy to promote cooperation and joint service restoration including exercises is to establish and maintain strong every day working relationships, within the sector and across sector boundaries, that will carry over to more challenging circumstances.

Recommendation 7: NRAs should consider a priority scheme that would give preferential treatment within the electronic communications sector and decrease service restoration times under exceptional circumstances.

Recommendation 8: NRAs, providers, actors in the energy sector and other societal functions should cooperate to establish information exchange mechanisms. These mechanisms should enable an efficient exchange of situational awareness information, forecasts of restoration times and other information that is essential for the efficient restoration after severe power cuts.

Power failures of longer duration are often connected with increased stress on society and the supply of electronic communications services is then even more important. The need for priority schemes and information exchange within the sector as well as with the energy sector, weather stations, the civil protection authorities and other societal functions can be considered as crucial in order to reduce the impact from service disruptions and outages.

References

Related ENISA papers

- Annual Incident Reports 2011, Analysis of the Article 13a incident reports of 2011, October 2012
  http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports
- Annual Incident Reports 2012, Analysis of Article 13a annual incident reports, August 2013 :
  http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports
- The ENISA guidelines on the implementation of Article 13a:
  https://resilience.enisa.europa.eu/article-13

Legislation

- Article 13a of the Framework directive of the EU legislative framework on electronic communications:
  http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0037:0069:EN:PDF
- Regulation on Information Management of Telecommunications Operations, FICORA 47 C/2009, Unofficial translation.
- Regulation on communications networks and services, FICORA 54 A/2012 M.
- Regulation on the Maintenance of Communications Networks and Communications Services, Procedures and Notifications in the Event of Faults and Disturbances, FICORA 57 A/2012 M, Unofficial translation.
- The Swedish Electricity Act (1997:857)

Other information sources

- 5th CEER Benchmarking Report on the Quality of Electricity Supply 2011, Council of European Energy Regulators (CEER)
  http://www.energy-community.org/pls/portal/docs/1522177.PDF
- Power failure statistics 2011, Local and regional networks (in Swedish), Swedish Energy Markets Inspectorate
- Surveys and interviews with National Regulatory Authorities described in annex A.
- Interviews with six providers across Europe.

Annex A: Web survey respondents

The following NRAs have provided information to the web survey:

- Austrian Regulatory Authority for Broadcasting and Telecommunication (RTR), Austria
- Belgian Institute for Postal services and Telecommunication, Belgium
- Commission for Communication Regulation, Ireland
- Communication Regulatory Authority of the Republic of Lithuania, Lithuania
- Croatian Post and Electronic Communication Agency (HAKOM), Croatia
- Czech Telecommunication Office, The Czech Republic
- Estonian Technical Surveillance Authority, Estonia
- Federal Network Agency, Germany
- Finnish Communication Regulatory Authority (FICORA), Finland
- Greek National Regulatory Authority (EETT)
- Hellenic Authority for Communication Security and Privacy, Greece
- Hellenic Authority for Communication Security and Privacy (ADAE), Greece
- Institut Luxembourgeois de Régulation, Luxembourg
- Malta Communication Authority, Malta
- Ministry of Economic Affairs & Radiocommunication Agency, The Netherlands
- Ministry of Economic Development (ISCTI), Italy
- Ministry of Transport and Communication, Latvia
- Ofcom, United Kingdom
- Office of Electronic Communication, Poland
- Office of Electronic Communication & Postal Regulation, Cyprus
- Post and Electronic Communication Agency of the Republic of Slovenia, Slovenia
- Radiocommunication Agency, the Netherlands
- Swedish Post and Telecom Authority, Sweden
- Telecommunication Regulatory Authority of the Slovak Republic, Slovakia

Annex B: Web questionnaire questions

The following questions were asked to the NRAs as part of the web questionnaire.

Question 1: Are there currently policies, in the form of legislation, ordinances or other form of mandatory directive, in place which contain requirements on operators within the electronic communications sector directed towards resilience aspects?

Question 2: Are there currently policies in place which are directly linked to operators' ability to withstand or recover from power cuts?

Question 3a: Do you as an NRA perform, compile or distribute risk assessments that include evaluations of the likelihood and consequences of power cuts in relationship to other threats?

Question 3b: What risk level has been associated to power cuts and how does this risk level compare to that of other threats?

Question 4a: Can you provide or estimate the time before a power disruption will lead to service disruptions within the electronics communications sector? Two or more alternatives can be chosen to reflect differences within the sector.

Answers are sought for fixed (circuit-switched) networks, fixed broadband networks, mobile networks, satellite networks and terrestrial mass communication networks

Question 4b: From these estimates (question 4a), how would you describe possible variations in the resilience of individual services that are carried over these networks?

Question 5a: To which extent do service providers deploy stationary, fuel-powered (diesel or petrol) power generators in different fixed and mobile networks?

Question 5b: To which extent do service providers deploy Uninterruptible power supply with batteries?

Question 5c: To which extent do service providers have access to mobile power generators that can be transported to maintain network operation?

Question 5d: To which extent do service providers make use of other forms of own-generated power supplies, such as solar powered power generators or fuel cells?

Answers are sought to the same network types as in question 4a.

Question 6a: Are you aware of any service provider that has taken steps to ensure increased reliability through specialized protection measures such as connection from different public main power networks?

Question 6b: Are you aware of any service provider that has taken steps to ensure increased reliability from actors within the energy sectors through commercial agreements with associated service level agreements?

Question 7: Overall, how would you rate the service providers' ability to cope with power cuts through existing physical protection measures to what can be regarded as a reasonable balance between incurred costs and risk levels?

Answers are sought to the same network types as in question 4a.

Question 8a: Has state funding or public-private partnerships nationally been used to improve the electronic communications sector's resilience to power cuts?

Question 8b: If yes, what such improvements have been made?

Question 8c: If no, why have no such improvements been introduced?

Question 9a: How do you overall rate the actors' individual abilities (discounting collaborations with other actors within and outside the sector) to respond to power cuts and act efficiently to minimize service disruptions and restore services after power cuts?

Question 9b: How do you overall rate the actors' ability to cooperate with other service providers within the electronic communications sector to respond to power cuts and act efficiently to minimize service disruptions and restore services after power cuts?

Question 9c: How do you overall rate the actors' ability to cooperate with actors within the energy sector (network owners) to respond to power cuts and act efficiently to minimize service disruptions and restore services after power cuts?

Question 10a: During service failures, are there information exchange mechanisms between providers, such as web-based solutions or contact paths to NOCs, which enable providers to share information regarding impact and forecast for restorations?

Question 10b: Are there established information exchange mechanisms where service providers within the electronics communications sector can provide information to authorities regarding the impact and forecast for restoration of communication services?

Question 10c: Are there established information exchange mechanisms where service providers within the electronics communications sector can provide information to the general public regarding the impact and forecast for restoration of communication services?

Question 10d: Are there information exchange mechanisms, e.g. web-based solutions or contact paths, between the eComms and energy sector, that enables eComms providers to get info regarding impact and forecast for the restoration of power to affected areas?

Question 11a: In the last 10 years, how many power cuts have required or could have benefited from coordinated restoration efforts involving actors from the electronic communications sector and the energy sector?

Question 11b: What have been the key lessons learned in those events?

Question 12a: In the last 10 years, how many exercises have been held involving actors from the electronic communications sector and the energy sector?

Question 12b: What have been the key lessons learned in those exercises?

Question 13a: To what extent do you think that customers within different customer segments consider resilience against power cuts as a differentiating factor in their choice of service provider?

Question 13b: To what extent do you think that operators consider resilience against power cuts as a differentiating factor for different customer categories?

Assessments were sought for ordinary customers, private companies and authorities.

Question 14: Do you have any priority restoration scheme where assets within the electronic communications sector are given preferential treatment under some specific conditions?

a. Priority in restoration within the energy sector

b. Prioritization from the transport sector, for example transportation of fuel to power generators

c. Priority access to fuel

Question 15a: How would you overall rate the importance of increasing the electronic communications sectors' ability to withstand and respond to power cuts against other risk mitigation activities?

Question 15b: What other resilience aspects would you place a higher value on and why?

Question 16: How would you rate the following measures with respect to their possible contribution to improve the electronic communications sectors' ability to withstand and respond to power cuts?

Options are:

a. Introducing or strengthening legislation in the electronic communications sector placing stricter requirements on service providers

b. Introducing or strengthening legislation in the energy sector placing stricter requirements on the frequency and duration of power cuts

c. Increasing commercial incentives for service providers in the electronic communications sector

d. Improved routines and technical systems for collaboration and information exchange between the two sectors

e. Increased number of cross-sector exercises geared towards restoration after significant power cuts

f. Introduction of priority restoration schemes within the utilities domain

g. Increase the number of mobile power generators that are available for use in the electronic communications sectors

Question 17: How would you rate the following measures to increase the electronic communications sectors' ability to withstand and respond to power cuts with respect to how difficult they would be to implement?

Options are as in question 17.

Question 18: What other options do you see that could bring improvements to the electronic communications sectors' ability to withstand and respond to power cuts?

ENISA
European Union Agency for Network and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office
1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

ISBN 978-92-9204-081-9
doi: 10.2824/29209
TP-04-13-140-EN-N

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu