Assessment of the concept of telecoms resilience in the context of an operational telecoms network supporting protection and control of the electricity distribution and transmission networks

A. Pérez Pastor *Universidad Pontificia de Comillas, MSc in Smart Grids studen*t

Resumen - Resilience, is a concept that has increased its importance and it is key to the telecommunication network strategy. However, this concept is still evolving and there is not a homogeneous definition of the term. We will talk here how to reach a resilient system. We will discuss some of the main concepts that are usually mistaken with resilience and its definition too. To correctly assess the resilience, this paper goes through different selected dimensions to have an understanding of the challenges and key notions that will lead to the elaboration of the metrics. Finally, the tool conception is discussed such as its limitations.

Index Terms - Resilience, Assessment, Cyber-physical system, Power, Services, Security, Vulnerability, Dimensions' analysis, framework

NOMENCLATURE

SPEN – Scottish Power Energy Networks, T&D – Transmission and Distribution, SPT – Scottish Power Transmission, SPD – Scottish Power Distribution, SPM – Scottish Power Manweb, CPS – Cyber-physical System, OFGEM – Office of Gas and Electricity Market, CPNI - Centre for the Protection of National Infrastructure, NIC - National Infrastructure Commission, E3C - Energy Emergencies Executive Committee , CIA - Confidentiality, Integrity and Availability, SDG – Sustainable Development Goal

I. INTRODUCTION

Nowadays, we are undeniably dependents of electricity and telecommunications systems. If we were blind to see it before, the COVID-19 pandemic has opened even more our eyes to this reality. This dependence highlights the need for reliable infrastructures, and that the operation and transmission of the electricity system is critical and must be able to guarantee the electricity supply. One of the main takeaways of the pandemic is the essential need for secure, efficient and resilient systems, especially when faced with an unforeseeable emergency situation that entails unpredictability and risks, among other factors. In order to preserve our way of life, the electricity system and telecommunication infrastructures are found to be at the heart of our society and economy.

New challenges have arisen that will be a difficulty when looking to enhance resilience, and we believe that telecommunication networks should be designed in such a way that they van cover services despite failures. This is the reason for many entities, such as international organisations, governmental bodies, regulatory bodies, academic/research institutions, industry players, and many other stakeholders, to put the focus on improving resilience.

To address this, the industry is looking to manage consumption more efficiently, improve systems and infrastructures, optimise operation, etc. However, some challenges have to be solved first. In this case, the challenge on which we will be focused on is the assessment of the resilience of telecommunication infrastructures, in the context of an operational network that supports the distribution and transmission of electricity.

Resilience is the key to cope with these situations, and both industry and research centres have sought to define this term without achieving a single definition. Therefore, this project will examine these definitions to find the one that best suits the needs of this study, in order to establish a framework and essential characteristics of a resilient grid.

A. Motivation and objectives

The main motivation of this project is to highlight the need for more efficient and resilient telecommunication networks, because of their essential character in order to preserve not only our way of life, but to maintain the current socio-economic system.

This motivation finds its way when analysing the situation of telecommunications networks, specifically those that help protection and control in the context of distribution and transmission networks, which contributes to modernizing electrical systems and facilitating access to reliable, safe and affordable energy. The progressive change and evolution of networks has revealed the importance of their resilience.

It has become clear that increasing the resilience of our networks is essential, yet what exactly does resilience mean? Does this imply increasing the redundancy of the equipment, or the size of the network, how does making it more intelligent influence resilience…? Taking these reflections further, we can come to wonder if an improvement in resilience would reduce operating costs, or if it would considerably reduce losses in such a way that the service offered responds more effectively and with a higher quality, etc.

We are facing though a real heterogeneity in terms of an existing common definition of the term resilience, which increases its implementation in networks difficulty. For that reason, we will redefine this term of resilience and this will allow us to evaluate it, based on specific aspects in order to build a framework and an assessment of the current situation of the networks.

Taking all these motivations into account, we could define the objectives as follows:

- Theorise the interdependence between the power and communication networks;
- Consider an historical overview of all the different definitions of resilience;
- Develop a homogeneous method to define the term;
- Establish a common definition of resilience in the power system;
- Analyse other terms relationship towards the resilience;
- Develop a regulatory analysis of the existing procedures and guidelines;
- Identify new challenges resilience will have to face;
- Establish a framework to assess the resilience level and how to possibly face the problems;
- Examine the different dimensions that affect to a greater or lesser extent the resilience of networks;
- Create a tool that will evaluate/assess the current resilience of the network.

To sum up, this project aims to provide a global vision of the state of the art on the telecom networks resilience, focusing on the aspects that may help to improve it. It would have some limitations as its purpose is not to establish regulations, standards or guidelines, but to assess the technology and strategies currently used.

B. Methodology

This project is mainly a research work, this study is carried out with the aim of giving visibility to resilience and seeking answers to the challenges it poses.

We will be using different resources that will allow us to study the term resilience in depth in our context, such as articles from specialised journals, reports from leading institutions in this field, legislative texts from national and international organisations, etc. This literature review will lead us to build a deep analysis of the selected dimensions that influence the resilience.

This study will enable us to build a tool to assess the resilience of the network, based on the theoretical background. By using the tool, we can reach some conclusions on the current situation of the network resilience; a tool that also has its limitations and possible further improvements to benefit an increased efficiency in the future.

The remainder of the paper is organized as follows. Section II. describes related theoretical background that would analyse the state of the art concerning the resilience term and will set a framework to work with. Section III introduces the technology and knowledge study, classified into the three selected dimension: Power, Services and Security. This would lead to the construction of the tool, Section IV, where we discuss the tool implementation, from the metrics selection to the objectives and limitations encountered. Section V concludes the paper.

II. Theoretical background

A. Interdependencies

Being able to serve our most basic needs, support the infrastructure development and help improving the productivity and the economy, we are in need of reliable and resilient energy and telecommunication systems, as well as water, transport, and many other services that do not have a direct impact on our analysis. In other words, resilience of those two systems is key to deliver reliable services. Both the telecoms network in support of the electric system and the electric system itself are infrastructures that work on its own, with some relationship between them. We will now see which type of connection and how this is important to take into consideration.

Considering both systems need each other and there is a bidirectional relationship, we confirm their interdependent correlation. It can be classified under three categories: physical, cyber and geographic.

In simple terms, the telecom network will need the power to function (physical), the power system needs the telecommunications services of control, protection etc. to correctly work (cyber), and different equipment will have a physical link in proximity to one another, which can be the reason of the damage propagation (geographical).

This interdependencies will help us keep an eye on the strategies and/or frameworks, in order to have a resilient-oriented perspective that takes into account the whole picture.

B. Resilience

"*Resilience*" is a word widely spread nowadays, as the main purpose of this project is to assess the resilience of the network, we will try to answer to what does resilience really means.

We will analyse below different *resilience* definitions from several fields, to reach an homogeneous definition for our purpose, and in the process be able to understand the challenges it faces, the main characteristics of a resilient network and other terms surrounding the subject.

1) New challenges

To have a resilient network is a challenge itself, but there are major challenges that arise and directly influence the resilience.

a) Climate change

The facts are undeniable, as the IPCC highlights, we can consider alarming the current climate situation. The last Assessment Report was really clear about the generalized, rapid and intensified worldwide effect [1], despite the exceptional efforts. We are all aware of some metrics that make even more tangible the situation: level of CO2 in the air (416ppm), temperature increase (1ºC), etc. These quantitative indicators, applied to our context, tell us that there is a direct correlation between the severity of the climate change and the increase in number and intensity of the unpredictable natural disasters. We can say that the last decades worst outages and blackouts have mostly to do with natural disasters.

All this evidence may help us reach a couple of main conclusions:

- The biggest outages happen to have increased in frequency over the last years, due to the amplified intensity and frequency of the extreme weather events, such as floods, storms, extreme heat days, longer dry seasons, hurricanes, tropical cyclones, etc.;
- Blackouts and outages do not only have power cut and recovery issues, in a logistical point of view, they can cause disruptions, chaos and even economic losses.

b) Demographic growth

Two increases are aligned, the demographic growth and the electrification. Would this be sustainable?

In general terms, the population size will increase 2 billion by 2030 which equals a 30% more [2]; while we want to achieve the 100% of access to energy and increase the electrification of more sectors.

We can ask ourselves if we will be able to achieve sustainability (and the SDGs targets) while both population and electrification are growing. To respond to this challenge it will be important to adapt our networks: more reliable, secure and resilient.

c) COVID-19

The pandemic has been a challenge for us all in almost every aspect, health, economy, etc. And it has of course also an impact on the energy sector.

We can say there have been some short-term consequences (power profile demands changes, electricity market evolution, variation of the generation mix, etc. [3]), and that the long-term consequences are yet to come. However, the pandemic has implied a change of our habits and the different strategies to face it might be a possible path to reach net-zero carbon emissions. Some experts say that "the electricity sector experienced a foretaste of the future, with higher renewable energy penetration and concerns for security of supply" [3] This will enlighten policy makers, regulators, etc.

It has been a challenge to cope with the lack of redundancy, to operate in such unexpected scenarios, in other words, we had to face a crisis which leads to the conclusion of the need of a resilient power system.

2) Definition

We have already mentioned the lack of a homogeneous definition of the term Resilience, which will help us have a common view on what are the big challenges we face to reach resilience. To dive into some different approaches without giving an extensive list, we will find below some key definitions, classified by the field where they come from (governmental, research, technical community, etc.):

TABLE 1: RESILIENCE DEFINITION ANALYSIS

Definition	Source	Classification
Resilience of the material to be the amount of energy the material can absorb and still return to its original state. If we are talking about stressing the material and having it return to its original state.	Education Institute	Physics
The capacity of social–ecological systems to adapt or transform in response to unfamiliar, unexpected and extreme shocks.	Ecologist Stephen Carpenter and economics Nobel laureate Kenneth Arrow	Ecology and economics
Resilience in terms of robustness and recovery characteristics of the power system during and after disasters.	National Association of Regulatory Commissioners (NARUC)	Governmental
Resilience is the capacity of an energy system to tolerate disturbance and to continue to deliver affordable energy services to consumers. A resilient energy system can speedily	Energy 2050: Making the Transition to a Secure Low-Carbon Energy System	Governmental

recover from shocks and can provide alternative means of satisfying energy service needs in the event of changed external circumstances		
The ability of a power system to tolerate disturbances and still provide an affordable service to all consumers	United Kingdom Research Centre (UKERC)	Research
Power grid resilience is defined as the ability to degrade gradually under increasing system stress and then to recover to its pre-disturbance secure state. Also, the degree to which the system can cascade provides a measure of system resilience	Power Systems Engineering Research Centre (PSERC)	Research
Anticipate, absorb, and rapidly recover from low-frequency high impact events	IEEE Power Energy	Technical community
Provides and maintains an acceptable level of service in the face of failures that disrupt its normal operation	European Network and Information Security Agency (ENISA)	Technical community

This leads to the proposition of the resulting definition:

Resilience: /riˈzilyəns/ *noun*, the ability of a power system to tolerate disturbances and still provide an affordable service to all consumer, by anticipating, absorbing, rapidly recovering and adapting from those faults and problems affecting the normal operation.

The resilience definitions refer several times to:

- Different characteristics of a resilient system (that sometimes may be mistaken with resilience);
- The resilient system stages (Fig. 1);

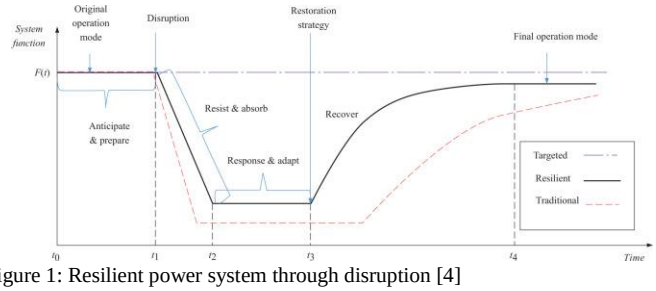


Figure 1: Resilient power system through disruption [4]

The terms whose definition we need to be clear about in order not to create further confusion are:

- *Reliability:*

  Resilience will have to do with disturbances and extreme events, including the recovery process, but we speak of reliability for the rate of occurrence. While resilience metrics speak about system response, reliability ones, would do so of system performance.

- *Robustness:*

  Robustness may refer to a more passive approach that require stronger coupling between network components and considers expected failure. And the resilience would have to do with an active approach demanding flexibility, adaptability and agility, and take into account unexpected catastrophic failures.

- *Security:*

  They are both subject to a time-varying evaluation, but the term security speaks of realistic disruptions whereas the resilience will be affected by those events less likely[1] to occur.

- *Vulnerability*[2]*:*

  "Vulnerability is the predisposition that deteriorates if a high-risk event occurs." [5] In other words, a good analysis of the vulnerabilities of our network gives an overview of the possible threats that could face the system.

C. Regulatory analysis and companies' role

We have seen that *resilience* seems to be in everyone's mind nowadays, as it is important in a technical aspect, we also have to keep in mind the regulatory approach. It is central that policymakers understand the key points of the state of the art and trade-offs, so they can know how to incentivize resilience. There is also a key point to keep an eye on: get a balance between the required investments, the companies and the customers' needs.

Without going in depth, the UK organizations that have analysed and framed some key points for resilience strategies, mainly do not give guidelines, requirements or concrete paths; they generally define resilience and give some ideas. We could say that they give an overall view and some recommendations but not always how to improve the resilience or where it is better to invest.

We will list below some organizations, the papers they have elaborated and their main ideas:

TABLE 2: RESILIENCE RELATED CONTRIBUTIONS

Organization	Papers	Contribution
OFGEM	K. Hurley, "Reliability and Safety Working Group (RSWG) meeting", OFGEM, 2012 Other discussions on Black Starts or Safety, resilience and reliability, etc. but no specific	Regulation of the Electric Network that has to be applied; DNOs preparation for high-risk events and building a robust system.

[1] They are usually high risk – low probability events.

[2] It is not a term that can be confounded with resilience, but has q great influence over it.

	conclusions for our project.	
OFCOM	Connected Nations Report, Security and Resilience chapter[3]	It is more focused on providers of communication network and services, but discusses some insightful reflexions.
UK Parliament	Infrastructure resilience inquiries[4]	Might give some ideas, but not directly related with our purpose.
UK Government	It chooses to give some guidance to the telecoms network regarding resilience[5]	The documents referred are usually about telephony systems, yet some strategies can be considered.
CPNI	Webpage offering guidance for UK infrastructures on resilience[6]	Does not have concrete conclusions by threat subjects related to physical and cyber security, resilience related.
NIC	Resilience infrastructure study[7] [6]	In general, NIC provides impartial expert advice and make independent recommendations to the government on economic infrastructure.
E3C	Final report on August 9th incident	Paper enlightening the importance of an operational telecommunications to increase the electricity network resilience (and ideas for mitigation)

There are other organizations that have also some papers, but as we first said, they mainly do not have directly to do with our purpose:

- Department for Business, Energy & Industrial Strategy (BEIS);
- Energy Networks Association (ENA);
- Electronic Communications Resilience & Response Group;
- Energy Research Partnership;
- Etc.

Moreover, the vast majority of companies subscribe to all the sustainability and energy transition goals and guidelines. This will not mean that they set by themselves any regulation, but they will seek to go in the same path, in this case: improve the resilience.

With regards to the concrete strategy of the Iberdrola group, – including Scottish Power Energy Networks - they work on an energy model based on decarbonization, the electrification of the economy and the dynamization of the territories, and this transition cannot avoid the incorporation of the renewables. All this goals to attain are part of an investment plan on the networks in which the group has allocated 27 billion euros.[8]

The Networks business' **goals** will be: zero accidents, offering an excellent service based on quality of the networks, maximise operation efficiency of the system and lead. the transformation towards a more efficient integration of distributed energy and to a cleaner model, by using smart grids. It also looks to avoid major **risks**, such as the operative ones (disturbances of the supply because of the weather events or accidents…) and the technological and cybersecurity ones, that may have an impact on the installations security or the service offered to the customers. To sum up, in few words, we can say that company's actions and activities are aligned with these strategies that will end up in achieving a resilience enhancement. Those actions are usually in the same way as the Sustainable Development Goals. That is how the companies will contribute to the society in such an important target.

D. Framework

It has been important to understand the traditional and the more resilience-oriented point of view in order to get what we will be facing, and which are the different aspects that have a direct impact on the resilience and which methods could lead our assessment, such as keep an eye on the different option of metrics elaboration we could use (quantitative and/or qualitative).

All these considerations led to the following framework elaboration:

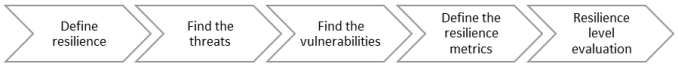


Figure 2: Resilience assessment framework

In order to go through the whole framework, we will need to analyse the three main dimensions impacting the resilience: Power, Services and Security.

III. Analysis of the Dimensions

The aforementioned framework and the overview into resilience lead us to a concrete procedure to assess the resilience of the telecoms network. Because of the state of the art, the available tools and the newness of the subject, we will use a qualitative approach, where we will try to show the different aspects that we can assess. In other words, in this part we will be able to analyse different characteristics of the network classified into different dimensions (Power, Services and Security), then we will create our path to assess the resilience according to some criteria.

The understanding and a deeper knowledge of each of the following dimensions, that are critical for SPEN, will go over different technologies and systems to identify requirements and advised steps towards a future resilience enhancement.

[3] https://www.ofcom.org.uk/__data/assets/pdf_file/0039/95898/CN16-07.pdf

[4] https://www.parliament.uk/globalassets/documents/post/postpn362-resilience-of-UK-infrastructure.pdf

[5] https://www.gov.uk/guidance/telecoms-resilience

[6] https://www.cpni.gov.uk/protection-infrastructure-0

[7] https://nic.org.uk/studies-reports/resilience/ and https://nic.org.uk/app/uploads/Anticipate-React-Recover-28-May-2020.pdf

[8] https://www.iberdrola.com/conocenos/lineas-negocio/redes

In each of the dimensions we will define the term and its importance to the network resilience, we will see the possible approach we can have and finally elaborate some gauged metrics. We will see how this analysis influences the resilience assessment structure. (Fig. 3)

A. *Power resilience*

The first dimension we could think of is **power** resilience. As we have seen before, the telecoms networks and the power system are essential for our day-to-day life, so we will be looking for the measures and technologies that will undergo major damages and facilitate a fast restoration.

If we define the power resilience dimension, we will be evaluating the time that will last the equipment once the primary power supply is removed.

This dimension concentrates on three things mainly, the time it will take to mitigate and minimize the disruption, whether it is public network or not, and which technology will serve for the backup generation. To those three, we can add those that have more directly to do with the vulnerability and the impact they can have economically, geographically, socially, etc. All these conclusions are reflected in the metrics elaboration.

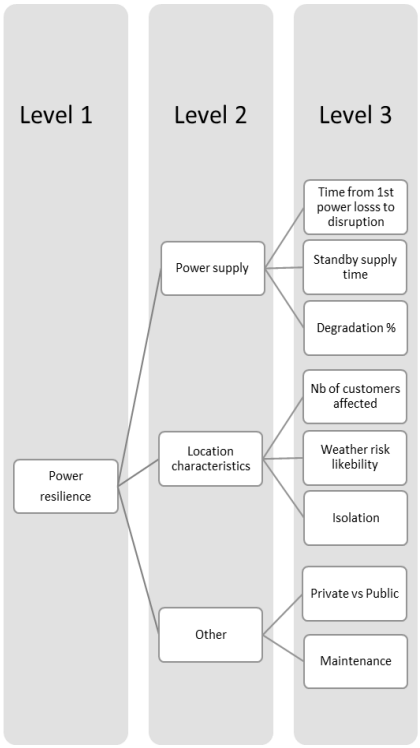


Figure 3: Power resilience structure

B. *Services resilience*

On one hand, we have already seen that the telecoms-power grid association serves several purposes and on the other hand, we are well aware of the diversity operational assets that serve Distribution or Transmission. By all this, we mean that when we talk about services resilience, we are evaluating how many services are going throw the same link and/or if whether having T&D on a same site has any benefits.

The objective of the Telecom network resilience strategy should be to assure the resilience of the telecom services needed by the electric network rather than the resilience of the telecom network itself. An important aspect to be considered is that the STN provides telecom services for both the transmission (SPT) and the distribution (SPD and SPM) electrical networks. Although all services are important, the impact of a problem in a service for the transmission network is potentially much higher than if something fails in the distribution networks. That is why "the level of physical security, power supply reliability and generally speaking the infrastructure supporting the telecom equipment should be aligned to those required for the transmissions' services." [7]

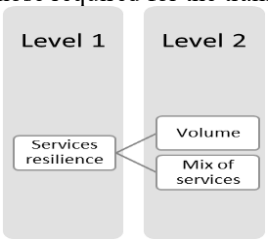


Figure 4: Services resilience structure

C. *Security resilience*

Last but not least, we will analyse the **security** dimension. The theoretical background help us realize the assumption about the increasing complexity of the Smart Grids, specially of a Cyber-Physical System. This intricacy of the networks enhances the vulnerability, there has been a fast deployment of the systems that enlightens the critical character of the security and rises the necessity of a resilient grid against physical and cyberattacks. The clear subdimensions will be physical and cyber security.

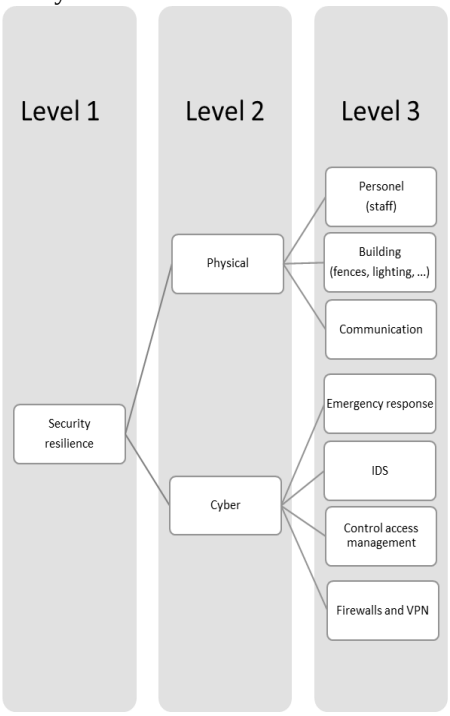


Figure 5: Security resilience structure

The physical security subdimension will concentrate on

preventing the physical access to the site, the equipment, etc. and avoiding harm and/or theft. We will divide the following analyses into three aspects, on one hand this inherent physical security measures (i.e. entrances, illumination, fences, etc.), followed by those contributing into the security management (i.e. security manager, security plan existence, security working group, etc.), to finish with the arise of some other ideas such as the preparation of the site for the extreme weather hazards or other. The creation of the survey and the subsequent assessment will be based on those three facets.

The cyber security will be better defined as "the methods to intercept and protect from cyberattacks and prevent disruptions or unauthorized access." [8] We could say that it is incredibly important to design a strong intrusion detection system (IDS), linked to the physical layer. To correctly detect and recover it is also significant to identify and be able to classify the threat so the operators can define the strategy to deal with it. To assess the vulnerability of the critical assets will give us the main guiding points where to fortify the network. In these cyber-physical systems, it will be critical to isolate in time the damaged point to mitigate the effect of the attack.

Let us keep in mind that adding the cyber layer not only affects the communication network and electronic devices, but will be able to damage the rest of the physical grid elements, hence a cyber-physical subdimension arises.

IV. Description of the Tool

The main goal of the study for SPEN is to ensure a well-functioning tool to assess resilience according to the dimensions and values of SPEN. The implementation of the tool looks for a good assessment and a simplification on the process, in order to have a value that measures the resilience of the grid and so its efficacity, its performance, its need for investment, etc. In a larger scope, we have looked that it is a tool that can be then implemented in the other companies from Iberdrola (Avangrid, etc.), this means that the metrics will have to be decided with this optic: decide metrics and strategies that can be valid for the rest of the countries too. (Fig. 6)

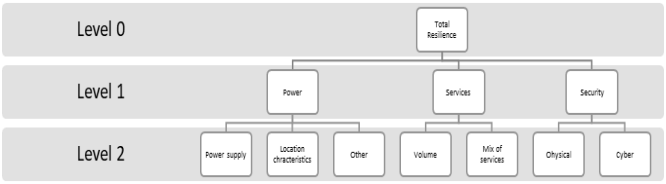


Figure 6:Resilience assessment structure[9]

To sum up, for our purpose, building the tool we mainly need two things:

- Deep theoretical knowledge on each of the selected dimensions in order to select key metrics and weight them correctly;
- Thought on the overall assessment process, from the standardized data collection to the data visualization in the form of a dashboard.

A. Metrics

As a dashboard is a management and steering tool, it is aimed to identify all the choices that led to the creation of this tool by keeping a meticulous aspect behind each reflection, especially that of the choice of indicators which will have consequences on the usefulness of the dashboard.

1) Selection

On one hand, it was necessary to identify the indispensable indicators that could be used as well as keep the most external view possible in order to be objective. At the same time, the aim was to provide good visibility of the current situation of the resilience in each point and to enable decision-making in the knowledge of its evolution and be able to invest where it would be more convenient.

During the process of creating the tool, the priority in the choice of indicators belonging to different pillars, one relating to the power, another to the services and the last one to the security aspect.

We will try keep an eye on the worldwide aspect, implementing metrics that might be useful for the other countries. That is the reason why we will have "rapid" surveys, and added to those, some wider questions that go deeper into each dimension so that it gives possibility of adapt better to every country situation.

2) Calculation

The survey will gather the main required information, considering the three levels in the resilience index (See Fig 3-5). The overall resilience index (RI) will consider the relative importance of each sublevel (Level 2 and 3), considering their contribution which will set the weight. In addition to the weight (relative importance), there is another analysis that will consider a ranked value for each subcomponent, from 0 to 10. Both the weight and the grade criteria have been assigned after a rigorous study of the state of the art and the current situation of the technology. (See Appendix)

To sum up, based on the beforementioned calculations, we will be able to get an overall weighted index obtained by using the following equation (1):

$$RI = \sum_{i=3}^{1} w_i \times G_i \qquad (1)$$

RI: *Resilience Index, Level* 1

w_i : *constant represents the weight of the components of each Level* (i)

G_i : *grade value of the dimensions component, from level* i

B. Tool Creation

The creation of a dashboard requires the selection of relevant tools. Mostly in every big multinational efficiency and efficacity are key and will lead to some decisions, in this

[9] The third level is not present here since it too detailed, but can be seen in Fig. 3-5.

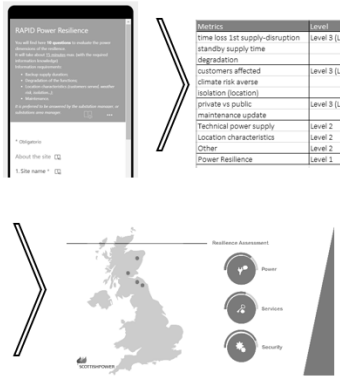
case, to the tool selection, i.e. sometimes we could find some more complete tools but because of their complexity would be avoided.

On the other hand, As for every new tool implementation, it should have a person in charge of collecting the data. This does not mean having to collect it personally but more keep track and make a reminder for those who will not complete it on time for give the proper and more complete information to the decision makers. This is why the tool is also equipped with a survey to answer easily and fast, it is an effective way of collecting data.

1) Tool Roadmap

Once the dimensions understood, we are able to build the metrics and the weighted criteria. All this will fit into the tool implementation, that makes it easy to use and has final visualization that eases the understanding and the decision making.

1. Survey completion;
2. Weighted grade calculation;
3. Incorporation to the dashboard.



Metrics	Level	Weight (0-1)	Grading criteria - Index
time loss 1st supply-disruption	Level 3 (Level 2 - technical power supply)	0,25	**0**: less than 1 hour/ **10**:10 hours
standby supply time		0,5	**0**: below 10 hours/**10**:120 hours
degradation		0,25	**0**: 100% / **10**:1-20%
customers affected	Level 3 (Level 2 - location characteristics)	0,5	**0**: more than 0,75 million//**10**: less than 0,15
climate risk averse		0,2	**0**: likely risk/ **10**: not likely
isolation (location)		0,3	**0**: isolated /**10**:not isolated
private vs public	Level 3 (Level 2 -	0,5	private: /public:
maintenance update		0,5	**10**: 0-2 years / **0**: more than 10 years
Technical power supply	Level 2	0,6	
Location characteristics	Level 2	0,25	
Other	Level 2	0,15	
Power Resilience	Level 1		

Figure 7: Tool implementation roadmap

C. Discussion and limitations

We also have to keep in mind that this is a tool that will serve to SPEN and Iberdrola as a model to build a wider and deeper one. It gives the main aspects to have in mind, the metrics and the criteria that has been selected; and has a theoretical background to rely on to be able to decide if build a more complex criterion.

Other key points to take into consideration would be to ensure that the survey and/or other steps of the roadmap to assess resilience are included into the workload and that there is some periodical dashboard actualizations o that it does not fall into oblivion.

Moreover, the company can decide to have other considerations into the resilience assessment and decide if include them in the same roadmap or in a separated way, for example the economic aspect, the network growth that want to be achieved, some of the Green Deal goals or other low carbon plans, etc.

Last but not least, we cannot forget that this is just a first resilience assessment, the technology is always improving and that there could be changes in the near future, it should be advisable to keep an eye to always improve the assessment.

The purpose of the tool is to achieve the project goal: to assess the resilience It is a fact that SPEN is already revising the sites and they are being prepared for upgrading. A concrete assessment of several dimensions is interesting for them because it can be helpful in the decision making of the different possible improvements.

However, as any other project and/or tool it is not perfect and, it has some limitations. Limitations that should be considered for a future implementation of the tool and to be aware of the gaps that might have the assessment.

1) Dimensions' limitation

The study of the resilience assessment is based on the deep state of the art of the three selected dimension: Power, Services and Security. We are about to see that we can see that they can also create some limitations to the purpose of the project:

1. The fact of analysing a cyber-physical system has many interconnectivities. This means that it can be difficult to consider a metric/criterion that only affects one of the dimensions;
2. The fact of having chosen the three pillars from which build our tool will imply to omit many other aspects that are part of the definitions, such as the stages of a resilient system, some characteristics of a resilient system, etc.
3. there are many aspects that SPEN (or Iberdrola and Avangrid in a near future) would want to consider some other aspects in parallel of this resilience assessment, or even build a dashboard that comprises them all (economic, the social impact, the engagement to social responsibility of the company, etc.).

2) Tool result limitation

We have selected a tool/roadmap that will reach a concrete figure that gives the current resilience situation. This is a simple, efficient, effective and gives an easy understanding which was the purpose of its construction. However, it has the limitation such as every simplification. Giving a concrete figure/result of the resilience of the system has needed not only a simplification of the interconnected metrics, but also of the weighting of each of them, e.g. considering the different important aspect of the fences (type, material, height, base, etc.), we could have given a concrete weight for each of them and this will give a more accurate "fences weight".

3) Qualitative metrics limitation

Having studied the different pillars on which to build the analysis, we have selected a more qualitative tactic which is probably the best approach.

However, if we try to have an external and overall point of view that also tries to see the application or the further development of the tool, we can say that keeping an only qualitative approach responds more to the advice purpose than look for a future enhancement of the network.

D. Future features

First of all. We should keep in mind that it is only a model that can be further developed. It is meant as a guide in order to create a wider tool.

A part for developing further the model, some future features could be added, such as:

1. Complete and RAPID surveys: this will give the possibility of having a wider study of the resilience, and somehow a little bit more accurate;
2. Comparison: Implementing it worldwide would give us the possibility to see all the different substations resilience, substation by substation;
3. Possible future scenarios: it would be advisable to add the possibility of creating future scenarios, in order to see whether the resilience evaluation will be;
4. White papers: since this discussion is quite new[10], based on these future scenarios or merely in the evolution of actual grid resilience enhancement, it could be considered to share the "good doings" on the subject. A probably good way of doing is by implementing a white paper.

V. Conclusion

To conclude, in simple words, the goal of assessing the resilience has been reached. Even though it is an early-stage model that should be modified to improve its future implementation (worldwide view, comparison between sites, etc.) As any other relatively new conversation-starter (on *resilience*) we take into account that the documentation and research related to the topic will not give us a specific solution, but more some ideas and guides that might be of good use. We would also want to enlighten the need of a strong theoretical background to build the tool and to keep developing, both the model and the tool itself. The tool has some limitations and we have suggested several modifications/improvements that might be useful in further studies. Last but not least, "Despite the increasing prioritization of resilience, formal approaches for understanding, analyzing, and improving resilience of control systems remain relatively new and under development." [9], which means that we should keep an eye to all the technologies advancements and possible investments that can be done in this topic: building a resilient system.

Appendix

We will find here the abovementioned grading criteria and metrics tables for each dimension:

Table 3: Power resilience metrics criteria

Metrics	Weight	Level	Grading criteria
Time loss 1st supply-disruption	0,25	Level 3 (Level 2 – technical power supply)	**0**: less than 1 hour/ **10**:10 hours
Standby supply time	0,5		**0**: below 10 hours/**10**:120 hours
Degradation	0,25		**0**: 100% / **10**:1-20%
Customers affected	0,5	Level 3 (Level 2 – location characteristics)	**0**: more than 0,75 million//**10**: less than 0,15
Climate risk averse	0,2		**0**: likely risk/ **10**: not likely
Isolation (location)	0,3		**0:** isolated /**10**: not isolated
Private vs public	0,5	Level 3 (Level 2 – Other)	**10**: private: //**0:** public:
Maintenance update	0,5		**10**: 0-2 years // **0**: more than 10 years
Technical power supply	0,6	Level 2	
Location characteristics	0,25		
Other	0,15		

Table 4: Services resilience metrics criteria

Metrics	Weight	Level	Grading criteria
Volume of services	0,4	Level 2	**0**: >20 services per protection link / **10**: only one service
Mix of services	0,6		**0**: mixed services /**10**: distribution

Table 5: Security resilience metrics criteria

Metrics	Weight	Level	Grading criteria
Manager position	0,07	Level 3 (Level 2 – Physical)	**0**: no manager/ **10**: security manager
Staff training	0,1		**0**: no trained staff/**10**: trained staff
Fences	0,2		**0**: low simple fence/**10**: double high fence
Lighting	0,03		**0**: only one item enlightened/**10**: every item is well illuminated
Gates/entrances	0,1		**0**: only one unseparated

[10] The resilience topic is not new, but there are not enough studies, regulations, requirements in order to completely have a guide on the procedure of resilience enhancement.

			entrance/**10**: differentiated entrances
CCTV	0,2		**0**: no CCTV/**10**: CCTV for ext. and int.
Security plan	0,15		**0**: no security plan/**10**: security plan
Security working group	0,15		**0**: no security working group/**10**: security working group
Emergency response	0,2	Level 3 (Level 2 - Cyber)	**0**: no emergency response/ **10**: emergency response
IDS	0,3		**0**: no IDS/**10**: IDS connected to SCADA and physical layer
Control access management	0,2		**0**: no CAS/**10**: CAS
Firewalls/VPN	0,3		**0**: no firewalls and VPN/**10**: firewalls and VPN
Physical Security	0,6	Level 2	
Cyber Security	0,4		

ACKNOWLEDGMENTS

First of all, I would like to thank Iberdrola and SP Energy Networks for giving me the opportunity to discover the professional world and for welcoming me during this internship.

I would particularly like to thank both my supervisors Charles Gilmour and Craig Michie, who accompanied me throughout this internship. I would also like to thank specially some of the people with whom I worked during the internship, Javier Andrés Pérez Abad (Iberdrola) and James Irvine (Strathclyde), for their increased confidence in me and their support.

I would also like to thank all the people I have worked with, my colleagues, and all those I have had the pleasure of meeting during my assignment, who have allowed me to grow personally and professionally.

I would like to thank ICAI and Strathclyde in particular, for welcoming me and giving me these opportunities.

I would also like to thank all those people who during my time in ICAI have helped and welcomed me.

Finally, I would like to thank my family and friends for their unconditional support.

To all of you, thank you.

REFERENCES

[1] P.R. Shukla, J. Skea, R. Slade, R. van Diemen, E. Haughey, J. Malley, M. Pathak, J. Portugal Pereira (eds.) *Technical Summary, 2019. In: Climate Change and Land: an IPCC special report on climate change, desertification, land degradation, sustainable land management, food security, and greenhouse gas fluxes in terrestrial ecosystems*, 2019

[2] Rehman, Abdul & Deyuan, Zhang. (2018). *Investigating the Linkage between Economic Growth, Electricity Access, Energy Use, and Population Growth in Pakistan*. Applied Sciences. 8.

[3] Bompard E, Mosca C, Colella P, Antonopoulos G, Fulli G, Masera M, Poncela-Blanco M, Vitiello S. *The Immediate Impacts of COVID-19 on European Electricity Systems: A First Assessment and Lessons Learned*. *Energies*. 2021.

[4] Yanling Lin, Zhaohong Bie, Aici Qiu, *A review of key strategies in realizing power system resilience*, Global Energy Interconnection, Volume 1, Issue 1, 2018, Pages 70-78

[5] Gholami, T. Shekari, M. H. Amirioun, F. Aminifar, M. H. Amini and A. Sargolzaei, "Toward a Consensus on the Definition and Taxonomy of Power System Resilience," in IEEE Access, vol. 6, pp. 32035-32053, 2018

[6] "Anticipate, react,recover: Resilient infrastructure system", National Infrastructure Commission, May 2020

[7] "Telecoms resilience strategy", Iberdrola paper, 2020

[8] T. Nguyen, S. Wang, M. Alhazmi, M. Nazemi, A. Estebsari and P. Dehghanian, "Electric Power Grid Resilience to Cyber Adversaries: State of the Art," in *IEEE Access*, vol. 8, pp. 87592-87608, 2020

[9] N. Jacobs, S. Hossain-McKenzie and E. Vugrin, "Measurement and Analysis of Cyber Resilience for Control Systems: An Illustrative Example," *2018 Resilience Week (RWS)*, 2018, pp. 38-46, doi: 10.1109/RWEEK.2018.8473549.

Alejandra Pérez Pastor was born and raised in Valladolid, on May 9th, 1997.

She received her degree of Energy Engineering from the Polytechnical University of Madrid (UPM) after having completed an exchange year in the National Polytechnique Institute in Grenoble (France). When starting her studies, she already knew that she wanted to be a change agent into today's world. Her years in the university years had only kept nourishing this dream in a more concrete way. Being an expert in the Energy field to be able to contribute with some expertise. With this idea close to her heart, she decided to keep gathering technical knowledge in the Energy field to be able to fulfill her life-goal During her year in France, she had the opportunity to work as project manager in Schneider Electric in the Sustainability department, leading Access to Energy projects. That is the reason why she decided to start a more specific master, Masters' Degree in Smart Grids in Universidad Pontificia de Comillas (ICAI) and the University of Strathclyde, that would give her the knowledge and experience to keep building the future of the energy domain. This Master has provided her the tools to understand the and will be soon working in Scottish Power.