Nuno Jorge de Freitas Martins

Licenciado em Ciências da Engenharia

Eletrotécnica e de Computadores

Electrical Grid Resilience in Critical Infrastructure

Dissertação para obtenção do Grau de Mestre em
Engenharia Eletrotécnica e de Computadores

Orientador: Pedro Miguel Ribeiro Pereira, Professor Auxiliar, Faculdade de Ciências e Tecnologia da Universidade NOVA de Lisboa

Coorientadores: David Miguel Monteiro Salgueiro, Licenciado – especialista ao abrigo do nº4 artº 21º do Dec-Lei 74/2012 de 13 Abril

Júri:

Presidente: Doutor Luís Filipe dos Santos Gomes

Arguente: Doutor Francisco Alexandre Ganho da Silva Reis

Vogal: David Miguel Monteiro Salgueiro, Licenciado

FACULDADE DE CIÊNCIAS E TECNOLOGIA
UNIVERSIDADE NOVA DE LISBOA

Setembro, 2019

Electrical Grid Resilience in Critical Infrastructure

Agradecimentos

Em primeiro lugar, gostaria de começar por agradecer ao meu orientador de tese, Professor Pedro Pereira e ao meu orientador de estágio Engenheiro David Salgueiro, por todo o Know-How, ajuda, disponibilidade e orientação no decorrer deste trabalho. Gostaria também de agradecer ao Professor Nelson Chibeles Martins pela sua ajuda numa fase crucial deste trabalho.

Gostaria também de agradecer a todos os meus colegas de curso, André Cuco, Bruna Bruno, Daniel Fernandes, Fábio Lopes, Gonçalo Queiroz, João Costa, João Lima, João Macau, Miguel Lourenço, Pedro Corista. Pedro Garcia e Rui Trindade, com quem trabalhei e estudei ao longo destes anos, que me ajudaram a chegar ao fim deste percurso e por todo o seu companheirismo. Aos membros da Missão País, Carlota Franco, Daniela Gaspar, Joana Barruncho, Vasco Leitão que me acompanharam e suportaram em momentos mais difíceis do curso e aos membros do Núcleo de Estudantes Católicos que me ajudaram na conceção deste projeto na nossa FCT, um grande obrigado.

Um Obrigado especial a todos os meus amigos dos *"Peanuts"*, que me acompanharam desde sempre e com quem foi possível partilhar momentos especiais ao longo do nosso percurso, com especial atenção ao Bruno Corgas por me ter apoiado de uma forma mais presente ao longo deste percurso e ao Tiago Nunes pelo apoio incondicional e ajuda que me deu no decorrer desta dissertação.

À minha comunidade, um grande obrigado por toda a sua preocupação ao longo do meu percurso, principalmente à Beta, Quim, Ana e Bruno.

Aos meus pais, gostaria de endereçar o mais profundo obrigado por todo suporte e apoio e por nunca terem desistido de mim mesmo quando eu duvidei. Tudo o que sou e serei a vocês o devo e não há palavras suficientes para agradecer tudo o que fizeram por mim. À minha irmã, obrigado por todo o apoio, carinho, amizade e por estares sempre disponível para esclarecer todas as minhas dúvidas de forma tão pronta e sincera.

Por fim gostaria de agradecer a uma pessoa que nestes últimos dois anos se tornou uma das minhas rochas, que nunca me deixou desistir e que teve sempre a capacidade de me apoiar nos momentos de maior cansaço e de maior felicidade, à minha namorada Maria. Gostaria de agradecer por tudo o que tens sido, por todo o teu amor, carinho, amizade e muita paciência que foram essenciais para a conclusão desta etapa tão importante da minha vida.

A todos muito obrigado!

Resumo

O aumento constante da população mundial e os constantes avanços tecnológicos, que originam novas soluções e equipamentos que se tornam indispensáveis no dia-a-dia do ser humano, fazem com que exista um considerável aumento do consumo de energia elétrica. É, portanto, essencial que se utilize este recurso da forma mais eficiente possível e de forma a que este chegue a todos com segurança.

Atualmente começa a surgir a necessidade de criar infraestruturas resilientes para que haja a capacidade de garantir o normal funcionamento destas após um fenómeno adverso de forma a que infraestruturas e sistemas dos quais dependemos não sejam comprometidos. Este problema aplica-se a infraestruturas que providenciam serviços essenciais no dia-a-dia de uma sociedade, como no caso de estudo específico, um Data Center. Nestes casos, o seu correto funcionamento é essencial em alturas de crise a empresas de tecnologia e outras entidades que fornecem serviços a outras empresas ou ao utilizador comum.

No seguimento deste problema, surge o tema desta dissertação, cuja implementação foi realizada em contexto empresarial. É, então, proposta uma metodologia que permite quantificar e avaliar o impacto que uma falha de um equipamento teve numa determinada infraestrutura, tendo em conta a sua importância e o tempo que demorou a sua resolução, e descrevê-lo de uma forma simples e de fácil compreensão. Isto pode ser útil para todos aqueles que no futuro tiverem necessidade de recorrer ao histórico de eventos, críticos e não-críticos, dessa infraestrutura. Para obter um valor quantitativo, recorrer-se-á a uma métrica que tenha em consideração as características técnicas da infraestrutura analisada.

Estas empresas precisam de se manter competitivas perante o seu publico alvo para que possam prosperar no mercado e é essencial que consigam perceber como agir perante uma falha num equipamento, ou componente, sem descurar a parte económica visto que todas as decisões tomadas a partir desse momento devem ter como objetivo voltar ao estado anterior ao evento da forma mais rápida possível. Existe, portanto, a necessidade de perceber o impacto que uma falha pode ter numa infraestrutura para que se possa atuar de acordo com a sua gravidade.

Nos testes realizados concluiu-se que o sistema forneceu valores que permitiam ordenar os eventos ocorridos ao longo de um ano de acordo com o seu real impacto e as simulações efetuadas a componentes escolhidos de forma aleatória ia de acordo ao que se pretendia.

Palavras chave: Resiliência, Infraestruturas Críticas, Processo de Poisson, Failure Modes Effect Analysis.

Abstract

The constant growth in world population and the constant technological advances, which lead to new equipment and solutions that become indispensable in the daily life of human beings, created a considerable increase in electricity's consumption. It is, therefore, essential to use this resource as efficiently as possible and in a way that reaches everyone safely.

The need for resilient infrastructures is now emerging so that there is the ability to ensure their normal functioning after an adverse phenomenon so that the infrastructures and systems we depend on are not compromised. This problem applies to infrastructures that provide essential services on a day-to-day basis to the society, such as in this specific case study, a Data Center. In these cases, proper functioning is essential in times of crisis to technology companies and other entities that provide services to other companies or the average user.

Following this problem arises the theme of this dissertation, whose implementation was carried out in a business context. A methodology is then proposed to quantify and evaluate the impact that an equipment's failure had on a given infrastructure, taking into consideration its importance and the time taken to resolve it, in a simple and easy to understand manner. This would be useful for all those who in the future need to recur to a detailed historical data, of critical and non-critical events, of this infrastructure. To obtain a quantitative value, a metric that considers the technical characteristics of the analyzed infrastructure will be used.

These companies need to remain competitive with their target audience so that they can thrive in today's market. It is essential that they can understand how to deal with a failure in an equipment or component without neglecting the economic side since all decisions made thereafter should aim to return to the pre-event state as quickly as possible. There is, therefore, a need to understand the impact that a failure can have on an infrastructure to act accordingly to its severity.

In the carried-out tests, it was concluded that the system provided values that allowed to order the events that occurred over a year according to their real impact and the simulations performed on randomly selected components were as intended.

Keywords: Resilience, Critical Infrastructures, Poisson Process, Failure Modes Effect Analysis

Table of Contents

A – List of Figures

B – List of Tables

C – List of Acronyms

AR	Annual Resilience
CAIFI	Customer Average Interruption Frequency Index
CVaR	Conditional Value at Risk
DHS	Department of Homeland Security
DOE	Department of Energy
FMEA	Failure Modes, Effect Analysis
GMP	Gross Municipal Product
GRP	Gross Regional Product
HVAC	Heating, Ventilation, and Air Conditioning System
IGS	Infrastructure General State
IT	Isolation Transformer
LVDB	Low Voltage Distribution Board
NASA	National Aeronautics and Space Administration
NZEB	Net Zero Energy Building
OMS	Outage Management Systems
SAIDI	System Average Interruption Duration Index
RAP	Resilience Analysis Process
RL	Resilience Loss
RM	Reliability and Maintenance
RPN	Risk Priority Numbers
UPS	Uninterruptible Power Supply
US Armed Forces	United States Armed Forces
VaR	Value at Risk
WTC	World Trade Center
ZEB	Zero Energy Building

1

Introduction

This introductory chapter is intended to make known what is going to be said throughout the dissertation, the problem to be solved and the importance of the solution to be developed. Immediately after that, the objectives that need to be fulfilled will be presented.

1.1. Motivation

Electricity is, today, a necessity. It is a resource that we use every day to work, to move around and to communicate. It is necessary in our homes, in our work or study places and in our devices. For those reasons the use of energy has been increasing. However, our most used sources of energy are finite, and their use in an excessive way can lead to have serious environmental issues. Energy consumption has increased significantly as reflected in the increase in CO_2 emissions, as shown in figure 1, and the demand for energy on a global scale is growing, with an increase of more than 40% between 2015-2030. According to the World Energy Outlook Special Report, *"Having remained broadly stable at around 4 Gt for much of the 1980s and 1990s, CO_2 emissions from industry have increased by 38% since the early 2000s, to reach 5.5 Gt."*[1]. Also, emerging countries are approaching the consumption levels of developed countries, which means that the values of CO_2 emissions will increase even more was we may confirm with the world atmospheric concentration of C02 values demonstrated in figure 1. Also, world population is also increasing which can deteriorate these numbers even more.

It is therefore very important that we begin to use energy in an intelligent and, above all, efficient way. According to [2], *"Energy efficiency is a way of managing and restraining the growth in energy consumption. Something is more energy efficient if it delivers more services for the same energy input, or the same services for less energy input"*. Basically, using less energy to provide the same service, which can be achieved by recurring to new technologies and new processes.

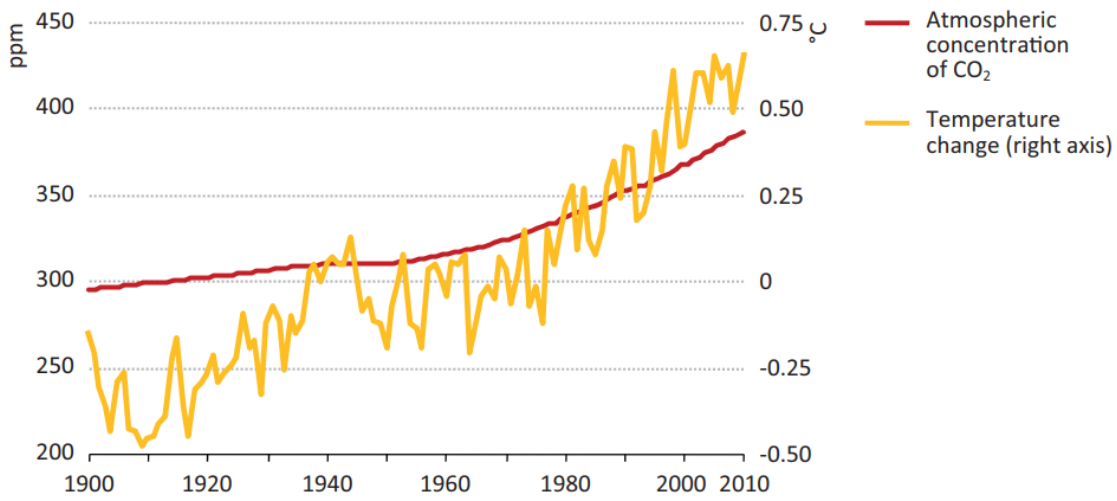

Figure 1 - World atmospheric concentration of CO2 and average global Temperature Change [1]

Using energy efficiently reduces greenhouse gas production and is a cheaper, faster and cleaner way to contain climate change. We can, therefore, conclude that by increasing energy efficiency we are in the right direction towards reducing, or at least not increasing the negative impacts on man-made climate change over the last few years, but that is not enough.

Another way to respond to this threat is to use renewable energy resources, as they are clean, avoid the emission of greenhouse gases and endless since they depend on natural resources. However, in the center of a city (which are currently some of the most energy-demanding places) the only source of energy that would be viable would be solar energy. Today, these types of technologies are more developed, more efficient and can be installed on the top of buildings, or other areas usually unimpeded and unused.

However, adding Solar Panels it is not enough. Improving our current buildings in order to use energy in an intelligent and efficient way it is also necessary. And it is in this sense that new measures and concepts such as the Net Zero Energy Building (NZEB) arises. The European Energy Performance of Buildings Directive (EPBD) requires that from 1 January 2019 on new public buildings, and from 1 January 2021 on new private buildings, the concept of NZEB is to be implemented.

In reference [3], authors use the general definition for Zero Energy Building (ZEB) given by The U.S. Department of Energy (DOE) Building Technologies Program: *"A net zero-energy building (ZEB) is a residential or commercial building with greatly reduced energy needs through efficiency gains such that the balance of energy needs can be supplied with renewable technologies."* Still, a NZEB is a complex concept and contains very varied terms and expressions and a NZEB definition can vary according to the author of the study, the article or even the country.

However, implementing it will not be easy. For a building to be considered NZEB it must follow to technical rules and standards. These require an advanced and specialized workforce and some of these rules may vary from country to country. The reference [4], draws attention to the fact that the workforce does not have the required know-how to carry out these changes in existing buildings or in new buildings. In addition, as new NZEB buildings begin to emerge, and even when photovoltaic panels are installed in older buildings, new grid problems may arise leading to

grid faults that often affect the population either through a localized fault or a large-scale fault. Problems may arise in buildings and facilities owned or operated by the energy operator, or human errors, though, it is also prudent to think that this type of fault can occur due to different natural phenomena. As an example, the hurricane Sandy that occurred in the United States of America and caused serious problems in the electrical network [5] or even by the hurricane Leslie that devastated the region of Aveiro, Portugal, in 2018. All of the factors described above have brought new challenges and problems that enable power outages.

But the hypotheses of having to adapt to hurricanes and different atmospheric phenomena should be equated. Reference [6] explicitly says *"While hurricanes occur naturally, human-caused climate change is supercharging them and exacerbating the risk of major damage."* It also notes that the number of storms is increasing which means that there is a necessity to adapt and to build more resilient infrastructure so that we can be prepared for a catastrophe. As Figure 1 shows, global temperatures are rising throughout the years, research presented in [7] has shown that increasingly violent storms will likely continue assaulting our coasts stating that *"severe storms will increase in a warmer environment"* and *"Thunderstorms typically occur in the warmest season of the year"*.

It is of utmost importance to learn how to adapt our infrastructures to ensure they are resilient in future climate disasters such as extreme heat, heavy rain, and drought. All the aforementioned disasters can change the way we think and idealize our cities, but that does not mean we should not create new ways to adapt to these problems without taking advantage of these new adaptations. In the United States, in one of New York's borough, Staten Island, a new project is beginning to take the form to create a *Seawall* which can withstand the massive waves by possible future thunderstorms [8]. They do not only need to *"withstand the prolonged barrage of pounding waves"* but *"they are considered vital to protect land and property that would otherwise be swept out to sea"*. However, it will have a public walkway and the *"boardwalk will be big enough to host concerts, carnivals, marathons, and cultural events"* according to the governor's office. Even though its prime goal is to shield people from a natural disaster, it can have other purposes.

Climate change is unpredictable, and it is as we know a continuous, worsening crisis. Resiliency is the idea that a city can respond to any type of threat without neglecting safeness and the enjoyment of a city. Power Outages can affect services that society takes for granted on a day-to-day basis, such as public transportation, public lighting, buildings of public interest (such as sports stadiums), factory industry or even hospitals and some of these infrastructures are essential to a country's normal functioning. Their disruption, in certain cases, should not happen at any cost and that is why some of them have some redundancy or emergency systems implemented to prevent such problems from happening.

In this sense, it is important to ensure that the Power Grid is resilient and that there is a rapid response in the event of a failure, in order to minimize the service replacement time as well as the number of consumers affected. A resilient power system can be the path to prevent and respond to a low-probability, high loss event because it is not possible to foretell all the events that can and do occur in a short and long term future [9].

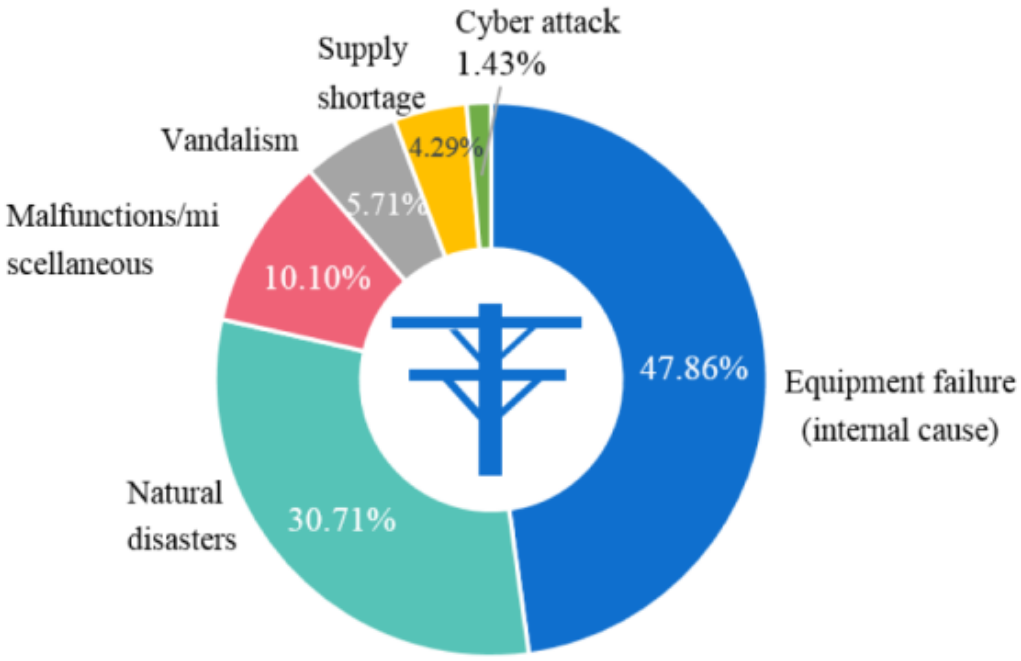

Figure 2 - Power outage causes for 140 worldwide outage data [9]

All those events may jeopardize not only public services that we rely on a daily basis but also companies, industries, and factories that need to be more competitive in today's global market. These companies need to improve and develop internally in order to *"be dynamic and flexible and meet the ongoing changes"* [10], to deal with the severity of competition and to increase customers' expectations creating a new commitment to eliminate product defects and make up for any kind of shortage and deviations in its performance.

For example, the fact that many telecommunication companies are currently implementing the fifth-generation cellular network technology, or 5G, which brings higher speeds, no interferences, and brings the ability to control machines, external devices, and other objects, is a challenge since all this technology makes it necessary to upgrade existing telecommunications infrastructures to accommodate it. One of the goals of the 5G network is to address some of the obstacles associated with the Internet of Things (IoT). The fact that IoT is increasingly common means that there is a need to create a more resilient infrastructure to all kinds of phenomena, as it implies digital interconnection to everyday objects with the Internet.

There has also been the massification of cloud storage services such as Google Drive and Dropbox, which ensure fast and uninterrupted access to information stored by the average user as long as there is an Internet connection. All this information is stored in Data Centers. The number of such infrastructures is growing, and they have the ability to provide other services to companies and institutions that have to remain uninterrupted at all costs. However, the possibility of a Data Center failure can be very hurtful not only to the company responsible for managing that infrastructure but also to companies that depend on that Data Center to access information or to provide services to third parties. Therefore, the need to make them more resilient arises. Due to this, there is a need to meet the interests of consumers who increasingly rely on these technologies for personal and professional purposes.

According to figure 2 approximately 30% of power outages derived from natural disasters and 48% derived from equipment failures, thus, having resilient critical infrastructures is becoming a common goal for many countries and entities. These infrastructures also have to be reliable but that may not be enough, regarding hospitals and telecommunications infrastructures, for example, since these mechanisms cannot fail at times of greater need. Also, lots of infrastructures are interdependent, which means that bigger importance to this matter must be given since the failing of infrastructure can prejudice others creating the possibility of a domino effect.

1.2. Goals

This dissertation has as main objective to create a methodology, that analyzes the failures and or incidents in a critical infrastructure and quantifies them, characterizing disruptive events by the level of urgency, and has the ability to report the event as soon as possible. To do so, some metrics will be used in order to get to a more conclusive result.

This type of methodology is going to be implemented in a Data Center and it is important nowadays because it allows an analyst, a manager or the "decision maker" to be able to respond to problems or failures that were unpredictable or some abnormal phenomena that may damage or jeopardize some sections of an infrastructure. This methodology also attempts to create an indicator that gives support in the decision-making process after a critical or non-critical event.

It is also important that this tool is able to provide targets according to the expected performance of an infrastructure, giving important information to the performance evaluation of it.

1.2.1. Main Contributions

This methodology does not exist in this company and will be implemented primarily on an infrastructure of major importance. It will be able to provide a value of the impact that an event has had on the infrastructure, considering some characteristics that were previously defined and characteristics that will be introduced at the time of evaluation. If the design and implementation of this system is successful, the company intends to implement this system in the remaining infrastructures, thus creating a more detailed historical data of it. This system also allows setting quantitative targets to be met by the infrastructure management and maintenance teams, providing an important tool for mitigating the impact of the events.

1.2.2. The Document's Structure

This Document's structure comprises 6 chapters (introduction, four core chapters and conclusion). The remain chapters are structured as follows:

- **Chapter 2: State of the Art** - This chapter involves researching sources and articles, by other authors, demonstrating what already exists and what has been implemented, associated with the dissertation's theme. Explored topics include the definition of resilience itself, with some of its challenges, metrics, and processes for achieving it, and the idea of critical structures that are of major importance today and create serious challenges for the future.

- **Chapter 3: Development** - This phase tries to explain which were the first steps, and their pre-requisites, used to implement this methodology and provides detailed information of every step taken to address this challenge.
- **Chapter 4: Implementation** - This chapter describes the infrastructure in which this work is going to be implemented and will also prove whether the chosen metric is applicable or not. All steps and decisions taken will be described in detail.
- **Chapter 5: Results Analysis** - It presents and analyses the obtained results from previous critical events in order to understand if they match what is intended. Some simulations are going to be realized in order to double-check whether the final values are consistent or not.
- **Chapter 6: Conclusions** - Finally, some conclusions and a brief resume about the carried-out work are going to be presented. It will provide an overview of the activities and steps developed throughout this dissertation in addition to a description of concepts and techniques aimed at improving this project methodology and implementation.

2

State of the Art

This chapter is going to dissert about the necessary definitions and concepts to understand the problem and to comprehend some of the issues that the industry has encountered throughout recent years and continues to face in the present. Initially, some importance is going to be given to the power grid infrastructure resilience since this infrastructure is crucial for providing constant power to other buildings. However, in the case of industrial complexes (that can go from industrial factories to communications compounds, like a Data Center) a bigger importance can be given since it depends on a constant Power Supply to feed all their components and important machinery contained within. Some of the solutions found and what can be done to prevent and to manage some fails will be presented. All this information is of the utmost importance to develop the proposed methodology.

2.1. Resilience, what is it?

According to the Oxford Dictionary, resilience is defined as: "*The capacity to recover quickly from difficulties; toughness*" or "*The ability of a substance or object to spring back into shape; elasticity*". These definitions does not differ much in the field of engineering with the example implied in reference [11] which says: *"The common use of resilience word implies the ability of an entity or system to return to normal condition after the occurrence of an event that disrupts its state. Such a broad definition applies to such diverse fields as ecology, materials science, psychology, economics, and engineering. "*

In engineering, the term "resilience" is used to determine the ability to prepare and adapt to changes in conditions and to quickly resist and recover from breakdowns, system failures, deliberate attacks, accidents, threats or natural disasters. Resilience should not be viewed as a substitute for infrastructure protection, but rather as a field in which it is important to invest and to improve, with measures that increase the agility of systems so that they are able to adapt and recover and as an object that is designed to foster system-wide investment strategies.

The electrical network can be used as an example. This industry has evolved considerably over the last century, with successive investments made over time by different entities, allowing

the network to develop and become safer while guaranteeing a higher quality service to all its users. Those facts have to be confirmed by some reliability indexes such as the System Average Interruption Duration Index (SAIDI) which measures the total duration of an interruption for the average customer during a given time period and the Customer Average Interruption Frequency Index (CAIFI) which measures the average number of interruptions per customer interrupted per year [12]. Some of this indexes can evaluate the duration, the frequency, the number of customers interrupted and measure the availability of the service and the need for better indicators which ultimately implies a greater development by companies in safer and more innovative solutions, thus obtaining better results in terms of their ability to support, respond and recover from a disruptive event, as shown in the next image.

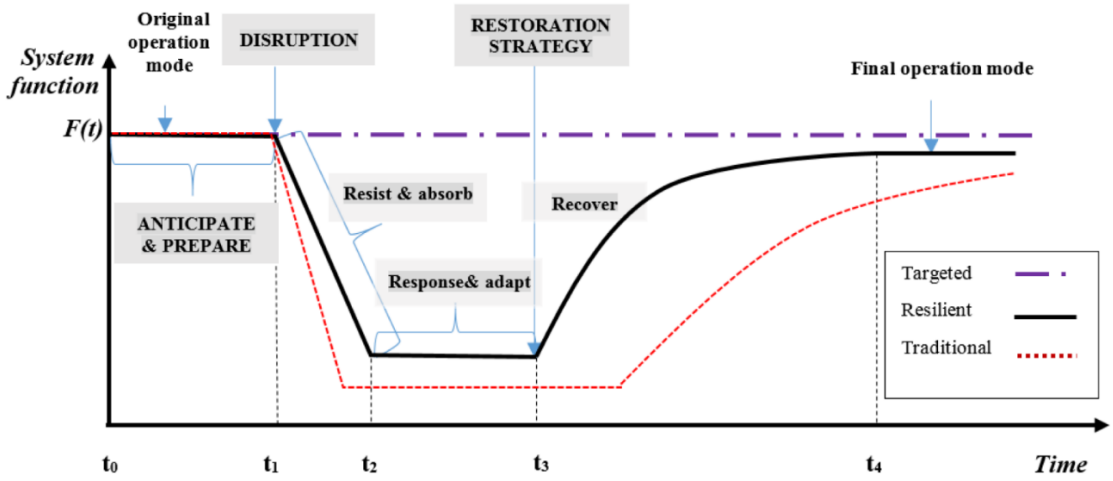

Figure 3 - The steps of a resilient Electrical System through a disruption event [9]

The Resilience Triangle, as is shown in figure 3, is according to [10] a *"tool developed in the field of civil engineering, with the objective of modeling the loss of resilience of a given structure during and after the occurrence of a disruption such as an earthquake."* This figure also shows the different phases that may occur after a disruptive event:

1. Anticipate & Prepare: Refers to the period before a disruption. Companies and entities should anticipate and prepare for any event to decrease both the likelihood and the impact of a risk;
2. Disruption: the moment in which a disruptive event takes place. If the disruption is not instantaneous, it may take some time to fully take place;
3. Resist & Absorb: the time that elapses between the beginning of the disruption and the end of it. While in some cases it can be abrupt, in others it may take some time to see the entire impact of the disruption
4. Response & Adapt: the initial response to the event, where measures are presented to control and prevent further damage;
5. Restoration Strategy and Recover: the first action by the affected entities in order to resume activities and go back to previous levels as soon as possible;
6. Final Operation Mode: the final state of the affected entity after all repairs and corrections. It should be noted that the final performance of equipment or building after reparations may be worse than before disruption (as shown in figure 3), equal or better depending on the corrections and solutions found. A similar description of this and the previous steps is also found on [13].

It is though very important to make a distinction between reliability and resilience. According to [14], resilience consists of low probability, high impact events and are more related to infrastructure recovery time. On the other hand, Reliability consists in High probability, low impact events that are more related with customer interruption time. And, while these two definitions are connected, it is also important to refer that a *"resilient grid is not necessarily one that is reliable and a reliable one is not necessarily resilient"* [15]. It is important to remember this since it can be easily adapted to an infrastructure or a component. This article also states that these definitions are important to guarantee that the entities responsible for the Power Grid can provide a quality service to everyone. Therefore, they have to be reliable, to deliver power in a consistent manner with as few disruptions as possible, and resilient, to prevent from possible rolling brownouts or possible cyber-threats.

It also refers to the importance of distinguishing blackouts from disasters saying: *"A blackout occurs when a large proportion of a power grid is disabled by a combination of unplanned contingencies, resulting in a temporary power interruption."* A disaster can relate to an event that was not expected and can create unavailability in a large section of the network. This type of events usually includes a blackout because of the destruction created. A power system that is reliable and well projected should be able to diminish the impact of the power disruption and should recover promptly from a blackout. So, being reliable to the blackouts that happen the most and resilient to events that do not happen much is of the utmost importance to ensure that the impact of any event is somewhat mitigated.

Infrastructure resilience is different from infrastructure security. While one is aimed at ensuring that infrastructure continues to meet the needs and assets of the community and all those who depend on it, infrastructure security is more related to preventing the occurrence of disruptive events in the future.

It could be considered that ideal resilience metrics would be obtained through retrospective and prospective analyzes, highly informative and with direct and consistent data. However, there are several trade-offs. Anyone who is analyzing the behaviors should consider which are the objectives of the analysis and what resources are available. It may be more interesting for the operator to use some metrics that are targeted at threats or to use widely-available metrics for the purpose of investing or planning an operational response to certain events or occurrences [5].

Achieving the resilience of a power grid has become a high priority for many countries in recent years to ensure a continuous power supply in certain areas. There are some measures that can be taken before, during and after a disruptive event that can make a difference at a time like this since it is not known when such an event can occur [9]. Also, the fact that the infrastructure is aging does not help. The document released by The White House explicitly says that in America *"The aging infrastructure is considered as the main cause for the power outages in the United States"* [16]. Therefore, to modernize the infrastructure is of the utmost importance to everyone involved.

Reference [14] proposes some measures to make the Power Grid more resilient, for example:

- Move the distribution and transmission lines to the underground;
- Upgrade the poles and other structures with stronger and more robust materials;
- Elevating substations;

- Relocating facilities to areas less prone to extreme weather;
- Reroute the transmission lines to areas less affected by weather;
- Create Redundant transmission routes.

Some of these measures are important to create a more sturdy, resourceful and flexible infrastructure, though some of it are not economically viable. In the case of moving distribution and transmission lines underground, the investment is too big, and the response and restoration time can be very time-consuming because of *"the inability of the repair crews to visually detect damaged components".*

However, this article leaves an important question, "Should we build a stronger and bigger grid or a smarter one?". By investing in a bigger and stronger network, with measures to improve robustness, the final result is a grid that is both reliable and resilient but too expensive and probably not cost-effective. It is therefore important to create a network that has smart solutions to provide continuous monitoring by the operator and control tools that can deal with some of the unexpected events in an efficient way. Creating Microgrids or Distributed Energy Systems are some of the measures proposed in [14].

This same question could be applied to an engineer in an initial phase of the conception and design of a building communications system: "Is it better to build an internal communications network with the latest and more advanced technologies, the fastest communication cables, with network connectors and signal amplifiers in almost every division, and create alternate signal routes to have a more safer and prone to failures network or is it better to study a more cost-effective and smarter solution that can do almost the same job but at smaller price?" It all depends on the budget and the final utility of this network system. A Grid Dispatch Center, for example, is more likely to need a more reliable and faster communication network than a personal domestic network.

2.2. Solutions and Improvement Methods

Applying solutions, using more resistant materials or control methods allows making a Power Network more resistant to possible disruptions that are becoming more frequent and more devastating. However, this brings significant challenges because the solutions applied in one place may not be feasible in another to make the grid more resilient and more efficient in the face of the possibility of critical events. Reference [9] clearly states that the best way to increase resilience lies in investing in system hardening and operational resilience strategies such as smart grids and distribution system resilience frameworks. Some of the hardening measures were already presented in the section 2.1 but it is important to refer that these measures may improve the durability and resilience of the infrastructure, but they are not resistant to every type of event.

A Smart Grid is a good solution to improve and to locate possible power failures and blackouts in an area which can be isolated and then rerouted to the power supply. It also gives the chance to maintain the power supply to critical customers or infrastructures. Therefore, [9] proposes a resilient load restoration algorithm in the distribution system through a backup Distributed Generator. Once there is a fault on a line, the radial topology of the network will partition into several islands separated by the faulted components, creating islands that are provided by distributed generators and others that are in a blackout. After identifying, locating and isolating the faults provoked by a disruptive event the restoration will occur.

A study, [17], conducted in Germany that indicates the experiences and challenges of integrating photovoltaic systems into the voltage grid shows that *"improved grid planning measures lead to a better use of the available low-voltage grid capacity*" which gives a bigger importance to implementing some of the measures mentioned in the previous points. It is, therefore, important to implement some measures to improve the network considering technical, economical and local factors such as the average power installed by each residence and the distance between residences that can bring problems in the low voltage network and geographical reasons. The solutions presented by this study were separated in three categories: Grid Optimization; Classic Grid Expansion Measures and the use of intelligent operating equipment.

2.2.1. Grid Optimization Measures

According to this study, the *"Grid optimization measures represent the most economical initial step and include, for instance, changes in grid structure and wide-area control*". So, [17] presents the following measures: individual tap changing of distribution transformers, wide-area control (for example, set the voltage of the transformers dynamically depending on the load situation), reactive power feed-in through photovoltaic inverters to maintain the voltage range in the Low Voltage Grid and changing the grid topology (to closed ring grid, for example) which reduces grid resistance, therefore reducing the voltage drop in the grid. All these measures are important to the distributor because they allow for better operation of the network and they can suit the voltage levels or load wanted to their need. The introduction of capacitor batteries into the Power Transformers is also benefiting not only the operator but also the owner of a complex that depends on internal Power Transformers because it reduces Joule losses. These solutions are capable of reducing both reactive energy losses and active energy losses considerably.

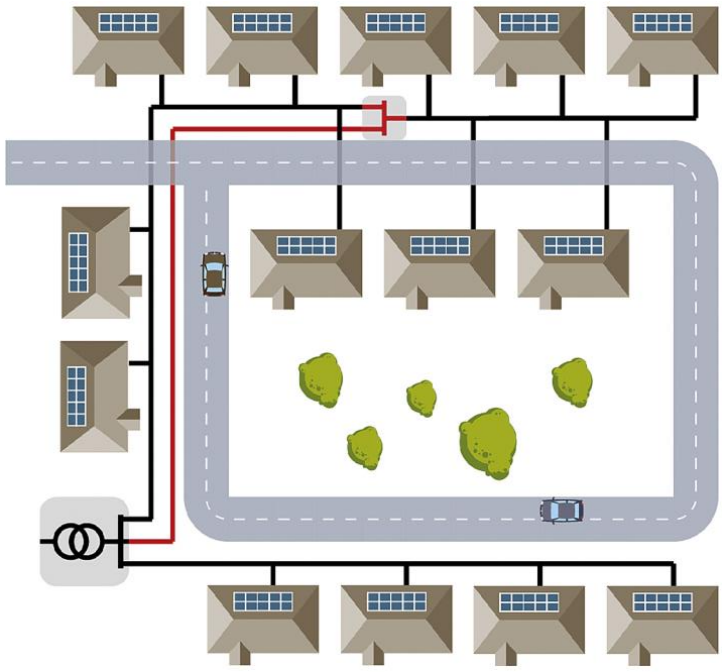

Figure 4 - A Representation of a parallel power line [17]

2.2.2. Classic Grid Expansion Measures

The main reason for the network expansion measures is to ensure compliance between the allowable limits for voltage and current. However, they remain viable solutions to some of the network problems. As measures to expand the Grid, the document proposes: replacing the local distribution transformer (to follow the rise of Photovoltaics), segmenting the local grid (to not exceed the capacity of the transformer), laying parallel cables (like the example presented in figure 4 to solve current or voltage issues that may come with cross-section of a cable), increasing the conductor cross-section (to reduce the voltage drop in the lines and to increase the current carrying capacity).

2.2.3. Use of intelligent operating equipment

These systems are relatively recent and *"present an economical alternative to classic grid expansion measures".* The authors present Voltage Regulators, to raise or lower the voltage levels according to the distributers needs, and Voltage-regulated local distribution transformers, to adjust the voltage ratio automatically without interrupting the Power Line. The first example is also pointed out as an economical and technological alternative to a classic expansion measure. The second example has the advantage of giving the possibility to maintain the low-voltage side of the transformer constant even when the voltage in the medium side increases.

2.3.Steps, Metrics and Measure to Achieve Resilience

To try to assess the resilience level of a network, some articles propose metrics or steps that can be used to try to evaluate the state of the network after a disruptive event. These metrics and methodologies should help companies, services and entities to better plan and respond to adverse events that at the present time are not addressed.

Reference [11] presents some metrics present in several studies that evaluate in a more quantitative way the performance of the system. Reference [18] suggests the use of agents to implement metrics because it enables to control physical and cyber systems. Reference [5] proposes the use of a framework to develop metrics to analyze the electricity grid and other energy sectors. Therefore, processes that can contribute to increasing the resilience of infrastructures and the development of adequate metrics, and metrics that can achieve a deterministic value of resilience lost will be presented.

2.3.1. Resilience Analysis Process

The Resilience Analysis Process was proposed in [19] *"as method for the assessment of baseline resilience and evaluation of resilience improvements."* This system uses the outputs from system models and historical data as the basis to create and develop grid resilience metrics for the power grid and other energy sectors and to obtain a response plan for the network.

This system is based in seven steps, as shown in figure 5, so that those who have the power to decide can assess the state of the system to later identify and analyze, through the proposals included in this model, which are the best strategies to increase resilience.

According to the system, these measures should be based on the performance demonstrated by the power systems and not by their attributes and they should quantify the outcomes of a stress situation or a disruption in the power grid which can be measured by the power not

delivered after a disruptive event, cost of recovery to the utility, population or service assets without power, among others.

It is important to refer that, according to [5], the proposed metrics are: Risk-Based since they include threat, vulnerability, and consequence as factors, to quantify the resilience of a system; Relatively Complex because the metrics are probabilistic and rely on stochastic models of grid operations that can be time and data consuming; Forward-looking considering that it recurs to metrics to project consequences for potential and future hazards; Broadly informative, the resulting metrics can provide information that can be essential long-term planning or investment; and More consistent, it relies on computational models to increase the consistency of the metrics.

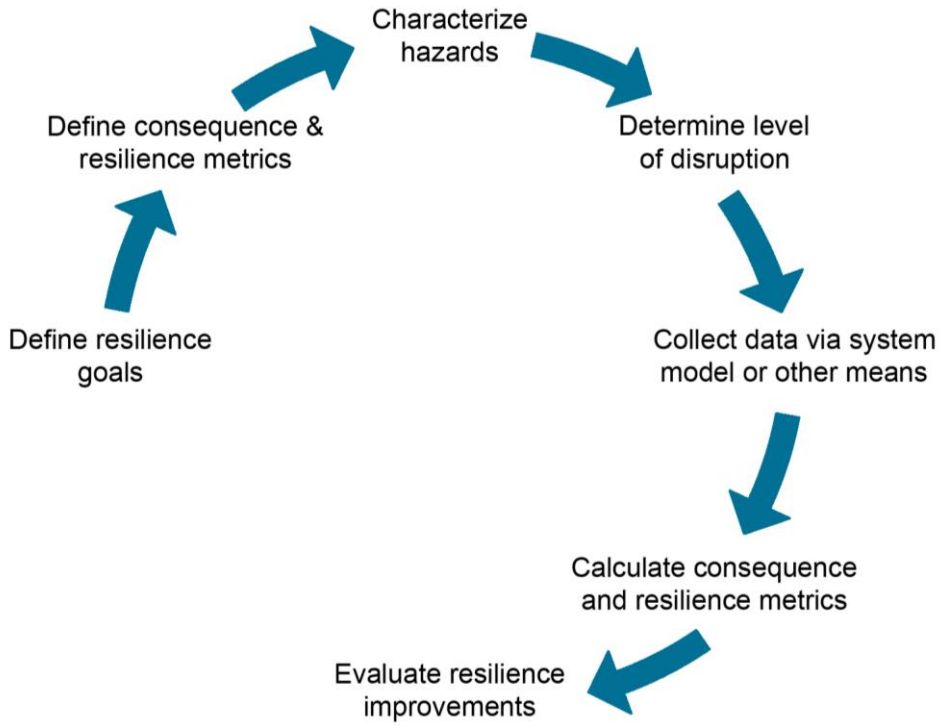

Figure 5 - The Resilience Analysis Process. Figure based on a graph present in E.Vugrin, 2017 [5]

2.3.1.1. Define Resilience Goals

Defining and specifying the Resilience Goals is the first step to establish the basis for all the following steps. It is important to discuss and determine whether the main goal is to assess the resilience of a power system due to previous events or evaluate possible system improvements. If the latter is chosen, a decision must be made about the considered changes and the types of questions the analysis should address. It is also necessary to know which are the characteristics of the infrastructure (geographic boundaries, physical and operational components, relevant time periods, etc.) where the goals will be applied and if there are any possible conflicting goals. Both reports, [5] and [19], leave these three examples as *"high-level goal language appropriate at this step of the process:*

- *Improving a regional electric grid's resilience to natural disasters;*
- *Deciding how to allocate a pipeline's capital investment and maintenance budget;*
- *Ensuring availability of power to medical or transportation systems during disasters."*

2.3.1.2. Define Consequence Categories and Resilience Metrics

The second step is to define the consequence categories and resilient metrics that serve as the basis for this process and these must reflect the resilience goals previously chosen. In some cases, outcome estimates and resilience metrics may focus on impacts recorded directly by an entity (undelivered energy, loss of revenue, cost of recovery, etc.), although, in some cases, direct impacts are part of the resilience assessment process. The Metrics that are selected should be specific enough to enable decision-making, whether for operational or planning purposes. The document [5] also presents a connection between consequence categories and the metrics that should be taken. The consequences and metrics should take into consideration spatial and temporal dimensions and the data that it is available. Table 1 gives some examples of consequence categories and their resilience metrics.

Table 1 - Examples of Consequence Categories for Consideration in Grid Resilience [5]

Consequence Category	Resilience Metric
Direct	
Electrical Service	Cumulative customer-hours of outages Cumulative customer energy demand not served Average number (or percentage) of customers experiencing outage during a specified time period
Critical Electrical Service	Cumulative critical customer-hours of outages Critical customer energy demand not served Average number (or percentage) of critical loads that experience an outage
Restoration	Time to recovery Cost of recovery
Monetary	Loss of utility revenue Cost of grid damages (e.g. repair or replace lines, transformers) Cost of recovery Avoided outage cost
Indirect	
Community Function	Critical services without power (e.g., hospitals, fire stations, police stations) Critical services without power for more than N hours (e.g. N > hours of back up fuel requirement)
Monetary	Loss of assets and perishables Business interruption costs Impact on Gross Municipal Product (GMP) or Gross Regional Product (GRP)
Other Critical assets	Key production facilities without power Key military facilities without power

2.3.1.3. Characterize Hazards

In this step it is important to specify the most concerning hazards, and their specifications, to try to minimize the consequences associated with those threats. It is of the maximum importance to have a prioritized list of interests to take into consideration: the likelihood of a hazard or threat happening; to be aware of the serious consequences that will be faced; the resources and priorities to perform the analysis. This step can also involve the formulation of hazard scenarios (when considering uncertainty) that details specific hazard conditions. It is also crucial to understand how the system should be able to absorb and adapt to different types of attacks or natural events.

2.3.1.4. Determine Level of Disruption

The fourth step specifies the level of structural damage, stress or other system impacts that the grid infrastructure and everything that is related is expected to endure under the hazard scenarios that were previously defined. This type of evaluation should be prepared to evaluate which infrastructures and properties are nonfunctional and degraded and to specify the severity of the damages and which are the necessary steps to obtain an overall system functionality. Nowadays, some models are able to estimate the potential losses from those events.

2.3.1.5. Collect Data via System Model or Other Means

This step consists in collecting consequence data via system models or other means. All this information can be collected by gathering systems, like an Outage Management Systems (OMS) present in most utilities. There are system-level computer models which can provide necessary power disruption estimates, when conducting forward-looking analyses. Recurring to data from communities describing the magnitude and duration of the disruption should be considered, in some cases. All this information can be used to evaluate how a system performs during a restoration period.

2.3.1.6. Calculate Consequences and Resilience Metrics

Calculating consequence estimates and resilience metrics is the next step. The system model outputs are converted to the resilience metrics defined during the second step. Resilience metrics can be consequence values, but in some cases, it may be preferable to combine it into a single value. It is possible to include uncertainty in the analysis and the system models are used to get multiple outcomes based on the previously characterized risks. It is also possible to include uncertainty in consequence estimates and resilience metrics by specifying the metrics statistical format. To define the uncertainty value, the statistical properties are used as: Quantiles (Confidence Intervals); Value at Risk (VaR) and Conditional Value at Risk (CVaR).

2.3.1.7. Evaluate Resilience Improvements

The seventh step has the goal of assessing the potential benefits and costs of the proposed resilience enhancing options. After accomplishing all the previous steps, it is now possible to evaluate the current network and define a baseline assessment of the resilience and then define what should be changed and where to invest in order to achieve a higher degree of resilience.

Another important test is to include the new modifications (for example, adding a redundant power line or turning off equipment in advance of a storm) in the system configuration and then repeat the previous steps again so that the analysts can evaluate whether it is beneficial to invest in those new measures. It is also, mandatory to recalculate new consequence estimations and the resilience metrics to determine the benefits.

2.3.2. Failure Modes, Effect Analysis

Failure Modes, Effect Analysis (FMEA) is a method to *"identify potential problems and prioritizing them so that you can begin to tackle or mitigate them"* [20]. This method can categorize an event so that the analyst or the manager can choose which is the best solution to an occurrence. Therefore, the main point of this "exercise" is to identify all the different failure modes that may occur and then evaluate the potentially damaging effects that these can create.

As the title implies, this process can be divided into two parts: The Failure Modes and Effect Analysis:

- **Failure Modes** – In any infrastructure, there are multiple things that can go wrong. All of those things are known as modes in the context of FMEA. It could be all kinds of failures that seem important to the designing team.
- **Effects Analysis** – This topic refers to the effects of an element of the process failing and the effect on the outcome created by that failure on the company's performance. It is important to investigate each failure and their causes to avoid or prevent, some situations in the future.

This process characterizes each Failure Mode into three categories, with a range from 1 to 10, that are described by [21] as:

- S = Severity of Failure, can be described as the intensity of the effect of the failure or how severe a consequence can be;
- O = Probability of Failure Occurrence (Frequency), is the possibility of occurrence of a potential cause or mechanism of failure or the frequency in which they occur;
- D = Detectability of Failure (Ease of Detection), as the probability of detection of a fault by the operator or end-user or if it is easy to stop, to see or identify.

All these variables are characterized in a scale from 1 to 10 like the one presented in table 2.

Table 2 - The range of every Variable of the FMEA Process

Range	Severity Scale (S)	Occurrence Scale (O)	Detection Certainty Scale (D)
	Probability of Failure	Possible Failure Rate	Probability of Failure
1	None	<1 in 1,500,000	Almost certain
2	Very Minor	1 in 150,000	Very High
3	Minor	1 in 15,000	High
4	Very Low	1 in 2,000	Moderately High
5	Low	1 in 400	Moderate
6	Moderate	1 in 80	Low
7	High	1 in 20	Very Low
8	Very High	1 in 8	Remote
9	Extremely High	1 in 3	Very Remote
10	Dangerously High	>1 in 2	Almost Impossible

As this table shows, every variable his evaluated from 1 to 10 creating 1000 different Risk Priority Numbers (RPN) since the end result corresponds to the multiplication of S, O, and D of each Failure mode:

$$RPN = S \times O \times D \tag{1}$$

Where:

- RPN = Risk Priority Number;
- S = Severity Scale;
- O = Occurrence Scale;
- D = Detection Certainty Scale.

So, while a Failure Mode with a value closer to 1 is nearly impossible to happen and may not affect the performance, a Failure Mode with an RPN value closer to 1000 has an extremely high probability of failure which could injure a customer or an employee.

So, by characterizing all the Failure Modes, it is, therefore, reasonable to prioritize them in order to face them, considering that the higher RPN value, the more unacceptable it is. With the priorities defined, a company or a team in charge of managing can begin to work through their list of potential process failures either one-by-one or in related groups, tackling the most dangerous problems first and the smaller ones last to try to minimize its exposure to risk as effectively as possible.

To do it, it is almost mandatory to review as many components, assemblies, and subsystems as possible to identify each possible failure mode, and their causes and effects. All of the

factors such as equipment, environment, materials, and human factors need to be considered, so, collecting accurate and thorough data on the project, analyzing documents, requirements, standards, the workplace and the conditions of working and interviewing informed and skilled people in the possible affected areas should be a priority to the team responsible for this task [21]. The flowchart, presented in figure 6, presents necessary steps for an FMEA implementation. However, this analysis may be further developed depending on whether or not the organization is interested in developing that infrastructure, its financial capacity and human resources.

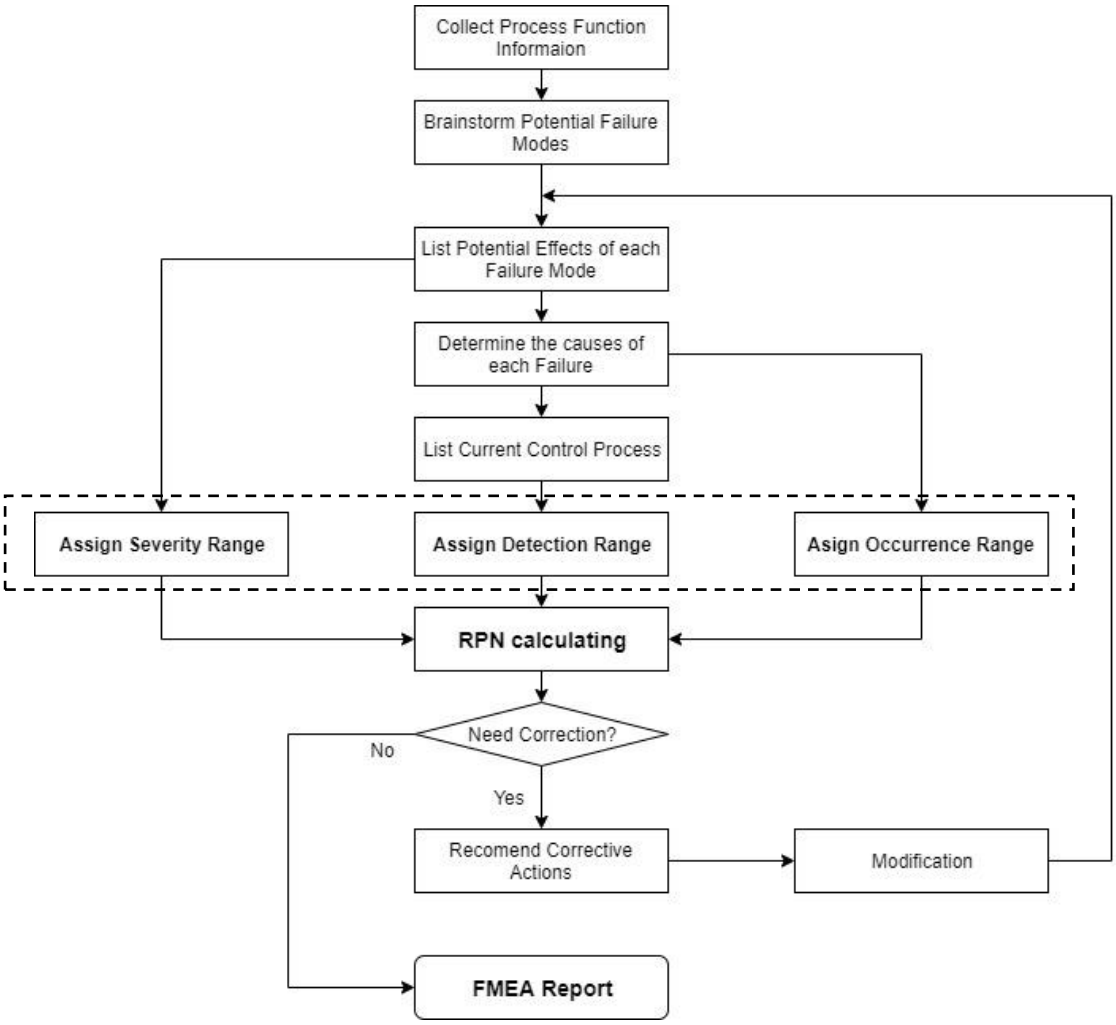

Figure 6 - A FMEA implementing cycle which carefully explains the necessary steps to apply this method. Figure based on a flowchart present in E. Pazireh, 2017. [21]

FMEA has been implemented since the 1950s in institutions such as the US Armed Forces, NASA, and companies such as Ford Motor Company and Peugeot-Citroen as a way to analyze products and industries. It is simple to use and offers an approach to quality engineering in order to reduce or eliminate the possibility of errors during the normal operation of the institution to which it was applied, reducing future errors. At first glance, it may seem that by instituting this process, problems will be solved temporarily. However, the main objective is to change the behavior of an institution in the face of certain events, so, the realization and execution of this method depends heavily on the members responsible for applying these changes. It is also

important to note that this process should always be regarded as a dynamic process meaning that it is important to revise it periodically to avoid increasing defects and to check if anything has changed [21].

2.3.3. The use of Agents

According to [18], an agent has the capacity to make pre-programmed decisions since it uses artificial intelligence mechanisms. The fact that he is semi-autonomous gives him some autonomy to decide what to do in certain situations. This point is important when it comes to resilience since it allows an agent to be able to remain alert and respond to disturbances if it is necessary. In order to do this, it is necessary to take into account some factors that can influence the final goals of an agent, such as: regulatory requirements of those who regulate this type of infrastructures; what kind of performance do you want (if it is aimed at increasing the quality of the network or a more efficient system) and the actual physical limitations that exist when applying this type of solution.

2.3.4. Quantitative Methods of Resilience Assessment

As it was mentioned earlier in this document, it is necessary to recur to resilience metrics to decide (whether for operational or planning purposes) and to get to the pretended goals. To do that, it is important to choose the metrics that meet the fundamental necessities, whether the goal is to obtain a deterministic performance-based approach which does not contain uncertainty, a probabilistic approach which *"captures the stochasticity associated with system behavior"*[22], or if they are time dependent or not. These measures compare the performance of a system before and after a certain event.

Reference [23] describes as *"a deterministic static metric for measuring the resilience loss of a community to an earthquake".* The presented formula is:

$$RL = \int_{t_0}^{t_1} [100 - Q(t)]\ dt \tag{2}$$

Where:

- RL = Resilience Loss;
- t_1 = Time at which a community returns to his normal state;
- t_0 = Time at which a disruption starts;
- 100 = Quality of the infrastructure before the disruption;
- $Q(t)$ = Quality of the infrastructure at a time t.

This metric compares the quality of the infrastructure before and after the disruption assuming that the infrastructure is at 100% before the earthquake. The values obtained by this equation give a deterministic level of the resilience of the grid: A lower *RL* indicates a high resilience level and a high *RL* level indicates a lower resilience level. These results can be analyzed over time in a resilience triangle model. It is also possible to associate this metric with table 1, in the Restoration category since it considers the time of recovery as a resilience metric.

Other authors, such as [24] , also use the resilience triangle model to calculate the resilience level. That metric has as objective to calculate *"the percentage of the total possible loss over some suitably long time interval T^*".* The formula is:

$$R(X,T) = \frac{T^* - \frac{XT}{2}}{T^*} = 1 - \frac{XT}{2T^*} \quad (3)$$

Where:

- R = Resilience Loss;
- X = The percentage of functionality lost after a disruption ($X \in [0,1]$);
- T = Time required for a full recovery ($T \in [0, T^*]$);
- T^* = A long time interval in which the lost functionality is calculated;

Both metrics are simple and give an idea of the time needed to recover the network to the levels registered prior to the disruption considering the lost functionalities and the recovery time to an equivalent level of "resilience". However, its linear recovery may not be realistic and the suggestion that the performance degradation after a disruption is immediate may not be valid to every system.

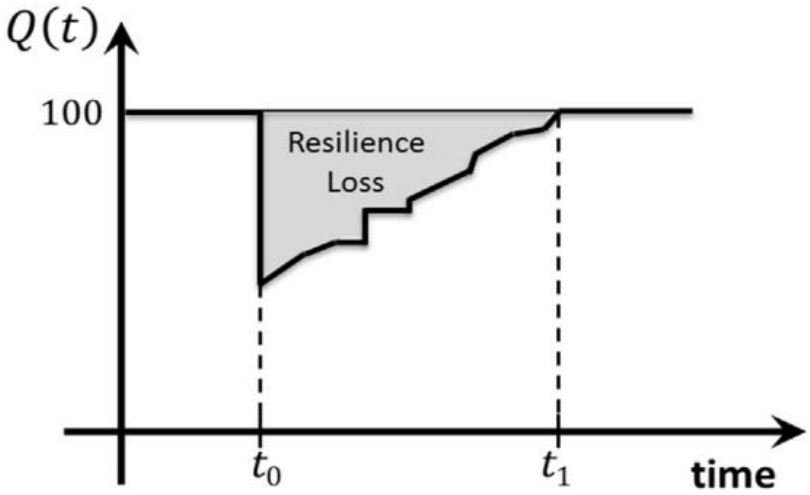

Figure 7 - A example of the Resilience lost according to the expression (2) [22]

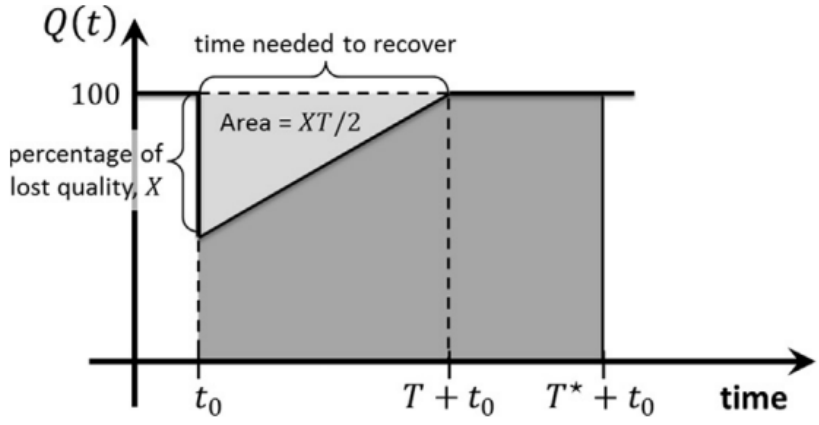

Figure 8 - A example of the Resilience lost according to the expression (3) [22]

Other author, [25], introduced local and global metrics that can be used to model the resilience of a public transportation safety system and air transportation systems, by the formula:

$$Global\ resilience = \int_{t_b}^{t_e} Local\ resilience = \int_{t_b}^{t_e} \frac{dS(t)}{dt} \quad (4)$$

Where:

- t_b = The time when the disturbance commences;
- t_e = The time when the disturbance ends;
- $S(t)$ = The sum of factors that can affect the system safety.

The last metric presented was proposed in [26]. This metric, like the first one presented, uses the Resilience triangle but considers past events (through a Poisson process that is going to be explained later) and the Non-Resilience per failure which gives it the ability to obtain safer and more reliable results. The developed formulas to obtain those values are:

$$Resilience\ per\ Failure\ (R_f) = \frac{(t_r - t_i)(Q_{100} - Q_r)}{2Q_{100}t} \quad (5)$$

$$Resilience\ (R_e) = 1 - \exp\left[-\lambda t\left(1 - p\overline{R_f}\right)\right] + \exp[-\lambda t] \quad (6)$$

Where:

- λ = The rate of a Poisson Process;
- t = Planning Horizon;
- p = Probability of a failure;
- R_f = Resilience per Failure;
- t_r = Time to recovery;
- t_i = Time of incident;
- Q_{100} = Capacity of the system;
- Q_r = Robustness of the system;

2.4. Critical Infrastructure

According to the Federal Energy Regulatory Commission [27], a *"Critical energy or electric infrastructure is a system or asset of the bulk-power system, (physical or virtual) that would be negatively affected by his incapacity or destruction of which would negatively affect: national security; economic security; public health or safety or any combination of such matters."*

Currently there are services and sites that require uninterrupted operation by private or public institutions. In these cases, a possible interruption may create serious problems that may jeopardize the normal functioning of certain services or even of a country. The National Infrastructure Protection Plan from the U.S. Department of Homeland Security (DHS) had 16 sectors and key assets considered as critical infrastructure including: Chemical; Commercial Facilities; Communications; Critical Manufacturing; Dams; Defense Industrial Base; Emergency Services; Energy; Financial Services; Food and Agriculture; Government Facilities; Healthcare and Public Health; Information Technology; Nuclear Reactors, Materials, and Waste; Transportation Systems; Water and Wastewater Systems [28]. In all these services, certain measures need to be applied in case of a disruptive event considering that some of these infrastructures are interdependent.

The World Trade Center (WTC) disaster can be used as an example about different interdependencies. According to [29] *"The building collapses triggered water-main breaks that*

flooded rail tunnels, a commuter station, and the vault containing all of the cables for one of the largest telecommunication nodes in the world. These included the Security Industry Data Network and the Security Industry Automation Corporation circuits used to execute and confirm block trades on the stock exchange. Before trading resumed on the New York Stock Exchange on Monday, September 17, 2001, the telecommunications network had to be reconfigured."

So, [29] clearly states that it is helpful to unify concepts in a *"smaller number of sectors based on common features"*. Therefore, the concept of a "lifeline system" (or simply lifelines) emerges. It was developed to evaluate the performance of large, geographically distributed networks during earthquakes, hurricanes, and other hazardous natural events and are grouped into six principal systems: electric power, gas, and liquid fuels, telecommunications, transportation, waste disposal, and water supply. These lifeline systems all influence each other, and daily infrastructures utilized by a large population have become more complex and interdependent, therefore, a failure in one of these can create chain failures. Thinking about critical infrastructure through the subset of lifelines may help to clarify features that are common to essential support systems.

Electric power networks, for example, provide energy for pumping stations, storage facilities, and equipment control for transmission and distribution systems for oil and natural gas. Oil provides fuel and lubricants for generators, and natural gas provides energy for generating stations, compressors, and storage, all of which are necessary for the operation of electric power networks. The continued operation of the telecommunications network, for example, is of major importance to the energy industry in order to allow continuous contact between various substations or infrastructures. Companies that provide services to other companies or entities, such as companies that store information in Data Centers, may also need a continuous power supply with the least possible power failures per year. For example, according to [30], the digital users are a contributor to the complexity of the Power Grid. He adds *"Some experts indicate that reliability will need to go from 99.9% (roughly 8 hours of power loss per year) to 99.99999999% reliability (32 seconds of power loss per year)."*

Coordinating all the systems, infrastructures and personnel, according to [30], may take some time and while some coordination occurs under computer control, a lot of it is still based on telephone calls between system operators at the utility control centers (especially during emergencies). This work proposes the use of agents, as previously mentioned, since this technology can make some decisions as soon as it detects any changes that may require it. Another document, [31], refers to the importance of developing a deeper understanding of the multiple interdependencies and their implications that are able to cover up multiple disciplines ranging from engineering and complexity science to sociology, policy research and political science. Modeling and simulation will be even more important in the development of this science.

It is, therefore, very important to promote behaviors and actions aimed at fomenting awareness, which requires public concern that can be informed through public education (via newspapers and television, for example) and through risk communication (which can be done by local professional societies).

2.5. Data Center

A Data Center is any facility that houses computer systems and other components, such as telecommunications and storage systems. Nowadays, this type of infrastructures has the capacity to provide services, not only to the regular consumer but also to large enterprises, financial institutions, government agencies that want fast Internet connectivity and non-stop operation to deploy systems and to establish a presence on the Internet providing some type of service to a large population, or that may want to store their data in a safe and secure network.

This type of installations are increasing, as well as the number of threats [32], and the operations made in this type of installations could be crucial for business continuity. A data center can be either a small server existing in a personal home or a building dedicated just for that purpose. Those buildings can be an industrial-scale operation, using as much electricity as a small town, and have to be equipped with all sorts of systems and equipment that can ensure the proper functioning of the entire Information Technologies (IT) systems. It requires equipment that has the ability to supply power continuously and with minimal fluctuations (such as a Uninterruptible Power Supply (UPS), Battery Banks and Emergency groups), redundant systems or backup components to ensure that services remain operational (if a fault occurs) and cooling equipment (like air conditioning systems) that has the ability to maintain a controlled environment as servers and other computing components can generate a lot of heat and various security devices [33].

To assure the quality of the services provided, this type of infrastructure needs to obey to some standards and characteristics and organizations like the Uptime Institute define, who evaluate and certify those installations. They currently define four tiers which *"describes the site-level infrastructure topology required to sustain data center operations"* [34]. The following are a brief summary of each of the Tiers:

- Tier I: Basic Capacity: There is a need to shut down the entire site to perform maintenance or repair operations. Capacity and distribution failures will impact the site.
- Tier II: Redundant Capacity Components: There is still a need to shut down the entire site extension to perform maintenance. Capacity failures can impact the site. Distribution failures will impact the site.
- Tier III: Concurrently Maintainable: Any capacity component and distribution path within a site can be removed in a manner designed to perform maintenance or replacement without impacting operations. The site will still be exposed to equipment failure or operator error.
- Tier IV: Fault Tolerant: An individual equipment failure or distribution path interruption will have no impact on operations. A fault tolerant site is also Concurrently Maintainable.

According to the aforementioned classifications, it can be said that a Tier III-rated data center is, therefore, a more complex infrastructure and requires more comprehensive behaviors and greater risk mitigation rigor than a Tier I. The installed infrastructure, the rigor and sophistication of the equipment and the management methodologies are established by the purposes of the data center. Its construction and location characteristics and its management and mode of operation also weigh in this assessment as these elements have various categories and components

with associated risks. Therefore, the identification and mitigation of their behaviors and risks are directly linked to the Tiers classification system.

But as it is possible to comprehend, this type of infrastructures is not fail-proof. The Uptime Institute Survey about 2018 Outages Results clearly states that *"Power was the most common cause of Level 4/5 outages from 2016 to 2018"*, as it can be seen in figure 9, and *"IT and Network were close behind"* (a disruption with of level 4/5 can be "Disruption of service and/or Operations" or a "Major and damaging disruption of services and/or operations") [35]. Though the proportion of more severe interruptions has been decreasing, when analyzing data from 2016 to 2018, a failure of just a few seconds can impact a direct customer in a few hours considering that some of the information may have been compromised. This survey also states that:

- "31% of respondents had an IT downtime incident or severe service degradation in the past year";
- "48% had an outage in their own site or service providers in the past three years";
- "80% report that their most recent outage was preventable".

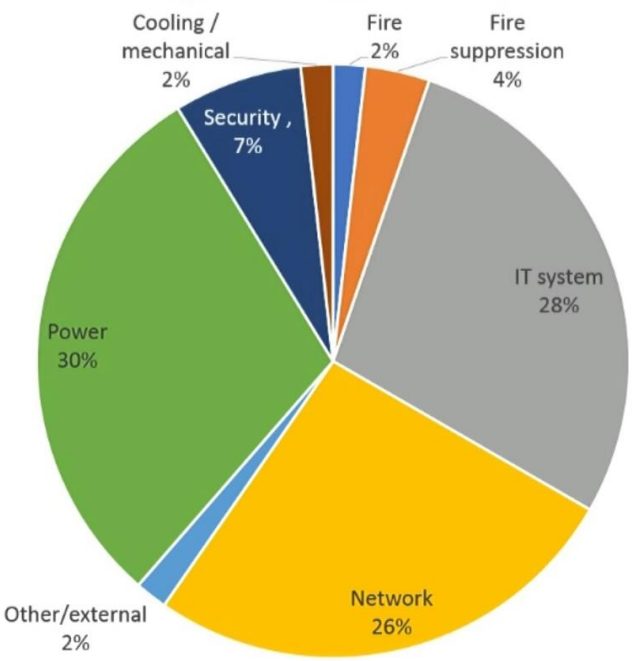

Figure 9 - Causes of Major Outages over Three Years [1]

[1] Figure Taken from https://uptimeinstitute.com/webinars/webinar-data-center-outage-trends-causes-and-updates

3

Development

After addressing some important themes for the execution of this project, such as Resilience, Resilience metrics, and Critical Infrastructure, this section will provide a detailed explanation of the quantification model factors, the chosen metric, and the failure mode tables. All of the steps taken were made according to the pre-requisites needed for their implementation. All steps taken throughout this part of the dissertation will be shown and explained to bring clarity to this process.

3.1. Initiation

After completing the initial research phase, it was concluded that there were two very important points that when combined could serve as the starting point of this work:

- Failure Modes, Effect Analysis (FMEA);
- The Resilience Triangle.

The *Failure Modes, Effect Analysis* method offers a very interesting idea of how to quantify and evaluate the impact of a failing component of an infrastructure. The idea of prioritizing certain events in detriment of less important ones is embodied deep within this method, and that makes it ideal to the pursued goal.

The Resilience Triangle, such as the one presented in figure 10, could be considered the starting point that can justify the choices taken throughout this work. The first impressions taken by analyzing the Triangle were that this figure was easy to be applied to what was pretended, was able to create a relationship between the impact of the event (vertical axis) and the time which has lasted (horizontal axis) of a certain component or equipment, providing a clear visualization of the magnitude of the disorder and the negative impact on system performance, and was of easy understanding. Nonetheless, this system does not take into account the aging effects of the infrastructure analyzed and in certain cases, this can influence the time of recovery of the infrastructure: while in certain cases the overall performance can come back to his normal state with a linear grow over time, in other cases that can happen in the instant right after the fixing of what

needed to be fixed, giving an almost instant time of recovery, unlike the one presented in figure 3, on Chapter 2.1.

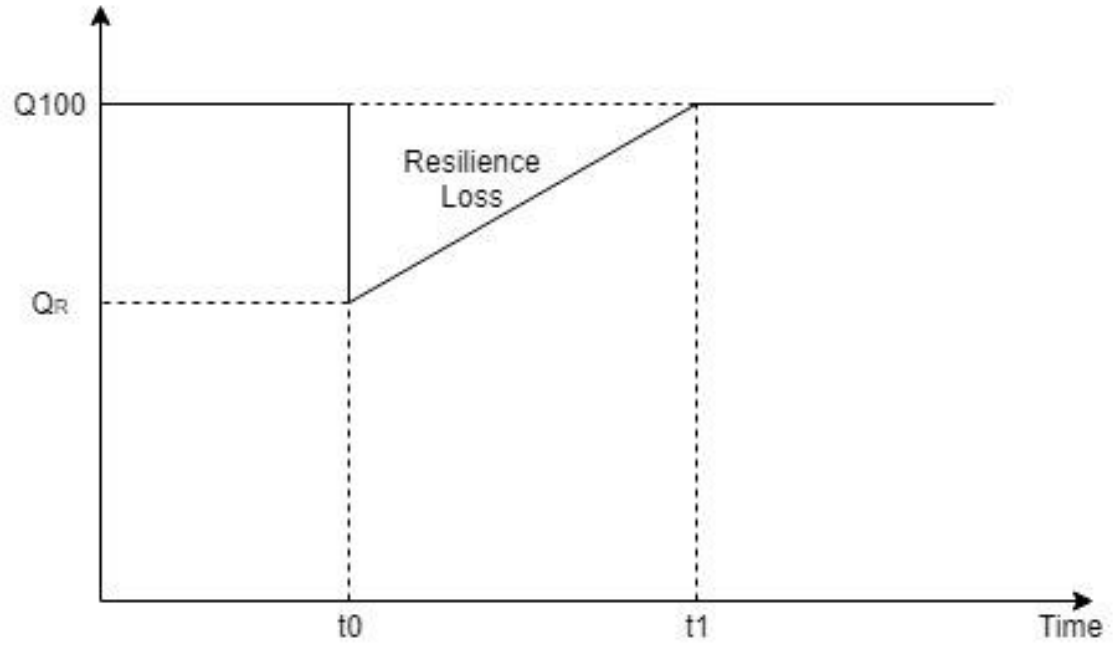

Figure 10 - A example of a Resilience Triangle

In the previous figure, the following acronyms represent:

- t_0 = Time of incident;
- t_1 = Time to recovery;
- Q_{100} = Capacity of the system;
- Q_r = Robustness of the system;

3.2. Quantification Model

The model to be developed must be easily understandable, leaving the least amount of questions, but at the same time must be complete so that future analysis of past events can be done safely and coherently. Therefore, there is a need to develop a model that can quantify an occurrence of what has happened.

For this to happen it is necessary to create a model that can quantify the impact of an occurrence on a given infrastructure and another model that with this information can calculate the impact it has had on the resilience of the infrastructure.

With this in mind, there were developed two models: one which can evaluate the impact that a failure has on the infrastructure and another that as the capability of calculating the final resilience impact that this event has on the infrastructure. These assumptions were thought off after some discussions about a deeper use of the Resilience Triangle.

3.2.1. The Incident and Failure Quantification Model of an Event

The first step was to start developing the incident and fault quantification model. To this end, it is intended to create a system that characterizes a piece of equipment through certain parameters.

So, this model is composed of 4 factors (Level, Significance, Redundancy and Type of Failure), which will be inserted by the analyst and that have different weights. These factors were chosen because combined they have the ability to characterize and differentiate a component regarding the infrastructure it is in, its technical characteristics and the importance that the company gives it. The combination of these factors may condition the level of the action itself after a disturbing event.

The weights must be calibrated in such a way that the result obtained is as close to reality as possible and so that in the event of the need to order all the events, they are ordered from the most important event to the one of the least importance. It is, therefore, necessary to describe the different variables and their subcategories for each of the factors to be introduced, so that all the components of the infrastructure to be analyzed can be defined quantitatively. This system should be applied to the Electrical system, the Heating, Ventilation, and Air Conditioning system (HVAC), and the Infrastructure Safety Systems. After defining all the factors from each component, they will be multiplied, giving a final value of the failures' impact of that component in that infrastructure. That value will correspond to the Risk Priority Number that will be explained further. This method is close to the one described by the FMEA process previously explained in chapter 2.3.2.

The biggest difference between the classifications that will be proposed is that each of the factors to be presented has between 3 or 4 values (or weights) ranging from 0 to 1, instead of the 10 assigned weights (in a range from 1 to 10) proposed in the FMEA system described in chapter 2.3.2. Each of the proposed values will be explained in order to clarify any doubts that may come from the manager responsible for characterizing a new component that can be added to the infrastructure, considerably simplifying the whole process of assigning values to each component. Since the value obtained by the proposed classification below will always be between 0 and 1, it can, therefore, be considered as a percentage value (comprised between 0 and 100%) allowing a more perceptible final value not only for the technician responsible for reporting an event but also for the manager responsible for all infrastructure.

In the process of attributing quantitative values to each factor's variable, it was decided to recur to the Fibonacci Scale, a sequence of numbers used for estimating the relative size of user stories in points. This sequence tends to facilitate the user from the perspective of estimating, seeing and understanding differences in order to obtain more coherent values.

To do it, it is of the utmost importance to utilize the Fibonacci's Sequence. The beginning of the sequence is: 1,1,2,3,5,8,13,21,34,55…

And to achieve these values the following calculations must be done:

$$F_0 = 0 \tag{7}$$

$$F_1 = 1 \tag{8}$$

$$F_n = F_{n-1} + F_{n-2} \quad (9)$$

So, after getting the first values of the scale and knowing the number of necessary values, the following sequence was generated to get the final proportions:

$$A_n = \frac{F_n}{\sum_{i=1}^{\alpha} F_i}, n \in [1, \alpha] \quad (10)$$

Where:

- α = the number of necessary values;
- F_n = the Fibonacci sequence values for each $n \in \mathbb{N}$.

Table 3 - The auxiliary values necessary to obtain the final weights

	$\alpha = 3$	$\alpha = 4$	$\alpha = 5$
$\boldsymbol{A_1}$	0.25	0.1429	0.0833
$\boldsymbol{A_2}$	0.25	0.1429	0.0833
$\boldsymbol{A_3}$	0.5	0.2857	0.1667
$\boldsymbol{A_4}$		0.4286	0.25
$\boldsymbol{A_5}$			0.4167

To conclude, to obtain the final weights, the following calculus must be done:

$$W_1 = 1 \quad (11)$$

$$W_n = W_{n-1} - A_{\alpha-n+2}, n \in [2, \alpha] \quad (12)$$

This sequence originated the following values to be applied in the factors that are going to be presented below.

Table 4 - The final weights, obtained with Fibonacci's sequence

	$\alpha = 3$	$\alpha = 4$	$\alpha = 5$
$\boldsymbol{W_1}$	1	1	1
$\boldsymbol{W_2}$	0.5	0.57	0.58
$\boldsymbol{W_3}$	0.25	0.29	0.33
$\boldsymbol{W_4}$		0.14	0.17
$\boldsymbol{W_5}$			0.08

With the exception of Redundancy, where the values would not be consistent with the true impact of an event, these values were assigned to the factors. Possible changes that have been made and the calibration process of these values will be explained in a later chapter.

3.2.1.1. Level

The first value to be introduced is the Level. This value attempts to aggregate devices and components that are in a certain position of the installation in the same group. The model under-study will have four levels with the following weights: A - 1st level; B - 2nd level; C - 3rd level; D - 4th level.

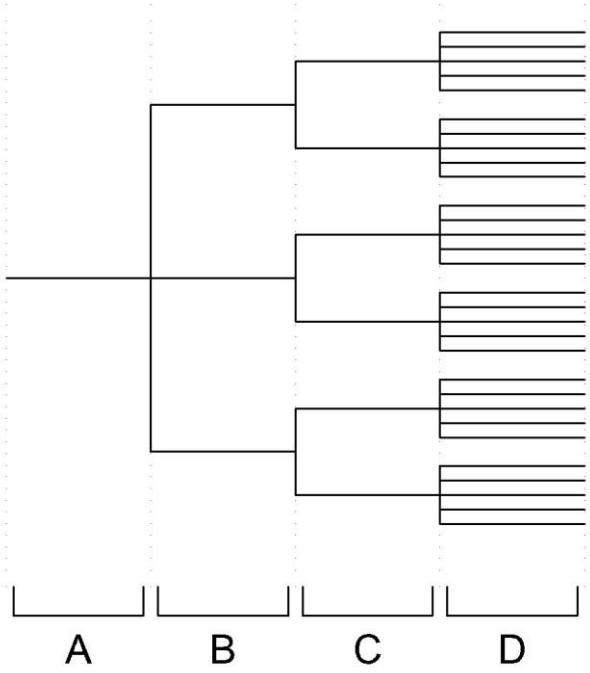

Figure 11 – A simplified scheme of a tree of energy with different levels

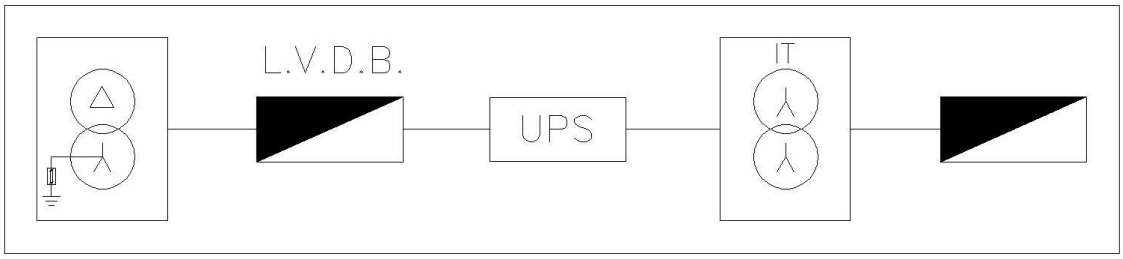

Figure 12 - An example of an arrangement of equipment through which the upstream downstream energy flow passes

Figure 11 demonstrates that a piece of equipment that is located in level C will be down-stream of the level A and B, therefore, the flow of energy needs to go first through these last levels. Figure 12, demonstrates an example of the components that are disposed in a power infra-structure of a building, showing the flow energy from the transformer to the power plug. The first component is the Transformer and is classified as Level A, the second is the LVDB (level B), the

third is the UPS (level B), the fourth is the Infrastructure Transformer (IT) (level C) and the last one is the Distribution Board (level C).

Table 3 will give a resume of the attributed values and the description of the levels will be as follows:

A. The first level (weight 1), will refer to components that are more upstream of the installation. In the case of the electrical installation, the components in question are those that supply energy to the installation, such as Extension of energy input in the building, Generator Group, Transformers; etc.
B. The second level (weight 0.57), refers to the components immediately following this first group: Low Voltage Distribution Board (LVDB); Uninterruptible Power System (UPS) etc.
C. The third level (weight 0.29), refers to Distribution Board's (DB), Isolation Transformers (IT), etc.;
D. Finally, the fourth level (weight 0.14) refers to the components downstream of the installation, namely: racks, lighting, outlets, etc.;

Table 5 - Weight and Degree of each Level

1st value: Level - Corresponds to the positioning of the equipment in the installation (where A is closer to the power source and D is farthest)				
Parameters	A	B	C	D
Weight of the Factor	1	0.57	0.29	0.14

3.2.1.2. Significance

Significance corresponds to the relevance of equipment previously defined by the company itself. The failure of certain equipment can jeopardize the continuity of its activity and it is important for the company that there is such a distinction between certain equipment to create a hierarchy of importance within a level so that it is possible to prioritize certain equipment to the detriment of others. The objective will be to create three levels with the following weights: 1 - 1st level; 2 - 2nd level; 3 - 3rd level. So, table 4 will give a resume of the attributed values and the description of the importance levels will be done as follows:

1. The first level (weight 1) will refer to components that are of major importance to the company and in which its failure is considered an Emergency since the service has been affected in its entirety. The company must make every effort to ensure that this type of equipment remains operable and usable;
2. The second level (weight 0.5) refers to equipment that is of great importance to the company and where its failure partially affects its activity. If they are not serviced quickly, they may jeopardize the normal functioning of the infrastructure or a part of it.
3. The third level (weight 0.25) refers to equipment that does not affect the normal activity of the company. These can be postponed indefinitely, as they do not jeopardize the normal functioning and safety of the infrastructure but must be resolved as soon as possible.

Table 6 - Weight and Degree of each Significance Level

2nd value: Significance - Corresponds to the importance of the equipment in the installation (where 1 is the most severe and 3 the least)			
Parameters	1	2	3
Weight of the Factor	1	0.5	0.25

3.2.1.3. Redundancy

The value of Redundancy considers the existence or otherwise of infrastructures or emergency systems that can maintain the normal operation of the infrastructure in case of need. Let us, therefore, consider the following 3 cases: No Redundancy (N); With Redundancy (N + 1); With Redundancy (2N), such that:

- N. No Redundancy (weight 1) refers to equipment and infrastructures that do not have any type of distress and where their failure can render unusable the equipment or infrastructure concerned and all those that are downstream of it. A fault in a piece of equipment that does not have any type of Redundancy and can be considered critical since this is the only distribution path of a certain service or component;
- N + 1. This type of Redundancy (weight 0.8) refers to equipment and infrastructures that have extra elements that can suppress an event or incident of equipment or component of the infrastructure. A fault in a piece of equipment will not be considered critical since there is more than one distribution path of a particular service or component, without prejudice to its normal operation;
- 2N. This type of Redundancy (weight 0.7) refers to equipment and infrastructures that exist in duplicate without being a single point of failure. In the event of an incident, a site or other type of service provided by an IT equipment will not be affected since the installation is prepared so that any of its components can be detached from the installation without affecting any service.

As it was previously done, the next table will give a resume of the attributed values.

Table 7 - Weight and Degree of each Redundancy Level

3rd value: Redundancy - Is there any Redundancy or Emergency?			
Parameters	N	N+1	2N
Weight of the Factor	1	0.8	0.7

3.2.1.3. Type of Failure

This value is important to characterize the urgency of a given failure within a piece of equipment, depending on the affected component. To do this, 3 levels of failure will be categorized as follows:

- Type 1 (weight 1) are faults that have left a piece of equipment or component inoperable and that may harm equipment and components downstream of it. The function desired by this equipment is not obtained, so the resolution of this problem must be urgent.
- Type 2 (weight 0.5) are faults that have caused serious damage, or which may create short term problems in the affected equipment or equipment downstream. There is a deviation outside the acceptable operating limits of equipment and the resolution of this problem should not be delayed for long.
- Type 3 (weight 0.25) are failures that did not affect equipment or components severely and that can be postponed since it does not compromise the normal functioning of this one and that they do not have an immediate and critical impact on its function.

Table 8 - Weight and Degree of each Type of Failure Level

4th Value: Type of Failure - Characterization of Importance and Urgency of a particular Failure			
Parameters	1	2	3
Weight of the Factor	1	0.5	0.25

3.2.2. Final Result (Risk Priority Number)

The Final Result, or Risk Priority Number (RPN), corresponds to the factor of each of the components that will serve as the differentiation element to classify the incidents in order of relevance. This number will emerge after a quantitative evaluation of all the factors previously considered and the main objective is to quantify all the events relative to their priority so that greater importance is given to the events with the highest RPN. To achieve this value, the used formula is:

$$RPN = L \times S \times R \times T \tag{13}$$

Where:

- $RPN =$ Risk Priority Number;
- $L =$ Level;
- $S =$ Significance;
- $R =$ Redundancy;
- $T =$ Type of Failure.

These results will be ordered according to a scale of five priorities and their value may determine the company's time of action concerning the event in question. The scale description will be done as follows:

- 1st - Emergency (weight between 0.58 and 1): This level will refer to events or incidents in which a failure, or lack of functioning, is considered an Urgency and should be treated with the greatest speed (in a matter of hours), since the normal functioning of the services may be in immediate danger. Failure or interruption may jeopardize the health, people' safety or damage to the building and may prevent the normal operation of all, or part of the infrastructure, or failures and interruptions in equipment downstream of the fault;

- 2nd - High (weight from 0.33 to 0.58): The second level refers to events or incidents that are of great importance to the company and which, if not taken care of quickly, can endanger the normal functioning of the infrastructure or a part of it, and it is, therefore, necessary that this type of situation be resolved in a short time (from 1 to 3 days);
- 3rd - Medium (weight from 0.17 to 0.33): This level refers to events that are important and not to be neglected. These can be completed within a longer period (15 days) if it does not cause abnormal functioning of the entire infrastructure, or part, or that endangers the safety of users;
- 4th - Low (weight 0.08 to 0.17): Refers to Work Orders that do not endanger the Infrastructure and the normal functioning of the building and that do not in any way compromise the safety of users. As a rule, this type of incident can be completed within a longer period (1 month), since the normal operation of the services will not be affected;
- 5th - Scheduled Maintenance (weight from 0 to 0.08): This level refers to events or incidents that can be delayed for a longer time (6 months) as they do not jeopardize normal operation and safety of infrastructure.

Table 9 - Range of each level of the final result

Colors: Gravity Level					
Parameters	5	4	3	2	1
Range of the Level	0% - 8%	8% - 17%	17% - 33%	33% - 58%	58% - 100%
Evaluation	Scheduled	Low	Medium	High	Emergency

3.2.3. The Resilience Quantification metric chosen (Ayyub, 2015)

The metric that was chosen to develop this model was presented in the article "Practical Resilience Metrics for Planning, Design and Decision Making" [26] and that was already analyzed in the chapter 2.2.5. It was decided to apply this metric as it was easy to understand not only at a development stage by an analyst or the developer but also at a future stage when anyone who has to use it in the business world and has never seen it can adapt to it and has the ability to improve it. It aims to achieve a final resilience value after an incident and takes into account the disruptive events occurred in the past, the length of time between the start of the incident and the final recovery time, the loss of resilience after a failure and other variables that will be further deepened forward.

3.2.3.1. Proposed Metrics and Variables

The formulas that will be used to obtain the final Resilience where already presented. However, it is important to realize that a minor change has been made to one of the formulas (5), which is taken into account in the article where it is located, and it is also important to describe how all the variables and values to be used in these formulas were calculated. Nonetheless the formulas and variables are as follows:

$$Resilience\ per\ Failure\ (R_f) = \frac{(t_r - t_i)(Q_{100} - Q_r)}{Q_{100}\, t} \quad (14)$$

$$Resilience\ (R_e) = 1 - \exp\left[-\lambda t\left(1 - p\overline{R_f}\right)\right] + \exp[-\lambda t] \quad (15)$$

Where:

- λ = The rate of a Poisson Process. A Poisson Process is a model for a series of discrete events where the average time between events is known but the exact timing of the events is random. The arrival of an event is independent of the event before, so, the waiting time between events is memoryless [36]. This point will be developed further;
- t = Planning Horizon;
- p = Probability of a failure;
- R_f = Resilience per Failure;
- $\overline{R_f}$ = Non-Resilience per Failure
- t_r = Time to recovery;
- t_i = Time of incident;
- Q_{100} = Capacity of the system;
- Q_r = Robustness of the system;

The following figure locates in a resilience triangle model some of the variables previously described.

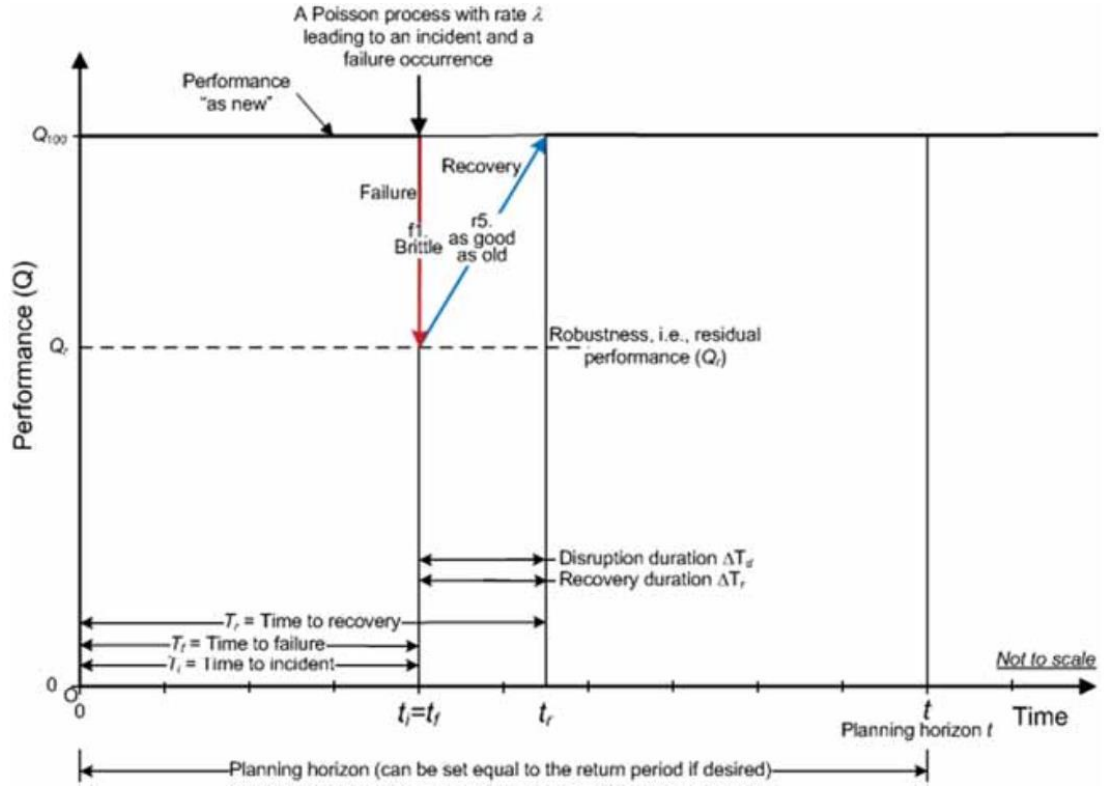

Figure 13 - Fundamental Resilience Case of Linear Recovery [26]

3.2.3.2. Variables and their characteristics

It is not only important to know what do the variables mean but it is also important to understand the way they were applied. Therefore, this section is going to be used to understand and explain how these values were obtained, besides the variable λ, which are going to be analyzed further.

- t - Planning Horizon;

The planning horizon considered in the resilience calculation was 1 year. The infrastructure in question has a useful life of approximately 40 years but to achieve a more tangible and not so infamous results, it was decided to consider the 1-year time horizon to be able to calculate a lost resilience value annually. Therefore, the value of t throughout the calculations will always be 1. However, it should be noted that other time periods could be considered.

- p - Probability of a failure;

This variable refers to the probability of a failure to happen. Considered that in the previous year 20 accidents happened, according to internal information, it makes sense to consider that the value of p is 1 since a disturbance is likely to occur in the future. However, if in the future that is not true, it is advised to recalculate that variable to obtain a more appropriate value given the current situation.

- R_f - Resilience per Failure;

Resilience per Failure refers to the area of the Resilience Triangle that was previously calculated. This area can be represented as the loss of functionality of the system. As it was mentioned before, the calculus of this value was slightly changed because while the previous case considers a linear recovery, it should be considered that when facing a step recovery, after the necessary repairs, the overall performance of the infrastructure returns to its previous value if aging effects are not taken into account by creating an area similar to the rectangle, such as the one presented in figure 14, rather than a triangle. So, in the denominator of formula (14), the value 2 must be removed, leaving it equal to $Q_{100}t$.

Figure 14 - A example of a Resilience Rectangle

- t_r , t_i - Time to recovery and Time of Incident;

These variables directly depend on the historical data of incidents that have occurred in this infrastructure. However, soon it was found that the historical data only contained the information regarding the day in which the event has occurred. Therefore, it will be considered that these values are referred to in days and to simplify the calculus and the insertion of data from the analyst, it will only be considered the difference between the time of the incident and the time to recover.

- Q_{100} = Capacity of the system;

This value refers to the initial capacity of the infrastructure, at which it can be assumed to be "as good as new", at 100%. To do so, let's assume that the value of this variable is 1.

- Q_r = Robustness of the system;

The Robustness of the system refers to the value that was previously calculated by the multiplication of the 4 factors of each component, or equipment, in chapter 3.2.1.

3.3. Failure Mode Tables

The creation of Failure Mode Tables arises from the need to give maintenance technicians and managers the ability to characterize, with a brief description, a maintenance event, fault or operation in a more concrete way so that in the future there will be the ability to analyze the entire historical data of a specific equipment or even an infrastructure. However, this work depends on a lot of research and fieldwork and according to [37] *" a clear understanding of the equipment's technical characteristics, its operating and environmental conditions, its potential failures and its maintenance activities"* to understand what are the possible faults in a piece of equipment since many faults and malfunctions, even being specific to equipment, may not happen since they are not in an environment that provides this specific occurrence. A uniform definition of failure and a method of classifying failures are essential when data from different sources (plants and operators) need to be combined in a common reliability and maintenance database. A common report for all equipment classes shall be used for reporting failure data.

Therefore, this work aims to:

- Create a table as straightforward as possible to leave out any doubts when reporting an event, but not too generic so that it will become too ambiguous in a future analysis;
- All components contained within must be equipment that must be properly classified in the Quantification Model;
- Every failure can have a small descriptive line with details about that failure.
- An equipment may have several failures and those failure may be common to various equipment. Common cause failures can be also considered common mode failures. Common mode failures can have different causes and common mode failures can also be common cause failures;
- All equipment and faults must have unique codes. A short range of codes may be too general to be useful. A long range of codes may give a more precise description but will slow the input process and may not be used fully by the data acquirer.
- It is also recommended that free text be included to provide supplementary information. A free-text field with additional information is also useful for quality control of data so that some detailed information may not be lost.

In recent times, greater emphasis has been placed on cost-effective design and maintenance for new and existing installations. Therefore, failure data, failure and maintenance mechanisms that are in any way related to industrial facilities have become very important and sharing this information between multiple companies or between different sectors of the same company can contribute to greater capacity of prevention or fault detection. So, it is important to have Reliability and Maintenance (RM) data, especially from critical equipment, in order to estimate the risk of hazards to people and the environment or to analyze system performance.

To better analyze and help in the decision-making moments it can be necessary to have data covering several years of operation in order to obtain a confident analysis. At the same time, it is essential that the causes of failures are clearly stated in order to prioritize and implement corrective actions that bring improvements, promoting bigger profits and bringing security in an enterprise.

4

Implementation

After understanding the factors of the incident's quantification model and understanding the chosen metric, it is necessary to implement it and adapt it to the infrastructure considering its characteristics. Therefore, this chapter will focus on the characteristics of the infrastructure, its past, and the importance of this infrastructure to the company. All the steps taken throughout the implementation of the Quantification Model will be presented and explained to bring clarity to this process. It will also test whether the sample of past events follows a Poisson process. This step is of utmost importance for this work. If it is not guaranteed that this is a Poisson process, it will not be possible to apply the chosen metric.

4.1. General characterization of the Building and its Power Installation

This work is going to be developed in a building that stores a Data Center. This building is currently of the utmost importance to the company responsible for it. It provides data storage and other internet services necessary not only to the company responsible for the building but also to third parties. Currently, there is a team responsible for the maintenance and management of the building, who makes all the decisions when an event happens or if a deeper intervention is required. There is another permanent surveillance team responsible for acting immediately if necessary. The company in question, having external customers, who would use this as Data Center to store information or to use other provided services, found that there was a need to improve both the power and HVAC supply conditions in order to maintain the correct functioning of all the systems. In the recent past, during a corrective maintenance action on UPS units, a malfunction has occurred that has jeopardized the exploitation of services by external customers. Differential faults have been detected in some UPS circuit breakers, and the sensitivities of said differential protection relays need to be adjusted. This all occurred after a maintenance action. As a result, redundancy has been lost in the Distribution Board fed through the power extension, increasing the risk of failures of a customer's mono powered circuits.

The Building is fed through the national power Grid in Medium Voltage (15 kV). It has three 1250 kVA transformers, which power their LVDB's. They all have a "Rescued Bus Bar"

and a “Normal Bus Bar”. All essential services are powered from the “Rescued Bus Bar”, being that the 3 existing UPS banks (600 kVA each) assure the uninterruptible power supplies to the data centers. All the existing services in the data center are bi fed (each Rack always receives power from two of the three existing Power Branch). The building also has three Emergency groups (one with 1000 kVA and 2 with 1250 kVA), to safeguard the rescued feeds. Nonetheless, as the building has been expanding over its lifetime, its power feeding characteristics give added complexity not only to the maintenance teams but also to possible future work and extensions.

So, through some documentation, it was possible to describe the following points:

- The building was built (and/or acquired for the holding company from a competing company) around 2001;
- In 2010 the building suffered an upgrade with the installation of an Emergency Group to support the existing one, and two emergency groups are now included in the complex, so that the second will be used as the safety to first one;
- In 2011, a new work was developed in order to accommodate the first Racks of a third-party company. A new Power and HVAC project was developed in order to make the previous installations into a 2N topology;
- In 2012, the new Auxiliary Services made major efforts to enhance 2N redundancy and add capacity to the existing data center, endowing it with a new Emergency Group, and new UPS, turning the entire data center into 2N to give the infrastructure the ability to provide uninterrupted power with the appropriate emergency relief infrastructures and critical HVAC infrastructures.

4.2. λ, The rate of a Poisson Process

This point comes as a deepen study of the metric proposed in chapter 3.2.3. Since obtaining the value of this variable is one of the most important points of the implementation process. This step is essential because if a Poisson process is not confirmed, it is not possible to apply this metric. It was, therefore, necessary to carry out a more in-depth study to see if this was the case and if it was possible to proceed accordingly.

To be able to verify that it is in fact a Poisson Process two rules must be obeyed:

- 1st step: The inverse of the standard deviation must be very close to the inverse of the mean of the data sample, as referred by [38];

$$\boldsymbol{\lambda} \approx \frac{1}{\sigma} \approx \frac{1}{\mu} \tag{16}$$

- 2nd step: The skewness of the sample must be very close to 2, as the reference [39] indicates.

So, the first step was to define the sample of events. Taking into account that reference [26] states *"Poisson process of stressors with an annual rate ($\boldsymbol{\lambda}$)"*(as shown in the next figure) and *“the planning horizon related to the stressor rate as $t = 1/\boldsymbol{\lambda}$"*, the first step was to determine if there was a certain degree of agreement between the sample of events.

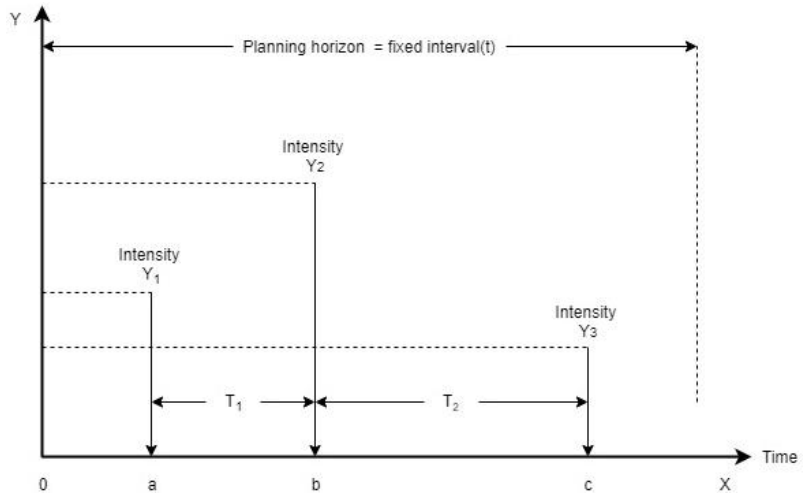

Figure 15 - Poisson process of a stressor with varied intensity. Based on a figure present in Ayyub, 2015. [26]

Therefore, all the events and the dates on which they occurred were gathered. Then, all events were sorted by occurrence date and the Δt value for the number of days between each occurrence was calculated. This Δt value will serve as the sample of events. In the next table, the variation between events and the dates in which they occurred are going to be displayed. The Δt values presented are in days.

Table 10 - Table with the events and the dates in which they occurred

Events	Date of Occurrence	ΔT between Events
1	16/11/2017	214
2	18/06/2018	4
3	22/06/2018	1
4	23/06/2018	3
5	26/06/2018	1
6	27/06/2018	15
7	12/07/2018	12
8	24/07/2018	12
9	05/08/2018	30
10	04/09/2018	2
11	06/09/2018	41
12	17/10/2018	13
13	30/10/2018	3
14	02/11/2018	38
15	10/12/2018	1
16	11/12/2018	6
17	17/12/2018	18
18	04/01/2019	5
19	09/01/2019	12
20	21/01/2019	57
21	19/03/2019	0

One of the values that quickly stood out was the fact that the first Δt value was noncompliant with the other Δt's. Still, the standard deviation and the mean values were calculated in order to check if the first step previously noted was valid. Unfortunately, that didn't happen, and the differences were so big that it made sense to check if there was some problem with the sample.

Therefore, the percentiles of normal distribution were calculated to find out if it made any sense to include that event in the data sample. Considering the fact that the value 214 is way beyond the 9995th percentile, it makes sense to exclude this event from the sample, as shown in the table below.

Table 11 - Percentiles from the sample of events

Percentile	
0,75	18
0,8	30
0,9	41
0,95	57
0,99	182.6
0,995	198.3
0,9995	212.43
0,99999	213.9686
0,999999	213.9969
0,9999999	213.9997

So, after removing the first event of the sample, new values of standard deviation and mean were calculated, and the results were much more adjusted to what it was pretended. And considering that the mean and standard deviation were approximately 0.069 and 0.064, respectively, as table 10 shows, it was assumed that they were very close and a delta value of 0.07 was taken as a good fit for the intended value.

Table 12 - Final values of Mean and Standard Deviation

Mean	14.42105
Standard Deviation	15.51677
λ (Mean)	0.069343
λ (Standard Deviation)	0.064446

After ensuring that the sample was already within the intended parameters, the next step was to calculate the delta's skewness of the events. To do it, the Excel function SKEW that obeys the following formula was used:

$$\frac{n\sum_{i=1}^{n}(x_i-\bar{x})^3}{(n-1)(n-2)s^3} \quad (17)$$

Where, according to [40]:

- n = The number of samples in the data set;
- x_i = Is a random variable of a data set;
- $\bar{x}$ = The mean of the data set;
- s = The standard deviation of the data set;

Skewness is a measure of symmetry of a determined data set or sample that may imply that the mean, the median, and the mode are not equal to each other. When these values are not the same, it is likely that some level of skewness is present in the analyzed data set.

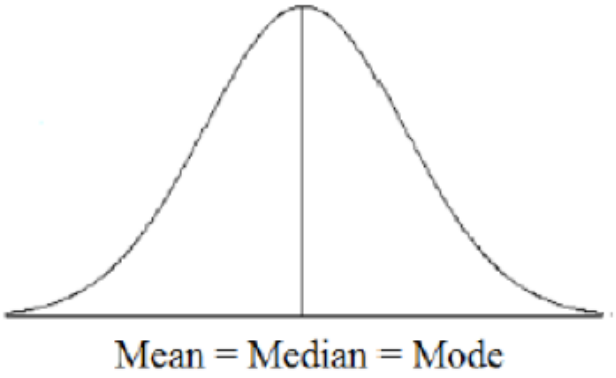

Figure 16 - Example of a normal distribution where the mean, the mode and the median are equal [2]

While the previous image shows a normal distribution in which the mean, the median, and the mode are equal, therefore creating a symmetric graph, a distribution that has a determined skewness may present a graph that may have a long tail pointing to the left (negative skew) or a long tail pointing to the right (positive skew).

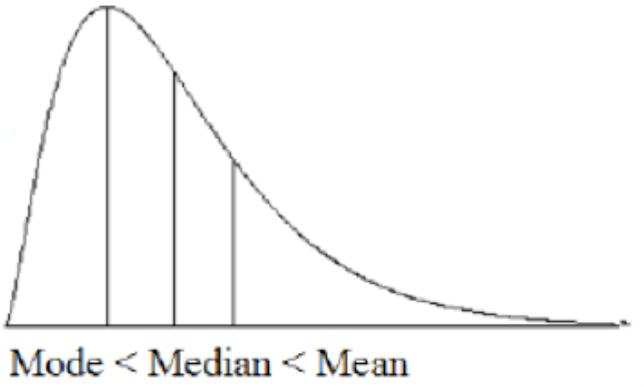

Figure 17 - Example of a data Sample that is positively skewed [3]

The value of the skewness is 1.549617 which means that the data sample is positively skewed. That shows that there are a bigger amount of smaller values than larger and that the mean is bigger than the median and the median is bigger than the mode, as table 13 shows, confirming what is being displayed in a previous image (Figure 17).[41]

Table 13 - Table with the calculated values of the mean, median and mode

Mean	14.42105
Median	12
Mode	1

[2] Image taken from: https://excel2007master.files.wordpress.com/2014/01/norm_dist.png
[3] Image taken from: https://excel2007master.files.wordpress.com/2014/01/positive.png

The value of the skewness may indicate that this process is not exactly a Poisson Process and that it's a bit of a "forced step" which may indicate that the data set may be not exactly exponential. Also, having a discrete sample instead of a continuous one may not help to achieve what is needed.

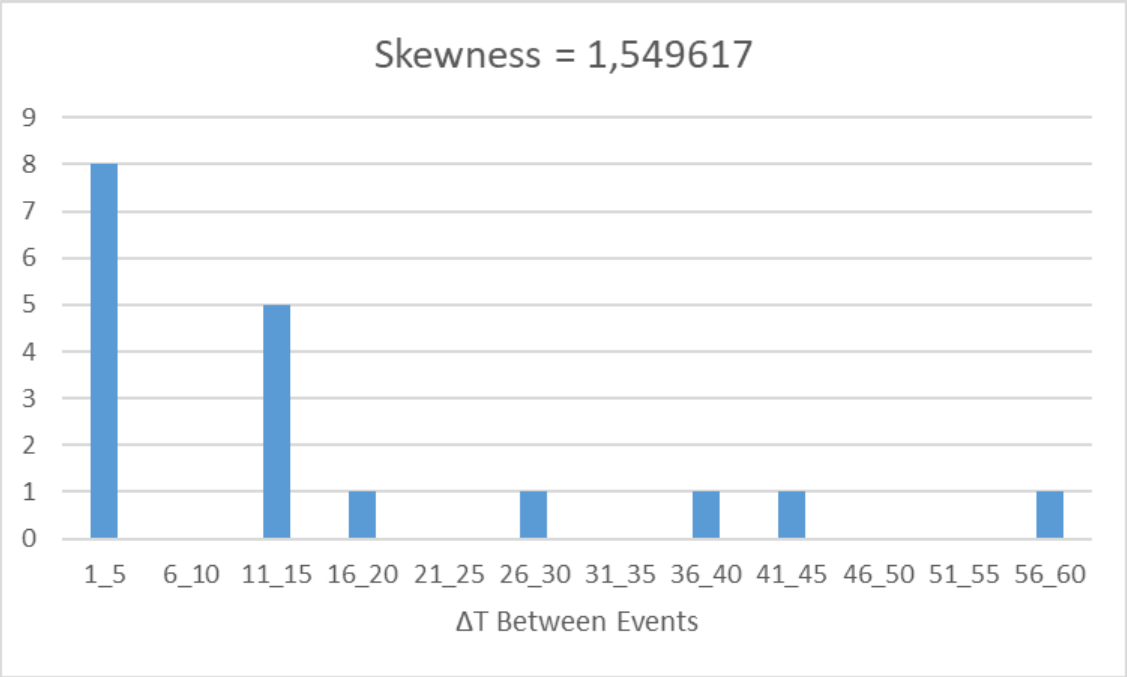

Figure 18 - Histogram of the Data Set

In the previous histogram, the X-axis contains the data divided into multiple groups with the same range and the Y-axis has the number of variables contained in a range (the number of values contained between 1 and 5, 6 and 10 etc.).The previous histogram also shows that the range of values is very dispersed. This can be caused by reporting failures made in the past.

A bigger number of events, therefore a bigger data sample, would probably contribute to a better value of skewness and would probably originate a graph more similar to the one present in figure 14. However, these values do not negate the possibility of not being in front of a Poisson Process, therefore, it was necessary to make a final test to reach a safer conclusion. So, the next step was to make a Kolmogorov-Smirnoff Test.

According to [42], *"The Kolmogorov-Smirnov one-sample test is a test of goodness of fit"*, which means that it is related with the degree of agreement between the distribution of a set of sample values (observed scores) and some specified theoretical distribution. It determines whether the scores in a sample can reasonably be presumed to derive from a population having a theoretical distribution.

Briefly, the test involves specifying the cumulative frequency distribution which would occur under the theoretical distribution and comparing that with the observed cumulative frequency distribution. The theoretical distribution represents what would be expected under H_0 (The null hypothesis). In this case:

- $H_0 =$ The data set follows an exponential distribution with rate $\boldsymbol{\lambda = 0,07;}$
- $H_1 =$ The data set does not follow an exponential distribution.

The point at which these two distributions, theoretical and observed, show the greatest divergence is determined. Reference to the sampling distribution indicates whether such a large divergence is likely on the basis of chance, so, the sampling distribution indicates whether divergence of the observed magnitude would probably occur if the observations were really a random sample from the theoretical distribution.

The Kolmogorov-Smirnov one-sample test treats individual observations separately, thus not losing any information throughout the combining of categories. When samples are small, the Kolmogorov-Smirnov test is applicable and may be more powerful than some of its alternatives.

This test focuses on the largest of the deviations between $F_0(x) - S_N(x)$, referring it as the maximum deviation. To reach this value, it is necessary to sort the sample values in ascending order (from the lowest value to the highest). And to reach the value of maximum deviation, the necessary formula is:

$$D = max|F_0(x) - S_N(x)| \tag{18}$$

Where:

- D = Maximum Deviation;
- $F_0(x)$ = It is a completely specified cumulative distribution function. That is, for any value of X, the value of $F_0(x)$ is the proportion of cases expected to have scores equal to or less than X. To reach to the expected value, the next formula will be used:

$$F_0(x) = 1 - e^{(-\lambda X_x)} \tag{19}$$

This is a cumulative distribution function of an exponential distribution, where:

  - λ = The delta value previously calculated, equal to 0,07, as stated in the null hypothesis.
  - X_x = The corresponding value of the data sample.
- $S_N(x)$ = It is the observed cumulative frequency distribution of a random sample of N observations. The formula is:

$$S_N(x) = \frac{N_x}{N_{max}} \tag{20}$$

Where:

  - N_x = is the number of observations equal to or less than X;
  - $N_{maximum}$ = The number of observations.

Table 14 - Calculated values from the Kolmogorov-Smirnoff Test

N_x	X_x	$S_N(x)$	$F_N(x)$	$\lvert F_N(x) - S_{N-1}(x)\rvert$	$\lvert F_N(x) - S_N(x)\rvert$
1	1	0.01754386	0.06760618	0.06760618	0.050062
2	1	0.035087719	0.06760618	0.05006232	0.032518
3	1	0.052631579	0.06760618	0.032518461	0.014975
4	2	0.070175439	0.130641765	0.078010186	0.060466
5	3	0.087719298	0.189415754	0.119240315	0.101696
6	3	0.105263158	0.189415754	0.101696456	0.084153
7	4	0.122807018	0.244216259	0.138953101	0.121409
8	5	0.140350877	0.29531191	0.172504893	0.154961
9	6	0.157894737	0.34295318	0.202602303	0.185058
10	12	0.175438596	0.568289477	0.41039474	0.392851
11	12	0.192982456	0.568289477	0.39285088	0.375307
12	12	0.210526316	0.568289477	0.37530702	0.357763
13	13	0.228070175	0.597475776	0.38694946	0.369406
14	15	0.245614035	0.650062251	0.421992075	0.404448
15	18	0.263157895	0.716345974	0.470731938	0.453188
16	30	0.280701754	0.877543572	0.614385677	0.596842
17	38	0.298245614	0.930051778	0.649350024	0.631806
18	41	0.315789474	0.943301073	0.645055459	0.627512
19	57	0.333333333	0.981500286	0.665710812	0.648167

After obtaining all the values for the maximum deviation, D, it is concluded that the maximum value calculated is 0,665710812. Next, a Kolmogorov-Smirnov table will be created to find out whether or not to reject the Data Sample.

So, for $N = 19$ and with an $\alpha = 0.01$ a critical value of 0,36117 is obtained, as shown in table 15, and considering that the used λ is 0,07 (a smaller α guarantees a smaller critical value for the sample N), it is possible to conclude that the data sample passes the Kolmogorov-Smirnoff

test, validating the value of λ. Since the test has not rejected the hypothesis of being an exponential distribution, with the λ presented above, and being a Poisson process, it is, therefore, possible to apply this metric in this project.

Table 15 - Critical Value of the maximum absolute difference between sample Fn(x) and population F(x) [43]

Number of trials, *n*	Level of significance, α			
	0.10	0.05	0.02	0.01
1	0.95000	0.97500	0.99000	0.99500
2	0.77639	0.84189	0.90000	0.92929
3	0.63604	0.70760	0.78456	0.82900
4	0.56522	0.62394	0.68887	0.73424
5	0.50945	0.56328	0.62718	0.66853
6	0.46799	0.51926	0.57741	0.61661
7	0.43607	0.48342	0.53844	0.57581
8	0.40962	0.45427	0.50654	0.54179
9	0.38746	0.43001	0.47960	0.51332
10	0.36866	0.40925	0.45662	0.48893
11	0.35242	0.39122	0.43670	0.46770
12	0.33815	0.37543	0.41918	0.44905
13	0.32549	0.36143	0.40362	0.43247
14	0.31417	0.34890	0.38970	0.41762
15	0.30397	0.33760	0.37713	0.40420
16	0.29472	0.32733	0.36571	0.39201
17	0.28627	0.31796	0.35528	0.38086
18	0.27851	0.30936	0.34569	0.37062
19	0.27136	0.30143	0.33685	0.36117
20	0.26473	0.29408	0.32866	0.35241
21	0.25858	0.28724	0.32104	0.34427
22	0.25283	0.28087	0.31394	0.33666
23	0.24746	0.27490	0.30728	0.32954
24	0.24242	0.26931	0.30104	0.32286

4.3. Characterization of each component

After concluding that this metric would be applicable, it was necessary to start to identify which were the components that needed to be classified in order to evaluate their impact in the main infrastructure. To do that, it was necessary to resort to the company's internal information system that contained all existing components in all of the companies' infrastructures. However, only components existing in this building are going to be classified in order to obtain a final Risk Priority Number.

At the time the characterization process had started, it was clear that some components had variables, which were of almost automatic classification, such as the Level and Redundancy considering that their position in the infrastructure and their redundancies were known. However, the Importance and the Type of Failure factors were not straightforward. So, it was important to find a way of comparing every single result of every component in order to get to an RPN that was compliant with to the intended purpose. The found solution was to create a fully automatic Excel file that had the ability to change the values of the variable weights and their degrees of importance, as demonstrated in chapter 3.2.1., so that a small adjustment applies to all modifications,

making it easier for those analyzing and comparing the results to have the possibility of later adjusting these values if needed.

It was also necessary to characterize the components in types of equipment that were considered essential and that could easily distinguish every component in a category that is considered essential to the company. Therefore, a component was characterized in one of four types of equipment:

- Energy: This category refers to all the essential components that ensure a proper and a continuous flow of energy in the building, and some of its emergencies, to ensure that there are no faults. For example, the Generator, Power Transformer, UPS and LVDB.
- HVAC: This category refers to all the components that assure the correct climatization of the building including fans and heaters, chillers, water deposits, fans and boilers
- Emergency: This category refers to essential components and systems of protection to the building, including the fire detection system, fire extinguishers, alarming systems, and distribution boards only dedicated to this type of systems.
- Others: This category refers to components or areas that were important to classify but were not fit to enter in one of the aforementioned categories.

So, after getting the list of every component and categorizing it with the previously described types of equipment, the next step was to ordinate every component in a list which would demonstrate every component and their evaluation in order to compare them. By doing this, it is possible to compare every component and evaluate if the obtained RPN value is consistent with what it is intended to achieve. All the classifications attributed to every component will be done according to the described in chapter 3.2.1.

Table 16 - Table with the attributed values of each variable

Data Center					
Type of Equipment	**Equipment**	**Failure Mode**	**Level**	**Significance**	**Redundancy**
Energy	Disconnector	Disconnector	A	1	N
Energy	Generator	Generator	A	1	2N
Energy	Transformer	Transformer	A	1	2N
Energy	LVDB	LVDB	B	1	2N
Energy	UPS	UPS	B	1	2N
Energy	Rectifier	Rectifier	B	1	2N
Energy	UPS's DB	Distribution Boards	B	1	2N
Energy	DB	Distribution Boards	B	1	2N
Energy	Diesel Storage Tanks	Storage Tanks	B	2	N
Energy	Battery Cabinets	Battery Cabinets	B	2	2N
Energy	Isolation Transformer	Transformer	C	1	N
Energy	Power Plugs	Power Plugs	D	3	N

Table 17 - The Resulting RPN from each component

Data Center		Type of Failure: 1		
Type of Equipment	Equipment	RPN - Type 1	IGS - Type 1	Priority - Type 1
Energy	Disconnector	70.00%	30.00%	1
Energy	Generator	70.00%	30.00%	1
Energy	Transformer	70.00%	30.00%	1
Energy	LVDB	39.90%	60.10%	2
Energy	UPS	39.90%	60.10%	2
Energy	Rectifier	39.90%	60.10%	2
Energy	UPS's DB	39.90%	60.10%	2
Energy	DB	29.00%	71.00%	3
Energy	Diesel Storage Tanks	28.50%	71.50%	3
Energy	Battery Cabinets	28.50%	71.50%	3
Energy	Isolation Transformer	29.00%	71.00%	3
Energy	Power Plugs	3.50%	96.50%	5

Tables 16 and 17 show what is intended in this part of the paper, to have a list of all characterized equipment and their respective RPNs in order to find possible inconsistencies. These tables also demonstrate that a component of the infrastructure from a lower Level can be more important than a component from a higher one, with the examples of the Isolation Transformer and the Battery Cabinets: the Isolation Transformer is classified as C in the level factor and has a higher RPN than the Battery Cabinets (classified as B in that category), meaning that it is possible to have a lower level on one of the 4 factors and a higher RPN. It is important to state that all the components categorized in that list belong to the same *"Type of Equipment"* and the same Failure Mode can be common to various equipment.

It is also important to mention the relevance that the Infrastructure's General State (IGS) has for this process. This value is essential to calculate the loss of resilience with the metric described in chapter 3.2.3.1., corresponding to the variable Q_r (Robustness of the system). With this value, it is possible to have a clearer view of the importance of the impacted component on the infrastructure and the company. To reach this value, one must simply subtract the RPN value from 100%, thus obtaining the supposed loss of robustness caused by the loss of this equipment in the analyzed infrastructure:

$$1 - RPN = IGS \tag{21}$$

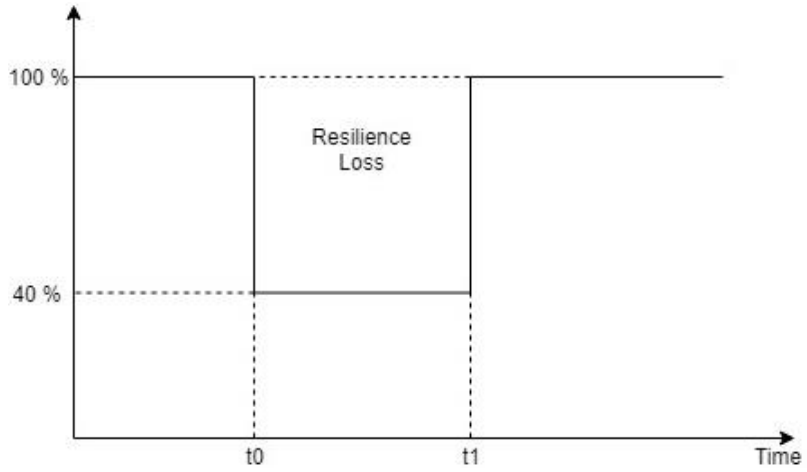

Figure 19 - The Infrastructure's General State after a type 1 failure of the Generator

4.3.1. Type of Failure

It was also relevant to analyze the impact of the Type of Failure's factor to the RPN. It is crucial to understand if this factor has the ability to distinctly change the RPN value in order to prioritize the urgency of a given failure, depending on the affected component. For example, Table 16 clearly shows that a Type 3 failure in a Diesel Storage Tank becomes less important than a Type 1 failure in a UPS.

This type of classification is what is intended to achieve, since in this way it is possible to act more accordingly to the real impact of the event, or a set of them, and therefore allowing the technicians to make a more appropriate decision. Also, the obtained result, for the purposes of statistical analysis, becomes more favorable as the impact on the resilience of a Type 1 event is considerably more destructive than a Type 2 event.

Table 18 - The impact of the Type of Failure factor in the RPN

Data Center	Type of Failure: 1		Type of Failure: 2		Type of Failure: 3	
Equipment	IGS - Type 1	Priority - Type 1	IGS - Type 2	Priority - Type 2	IGS - Type 3	Priority - Type 3
Disconnector	30.00%	1	65.00%	2	82.50%	3
Generator	30.00%	1	65.00%	2	82.50%	3
Transformer	30.00%	1	65.00%	2	82.50%	3
LVDB	60.10%	2	80.05%	3	90.03%	4
UPS	60.10%	2	80.05%	3	90.03%	4
Rectifier	60.10%	2	80.05%	3	90.03%	4
UPS's DB	60.10%	2	80.05%	3	90.03%	4
DB	71.00%	3	85.50%	4	92.75%	5
Diesel Storage Tanks	71.50%	3	85.75%	4	92.88%	5
Battery Cabinets	71.50%	3	85.75%	4	92.88%	5
Isolation Transformer	71.00%	3	85.50%	4	92.75%	5
Power Plugs	96.50%	5	98.25%	5	99.13%	5

4.3.2. Calibration

As a way to manage the obtained results, it was necessary to proceed to some type of calibration, regardless of their accuracy and safeness. The first step was to comprehend if the multiplications of every factor of equipment made sense not only to the managers responsible for taking care of the facility but also to the technicians responsible for making the initial reports and applying the necessary resolutions mandated by the responsible managers. It was also necessary to understand if the obtained RPN defined a priority type appropriated to the type of equipment and the type of failure in question.

Therefore, to try to understand what those results would be, an analysis was executed to all of those values by performing all possible multiplications in order to understand if the results obtained created a wide enough range that was feasible to the expected finality. So, the multiplications were made by the following order, and some of those will be presented in tables 19 and 20. The remaining tables, and some auxiliary tables, will be shown in Annex A and the colors used in these tables match those described in chapter 3.2.2. and in table 9.

$$Level\ (L) \times Significance\ (S) = LS_{values} \tag{22}$$

$$LS_{values} \times Redundancy\ (R) = LSR_{values} \tag{23}$$

$$LSR_{values} \times Type\ of\ Failure = All\ possible\ RPN\ values \tag{24}$$

After this calibration and to try to understand if the obtained results would be adequate to what was intended, *RapidMiner* software was used.

RapidMiner is a Data Science software that provides an integrated environment for data preparation, machine learning, and predictive analytics that can support every step of the machine learning process. However, for it to be able to do this kind of analysis, it would require at least 100 lines (where each line would correspond to 1 component) and the final list of components had only 63. Considering that the use of this software was inconclusive, it was therefore decided to discard its use.

Table 19 - The Possible Results of Multiplying every value of the Level by every Significance value

1st value: Level		2nd value: Significance		
		1	2	3
		1	0.5	0.25
A	1	1	0.5	0.25
B	0.57	0.57	0.285	0.1425
C	0.29	0.29	0.145	0.0725
D	0.14	0.14	0.07	0.035

Table 20 - The Possible Results of Multiplying every value of the Level, Significance, Redundancy and Type of Failure

Level × Redundancy × Significance	4º value: Types of Failure		
	1	2	3
	1	0.5	0.25
1	1	0.5	0.25
0.8	0.8	0.4	0.2
0.7	0.7	0.35	0.175
0.57	0.57	0.285	0.1425
0.5	0.5	0.25	0.125
0.456	0.456	0.228	0.114
0.4	0.4	0.2	0.1
0.399	0.399	0.1995	0.09975
0.35	0.35	0.175	0.0875
0.29	0.29	0.145	0.0725
0.285	0.285	0.1425	0.07125
0.25	0.25	0.125	0.0625
0.232	0.232	0.116	0.058
0.228	0.228	0.114	0.057
0.203	0.203	0.1015	0.05075
0.2	0.2	0.1	0.05
0.1995	0.1995	0.09975	0.049875
0.175	0.175	0.0875	0.04375
0.145	0.145	0.0725	0.03625
0.1425	0.1425	0.07125	0.035625
0.14	0.14	0.07	0.035
0.116	0.116	0.058	0.029
0.114	0.114	0.057	0.0285
0.112	0.112	0.056	0.028
0.1015	0.1015	0.05075	0.025375
0.09975	0.09975	0.049875	0.0249375
0.098	0.098	0.049	0.0245
0.0725	0.0725	0.03625	0.018125
0.07	0.07	0.035	0.0175
0.058	0.058	0.029	0.0145
0.056	0.056	0.028	0.014
0.05075	0.05075	0.025375	0.0126875
0.049	0.049	0.0245	0.01225
0.035	0.035	0.0175	0.00875
0.028	0.028	0.014	0.007
0.0245	0.0245	0.01225	0.006125

4.4. Failure Modes Table

To create the Failure Modes Table, it was necessary to resort to documents and files that already had some information about the previously characterized components. Although some files were in no way related to the concerned infrastructure (documents [44] and [37] are related to petrochemical infrastructures and references [45] and [46] provided important information related to HVAC components), they contained essential information for the final table. Some information was also requested to entities, responsible for supplying or providing maintenance to the component, to provide as much information as possible in order to build a tool that would be useful to the entire final system.

After gathering all this information, it was necessary to create tables for each component previously analyzed, with the possible flaws and some of their details. It was easily realized that there were failures common to several components and other quite similar that could be combined.

After making all these combinations and completing the tables of each of the components, the final table was created. In order for it to be easily understood, it was intended to be as straightforward as possible so as not to raise doubts in the reporting process of an event, such as was previously described in chapter 3.3. Whenever possible, a short line with details of the fault was added, when it was thought that a short description could help clarify any doubts when classifying a possible failure. The final table was left with about 90 possible failure modes and all faults and equipment each having unique codes.

So, in order to better understand the final table, it is important to leave some helpful notes, and thus, in order to better understand the created table. Therefore:

- Nº of implications per failure – Number of components where this fault can be found;
- Failure Mode code - A unique code for each failure mode;
- Description - Brief description about the detected problem;
- Details - Brief description with some details of the failure that can help in the reporting phase of the event and to clarify a possible doubt;
- Equipment class code - A unique code for each of the equipment.

This table is a continuous work and requires frequent update so that future events are more accurately characterized. By heavily recurring to this table, not only in an event occurred in the analyzed infrastructure but also on new infrastructures with other management teams, it is possible to improve it with better and safer information that could be obtained in the reporting processes of those events. A complete table will be shown in Annex C.

Table 21 - Example of Failure Modes tables extracted from [37] [4]

ISO-14224-2016					
		Equipment class code	**CE**	**CO**	**EG**
Failure mode code	**Description**	**Examples**	**Combustion engines**	**Compressors**	**Electric Generators**
AIR	Abnormal instrument reading	False alarm, faulty instrument indication	X	X	X
BRD	Breakdown	Serious damage (seizure, breakage)	X	X	X
ERO	Erratic output	Oscillating, hunting, instability	X	X	
ELF	External leakage - fuel	External leakage of supplied fuel/gas	X		
ELP	External leakage - process medium	Oil, gas, condensate, water		X	
ELU	External leakage – utility medium	Lubricant, cooling water	X	X	X
FTS	Failure to start on demand	Doesn't start on demand	X	X	X
HIO	High output	Overspeed/output above acceptance	X	X	
INL	Internal leakage	Leakage internally of process or utility fluids	X	X	
LOO	Low output	Delivery/output below acceptance	X	X	X
NOI	Noise	Abnormal noise	X	X	X
OHE	Overheating	Machine parts, exhaust, cooling water	X	X	X
PDE	Parameter deviation	Monitored parameter exceeding limits, e.g. high/low alarm	X	X	X
PLU	Plugged/ choked	Flow restriction(s)	X	X	
SER	Minor in-service problems	Loose items, discoloration, dirt	X	X	X
STD	Structural deficiency	Material damages (cracks, wear, fracture, corrosion)	X	X	X
STP	Failure to stop on demand	Doesn't stop on demand	X	X	X
OTH	Other	Failure modes not covered above	X	X	X
UNK	Unknown	Too little information to define a failure mode	X	X	X
UST	Spurious stop	Unexpected shutdown	X	X	X
VIB	Vibration	Abnormal vibration	X	X	X

[4] This table was extracted from [37], table B.6, page 187. This table is not complete and does not have all the components with their respective failure modes from the original table

Table 22 - Sample of the final Failure Modes Table [5]

				Energy		
			Equipment Class Code	GER	COMP	ELEM
Nº of implications per failure	Failure mode code	Description	Details	Generators	Compressors	Electrical Motors
20	ALAR	Alarm / Parameter Deviation	Monitored parameters exceeding tolerances. Ex: Default Alarm	X	X	X
14	DPF	Downstream Power Failure	Equipment Power Failure, Power Outlets failure etc.	X		
1	FREG	Failure to Regulate	Valve Stuck / Control Valves Only			
16	FSD	Failure to start on demand	Does not start or open after order or failed to respond to signal/activation	X	X	X
2	FSD	Failure to start on demand	Protection device/circuit breaker/switch fails after a circuit fault			
3	FFAI	Fuel Failure	Missing or Unusable Fuel	X		
2	GFAI	Gas Failure	Gas Failure			
1	NETF	Internet Network Failure	Temporary or permanent Inoperable Internet Network			
1	MUDA	Mud accumulation	Mud accumulation			
2	SINF	Synchronization Failed	Unable to synchronize the generator	X		
13	UPF	Upstream Power Failure	Failure in Energy Supply	X		
3	WATF	Water Failure	Missing or Unusable water			
0	SENSF	Sensor failure	Sensor, camera or similar equipment malfunction			
0	DBAT	Damaged Battery	Inoperative Battery or Low Capacity			
0	STOP	Locked / Stop	Component unable to function, locked or jammed			
3	UNK	Other / Unknown	Failure modes not specified, too little information to set a failure mode, Specify in comment field	X	X	X

[5] This table is not complete and does not have all the components with their respective failure modes. The complete one is displayed in Annex C.

5

Results Analysis

After ensuring that it is possible to apply the chosen metric to the infrastructure and after characterizing all the components, according to the factors previously described in the development chapter, the final phase would have to be the Results Analysis. This chapter aims to calculate the final resilience values of the events that have occurred and other random events for test effects. The final values are going to be displayed and discussed in order to understand if they match the intended results. All the necessary details will be presented to clarify possible doubts and to bring clarity to this process.

5.1. Calculus of the final Resilience Values

Since all the values obtained were already close to what would be expected, the Resilience loss caused by the impact of each of the failures in the last year was calculated. To make this possible, it was necessary to identify which component was affected by each event and the time that elapsed between the beginning of the event and the end of it. A new list was created to analyze all the necessary information and to try to comprehend the impact of that event considering his characteristics.

So, table 23 will show the calculated resilience losses after each event. Some information about each event (as the ratings assigned to each of the factors of the component affected by the event) will be put aside to respect company's policies. The last line will show the final results with two type of results to be compared. The first results will recur to the applied metric (with the Poisson Process) and the others do not consider the Poisson Process and the planning horizon. Those results obey to the next formulas:

$$Resilience\ per\ Failure\ (R_f) = \frac{(t_r - t_i)(Q_{100} - Q_r)}{2Q_{100}t} \tag{25}$$

$$Resilience\ (R_e) = 1 - \exp\left[-\lambda t\left(1 - p\overline{R_f}\right)\right] + \exp[-\lambda t] \tag{26}$$

Table 23 - Final Resilience values from the failure events occurred in a year

						With Poisson Process			Without Poisson Process		
No	RPN	IGS	P	Δ_{Time}	$\overline{R_f}$	CR_1	LR_1	$CombR_1$	CR_2	LR_2	$CombR_2$
June 2018											
1	0.232	0.768	3	1	0.00064	0.99996	0.00004	0.99996	0.99977	0.00023	0.99977
2	0.232	0.768	3	3	0.00191	0.99988	0.00012	0.99983	0.99930	0.00070	0.99906
3	0.232	0.768	3	2	0.00127	0.99992	0.00008	0.99975	0.99953	0.00047	0.99860
4	0.232	0.768	3	1	0.00064	0.99996	0.00004	0.99971	0.99977	0.00023	0.99836
5	0.098	0.902	4	1	0.00027	0.99998	0.00002	0.99969	0.99990	0.00010	0.99826
			Total	8	0.00472		0.00031	0.99969		0.00174	0.99826
July 2018											
6	0.07	0.93	5	1	0.00019	0.99999	0.00001	0.99968	0.99993	0.00007	0.99819
7	0.399	0.601	2	1	0.00109	0.99993	0.00007	0.99961	0.99960	0.00040	0.99779
			Total	2	0.00128		0.00008	0.99961		0.00047	0.99779
August 2018											
8	0.232	0.768	3	1	0.00064	0.99996	0.00004	0.99957	0.99977	0.00023	0.99756
			Total	1	0.00064		0.00004	0.99957		0.00023	0.99756
September 2018											
9	0.57	0.43	2	5	0.00781	0.99949	0.00051	0.99906	0.99712	0.00288	0.99467
10	0.399	0.601	2	1	0.00109	0.99993	0.00007	0.99899	0.99960	0.00040	0.99427
			Total	6	0.00890		0.00058	0.99899		0.00329	0.99427
October 2018											
11	0.29	0.71	3	10	0.00795	0.99948	0.00052	0.99847	0.99707	0.00293	0.99134
12	0.7	0.3	1	1	0.00192	0.99987	0.00013	0.99834	0.99929	0.00071	0.99063
			Total	11	0.00986		0.00064	0.99834		0.00364	0.99063
November 2018											
13	0.399	0.601	2	1	0.00109	0.99993	0.00007	0.99827	0.99960	0.00040	0.99023
			Total	1	0.00109		0.00007	0.99827		0.00040	0.99023
December 2018											
14	0.399	0.601	2	5	0.00547	0.99964	0.00036	0.99791	0.99798	0.00202	0.98821
15	0.035	0.965	5	1	0.00010	0.99999	0.00001	0.99791	0.99996	0.00004	0.98818
16	0.57	0.43	2	5	0.00781	0.99949	0.00051	0.99740	0.99712	0.00288	0.98529
			Total	11	0.01337		0.00087	0.99740		0.00494	0.98529
From January to March 2019											
17	0.232	0.768	3	1	0.00064	0.99996	0.00004	0.99736	0.99977	0.00023	0.98509
18	0.232	0.768	3	10	0.00636	0.99959	0.00041	0.99695	0.99765	0.00235	0.98275
19	0.399	0.601	2	30	0.03279	0.99786	0.00214	0.99480	0.98774	0.01226	0.97048
			Total	41	0.03979		0.00260	0.99480		0.01484	0.97048
March 2019											
20	0.7	0.3	1	2	0.00384	0.99975	0.00025	0.99455	0.99859	0.00141	0.96907
			Total	2	0.00384		0.00025	0.99455		0.00141	0.96907
Final Results											
			Total	83	8%		0.545%	99.455%		3.097%	96.903%

In this table, the following acronyms represent:

- No = Corresponds to the occurrence and order by which them occurred;
- RPN = Risk Priority Number;
- IGS = Infrastructure's General State;
- P = Priority;
- $\Delta_{Time}=$ Corresponds to the time occurred between the beginning of the event and the end of it $(t_r - t_i)$;
- $\overline{R_f}$ = Non-Resilience per Failure;
- CR_x = The Calculated Resilience obtained by formulas (25) and (26), which are the same as formulas (5) and (6). It corresponds to CR_1 and CR_2 respectively;
- LR_x = Loss of Resilience, obtained by subtracting 1 to the previously calculated value, which corresponds to LR_1 and LR_2 respectively;
- $CombR_x$ = Combined Resilience corresponds to subtracting LR_x from $CombR_{x-1}$, originating $CombR_x$.

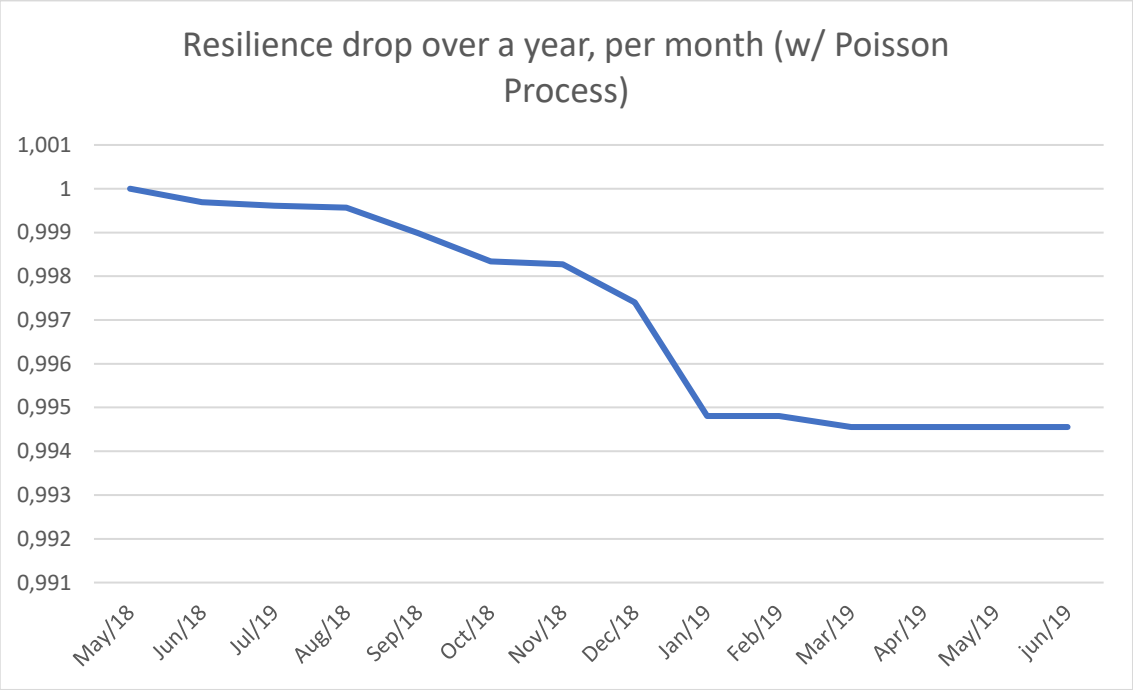

Figure 20 - Resilience drop over a year, per month, recurring to the Poisson Process

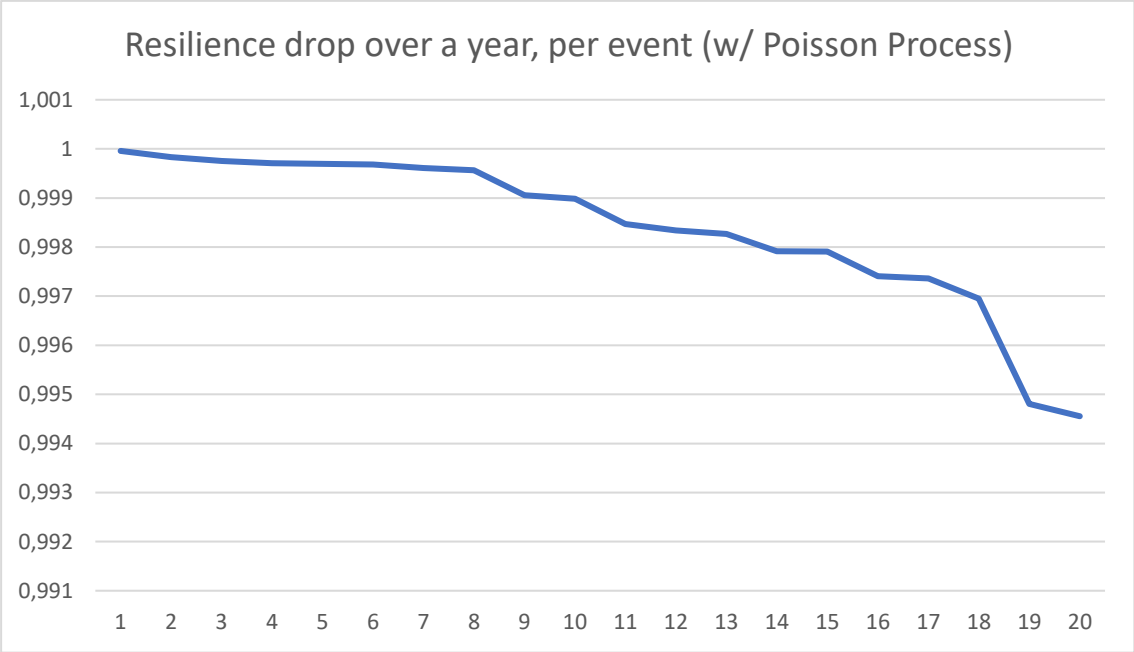

Figure 21 - Resilience drop over a year, per event, recurring to the Poisson Process

These latter graphs (figure 20 and 21) refer to the resilience lost, throughout a year, of the analyzed infrastructure. By analyzing them, it is possible to understand that the resilience drop is greater depending on the impact that the event has had on the infrastructure. Both graphs show that January was the month with the biggest drop and was due to the fact that those were the months with the highest failure impact.

5.2. Obtained Results

Given the obtained results, it is possible to immediately compare them since they are quite discrepant. The combined loss of resilience over a year, using the Poisson process (0.545%), seems to be close to reality, therefore, losing the same amount of resilience in 10 years would be 5.45%. By not recurring to the Poisson variable, a value of 3.0966% per year would be obtained. Therefore, by applying the same method of considering the same loss of resilience per year in a 10 years span, this value would be at 30.966%. Those results seem unlikely to occur since, under these conditions, the probability that the infrastructure is profitable would be very low, making it an unwanted business to the company.

Table 24 - Resilience Results considering and not considering Poisson

Final Results			
With Poisson Process		Without Poisson Process	
Combined Loss of Resilience	Final Resilience value	Combined Loss of Resilience	Final Resilience value
0.5452145%	99.4554113%	3.0965816%	96.9034184%

However, even though the results would seem to go accordingly to what was expected, it was decided to test other possible events to see if the results would remain consistent. It was decided to choose elements that had different Risk Priority Number's in order to not test values

that were close and to try the different types of failure so that it was possible to compare the final values. This process was necessary to comprehend if this factor would make a significant difference in this process. The chosen equipment were Power Plugs (3.5% RPN), Battery Cabinets (28.5% RPN), LVDB (39.9% RPN), Chiller (70% RPN) and Isolation Transformer (100% RPN) and they will be presented respectively by this order, in table 25. So, to each of these equipment 3 results were obtained, knowing that each of these had a different type of failure and timeline.

By looking at table 23 and figure 25, it can be observed that the results are in line with what was expected and that a clear distinction can be made between a type 3 failure event and a type 1 failure event, thus proving the importance of this factor to the system. It is important to state that in table 25, the T stands for Type of Failure and events n_o 1,4,7,10 and 13 are failures of type 1, events n_o 2,5,8,11 and 14 are failures of type 2 and events n_o 3,6,9,12 and 15 are failures of type 3.

Therefore, it is possible to conclude that using the initially proposed metric allows to obtain values that are much closer to reality and that provide an interesting indicator, to the infrastructure manager, by setting annual targets to meet company's expectations. It can also allow a new level of analysis by attempting to understand if it is in any way feasible, after a disruptive event, to: repair the affected equipment, replace the affected equipment with an equivalent or replace the affected equipment with a higher quality one.

Table 25 - Final Resilience values from the simulated events

							With Poisson Process			Without Poisson Process		
No	T	RPN	IGS	P	Δ_{Time}	$\overline{R_f}$	CR_1	LR_1	$CombR_1$	CR_2	LR_2	$CombR_2$
Equipment: Power Plugs; Level: D; Significance: 3; Redundancy: N												
1	1	0.035	0.965	5	1	0.000096	0.999994	0.000006	0.999994	0.999965	0.000035	0.999965
2	2	0.0175	0.9825	5	2	0.000096	0.999994	0.000006	0.999994	0.999965	0.000035	0.999965
3	3	0.00875	0.99125	5	3	0.000072	0.999995	0.000005	0.999995	0.999974	0.000026	0.999974
Equipment: Battery Cabinets; Level: B; Significance: 2; Redundancy: S(2N)												
4	1	0.285	0.715	3	1	0.000781	0.999949	0.000051	0.999949	0.999713	0.000287	0.999713
5	2	0.1425	0.8575	4	2	0.000781	0.999949	0.000051	0.999949	0.999713	0.000287	0.999713
6	3	0.07125	0.92875	5	3	0.000586	0.999962	0.000038	0.999962	0.999785	0.000215	0.999785
Equipment: LVDB; Level: B; Significance: 1; Redundancy: S(2N)												
7	1	0.399	0.601	2	1	0.001093	0.999929	0.000071	0.999929	0.999598	0.000402	0.999598
8	2	0.1995	0.8005	3	2	0.001093	0.999929	0.000071	0.999929	0.999598	0.000402	0.999598
9	3	0.09975	0.90025	4	3	0.000820	0.999946	0.000054	0.999946	0.999698	0.000302	0.999698
Equipment: Chiller; Level: A; Significance: 1; Redundancy: S(2N)												
10	1	0.7	0.3	1	1	0.001918	0.99987	0.00013	0.99987	0.99929	0.00071	0.99929
11	2	0.35	0.65	2	2	0.001918	0.99987	0.00013	0.99987	0.99929	0.00071	0.99929
12	3	0.175	0.825	3	3	0.001438	0.99991	0.00009	0.99991	0.99947	0.00053	0.99947
Equipment: Isolation Transformer; Level: A; Significance: 1; Redundancy: N												
13	1	1	0	1	1	0.002740	0.999821	0.000179	0.999821	0.998991	0.001009	0.998991
14	2	0.5	0.5	2	2	0.002740	0.999821	0.000179	0.999821	0.998991	0.001009	0.998991
15	3	0.25	0.75	3	3	0.002055	0.999866	0.000134	0.999866	0.999243	0.000757	0.999243

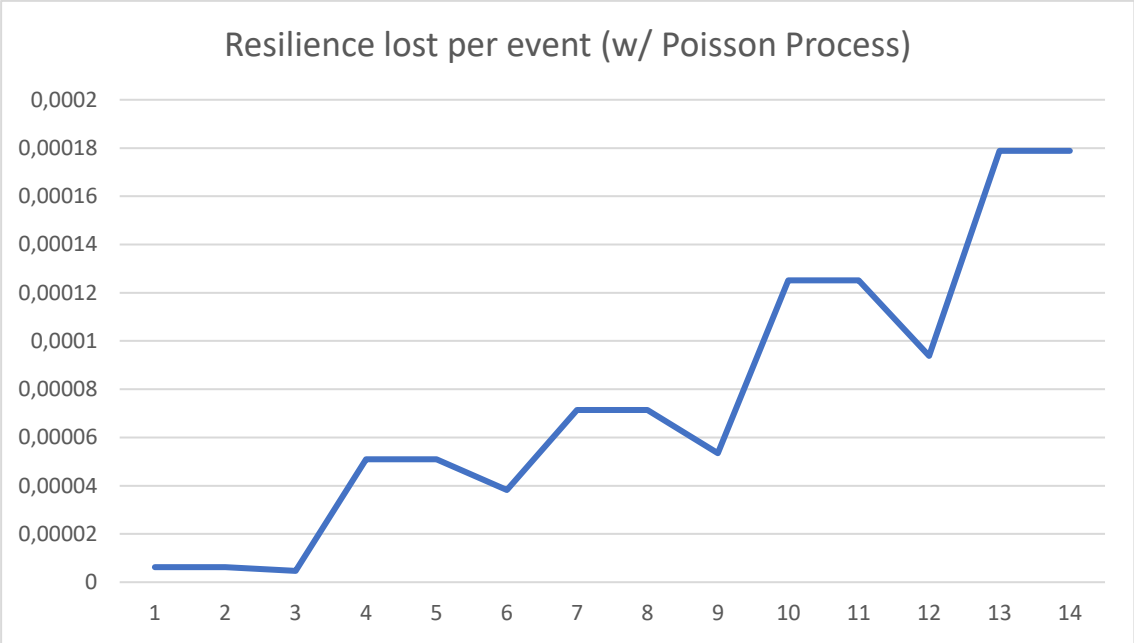

Figure 22 - Resilience lost per event, from the simulated events (w/ Poisson Process)

All of these options can and should account the possible impact that an equipment has had on the loss of resilience, considering its characteristics and the length of time it has remained inoperative. However, the obtained value recurring to Poisson (0.545%) does not mean that the infrastructure has lost its performance capability. Figure 23 allows us to conclude that there are several different ways for an infrastructure to lose performance and recover it after an event. It is, therefore, possible to affirm that:

- By replacing the affected equipment with a better than the previous one, it can be considered that the building's Performance has gone to a better state than the previous one;
- By replacing the affected equipment with equipment as good as the previous one, it can be considered that the building's performance has maintained its previous level of performance;
- By repairing the affected equipment, it could be considered that the infrastructure would be in an as good as old situation, so possible aging effects on that equipment would have to be considered.

Therefore, taking into account the results obtained in table 23, and after analyzing all the values obtained in the simulations performed in table 25, it is possible to state that the values are in accordance with what is intended and that the results are quite satisfactory since they make it possible to sort all the components analyzed in a consistent manner with the concerned infrastructure and the company responsible for it. In this way, the company can have in its possession a tool that will make it possible to create a data history that allows it to evaluate, through a quantifiable value, all the events that take place over time. This will enable to more accurately assess all future decisions on equipment, components or even an area of the infrastructure that has been affected.

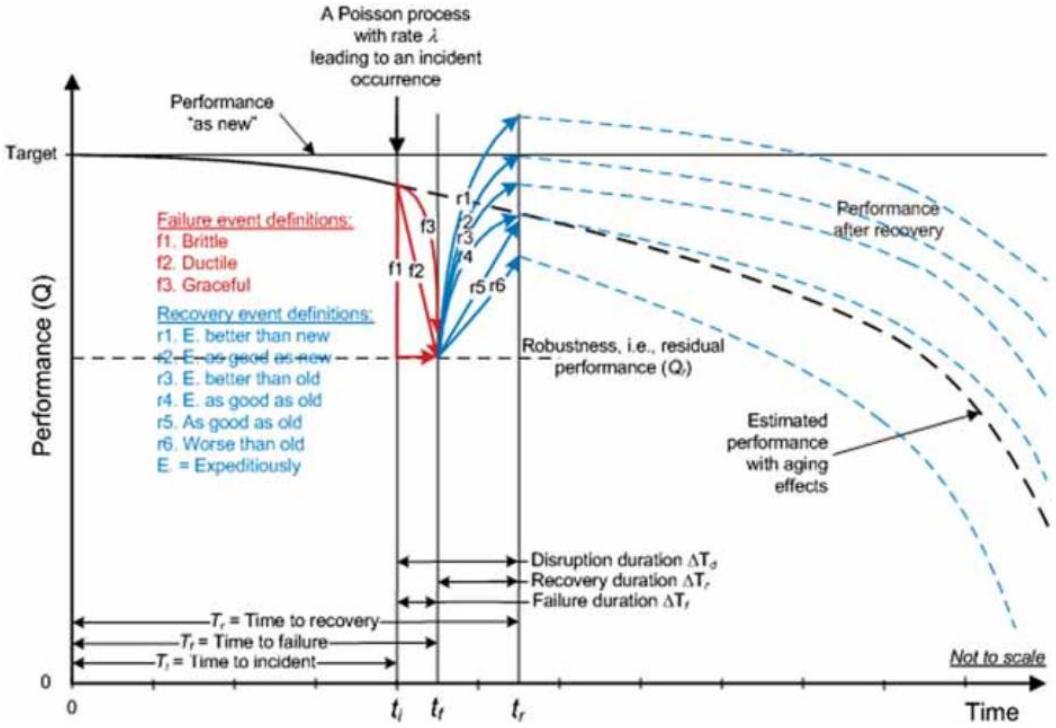

Figure 23 - Proposed definitions of Resilience Metrics [26]

This system also has the ability to shape and adapt to other infrastructures after making the necessary adjustments. Like it was previously shown, the attributed values of the factors for a piece of equipment may depend on his specifications or characteristics and it is feasible that an equipment may have different characteristics in different infrastructures. For example, a type 1 failure in a diesel storage tank in the analyzed infrastructure has an RPN of 28.5% as it has no redundancy. If there is another infrastructure that has a diesel tank with redundancy levels of N + 1 or 2N, it will get an RPN of 22.8% or 19.95%, respectively, if the other factors maintain their values.

It can then be concluded that the chosen metric and the processes used to calculate the impact of an event on the resilience of a building goes in accordance to what was intended, providing an important tool not only for the building management team but also for other personnel, responsible to evaluate its performance over time.

5.3. Tool Assumptions and method of Operation

In order to summarize the functioning and to mention the most important aspects to be considered for the implementation of this event reporting methodology, it is important to start by remembering the Resilience Analysis Process, explained in chapter 2.3.1. This process draws attention to factors that should be considered, ranging from the financial, legislative and local factors to the more technical part. The final objectives and the level of pretended resilience can vary depending on the location and the entities involved.

So, the first objective should be defining Resilience targets and goals, as chapter 2.3.1.1, *"Define Resilience Goals"*, states. The other steps will be referred to over the next points. Therefore, to explain the possible functioning of this tool, throughout an event, a demonstrative diagram will be presented (figure 24) with the following steps that were considered:

- Incident identification: The technician, who is responsible for reporting the incident identifies in the system, which component was affected to automatically obtain its failure mode, level, significance, and redundancy.
- Categorization: After obtaining the affected component values, the technician characterizes the type of failure deterministically, with the range previously described in chapter 3.2.1.4. in order to obtain the necessary RPN. Then, the Failure Modes table is used to describe the event. If necessary, some commentaries can be added to better describe the occurred event. This point is close to the one explained in RAP's 4th Step, *"Determine Level of Disruption"*, chapter 2.3.1.4.
- Prioritization: The system, through the RPN classification, will try to classify the event according to its importance. If this is the only active event, it will appear as the only event to be resolved as there is no other process in progress. If there are other events that are still in the resolution process, the system itself will rearrange to prioritize events considering their RPN's.
- Response and Diagnosis: Decision-making managers will need to assess what action is going to be taken and evaluate the event. The response shall be in accordance with the severity parameters previously characterized in chapter 3.2.2. where a level 5 event can be resolved over a longer period of time and a level 1 event is of the utmost emergency.
- Resolution and Recovery: In this time, measures have to be presented to control and prevent further damage. The first actions must be taken in order to resume activities and go back to previous levels as soon as possible.
- Closure: After all resolution processes are completed and the event is resolved, the event is closed and terminated in the system. Then it will be possible to calculate the final value of resilience lost with this event, as it depends on its start and completion time. It should be evaluated, at this moment, whether all the steps and decisions taken throughout the event are in accordance with what is intended or if any decision has affected the normal functioning of the infrastructure. It is also important to reevaluate if the previously set annual targets are still viable. The 6th and 7th chapter 2.3.1.6. *"Calculate Consequences and Resilience Metrics"* and chapter 2.3.1.7. *"Evaluate Resilience Improvements"* are very similar to this point.

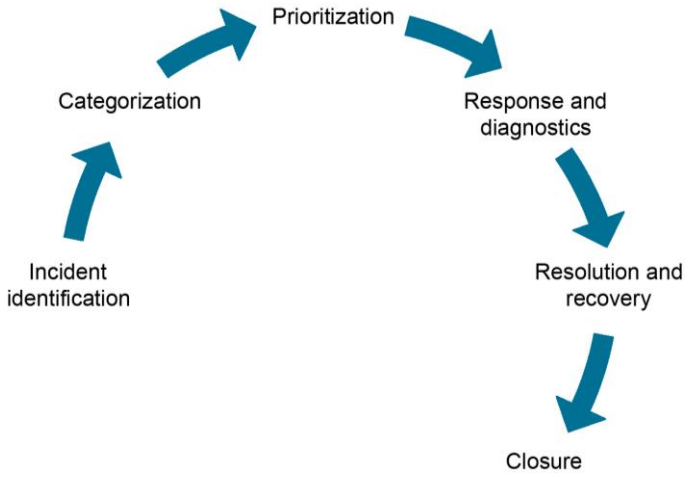

Figure 24 - Demonstrative diagram of the proposed steps to take when an incident occurs

6

Conclusions

The main objective of this dissertation was the construction of a system that could quantify a disruptive event according to its impact and severity. This would always aim to achieve a greater economic efficiency on the part of the company where this system was applied.

The research phase was more time consuming and complicated than expected as the company did not have a built idea of how to reach the desired solution. Intensive research was made to find a solution that could provide the company with a system that was easy to understand, that offered a value that made sense, and that allowed an in-depth analysis of an event to meet what was intended.

After this phase was completed, the development of the methodology started. One of the first challenges was that the historical data of past disruptive events was considerably small, and the time sample was discrete (since Δ_{Time} are presented in days, not hours). A continuous-time sample with more events would contribute considerably to safer and more concrete values. However, as it was proved that there were no tests that rejected the hypothesis of applying this metric, it was possible to continue developing it.

The obtained values of past events and simulations made possible to conclude that this tool can be very interesting for the company. It is possible to create annual targets in order to evaluate if the performance of the infrastructure in question is within the desired parameters, or, if it is more reasonable to replace a component instead of repairing it, if the resolution time after an error was too big.

Even knowing that this system only has the ability to evaluate the impact of an event after that it has occurred, its implementation can also contribute to the decrease of disruptive events in a medium or long term. Creating annual targets and having a more detailed data history of the impact and duration of each event can contribute to greater attention from all of those involved in the infrastructure maintenance and management teams, and even create new preventive habits and processes that may mitigate the possibility of an occurring event.

Applying this system on infrastructures does not invalidate the use of predictive models that recur to Artificial Intelligence or Decision Trees that can predict the existence of an event or how to act when facing factors that may jeopardize the correct functioning of system infrastructure. All of these technologies combined can improve the performance of infrastructure.

This system also offers the possibility to apply it to other infrastructures, after applying all the necessary changes regarding the four previously proposed factors and by confirming if it is possible to apply the metric by checking if the Poisson Process still applies, giving the company the possibility to create a broader track record in a set of several infrastructures. Sharing this type of information between infrastructures can contribute to better overall performance on a piece of equipment and improve the failure mode table with new failures that may have occurred elsewhere.

The direct contact with technicians and management teams made it possible to clarify some doubts that were crucial to a correct understanding of the infrastructure in question. The visualization of associated documentation, such as technical reports, and visits to the infrastructure gave a clearer idea of some of the recurring problems and allowed the acquisition of various technical and business knowledge.

For the reasons mentioned above, it can be concluded that all the objectives outlined for this dissertation were successfully achieved and all the steps and explanations have been taken in order to successfully apply to this system.

As future work, it should also be noted that it is important to make annual adjustments to the values of the resilience calculation variables, namely the λ. The existence of a larger sample, and preferably a continuous-time sample, enables a safer λ value that can be increasingly closer to reality. It is important to note that although the degree of accuracy of the system corresponds to the expected results, improving the RPN's values throughout the time it is an important step to improve the accuracy of the obtained results. Also, improving the failure mode table to make it as complete and as clear as possible is an important step.

As times goes by, there might be a need to add new variables to the Model, bringing new challenges to the analyst to the possible descriptions and characteristics of the variable. As such, variables such as occurrence and uncertainty may be considered in the future, where:

- Occurrence - Probability of a fatality or a failure occurring in a component for a given reason. Should a UPS fail (which is very rare) an extra rating could be attributed to it. However, does it make sense that the weight to be assigned is greater for components that are less likely to occur?
- Uncertainty - If an accident has occurred in a certain stage or a certain component and if in a certain period immediately before the accident there were more incidents, then the final weight of the incident can increase because the second incident can be a consequence of the first.

Bibliography

[1] International Energy Agency, "World Energy Outlook Special Report," *World Energy Outlook Spec. Rep.*, pp. 1–200, 2015.

[2] S. Kramer and S. Engell, *Resource Efficiency of Processing Plants*. Weinheim, Germany: Wiley-VCH Verlag GmbH & Co. KGaA, 2018.

[3] P. Torcellini, S. Pless, and M. Deru, "Zero Energy Buildings: A Critical Look at the Definition," Springer New York, New York, NY, 2006.

[4] S. Attia *et al.*, "Overview and future challenges of nearly zero energy buildings (nZEB) design in Southern Europe," *Energy Build.*, vol. 155, no. September, pp. 439–458, 2017.

[5] E. Vugrin, A. Castillo, and C. Silva-monroy, "Resilience Metrics for the Electric Power System : A Performance-Based Approach," no. February, p. 49, 2017.

[6] K. E. Trenberth, L. Cheng, P. Jacobs, Y. Zhang, and J. Fasullo, "Hurricane Harvey Links to Ocean Heat Content and Climate Change Adaptation," *Earth's Futur.*, vol. 6, no. 5, pp. 730–744, 2018.

[7] "Warming seas may increase frequency of extreme storms – Climate Change: Vital Signs of the Planet," 2019. [Online]. Available: https://climate.nasa.gov/news/2837/warming-seas-may-increase-frequency-of-extreme-storms/.

[8] "Staten Island seawall: Designing for climate change - CNN Style," 2019. [Online]. Available: https://edition.cnn.com/style/article/staten-island-seawall-climate-crisis-design/index.html.

[9] Z. Bie, Y. Lin, G. Li, and F. Li, "Battling the Extreme: A Study on the Power System Resilience," *Proc. IEEE*, vol. 105, no. 7, pp. 1253–1266, 2017.

[10] M. Bevilacqua, F. E. Ciarapica, and G. Marcucci, "Supply Chain Resilience Triangle: The Study and Development of a Framework," *World Acad. Sci. Eng. Technol. Int. J. Soc. Behav. Educ. Econ. Bus. Ind. Eng.*, vol. 11, no. 8, pp. 2046–2053, 2017.

[11] S. Hosseini, K. Barker, and J. E. Ramirez-Marquez, "A review of definitions and measures of system resilience," *Reliab. Eng. Syst. Saf.*, vol. 145, pp. 47–61, Jan. 2016.

[12] L. Layton, L. T. Marques, D. Shirmohammadi, H. W. Hong, A. Semlyen, and G. X. Luo, "Electric System Reliability Indices," *IEEE Trans. Power Syst.*, vol. 3, no. 21, p. 12, 2004.

[13] Y. Sheffi and J. Rice Jr, "A Supply Chain View of the Resilient Enterprise," *MIT Sloan Manag. Rev.*, vol. 47, 2005.

[14] M. Panteli and P. Mancarella, "The Grid: Stronger, Bigger, Smarter?," *IEEE Power Energy Mag.*, vol. 13, no. june, pp. 58–66, 2015.

[15] A. Clark-Ginsberg, "What's the difference between Reliability and Resilience?," Technical Report, 2016.

[16] E. Office and P. August, "White House 2013 - Grid Resiliency and Economic Benefit," Technical Report, 2013.

[17] B. Bayer, P. Matschoss, H. Thomas, and A. Marian, "The German experience with integrating photovoltaic systems into the low-voltage grids," *Renew. Energy*, vol. 119, pp.

129–141, Apr. 2018.

[18] K. Eshghi, B. K. Johnson, and C. G. Rieger, “Power system protection and resilient metrics,” in *Proceedings - 2015 Resilience Week, RSW 2015*, 2015, pp. 212–219.

[19] C. H. and L. P. W. JP Watson, “Conceptual framework for developing resilience metrics for the electricity, oil, and gas sectors in the United States,” *Energy.Gov*, pp. SAND2014-18019, 2015.

[20] Adam Henshall, “FMEA: How to Prevent the £100m British Airways Catastrophe | Process Street | Checklist, Workflow and SOP Software,” 2019. [Online]. Available: https://www.process.st/fmea/.

[21] E. Pazireh, A. H. Sadeghi, and S. Shokohyar, “Analyzing the enhancement of production efficiency using FMEA through simulation-based optimization technique: A case study in apparel manufacturing,” *Cogent Eng.*, vol. 4, no. 1, pp. 1–12, 2017.

[22] S. Hosseini, K. Barker, and J. E. Ramirez-Marquez, “A review of definitions and measures of system resilience,” *Reliab. Eng. Syst. Saf.*, vol. 145, pp. 47–61, 2016.

[23] M. Bruneau *et al.*, “A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities,” *Earthq. Spectra*, vol. 19, no. 4, pp. 733–752, Nov. 2003.

[24] C. W. Zobel, “Representing perceived tradeoffs in defining disaster resilience,” *Decis. Support Syst.*, vol. 50, no. 2, pp. 394–403, Jan. 2011.

[25] S. Enjalbert, F. Vanderhaegen, M. Pichon, K. A. Ouedraogo, and P. Millot, “Assessment of Transportation System Resilience,” in *Human Modelling in Assisted Transportation*, Milano: Springer Milan, 2011, pp. 335–341.

[26] B. M. Ayyub, “Practical Resilience Metrics for Planning, Design, and Decision Making,” *ASCE-ASME J. Risk Uncertain. Eng. Syst. Part A Civ. Eng.*, vol. 1, no. 3, p. 04015008, 2015.

[27] “FERC: Critical Energy/Electric Infrastructure Information (CEII),” 2018. [Online]. Available: https://www.ferc.gov/legal/ceii-foia/ceii.asp.

[28] U.S. Department of Homeland Security, “NIPP 2013: Partnering for Critical Infrastructure Security and Resilience,” 2013.

[29] T. D. O’Rourke, “Infrastructure Interdependencies and Resilience,” in *Chile Earthquake of 2010*, Reston, VA: American Society of Civil Engineers, 2013, pp. 365–386.

[30] M. Amin, “Toward self-healing energy infrastructure systems,” *IEEE Comput. Appl. Power*, vol. 14, no. 1, pp. 20–28, 2001.

[31] S. M. Rinaldi, “Modeling and simulating critical infrastructures and their interdependencies,” *37th Annu. Hawaii Int. Conf. Syst. Sci. 2004. Proc.*, vol. 00, no. C, p. 8 pp., 2004.

[32] Y. H. Khalil, A. Elmaghraby, and A. Kumar, “Evaluation of resilience for data center systems,” *Proc. - IEEE Symp. Comput. Commun.*, pp. 340–345, 2008.

[33] C. Harvey, “What is a Data Center?,” 2017. [Online]. Available: https://www.datamation.com/data-center/what-is-data-center.html.

[34] L. Uptime Institute, “Data Center Site Infrastructure Tier Standard : Operational Sustainability,” 2010.

[35] A. Lawrence, C. Brown, and T. Traver, “Webinar: Data Center Outage Trends, Causes and Costs,” 2019. [Online]. Available: https://uptimeinstitute.com/webinars/webinar-

data-center-outage-trends-causes-and-updates.

[36] W. Koehrsen, “The Poisson Distribution and Poisson Process Explained,” 2019. [Online]. Available: https://towardsdatascience.com/the-poisson-distribution-and-poisson-process-explained-4e2cb17d459.

[37] The British Standards, *Petroleum, petrochemichal and natural gas industries — Collection and exchange of reliability and maintenance data for equipment (ISO 14224:2016)*. 2016.

[38] R. E. Walpole, R. H. Myers, S. L. Myers, and K. Ye, *Probability & Statistics for Engineers & Scientists*, 9th ed. Prentice Hall, 2012.

[39] “NIST/SEMATECH e-Handbook of Statistical Methods,” 2003. [Online]. Available: https://www.itl.nist.gov/div898/handbook/index.htm.

[40] “Symmetry, Skewness and Kurtosis | Real Statistics Using Excel,” 2014. [Online]. Available: http://www.real-statistics.com/descriptive-statistics/symmetry-skewness-kurtosis/.

[41] “Skewness of Data | Excel with Excel Master,” 2016. [Online]. Available: https://excelmaster.co/skewness-of-data/.

[42] P. H. Furfey and S. Siegel, “Nonparametric Statistics for the Behavioral Sciences,” *Am. Cathol. Sociol. Rev.*, vol. 18, no. 2, p. 163, 2007.

[43] P. D. T. O’Connor and A. Kleyner, “Appendix 3: Kolmogorov-Smirnov Tables,” *Pract. Reliab. Eng.*, pp. 455–456, 2011.

[44] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO 14224:1999(E), *Petroleum and natural gas industries — Collection and exchange of reliability and maintenance data for equipment*, vol. 1999. 1999.

[45] G. Farquharson, “HVAC Systems Failure Modes,” 2015. [Online]. Available: https://www.pharmout.net/wp-content/uploads/2016/07/2015_GMP_Validation_Forum_D1.T2.3.2-GJF-T2-04-HVAC-Failure-Modes-2015-07-05.pdf.

[46] M. Kamutzki, “Fan failures: five typical problems and what causes them,” 2016. [Online]. Available: https://www.plant.ca/features/163687/.

Annex A – Auxiliary Calibration Tables

As it was described in chapter 4.3.2. a calibration was performed to analyze if the values were according to what was expected. So, every auxiliary table with the analyzed results that were not displayed previously are going to be presented. Once again, the colors used in these tables match those described in chapter 3.2.2. and in table 9.

Table 26 - The Possible Results of Multiplying every Level value by every Redundancy value

1st value: Level		3rd value: Redundancy		
		N	N+1	2N
		1	0.8	0.7
A	1	1	0.8	0.7
B	0.57	0.57	0.456	0.399
C	0.29	0.29	0.232	0.203
D	0.14	0.14	0.112	0.098

Table 27 - The Possible Results of Multiplying every Significance value by every Redundancy value

2nd value: Significance		3rd value: Redundancy		
		N	N+1	2N
		1	0.8	0.7
1	1	1	0.8	0.7
2	0.5	0.5	0.4	0.35
3	0.25	0.25	0.2	0.175

Table 28 - The Possible Results of multiplying every Level value by the multiplied results of table 27

1st value: Level		2nd value: Significance × Redundancy								
		1	2	3	4	5	6	7	8	9
		1	0.8	0.7	0.5	0.4	0.35	0.25	0.2	0.175
A	1	1	0.8	0.7	0.5	0.4	0.35	0.25	0.2	0.175
B	0.57	0.57	0.456	0.399	0.285	0.228	0.1995	0.1425	0.114	0.09975
C	0.29	0.29	0.232	0.203	0.145	0.116	0.1015	0.0725	0.058	0.05075
D	0.14	0.14	0.112	0.098	0.07	0.056	0.049	0.035	0.028	0.0245

Table 29 - The Possible Results of multiplying every Significance value by the multiplied results of table 26

Level × Redundancy	2nd value: Significance		
	1	2	3
	1	0.5	0.25
1	1	0.5	0.25
0.8	0.8	0.4	0.2
0.7	0.7	0.35	0.175
0.57	0.57	0.285	0.1425
0.456	0.456	0.228	0.114
0.399	0.399	0.1995	0.09975
0.29	0.29	0.145	0.0725
0.232	0.232	0.116	0.058
0.203	0.203	0.1015	0.05075
0.14	0.14	0.07	0.035
0.112	0.112	0.056	0.028
0.098	0.098	0.049	0.0245

Table 30 - The Possible Results of multiplying every Significance value by the multiplied results of the multiplication between Level and Significance (displayed on table 19)

Level × Significance	3rd value: Redundancy		
	N	N+1	2N
	1	0.8	0.7
1	1	0.8	0.7
0.57	0.57	0.456	0.399
0.5	0.5	0.4	0.35
0.29	0.29	0.232	0.203
0.285	0.285	0.228	0.1995
0.25	0.25	0.2	0.175
0.145	0.145	0.116	0.1015
0.1425	0.1425	0.114	0.09975
0.14	0.14	0.112	0.098
0.0725	0.0725	0.058	0.05075
0.07	0.07	0.056	0.049
0.035	0.035	0.028	0.0245

Annex B – The resulting RPN's

As described in chapter 4.3, it was necessary to characterize all the components in order to obtain their respective RPN's. Therefore, a more complete table similar to table 16 and 17 was created containing all the obtained classifications with the different types of failure. As in the above tables, the types of equipment will be as described in that chapter. The utilized colors will match those described in chapter 3.2.2. and in table 9. Some of the utilized acronyms were:

- L = Level;
- S = Significance;
- R = Redundancy;
- RPN = Risk Priority Number;
- IGS = Infrastructure's General State;
- P = Priority.

Table 31 - The complete table with the Resulting RPN's from each component

Data Center						Type of Failure: 1			Type of Failure: 2			Type of Failure: 3		
Type of Equi-pment	**Equipment**	**Failure Mode**	*L*	*S*	*R*	*RPN*	*IGS*	*P*	*RPN*	*IGS*	*P*	*RPN*	*IGS*	*P*
Energy	Disconnector	Disconnector	A	1	2N	70.00%	30.00%	**1**	35.00%	65.00%	**2**	17.50%	82.50%	**3**
	Generator	Gerador	A	1	2N	70.00%	30.00%	**1**	35.00%	65.00%	**2**	17.50%	82.50%	**3**
	Transformer	Transformer	A	1	2N	70.00%	30.00%	**1**	35.00%	65.00%	**2**	17.50%	82.50%	**3**
	LVDB	LVDB	B	1	2N	39.90%	60.10%	**2**	19.95%	80.05%	**3**	9.98%	90.03%	**4**
	UPS	UPS	B	1	2N	39.90%	60.10%	**2**	19.95%	80.05%	**3**	9.98%	90.03%	**4**
	Rectifier	Rectifier	B	1	2N	39.90%	60.10%	**2**	19.95%	80.05%	**3**	9.98%	90.03%	**4**
	UPS's DB	Distribution Boards	B	1	2N	39.90%	60.10%	**2**	19.95%	80.05%	**3**	9.98%	90.03%	**4**
	DB	Distribution Boards	C	1	N	29.00%	71.00%	**3**	14.50%	85.50%	**4**	7.25%	92.75%	**5**
	Diesel Storage Tanks	Storage Tanks	B	2	N	28.50%	71.50%	**3**	14.25%	85.75%	**4**	7.13%	92.88%	**5**
	Battery Cabinets	Battery Cabinets	B	2	N	28.50%	71.50%	**3**	14.25%	85.75%	**4**	7.13%	92.88%	**5**
	Isolation Transformer	Transformer	C	1	N	29.00%	71.00%	**3**	14.50%	85.50%	**4**	7.25%	92.75%	**5**
	Power Plugs	Power Plugs	D	3	N	3.50%	96.50%	**5**	1.75%	98.25%	**5**	0.88%	99.13%	**5**
HVAC	Chiller	Chiller	A	1	2N	70.00%	30.00%	**1**	35.00%	65.00%	**2**	17.50%	82.50%	**3**
	Boilers	Boilers	A	1	2N	70.00%	30.00%	**1**	35.00%	65.00%	**2**	17.50%	82.50%	**3**
	HVAC's DB	Distribution Boards	B	2	N	28.50%	71.50%	**3**	14.25%	85.75%	**4**	7.13%	92.88%	**5**
	Water Distribution Network	Hydraulic System	B	2	N	28.50%	71.50%	**3**	14.25%	85.75%	**4**	7.13%	92.88%	**5**
	Water Storage Tanks	Storage Tanks	A	3	N	25.00%	75.00%	**3**	12.50%	87.50%	**4**	6.25%	93.75%	**5**
	Fresh Air Handling Unit	AHU	C	1	N	29.00%	71.00%	**3**	14.50%	85.50%	**4**	7.25%	92.75%	**5**
	VRV	Split / VRV	C	1	N	29.00%	71.00%	**3**	14.50%	85.50%	**4**	7.25%	92.75%	**5**
	High Pressure Air Handling Unit	AHU	C	1	N+1	23.20%	76.80%	**3**	11.60%	88.40%	**4**	5.80%	94.20%	**5**
	SPLIT	Split / VRV	D	1	N	14.00%	86.00%	**4**	7.00%	93.00%	**5**	3.50%	96.50%	**5**
	Fan Coil Unit	Fan Coil Unit	D	2	N	7.00%	93.00%	**5**	3.50%	96.50%	**5**	1.75%	98.25%	**5**

Data Center						Type of Failure: 1			Type of Failure: 2			Type of Failure: 3		
Type of Equi-pment	**Equipment**	**Failure Mode**	*L*	*S*	*R*	*RPN*	*IGS*	*P*	*RPN*	*IGS*	*P*	*RPN*	*IGS*	*P*
HVAC	Water Pump	Pumps	D	1	2N	9.80%	90.20%	**4**	4.90%	95.10%	**5**	2.45%	97.55%	**5**
	Heat exchanger	Heat exchanger	D	3	N	3.50%	96.50%	**5**	1.75%	98.25%	**5**	0.88%	99.13%	**5**
	Heaters	Heaters	D	3	N	3.50%	96.50%	**5**	1.75%	98.25%	**5**	0.88%	99.13%	**5**
	Fans	Fans	D	3	N	3.50%	96.50%	**5**	1.75%	98.25%	**5**	0.88%	99.13%	**5**
Emergency	Isolation Transformer	Transformer	A	1	N	100.00%	0.00%	**1**	50.00%	50.00%	**2**	25.00%	75.00%	**3**
	Security DB	Distribution Boards	B	1	N	57.00%	43.00%	**2**	28.50%	71.50%	**3**	14.25%	85.75%	**4**
	Fire Alarm Control Unit	FACU	B	1	N	57.00%	43.00%	**2**	28.50%	71.50%	**3**	14.25%	85.75%	**4**
	Automatic Fire Suppression System	FACU	B	1	N	57.00%	43.00%	**2**	28.50%	71.50%	**3**	14.25%	85.75%	**4**
	Emergency Electric Pumps	Pumps	B	1	2N	39.90%	60.10%	**2**	19.95%	80.05%	**3**	9.98%	90.03%	**4**
	Motor Pumps	Motor Pumps	B	1	2N	39.90%	60.10%	**2**	19.95%	80.05%	**3**	9.98%	90.03%	**4**
	Centralized Technical Management Sys-tems	CTMS	B	1	N	57.00%	43.00%	**2**	28.50%	71.50%	**3**	14.25%	85.75%	**4**
	CCTV Systems	CCTV	B	1	N	57.00%	43.00%	**2**	28.50%	71.50%	**3**	14.25%	85.75%	**4**
	Fire Aspiration Detection System	FADS	C	1	N	29.00%	71.00%	**3**	14.50%	85.50%	**4**	7.25%	92.75%	**5**
	Flood Detection System	FACU	C	1	N	29.00%	71.00%	**3**	14.50%	85.50%	**4**	7.25%	92.75%	**5**
	Intrusion Alarms	IAL	B	1	N	57.00%	43.00%	**2**	28.50%	71.50%	**3**	14.25%	85.75%	**4**

Data Center						Type of Failure: 1			Type of Failure: 2			Type of Failure: 3		
Type of Equi-pment	**Equipment**	**Failure Mode**	*L*	*S*	*R*	*RPN*	*IGS*	*P*	*RPN*	*IGS*	*P*	*RPN*	*IGS*	*P*
Emergency	Gas Detection Systems	GDS	B	1	N	57.00%	43.00%	**2**	28.50%	71.50%	**3**	14.25%	85.75%	**4**
	Fire Extinguishers	Fire Extinguishers	D	1	N	14.00%	86.00%	**4**	7.00%	93.00%	**5**	3.50%	96.50%	**5**
	Fire Hose Reels	Fire Hose Reels	D	1	N	14.00%	86.00%	**4**	7.00%	93.00%	**5**	3.50%	96.50%	**5**
	Cylinders for Automatic Fire Suppres-sion	Cylinders for Automatic Fire Suppres-sion	D	1	N	14.00%	86.00%	**4**	7.00%	93.00%	**5**	3.50%	96.50%	**5**
Others	Wiring Closet	Wiring Closet	D	1	2N	9.80%	90.20%	**4**	4.90%	95.10%	**5**	2.45%	97.55%	**5**
	PDU	PDU	D	2	N	7.00%	93.00%	**5**	3.50%	96.50%	**5**	1.75%	98.25%	**5**

Annex C – The Complete Failure Mode Table

As described in chapter 4.4, a Failure Modes Table was created in order to better classify every event. This table is more complete version of table 22, presented in chapter 4.4, and will follow the same construction. Some of the utilized acronyms were:

- Nº of implications per failure – Number of equipment where this fault can be found;
- Failure Mode code - A unique code for each failure mode;
- Description - Brief description about the detected problem;
- Details - Brief description with some details of the failure that can help in the reporting phase of the event and to clarify a possible doubt;
- Equipment class code - A unique code for each of the equipment.

Table 32 - The Complete Failure Mode Table

				Energy									HVAC											Emergency											Others							
			Equipment Class Code	GEN	COMP	ELEM	UPS	PT	RET	QELE	BBAT	STAN	BOIL	PUMP	CHIL	WHEAT	HEXCH	HEAT	HYDS	HYDS	UCC	FCU	FAN	AIRF	AFSS	GDS	MPUMP	IAL	CCTV	SACA	CTMS	FEXT	FHOS	CAFS	WELL	WCLOS	PC	ROOM	BUILD	ELEV	ACB
No of implications per Failure	Failure Mode Code	Description	Details	Generators	Compressors	Electrical Motors	Uninterruptible Power Supply	Transformers	Rectifier	Distribution Board	Battery Cabinets	Storage Tanks	Boilers	Pumps	Chiller	Water Heaters	Heat Exchangers	Heaters	Hydraulic System	Split / VRV	UCC	Fan Coil Unit	Fans	Air Filtration	Automatic Fire Suppression System	Gas Detection System	Motor Pumps	Intrusion Alarms	CCTV Systems	Security and Access Control Systems	Centralized Technical Management Systems	Fire Extinguishers	Fire Hose Reels	Cylinders for Automatic Fire Suppression	Wells	Wiring Closets	PC's	Rooms	Buildings	Elevators	Access Control Barriers
13	ASR	Abnormal Sensor Reading	False alarm, Faulty instrument indication	X	X	X		X				X	X	X	X		X	X	X								X										X				
4	AIRD	Air flow decreased / Reduced air quantity																		X	X	X	X																		
20	ALAR	Alarm / Parameter Deviation	Monitored parameters exceeding tolerances. Ex: Default Alarm	X	X	X	X	X	X		X	X	X	X			X	X	X						X	X	X	X	X	X	X										
1	ALAH	Alarm Level - High	Excess water / gas / diesel etc.									X																														
1	ALAL	Alarm Level - Low	Lack of water / gas / diesel etc.									X																														
4	ARGW	Arcing results in contact getting welded																		X	X	X	X																		
3	BCS	Bad Conservation State	Visible Damage, Damaged components (handle, hose, drum, bracket, etc.) or in poor condition, may present strange objects / traces																													X	X	X							
4	CDCS	Carbon deposits on contact surface																		X	X	X	X																		
4	CIRP	Circuit Problem																		X	X	X	X																		
4	COMPB	Compressor Breakdown																		X	X	X	X																		
1	CLW	Control line to well communication	Loss of hydraulic control fluids to the wellbore																																X						
6	DAMB	Damaged Battery	Inoperative Battery or Low Capacity								X														X	X		X		X	X										
2	DAMS	Damaged Seal	Strip that prevents the pin from exiting does not exist or shows signs of damage																													X									X
2	DOP	Delayed Operation	Delayed opening / closing time												X				X																						
4	DESP	Design Problem																		X	X	X	X																		
1	DHEPF	Dirty HEPA Filter																						X																	
14	DPF	Downstream Power Failure	Equipment Power Failure, Power Outlets failure etc.	X			X	X	X		X					X				X	X	X	X				X									X	X		X	
2	DBB	Drive belt break																		X			X																		
4	DPR	Dust particles in refrigerant																		X	X	X	X																		
14	ERRO	Erratic Output	Instable	X	X	X	X	X	X				X	X											X	X	X	X		X	X										
4	ELO	Excess load on relay																		X	X	X	X																		
1	FSR	Failed to Set / Recover	Tuning / Recovery Operations Failed																																		X				
4	FPST	Fails to provide starting torque																		X	X	X	X																		
1	FSOF	Failure of Specific Software	Failure of Software Used by a Minority of the Company																																		X				
1	FWSO	Failure of Windows Software	Software Failure Common to the majority of the Company																																		X				
1	FTD	Failure to Disconnect	Failed to disconnect top conductor												X																										
2	FOD	Failure to Open on Demand	Does not open after order, stuck or does not fully open																																X						X
1	FOD	Failure to Open on Demand	Disjuntor / Fusivel / disconector não consegue abrir quando exigido							X																															
5	FREG	Failure to Regulate	Valve Stuck / Control Valves Only						X											X	X	X	X																		
16	FSTA	Failure to Start on Demand	Does not start or open after order or failed to respond to signal/activation	X	X	X	X	X	X				X	X	X										X	X	X	X	X	X	X										
2	FSTA	Failure to Start on Demand	Protection device/circuit breaker/switch fails after a circuit fault							X																											X				
3	FSTO	Failure to Stop on Demand	Does not close after order, Valve does not close after order																X																X						X
1	FSTO	Failure to Stop on Demand	Circuit breaker / Fuse cannot close when required							X																															

				Energy										HVAC													Emergency										Others						
			Equipment Class Code	GEN	COMP	ELEM	UPS	PT	RET	QELE	BBAT	STAN	BOIL	PUMP	CHIL	WHEAT	HEXCH	HEAT	HYDS	HYDS	UCC	FCU	FAN	AIRF	AFSS	GDS	MPUMP	IAL	CCTV	SACA	CTMS	FEXT	FHOS	CAFS	WELL	WCLOS	PC	ROOM	BUILD	ELEV	ACB
No of implications per Failure	Failure Mode Code	Description	Details	Generators	Compressors	Electrical Motors	Uninterruptible Power Supply	Transformers	Rectifier	Distribution Board	Battery Cabinets	Storage Tanks	Boilers	Pumps	Chiller	Water Heaters	Heat Exchangers	Heaters	Hydraulic System	Split / VRV	UCC	Fan Coil Unit	Fans	Air Filtration	Automatic Fire Suppression System	Gas Detection System	Motor Pumps	Intrusion Alarms	CCTV Systems	Security and Access Control Systems	Centralized Technical Management Systems	Fire Extinguishers	Fire Hose Reels	Cylinders for Automatic Fire Suppression	Wells	Wiring Closets	PC's	Rooms	Buildings	Elevators	Access Control Barriers
11	FSD	Failure to Stop on Demand	Does not stop after order / Failed to stop upper drive or incorrect shutdown process	X	X	X							X	X	X					X	X	X	X				X														
20	FALA	False Alarm / Unexpected Operation	Premature Shutdown / Stop, Unexpected Operation / Failure to Operate as Required, Junk Start	X	X	X	X	X	X				X	X	X				X						X	X	X	X	X	X	X				X					X	X
1	FALA	False Alarm / Unexpected Operation	Unintentional disconnection of a circuit / Intermittent disconnection or connection with unintended operation.							X																															
1	FALA	False Alarm / Unexpected Operation	Unwanted opening or closing																X																						
2	FAFA	Fan Failure																		X			X																		
14	FAI	Fault alarm not Issued	CTMS / or on equipment	X	X	X	X	X	X	X	X		X	X	X			X	X								X														
4	FOF	Faulty Output Frequency	Wrong / oscillating frequency	X			X		X																		X														
3	FOV	Faulty Output Voltage	Wrong / unstable output voltage				X	X	X																		X														
1	HEPFL	Final HEPA filter leak test failure																						X																	
4	APF	Frequent Starting and Stopping																		X	X	X	X																		
3	FUFA	Fuel Failure	Missing or Unusable Fuel	X									X														X														
2	GFA	Gas Failure	Gas Failure										X																										X		
5	HEATN	Heat is not exchanging	Insufficient Heat / Cold														X			X	X	X	X																		
8	HIO	High Output	Excess of Speed / Output above specification	X	X	X							X	X	X				X								X														
3	ILOC	Improper Location / Unavailable Access	Out of specific support, or in a location other than as indicated on emergency plans, Access blocked																													X	X	X							
4	INCAP	Incorrect selection of Capillary bore and length																		X	X	X	X																		
4	INOH	Inoperative Humidifier																		X	X	X	X																		
2	IPRE	Insufficient Pressure	Pressure gauge arrow not in “green” zone																													X		X							
4	ISGS	Internal springs get stuck																		X	X	X	X																		
1	NETF	Internet Network Failure	Temporary or permanent Inoperable Internet Network																																				X			
15	LEXT	Leak - External	Fuga numa zona não controlada/meio ambiente, de um liquido ou gás (Óleos, Gáses, Combustiveis, etc.)	X	X	X		X		X		X	X	X	X	X	X	X	X								X								X						
14	LINT	Leak - Internal	Leakage of a liquid or gas (Oils, Gases, Fuels, etc.) in a controlled zone / space / without contact with the environment	X	X			X		X		X	X	X	X	X	X	X	X								X								X						
4	LCP	Leakage in closed position	Leakage through valve in "closed" position												X	X			X																X						
3	STOP	Locked / Stop	Component unable to function, locked or jammed													X																								X	X
6	LCON	Loose Connection	Failed to connect												X					X	X	X	X														X				
12	LOO	Low Output	Performance below specifications / Fan is too quiet	X	X	X							X	X	X				X	X	X	X	X				X														
32	MIS	Minor Issues in Service	Loose Items, Discoloration, Dirt, etc.	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X						X	X	X	X	X	X	X	X	X	X		X	X	X	X	X	X
1	MIS	Minor Issues in Service	Diffusers / Grates / Signage / Lighting																																			X			
2	MOTFA	Motor or contactor failure	Engine does not start at all / Engine malfunction																	X			X																		
1	MUDA	Mud accumulation	Mud accumulation									X																													

				Energy									HVAC												Emergency										Others						
			Equipment Class Code	GEN	COMP	ELEM	UPS	PT	RET	QELE	BBAT	STAN	BOIL	PUMP	CHIL	WHEAT	HEXCH	HEAT	HYDS	HYDS	UCC	FCU	FAN	AIRF	AFSS	GDS	MPUMP	IAL	CCTV	SACA	CTMS	FEXT	FHOS	CAFS	WELL	WCLOS	PC	ROOM	BUILD	ELEV	ACB
No of implications per Failure	Failure Mode Code	Description	Details	Generators	Compressors	Electrical Motors	Uninterruptible Power Supply	Transformers	Rectifier	Distribution Board	Battery Cabinets	Storage Tanks	Boilers	Pumps	Chiller	Water Heaters	Heat Exchangers	Heaters	Hydraulic System	Split / VRV	UCC	Fan Coil Unit	Fans	Air Filtration	Automatic Fire Suppression System	Gas Detection System	Motor Pumps	Intrusion Alarms	CCTV Systems	Security and Access Control Systems	Centralized Technical Management Systems	Fire Extinguishers	Fire Hose Reels	Cylinders for Automatic Fire Suppression	Wells	Wiring Closets	PC's	Rooms	Buildings	Elevators	Access Control Barriers
2	NOUT	No Output	No Output																						X	X															
4	NSEM	No Servicing of Motor																		X	X	X	X																		
17	NOI	Noise	Abnormal / Excessive Noise / Fan too noisy	X	X	X	X	X	X	X			X	X	X				X	X	X	X	X				X													X	
4	OILR	Oil in the refrigerant																		X	X	X	X																		
33	UNK	Other / Unknown	Failure modes not specified, Too little information to set a failure mode, Specify in comment field	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X						X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
3	OED	Out of the Expiration Date	Not marked on CE label or maintenance date invalid																													X	X	X							
1	OAFB	Outside air filtration blockage (normal & abnormal events)	May occur prior to filtration or with outside air (normal and abnormal events)																					X																	
17	OVEH	Overheating	Overheating / Relay Winding Overheats	X	X	X	X	X	X	X			X	X	X			X	X	X	X	X	X				X														
10	CHOK	Plugged / Choked	Partial or Total Flow Restriction / Blocked Piping	X	X							X	X	X			X	X	X								X								X						
1	PCL	Premature Closure	Premature valve closure without command																																X						
4	REIO	Restricted air inlet and outlet																		X	X	X	X																		
6	SENSF	Sensor failure	Sensor, camera or similar equipment malfunction																						X	X		X	X	X	X										
4	SBBP	Shaft Balance and Bearing Problem																		X	X	X	X																		
1	STOR	Stop Regulating	Valve Stuck / Control Valves Only																X																						
33	STMA	Structural Deficiencies - Major	Major Material Damage (Cracks, Fractures, Reservoir Breakage, Motor Windings Are Weak / Insulation Defects)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X		X	X	X	X	X	X	X				X	X		X	X	X	X
34	STMI	Structural Deficiencies - Minor	Minor Material Damage (wear, corrosion, Dirty Fan Blades, Dirty Coils, Refrigerant Dust Particles, Chipped Contact Surfaces, Weak Fan Condenser)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X		X	X	X	X	X	X	X				X	X	X	X	X	X	X
2	SINF	Synchronization Failed	Unable to synchronize the generator	X																							X														
6	TEMH	Temperature - High	Temperature above acceptable value									X				X	X	X	X																			X			
6	TEML	Temperature - Low	Temperature below acceptable value									X				X	X	X	X																			X			
4	THEN	Thermostat not kept in proper position																		X	X	X	X																		
4	TMMR	Too much moisture in refrigerant																		X	X	X	X																		
13	UPF	Upstream Power Failure	Failure in Energy Supply	X			X	X	X		X		X							X	X	X	X				X												X		X
14	VIB	Vibration	Abnormal / Excessive Vibration / Fan is vibrating	X	X	X				X			X	X					X	X	X	X	X				X													X	X
3	FH2O	Water Failure	Missing or Unusable water										X			X																							X		
4	WCOP	Worn out particles from the compressor parts																		X	X	X	X																		
528	Total		Total of implications per Equipment	24	19	17	15	17	16	14	9	14	23	19	19	12	12	13	23	35	32	32	35	3	11	11	24	10	8	10	10	7	5	6	12	4	10	9	7	9	11