UNIVERSITY OF SÃO PAULO
SÃO CARLOS ENGINEERING SCHOOL

Michel Bessani

Resilience and Vulnerability of Power Distribution Systems: Approaches for Dynamic Features and Extreme Weather Scenarios

São Carlos

2018

Michel Bessani

Resilience and Vulnerability of Power Distribution Systems: Approaches for Dynamic Features and Extreme Weather Scenarios

Thesis presented to the São Carlos Engineering School, University of São Paulo, to obtain the degree of Doctor of Science - Electrical Engineering Program

Concentration Area: Dynamic Systems

Supervisor: Prof. Dr. Carlos Dias Maciel

São Carlos

2018

Trata-se da versão corrigida da tese. A versão original se encontra disponível na EESC/USP que aloja o Programa de Pós-Gaduação de Engenharia Elétrica.

Ficha catalográfica elaborada pela Biblioteca Prof. Dr. Sérgio Rodrigues Fontes da EESC/USP com os dados inseridos pelo(a) autor(a).

Bessani, Michel
B557r Resiliência e vulnerabilidade de sistemas de distribuição de energia: abordagens para características dinâmicas e cenários climáticos severos / Michel Bessani; orientador Carlos Dias Maciel. São Carlos, 2018.

Tese (Doutorado) - Programa de Pós-Graduação em Engenharia Elétrica e Área de Concentração em Sistemas Dinâmicos -- Escola de Engenharia de São Carlos da Universidade de São Paulo, 2018.

1. Resiliência. 2. Vulnerabilidade. 3. Robustez. 4. Confiabilidade. 5. Sistemas de Distribuição de Energia. 6. Infraestruturas Críticas. I. Título.

Eduardo Graziosi Silva - CRB - 8/8907

FOLHA DE JULGAMENTO

Candidato: Engenheiro **MICHEL BESSANI**.

Título da tese: "Resiliência e vulnerabilidade de sistemas de distribuição de energia: abordagens para características dinâmicas e cenários climáticos severos".

Data da defesa: 06/06/2018.

Comissão Julgadora: **Resultado:**

Prof. Associado **Carlos Dias Maciel**
(Orientador)
(Escola de Engenharia de São Carlos/EESC) Aprovado

Prof. Associado **João Bosco Augusto London Junior**
(Escola de Engenharia de São Carlos/EESC) Aprovada

Prof. Titular **Jorge Alberto Achcar**
(Instituto de Ciências Matemáticas e de Computação/ICMC-USP) Aprovado

Prof. Dr. **Jose Antonio Perrela Balestieri**
(Universidade Estadual Paulista " Júlio de Mesquita Filho"/UNESP - Guaratinguetá) APROVADO

Prof. Dr. **José Alexandre Matelli**
(Universidade Estadual Paulista " Júlio de Mesquita Filho" /UNESP - Guaratinguetá) APROVADO

Coordenador do Programa de Pós-Graduação em Engenharia Elétrica:
Prof. Associado **Luís Fernando Costa Alberto**

Presidente da Comissão de Pós-Graduação:
Prof. Associado **Luís Fernando Costa Alberto**

This Thesis is dedicated to my parents
Oscar and Irene

Esta Tese é dedicada aos meus pais
Oscar e Irene

ACKNOWLEDGEMENTS

First and foremost, I have to thanks my parents, Oscar and Irene, for their love and support throughout my life and by teaching me that what we learn will always be ours. Thank you both for giving me the necessary strength to reach my objectives. I also would like to thanks my sister, Lorena, which deserve my wholehearted thanks as well.

Thanks also to Viviane for being so supportive throughout this journey, for the understanding and encouragement in many moments.

I would like to sincerely thanks my doctorate supervisor, Carlos Dias Maciel, for his guidance and support throughout this study and especially for his confidence in me.

To the many friends I made during the postgraduate journey, in especial Julio and Tadeu, for all the good times we have spent so far.

I also thank all the staff and professors who have contributed in some way to the progress of my post-graduation and also to my personal and professional growth during this stay in the department of electrical and computer engineering at São Carlos school of engineering.

Thanks to the Coordination for the Improvement of Higher Education Personnel (CAPES) for the financial support during the doctorate.

"All models are wrong,
but some are useful."
George Box

"The significant problems we face
cannot be solved at the same level of thinking
we were at when we created them."
Albert Einstein

ABSTRACT

BESSANI, M. **Resilience and Vulnerability of Power Distribution Systems**. 2018. 188p. Thesis (Doctorate) - São Carlos Engineering School, University of São Paulo, São Carlos, 2018.

Our society is heavily dependent on commodities, as water and electricity, supplied to final users by engineered systems, which are known as critical infrastructures. In such context, the understanding of how such systems handle damaging events is an important aspect and is a current concern of researchers, public agents, and society. How much of performance a system loses due to damages is related to its vulnerability, and the ability to absorb and recover successfully from damages is its resilience. In this study, approaches to assess the vulnerability and resilience of power distribution systems by evaluating dynamic features, as the processes of failure and repair, and system reconfiguration for vulnerability, and the effects of extreme weather scenarios for resilience together with the processes of failure of repair are presented. Such approaches were applied on systems previously presented in the literature, and also on a Brazilian power distribution system. A Monte Carlo simulation was applied to evaluate this systems, models for time-to-failure and time-to-repair under different circumstances were obtained from historical data, and a method to use the models of time-to-failure during the vulnerability analysis was introduced. In addition, an assessment of the impact of reconfiguration capability on vulnerability is also carried out, and a resilience assessment under different climate scenarios has been developed. The time-to-failure and repair models highlighted how external factors modifies the Brazilian system failure and repair dynamics, the use of time-to-failure models during vulnerability analysis showed that the consideration of the failure dynamic of the types of elements give different results, and the time domain allows new analysis' perspectives. The investigation indicated that the vulnerability reduction due to reconfiguration is affected by the number of switches and also the maximum load capacity of the distribution system feeders. The resilience assessment showed that for structural connectivity, larger distribution networks are less resilient, while for electricity delivery, a set of features, related with the topological and electrical organization of such networks, seems to be associated with the network service resilience, such information is useful for system planning and management. The dynamics evaluated in this study are relevant to vulnerability and resilience of such systems, and also to other critical infrastructures. Moreover, the developed approaches can be applied to other systems, as transportation and water distribution. In future studies, other power distribution systems features, as distributed generation and energy storage, will be considered in both, vulnerability and resilience analysis.

Keywords: Resilience. Vulnerability. Robustness. Reliability. Power Distribution Systems. Critical Infrastructures.

RESUMO

BESSANI, M. **Resiliência e Vulnerabilidade de Sistemas de Distribuição de Energia**. 2018. 188p. Tese (Doutorado) - Escola de Engenharia de São Carlos, Universidade de São Paulo, São Carlos, 2018.

Nossa sociedade é altamente dependente de commodities, como água e eletricidade, fornecidas para os usuários por sistemas de engenharia, conhecidos como infraestruturas críticas. A compreensão de como tais sistemas lidam com eventos prejudiciais é uma preocupação atual de pesquisadores, agentes públicos e sociedade. A perda de desempenho de um sistema devido a danos é relacionada à sua vulnerabilidade, e a capacidade de absorver e se recuperar dos danos é a resiliência. Neste estudo, são apresentadas abordagens para avaliar a vulnerabilidade e resiliência de sistemas de distribuição de energia considerando características dinâmicas, como os processos de falha e reconfiguração do sistema, para a vulnerabilidade, e os efeitos de climas extremos na resiliência com os processos de falha e reparo. Tais abordagens foram aplicadas em sistemas previamente apresentados na literatura, e também em um sistema brasileiro. Simulação de Monte Carlo foi utilizada para avaliar as dinâmicas de falha e reparo do sistema utilizando de modelos obtidos a partir de dados históricos, e um método para usar os modelos de tempo-até-falha durante a análise de vulnerabilidade também foi apresentado. Além disso, uma avaliação do impacto da dinâmica de reconfiguração na vulnerabilidade foi realizada e uma avaliação de resiliência sob diferentes cenários climáticos foi desenvolvida. Os modelos tempo-para-falha e reparo destacaram como fatores externos modificam as dinâmicas de falha e reparo do sistema brasileiro, o uso de modelos de confiabilidade na análise de vulnerabilidades mostrou que a consideração dos diferentes tipos de elementos geram resultados diferentes e o domínio de tempo permite novas perspectivas de análise. A investigação da reconfiguração indicou que a redução da vulnerabilidade devido à reconfiguração é afetada pelo número de chaves e também pela máxima capacidade de carga dos alimentadores do sistema de distribuição. A avaliação de resiliência mostrou que, para conectividade estrutural, redes de distribuição maiores são menos resilientes, enquanto que para fornecimento de energia, um conjunto de características, relacionados com a organização topológica e elétrica dessas redes parece ser associado à resiliência do serviço, informação útil para o planejamento. As dinâmicas avaliadas neste estudo são relevantes para a vulnerabilidade e resiliência de tais sistemas, e também para outras infraestruturas críticas. Além disso, essas abordagens podem ser aplicadas a outros sistemas, como transporte e distribuição de água. Em estudos futuros, outras características de sistemas de distribuição de energia, como geração distribuída e armazenamento de energia, serão consideradas nas análises de vulnerabilidade e resiliência.

Palavras-chave: Resiliência. Vulnerabilidade. Robustez. Confiabilidade. Sistemas de Distribuição de Energia. Infraestruturas Críticas.

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS AND ACRONYMS

AENS	Average Energy Not Supplied
AIC	Akaike Information Criterion
ASAI	Average Service Availability Index
BIC	Bayesian Information Criterion
CI	Critical Infrastructure
CA	Concurrent Attacks
CAIDI	Customer Average Interruption Duration Index
CAIFI	Customer Average
CCR	Cumulative Collapse Rate
CIPRNet	Critical Infrastructure Preparedness and Resilience Research Network
CN	Complex Netwoks
CPPS	Cyber-Physical Power System
CPS	Cyber-Physical System
CPPDS	Cyber-Physical Power Distribution Systems
CR	Collapse Rate
CV	Coefficient of Variation Interruption Frequency Index
DG	Distributed Generator
DOC	Distribution Operation Center
DS	Distribution System
EENS	Expected Energy Not Supplied
ENS	Energy Not Supplied
EPCIP	European Programme for Critical Infrastructure Protection
ER	Erdös and Rényi
ERM	Entity Relationship Model

E&RE	Extremes and Rares Events
EW	Exponentiated Weibull
FDIR	Fault Detection, Isolation, and Service Restoration
ICT	Information and Communication Technologies
IEEE	Institute of Electrical and Electronics Engineers
IPCC	Intergovernmental Panel on Climate Change
KM	Kaplan-Meier Estimator
LCC	Largest Connected Component
LOLE	Loss of Load Expectation
LOLF	Loss of Load Frequency
LOLP	Loss of Load Probability
MCS	Monte Carlo Simulation
micro-CHP	Micro combined heat and power
MLE	Maximum Likelihood Estimate
MSE	Mean Squared Error
MTBF	Mean Time Between Failure
MTTF	Mean Time to Failure
MTTR	Mean Time to Repair
SDN	Spatial Distribution Network
SRA	Society of Risk Analysis
OS	Operational System
PS	Power System
PTDF	Power Transmission Distribution Facotrs
PND	Power Not Delivered
QoS	Quality of Service
RAW	Resilience Achievement Worth

RE	Resilience Engineering
REDS	Repository of Distribution Systems
RTO	Response Time of Operation
RTS	Reliability Test System
SA	Sequential Attacks
SAIDI	System Average Interruption Duration Index
SAIFI	System Average Interruption Frequency Index
SCC	Sourced Connected Component
SF	Scale-free
SG	Smart Grid
SGAM	Smart Grid Architecture Model
SoS	System of Systems
US DoE	United States Department of Energy
WSU	Washington State University

LIST OF SYMBOLS

A	Adjacency matrix
e	Edge
E	Edges set
H	Entropy
λ	Failure Rate
G	Graph
r	Graph assortativity coefficient
$\overline{k}$	Graph average degree
L	Graph average geodesic path
C	Graph clustering coefficient
δ	Graph density
D	Graph diameter
$p(k)$	Graph degree probability
E	Graph efficiency
N	Graph order
d	Geodesic path
M	Graph size
I	Impact
q	Network route factor
$r_{xy.\mathbf{z}}$	Partial correlation
r_{xy}	Pearson correlation
P	Performance
R	Reliability function
Я	Resilience

S	Survival Function
v	Vertex
k	Vertex degree
V	Vertices set
$\overrightarrow{g}$	Vertex spatial position
W	Weight matrix

CONTENTS

1 INTRODUCTION

Our modern society is increasingly dependent on commodities, as water, gas, and electricity (YUSTA; CORREA; LACAL-ARÁNTEGUI, 2011), and their efficient delivery is fundamental for other essential services do not stop, such as financial, communication and health. As a consequence, such engineered systems are classified as Critical Infrastructures (CIs) (ZIO, 2016a). In general, a CI is an engineered system with major importance to comfort and safety of our society (YUSTA; CORREA; LACAL-ARÁNTEGUI, 2011). Moreover, economic and social development and homeland security are also reliant on CIs (BROWN et al., 2006; HUANG; LIOU; CHUANG, 2014).

The delivery of such commodities to final users is performed by Spatial Distribution Networks (SDN), which are infrastructures or facilities with elements and topologies related to geographic constraints, and are responsible for promoting the flow of goods and services from the source to the end users (GASTNER; NEWMAN, 2006). Gas (CARVALHO et al., 2009), water (YAZDANI; JEFFREY, 2011), and power (LUO; PAGANI; ROSAS-CASALS, 2016) distribution systems are examples of SDN. In general, they are located in urban areas where the majority of end users are and need to cover all the area to meet users' demand.

The way a CI handles with damaging events is an essential aspect (LABAKA; HERNANTES; SARRIEGI, 2015), and some questions naturally arise: What are the system' parts that will be more disruptive if lost (NICHOLSON; BARKER; RAMIREZ-MARQUEZ, 2016)? How will it handles extreme situations such as natural disasters (PANTELI; MANCARELLA, 2015a) or crises (CARVALHO et al., 2014)? How will be the performance loss if it suffers a planned attack (WANG et al., 2017)? Such questions do not have a simple rule to be applied, and rational thinking can generate limited results, as presented in (ALDERSON et al., 2013) and (GHEDINI; RIBEIRO, 2011).

Correct identification of threats, unexpected events, brittleness, and human factors are related with analysis (ZIO, 2016a) and management (WOODS, 2015) of CIs. Such systems are exposed to different threats, e.g., ageing and failures of elements (BOLLEN, 2000), acute demand increase (PAHWA; SCOGLIO; SCALA, 2014), natural hazards as environment and climate changes (REE et al., 2005), human operator errors (AMIN, 2010; BILIS; KRÖGER; NAN, 2013), and also premeditated attacks (BROWN et al., 2006). All these threats corroborate with the issues previously mentioned and reinforce the affirmative that does not exist a simple rule to be applied.

The capacity of a system to withstand disruptive events is related to the system Vulnerability. The Society for Risk Analysis (SRA) defines, in their Risk Glossary (SRA,

Society of Risk Analysis, 2015), that Vulnerability is the expected damage, or uncertainty on damage, caused by a hazard, and Robustness is its opposite concept. The Risk Glossary also defines that Risk is: "The combination of the probability of a hazard occurring and a vulnerability measure given the occurrence of the hazard", and risk analysis is the systematic process to understand the risks with the available knowledge. Another concept related to systems is how they recover from damaging events after withstanding the disruptive event (ZIO, 2016a), which is related to system resilience. According to a report generated by the U.S. National Academy of Sciences, Engineering, and Medicine (2012), resilience can be defined as "The ability to prepare and plan for, absorb, recover from, or more successfully adapt to actual or potential adverse events".

Considering such definition, resilience can be separated into short and long-term (PANTELI; MANCARELLA, 2015b). The former is related to how a system resists to ongoing stressing events, i.e., vulnerability - redundancies or resources to accommodate damages, and recovery - the capability to restore the performance lost due to damages. The latter is about adaptations or improvements to better sustain and recover performance due to future hazards, which can be done by learning from past events. Such concept of system resilience covers the concept of vulnerability together with reliability and recovery (RAMIREZ-MARQUEZ et al., 2018).

Besides, CIs are designed to function for decades (ZIO, 2016a) passing by maintenance, updating, and integration with new technologies, including the Information and Communication Technologies (ICT) (SHIN; HE; ZHANG, 2014), which are being integrated with the majority of engineered systems (BOYES, 2013). Such integration are resulting in Cyber-Physical Systems (CPSs) (WANG et al., 2015), which are networked systems with actuators, sensors, and processors designed to interact with physical components, including the system user or operator. These components allow a system operation based on real-time information and control (RAJKUMAR et al., 2010). Examples of CPSs are the Smart Grids (SHAUKAT et al., 2018) and the Industry 4.0 (XU; XU; LI, 2018).

Despite such improvements, the diversity and number of elements on CIs are increasing due to such integration with ICTs, and consequently, presenting new challenges concerning representation, modeling, and phenomena quantification (ZIO, 2007; SHIN; HE; ZHANG, 2014). Such CPSs presents some features as self-organization, emergent properties (properties that cannot be described solely by the system elements), as adaptability, non-linearity, and dynamic characteristics. All that lead to their classification as Complex Systems (OTTINO, 2004). Differently, from simple or complicated systems, Complex Systems cannot be described by quantitative "laws" (AMARAL; OTTINO, 2004). Regarding Vulnerability and Resilience analysis (ZIO, 2016a), an integration of methods is necessary to obtain a holistic view of such CIs, by accounting different perspectives of the system' complexity and uncertainties as topology, functioning, operation, and static and dynamic

characteristics.

A variety of approaches can be used to analyze the Vulnerability (KRÖGER; ZIO, 2011) of CIs. The use of historical data about elements failure together with statistical analysis can be used to model the failure process of elements by using Reliability Analysis (KAPUR; PECHT, 2014). Reliability Analysis is based on Probability Theory, and Statistics (ZIO, 2009) and uses random variables to model failure rates and probabilities of a system, or element, proper functioning during a mission time T. The reliability models can be used to infer what are the critical elements of a given system, and also quantify the impact of different covariates on the CI performance, as in (YAMIJALA; GUIKEMA; BRUMBELOW, 2009; LIU et al., 2015).

It can also be performed by using probabilistic modeling, as Markov models (IYER; NAKAYAMA; GERBESSIOTIS, 2009), which describes the probability of elements transition among their possible states, and Bayesian Networks (LANGSETH; PORTINALE, 2007), which model the probabilistic dependence among the random variables, as system and element states (DAEMI; EBRAHIMI; FOTUHI-FIRUZABAD, 2012). The use of probabilistic models presents a challenge related to the exponential growth of models due to the increase in the number of variables and states. Agent-Based Modelling also can be used to evaluate reliability and risks (SCHLÄPFER; KESSLER; KRÖGER, 2008; ZECHMAN, 2011), describing socio-technical aspects, like physical laws, flow, system operation, and customers demand.

Another framework useful to perform Vulnerability analysis is Complex Networks (CN), which is an interdisciplinary theoretical framework useful for understanding dynamics and characteristics of Complex Systems (MAURER; SCHNELLER; OMER, 2014). CN theory uses a graph that describes its underlying structure and the connectivity between its elements is interpreted by statistical models. Such representation allows investigation of different features. CN field address different phenomena, from social (LUSSEAU, 2003) and biological (GAO; BARZEL; BARABÁSI, 2016) to engineered systems (LI; CHEN, 2003; CHU; IU, 2017). It also can be employed for different dynamic processes, as Epidemiological Process (PASTOR-SATORRAS et al., 2015), Network Growth (SONG; HAVLIN; MAKSE, 2006), Search on Networks (BRIN; PAGE, 1998), and Vulnerability (SILVA; SOUZA; TABAK, 2017; BARABÁSI, 2016; KOTT; ABDELZAHER, 2014; YAZDANI; JEFFREY, 2010).

CN Vulnerability analysis (ALBERT; JEONG; BARABÁSI, 2000; WANG; CHEN, 2003) already had been performed in different systems, as gas (CARVALHO et al., 2009), biological (KUNERT-GRAF; SAKHANENKO; GALAS, 2017), and power systems (ALBERT; ALBERT; NAKARADO, 2004; ROSAS-CASALS; VALVERDE; SOLÉ, 2007; PAGANI; AIELLO, 2015). Since its introduction by Albert, Jeong e Barabási (2000), CN Vulnerability analysis can be performed by simulating removals, due to errors or

attacks, of system elements and quantifying the impact of such removals. Attacks are simulated by removing elements respecting some measure of importance, e.g., the number of connection of each element, while errors are simulated following the hypothesis of equal failures probabilities for elements' random removals.

Vulnerability Analysis also has two different approaches to deal with element removals (BOCCALETTI et al., 2006). The former is the Static Vulnerability, where the central question is about the capability of communication between network elements after the removals. Such approach is related to percolation theory (COHEN et al., 2000) and had been used to investigate epidemiological process and vulnerability on networks (NEWMAN, 2003b). Thinking on a communication network, after removals the network can be split into two or more connected components[1]. The elements in each component can communicate with each other, and the component with more elements preserves most of the original performance of the network.

Such analysis is focused on understanding the redundancy level in a network structure, i.e., how difficult is to split the network into two or more connected components, and how these components will handle with future damaging events. Static Vulnerability has analytical results based on percolation theory as performed in (COHEN et al., 2000; COHEN et al., 2001). Moreover, it also can be carried out using numerical analysis, as in (BRODER et al., 2000; ALBERT; JEONG; BARABÁSI, 2000), which investigated the Internet and a sample of the World Wide Web Vulnerability to errors and attacks.

Besides such analysis methodologies, Static Vulnerability can also be performed by using spectral properties of networks (WU et al., 2011). A graph spectrum is defined over the connections between its elements. The study of Fiedler (1973) showed that from the graph spectrum is possible to describe how well connected the graph is, and consequently how difficult is to split the network into two or more connected components. Such spectral metrics already had been used to characterize Static Vulnerability of water (YAZDANI; JEFFREY, 2010) and power (PAGANI; AIELLO, 2015) distribution systems, and also to measure the Vulnerability of adaptive multi-robot networks undergoing errors (GHEDINI; RIBEIRO; SABATTINI, 2016).

The last is Dynamic Vulnerability, which accounts the dynamical response of a system during damages occurrence. Such analysis has a qualitative role, but provides useful information about undesired effects (BOCCALETTI et al., 2006), as the criticality of elements (ZIO; SANSAVINI, 2011). The dynamics with main focus is the flow redistribution over a system after element loss, the quantities flowing over its structure will be redistributed over the network, and for systems where the elements are responsive to overload, it can initiate a cascade of overload failures or disconnections. It is the case of different engineered

[1] A component is a set of elements where all they can be reachable from the others. See Section 2.2

systems, as water (SHUANG; ZHANG; YUAN, 2014), transportation (YANG; HUANG; GUAN, 2014), and power (REN et al., 2016) systems. In the case of power systems, one of the factors related to large-scale electricity interruptions, or *blackouts*, are such cascading failures (DOBSON et al., 2007).

Similarly, Resilience also can be analyzed from different perspectives and approaches. In (WOODS, 2015), four perspectives to study resilience were presented. *i)* Resilience as the capability of a system to rebound from damages to normal activities. *ii)* Resilience as Robustness, by measuring the ability to absorb damages. *iii)* Resilience as the adaptive capacity to overcome unexpected events. *iv)* Resilience as sustained adaptability, the ability to being adapted to future unforeseen events as conditions evolve continuously. In this study, we adopted the Resilience definition of the U.S. National Academy of Sciences, Engineering, and Medicine (2012), which includes the perspectives *iii* and *iv*, as respectively the short and long-term resilience explained previously.

Examples of Resilience analysis are (FARR; HARER; FINK, 2014) that investigates the capability of a network to withstand damages by the repair of its flow by adding new connections, enabling the recovery from damages. Similarly, Shang (2015) assess the effect of only damaged links recovery by self-healing of nodes. Morone et al. (2016) investigated the consequences on the resilience due to the possibility of activating fixed backup redundancy links. Quattrociocchi, Caldarelli e Scala (2014) investigated the possibility of self-healing impact on different networks topology, and considering errors and attacks scenarios. All these studies agree that reconfiguration, or self-healing, are dynamic features capable sustain and recovery performance loss due damaging events, i.e., such capacities result in more resilient systems.

Regarding the approaches, the review (HOSSEINI; BARKER; RAMIREZ-MARQUEZ, 2016) distinguished between qualitative and quantitative approaches for resilience evaluation. The former is based on frameworks to identify different features related to resilience aiming resilience best practices, as threats, players, recovery activities, and robustness. The last is related with measures to quantify resilience, both general domain-free, and specialized domain-specific. General resilience quantification is by measuring system performance in a manner that allows comparison between different systems with comparable basic logic. Such resilience metrics are characterized as deterministic, without accounting the uncertainties into the quantification, and probabilistic measures, that consider the related stochasticity, e.g., the probability of damages occurrence and availability of resources to overcome performance degradation.

The domain-specific resilience quantification is explicit to a particular type of system and deals with the system underlying structure and behavior (HOSSEINI; BARKER; RAMIREZ-MARQUEZ, 2016). As examples, (KOUTSOUKOS et al., 2018) presents a modeling and simulation platform for evaluation of CPS resilience, which is applied to

smart transportation systems. (HOSSEINI; BARKER, 2016) presents a model to quantify the resilience of an inland waterway port. (FU et al., 2017) present an approach to assess the resilience of transmission grids facing the changes in demand and also climate hazards, and in (KWASINSKI, 2016), a set of metrics were proposed and applied to quantify resilience of power distribution systems using data from recent natural disasters.

Some methodologies already mentioned to perform Vulnerability analysis also can be used to assess Resilience. As the Bayesian Networks (LANGSETH; PORTINALE, 2007), which model the probabilistic dependence among random variables, which can be system and element states (HOSSEINI; BARKER, 2016), or the relationships among the elements states and the attributes related to system resilience (YODO; WANG; ZHOU, 2017). Such approach allows understanding the relationship among variables and also to perform inferences. CN also can be used to assess Resilience, as in (GAO; BARZEL; BARABÁSI, 2016; GHEDINI; RIBEIRO, 2014; TRAN et al., 2017; KIM et al., 2017), where CN metrics and approaches are used to develop the resilience assessment.

Electric Power System (PSs) are CIs exceptionally important (RINALDI; PEERENBOOM; KELLY, 2001), since other fundamental systems, like banking, health, water, gas, and telecommunication are dependent on electric energy to proper functioning. As a consequence, electricity interruptions due failures on PSs cause adverse effects for final users, and also for other CIs. PSs are networked systems responsible for transmitting and delivering electricity from suppliers to final users, which is exposed to a variety of threats (BOMPARD et al., 2013). A PS is composed of (GRIGSBY, 2016) generating stations, responsible for producing electric energy, which is transmitted in high voltages by Transmission Networks to distribution substations, which deliver low voltage electricity to final users by Distribution Systems.

The PS is one case of a CI that has been integrated with ICT, which results in Cyber-Physical Power Systems (CPPS), or simply the Smart Grid (SG). Such integration has generated major changes in the PS operation, real-time monitoring and control (FARHANGI, 2010), capacity of self-healing (RAMCHURN et al., 2012), bidirectional flow and distributed generation (FANG et al., 2012), demand management (ANJANA; SHAJI, 2018), micro-grids and advanced sensing and measurement systems (TUBALLA; ABUNDO, 2016).

The process of transforming the PSs on SGs presents several challenges (XENIAS et al., 2015; SELVAM; GNANADASS; PADHY, 2016), particularry for instrumentation (BHATT; SHAH; JANI, 2014), communication and information management (BAEK et al., 2015), operational proceedings changes (HEYDT, 2010) and the improvement of reliability, robustness and resilience of SG (HEYDT, 2010; FANG et al., 2012; BHATT; SHAH; JANI, 2014; WANG et al., 2016; BIE et al., 2017). The emerging of smart features are happening on both, Transmission (LI et al., 2010) and Distribution (AIELLO; PAGANI,

2016) systems.

An important trend in power Distribution Systems (DSs) that is reinforced by the current ICT integration on its physical layer is the Fault Detection, Isolation, and Service Restoration (FDIR) procedures (ZIDAN et al., 2016). Such steps are related to the system reconfiguration capability, that can be performed by human operators or automatically knowns as the self-healing capability of DSs, which can be described as (ZIDAN; EL-SAADANY, 2012) the network ability to automatically reconfigure itself in a quick and flexible manner to restore functional loads that become out-of-service due to failure(s) between them and the DS flow source, generally the network feeder. This FDIR trend is also motivated by the knowledge that the most power interruptions occur on the DSs (KAVOUSI-FARD; NIKNAM, 2014; US DOE, 2017), including in the Brazilian PS (ANEEL, Brazilian Electricity Regulatory Agency, 2017).

Although Power Systems already has their Vulnerability investigated, the majority of studies focused on the Transmission System, and a minority investigated DSs (CUADRA et al., 2015; PAGANI; AIELLO, 2015; LUO; PAGANI; ROSAS-CASALS, 2016), which is the part where most power interruptions occur (KAVOUSI-FARD; NIKNAM, 2014). Such studies used real-world DSs samples from Netherlands and Spain, or synthetic DSs. Furthermore, the majority of studies on DS investigated only the Static Vulnerability, without contemplating the current features of DS, as the FDIR, or Self-Healing capability, which is related to the DSs ability to reduce the consequences of adverse events.

Only (LUO; PAGANI; ROSAS-CASALS, 2016) investigated they dynamic vulnerability of DSs by cascading failures, but without self-healing features. The disregard of such types of dynamics provides incomplete results with the current reality of DSs. Specifically to the Self-Healing of CN, there is a need for more investigations (SHANG, 2015), as the time delay to the self-healing response due to failures or attacks, which will also need the time domain during vulnerability analysis. In (ZHU et al., 2014; YAN et al., 2015; YAN et al., 2017), the time domain was considered during vulnerability analysis of Transmission Systems to attacks. Luo, Pagani e Rosas-Casals (2016) also argue that more specific metrics accounting electrical features, and representation models dealing with the different dynamics, are necessary to deal with DSs vulnerability.

In the same direction, since its introduction by Albert, Jeong e Barabási (2000), numerical vulnerability analysis is performed by simulating removal of networks elements and quantifying the performance loss due to removals. The errors are simulated following the hypothesis of equal failures probabilities for all elements susceptible to errors. All the vulnerability studies presented above, and the ones considered in the review (CUADRA et al., 2015), performed vulnerability analysis to errors with the equal failure probabilities premise. However, such premise does not contemplate the current challenges of modeling and analyzing engineering systems (ZIO, 2016a), which have both structural and dynamic

complexity.

The case of PSs resilience studies is slightly different. As the resilience concept englobes different features of a given system, there are several approaches to deal with PSs resilience. For transmission systems, they are related to resilience assessment under different conditions by performing scenario-based Monte Carlo simulations, and also using CN metrics and models with assumptions of the numerical vulnerability analysis mentioned previously, optimization studies to enhance resilience against attacks, and resilience-based component importance. There are also different studies about DSs resilience, as customers interruption duration analysis, quantification of DSs resilience by combining specific features with CN metrics, resilience-based service restoration optimization, evaluation of smart grids related features (e.g., micro-grids, distributed generation and energy storage).

A recent report from the United States Department of Energy (US DoE) related to the challenges of electric power systems Reliability, Robustness, and Resilience (US DOE, 2017), discuss the needs of methods to deal with the old and new threats the PSs faces, as the extreme weather events that will increase in frequency and intensity, cyber threats, and physical threats. Such need is also a concern of the European Union addressed by the European Programme for Critical Infrastructure Protection (EPCIP) which resulted in the Critical Infrastructure Preparedness and Resilience Research Network (CIPRNet) project (European Commission, 2017).

However, there is a need for investigating the aspects related with extreme weather effects on the resilience of PDSs (PANTELI; MANCARELLA, 2015b; FU et al., 2017; KWASINSKI, 2016; BIE et al., 2017; US DOE, 2017). Moreover, the DSs is the part where most power interruptions occur (KAVOUSI-FARD; NIKNAM, 2014; US DOE, 2017), including in the Brazilian PS (ANEEL, Brazilian Electricity Regulatory Agency, 2017). Furthermore, the intensity and probability of extreme weather events will increase in the follows years as stated in the 2014 Intergovernmental Panel on Climate Change (IPCC) report (PACHAURI et al., 2014).

In this sense, the use of simulations approaches capable of performing specific scenarios analysis is a manner to deal with these low probability high impact events, or "surprising" events (ZIO, 2016a). As a consequence, the Resilience and Vulnerability of DSs must be investigated in a manner that allows the consideration of different scenarios related to external threats, as the weather, and also cultural changes related with smart features and renewable energy sources penetration, and the transformation of consumer units into active agents in the energy market, which will drastically affect DSs reality (SHAUKAT et al., 2018).

1.1 Objectives

Considering such statements, this doctoral research aimed to develop vulnerability and resilience assessment approaches applied to power distribution systems capable of dealing with dynamic features, as the processes of failure and the system reconfiguration during contingencies for vulnerability, and evaluation of extreme weather scenarios effect on the system resilience together with the processes of failure and repair. The originality is related with the consideration of different failures patterns during vulnerability analysis, and also the evaluation of how extreme weather scenarios affects the resilience of power distribution systems. Such analysis are performed by Monte Carlo simulation where the effect of such features can be considered. In addition, the effect of human operator decision during failures in the reliability indices of power distribution systems is also assessed by Monte Carlo simulation.

This research was developed using DSs previously presented in the literature, and also using a DS from a Brazilian power distribution company. With the aim of developing such assessment approaches to power distribution systems vulnerability and resilience, this Thesis specific objectives are:

- Apply the Monte Carlo simulation to explore power distribution systems dynamics;
- Obtain Reliability models describing the *failure* and *repair* process from historical data accounting different scenarios for the Brazilian DS;
- Develop an approach to account variable failure rate and reconfiguration dynamics during vulnerability analysis.
- Investigate the self-healing capacity of DSs in the context of vulnerability;
- Develop a resilience assessment method accounting the failure and repair processes and quantifying the effect of different scenarios related to weather conditions;
- Perform a characterization of the Brazilian DS;
- Apply the scenario-based resilience assessment in the Brazilian DS.
- Perform a Vulnerability Analysis of the Brazilian DS;

1.2 Outline

In the remaining of this thesis, the necessary background with previous results from the literature, the achieved results and next steps are be presented. Chapter 2 contains the background, where Resilience is formally defined and previous results from the literature are presented in Section 2.1, followed by a Section about Complex Networks -

Section 2.2, containing the fundamental of CN characterization together with a subsection about Spatial Distribution Networks. In Section 2.3, Vulnerability Analysis is formally presented, with the primary results for Power Systems Vulnerability from the literature review, and with a specific subsection for Power Distribution Systems Vulnerability. Also, a Section 2.4 for present Reliability Engineering concepts, as systems reliability and DS reliability. Chapter 3 presents the research materials and methods, which includes the used DSs data, and how the presented concepts are utilized to achieve the thesis objectives. In Chapter 4, the results are presented and discussed, following the Chapter 3 organization. The Chapter 5 concludes this thesis, and presents the next steps of this research.

2 BACKGROUND

This Chapter presents the theoretical background of the concepts exploited in this thesis are presented. In addition, some methods and results from the literature are also mentioned. The aim is to highlight the motivation of the different studies in each type of concept related to how a system can handle damaging events.

2.1 Resilience

Systems resilience concept is used across disciplines and applications, and its definition varies among them. For example, in ecological systems Resilience is "a measure of the persistence of systems and of their ability to absorb change and disturbance and still maintain the same relationships between populations or state variables" (HOLLING, 1973, p. 14). In psychology, it is generally defined as "positive adaptation despite adversity (FLEMING; LEDOGAR, 2008, p. 2)". Such definition is dependent on the particular context where resilience is applied (HOSSEINI; BARKER; RAMIREZ-MARQUEZ, 2016), as social, organizational, economic and engineering domains.

In the engineering application, the first publications about Resilience Engineering (RE) began in the early 21st century (RIGHI; SAURIN; WACHS, 2015), and RE is presented as a new approach to complex socio-technical systems safety management. Hollnagel, Woods e Leveson (2006) says that resilience is a proactive view of system safety as "something a system or organization *does*, rather than something or an organization *has* (HOLLNAGEL; WOODS; LEVESON, 2006, p. 347)". In this sense, a resilient system must be capable of anticipating, perceive and respond to changes or threats caused by internal and external factors.

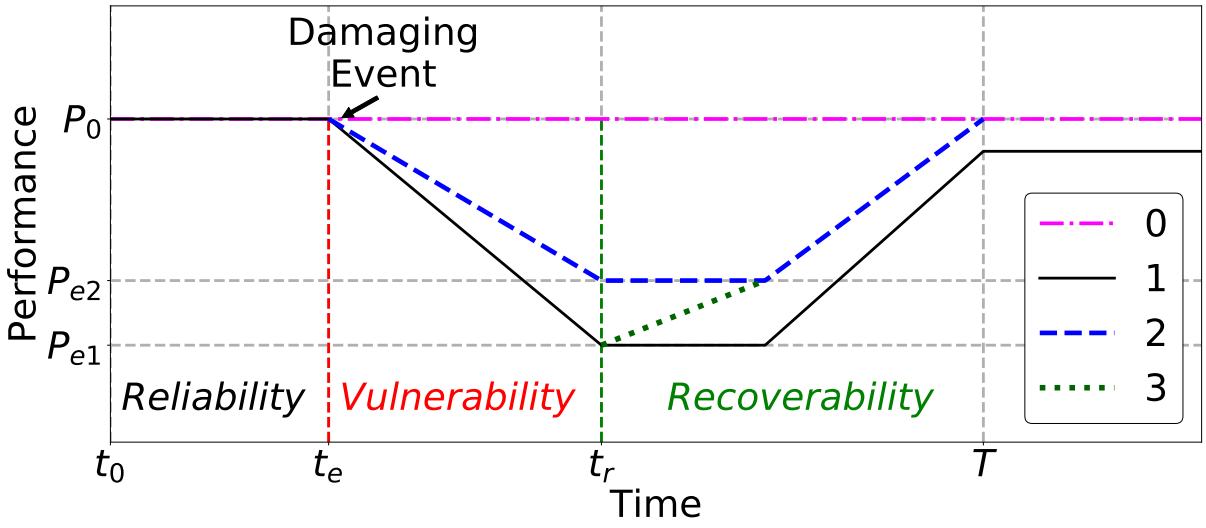
Another motivation of RE is the recent occurrence of extreme events that caused significant economic and social loss due to damages on different CIs (HOSSEINI; BARKER; RAMIREZ-MARQUEZ, 2016), like hurricanes, earthquakes, storms, and tsunamis. Moreover, the prediction is that such events will increase both in intensity and frequency of occurrence in the coming years (PACHAURI et al., 2014), being a current focus of academic research and government entities.

As the focus of this study is DSs Resilience, it was adopted the definition of the US National Academy of Sciences, Engineering, and Medicine (2012) that "Resilience is the ability to prepare and plan for, absorb, recover from, or more successfully adapt to actual or potential adverse events". Based on such definition, resilience can be divided into short and long-term (PANTELI; MANCARELLA, 2015b). The former accounts with the system resistance to stressing events, i.e., vulnerability, lack of redundancy or resources to

accommodate damages, and recovery capability to restore performance after damages. The latter is about future improvements or adaptations to handle future hazards considering lessons from past events.

Such definition of short-term resilience is illustrated in Figure 1, with a general view of a system's performance under different arrangements. t_e is the instant when a damaging event happens, and consequently reduces the system performance from P_0 to P_{e1} and P_{e2}, where P_{e1} is for arrangement 1, and P_{e2} for arrangement 2. Such performance drop is related to the system vulnerability to the damaging event. In arrangement 3, the performance changes from P_{e1} to P_{e2} after the damage, which is a consequence of the use of resources to perform a fast and partial recovery from damages before the total recovery, in DSs it is the system reconfiguration capability. After the damaging event and system reconfiguration, the system is fully recovered in instant T, returning to its original performance. For arrangement 1, the recovery is made until a lower performance than the original 1.

Figure 1 – System performance curve due to the occurrence of a damaging event under different arrangements. 0 indicates the default system performance, and 1, 2, and 3 are arrangement with different features that affect system resilience, as higher vulnerability, resources to reduce the suffered damage, and recovery capability.



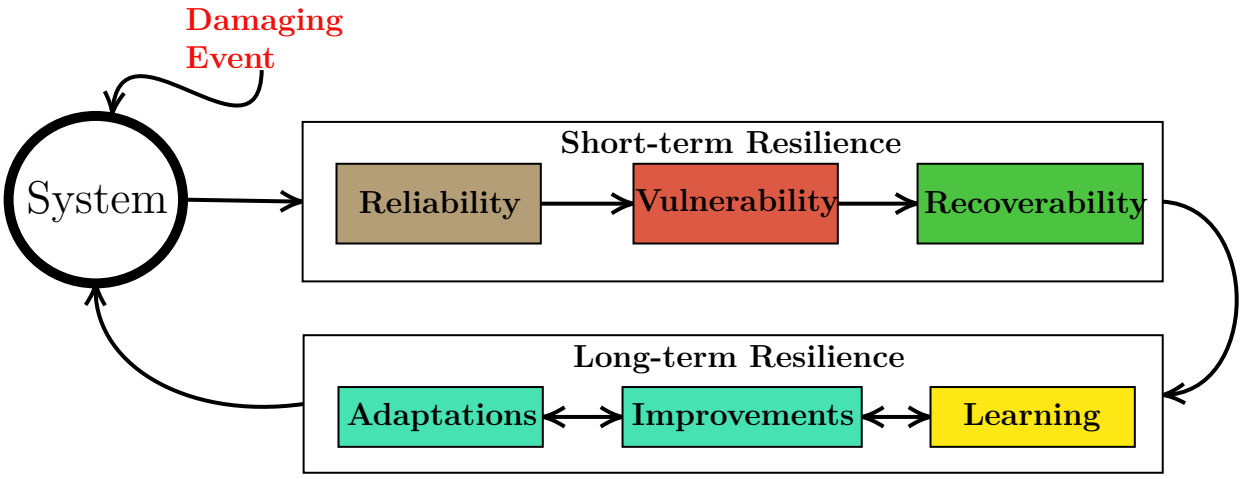
Source:Author

The Figure 1 also presents the different aspects that affect the system resilience: reliability, vulnerability, and recoverability. Reliability is related to how well the system was designed to tolerate high probability low damaging events, e.g., by redundancies. When low probability high impact events happen, the system experiences a considerable performance degradation, related to its vulnerability, and if a system has a high vulnerability, it can collapse after a high impact damaging event. After the performance loss, recoverability

is fundamental to the system bounce back to functional performance and is related to readiness and resources to restore its original, or an acceptable, performance. All these aspects influence the system resilience, and any improvement of such characteristic will result in a more resilient system.

The long-term resilience can be illustrated as in Figure 2. The idea of how the short-term resilience outcomes are related to the long-term one. The aspects, reliability, vulnerability, and recoverability can be analyzed after the damaging event is overcome, and much about the system resilience can be learned, which can result in improvements and adaptations to the system face future high impact hazards. Of course, the learning aspect is dependent on the quantification capability of risks and studies investigating future adverse scenarios. The adaptations and improvements are done to enhance the system resilience to both, expected and unforeseeable damaging events.

Figure 2 – Illustration of how the short and long-term resilience are related.



Source: Author

In this manner, different approaches can be used to quantify a system resilience, the review (HOSSEINI; BARKER; RAMIREZ-MARQUEZ, 2016) presents several ways to measure a system resilience, as deterministic and dynamics metrics. Here, the metric proposed in (OUYANG; DUEÑAS-OSORIO, 2012) for resilience calculation is adopted, since it is capable of measuring the system robustness, redundancy, resources, and recovery features. It considers the ratio between the desired performance (equal to P_0) and the dynamic performance $P(t)$ over a time interval T. Resilience ($\text{Я}(T)$)[1] is calculated as follows:

$$\text{Я}(T) = \frac{\int_T P(t)dt}{\int_T P_0 dt} \tag{2.1}$$

Such metric is in the range $[0, 1]$, where 1 happens when the performance over T is always equal to the desired performance P_0. This normalized range is useful to allow

[1] $R(t)$ notation is reserved for the Reliability function.

comparison between different systems and arrangements, e.g., the arrangements in Figure 1 result in $Я_0 = 1 > Я_2 > Я_3 > Я_1$. Different hazards impacts are measured during the time interval T by using the $P(t)$ values. An important aspect is a need of defining a performance measure to calculate $Я$. It can be related to social, organizational and economic aspects of the analyzed system (OUYANG; DUEÑAS-OSORIO, 2012), like connectivity, customers being served, and power delivered.

2.1.1 Power Systems Resilience

Recently, many studies about the resilience of power infrastructures were performed, for both transmission and distribution systems. These studies are related to resilience assessment and optimization, and using approaches as Monte Carlo simulation, mathematical optimization, historical data analysis, complex networks metrics and models, and resilience-based component importance metrics. In the following paragraphs, we list recent studies about electric power systems resilience, first the studies related to power transmission resilience, followed by the studies of power distribution resilience.

For transmission systems, (OUYANG; DUEÑAS-OSORIO, 2012) performed a dynamic resilience assessment of the power transmission system in Harris County, Texas, USA, considering random failures, cascading failures due to overloads, and exponential restoration time for the assessment using stochastic simulation. Such methodology was applied for scenarios of system evolvement by load growth and capacity improvements, and discuss the resilience enhancement due to improved situational awareness, demand management, and distributed generation integration. The resilience was assessed using the total power delivered. They concluded that such improvements might improve system resilience in the short-term, but without proper management, these factors can weaken resilience in the long-term.

The study (PANTELI; MANCARELLA, 2015b) used the IEEE 6-bus reliability test system for evaluating the resilience of power transmission systems to extreme weather events. The evaluation uses a Monte Carlo simulation together with fragility curves that describe the wind speed effect on the failure probability of the system transmission lines and result in a performance time-series. The system transmission lines were considered in two weather regions where the weather effect is different. The resilience assessment was done to compare the original system resilience with three cases of resilience enhancement by robust, redundancy and response improvements, where the resilience was measured by using the Loss of Load Probability (LOLP) and Loss of Load Expectation (LOLE) reliability indices. The model indicated that the robustness and redundancy improvements result in the higher resilience by the LOLP and LOLE indices reduction in the IEEE 6-bus system.

A similar approach to (PANTELI; MANCARELLA, 2015b), was also used in (PAN-

TELI et al., 2017a), but using the Grand Britain power transmission system and with more weather regions. The simulation assumed one winter week where the peak demand and extreme winds are expected for such system. The resilience was estimated using the Loss of Load Frequency (LOLF) and the Expected Energy Not Supplied (EENS) reliability indices, and the resilience enhancement due to redundancy, robustness, and responsiveness improvement was assessed in a normalized way by the Resilience Achievement Worth (RAW) index. They noticed that the increase in the robustness to extreme wind event has the higher increase in system resilience, which is a consequence of the reduction of the wind speed effect on failure probabilities by the robustness increase. The resilience enhancement due to redundancy and responsiveness depends on the targeted event, in this case, wind speed.

In (ESPINOZA et al., 2016), a similar approach to (PANTELI et al., 2017a) was used to asses the Grand Britain power transmission system resilience due to floods and windstorms. They observed that normal weather does not cause significant disruptions, as expected, and for intense or extreme weather the risk of blackouts is real. They evaluated the same resilience enhancement strategies, and the improvement of the system components is the one that resulted in the higher resilience, followed by improvements in restoration procedures, and the redundancy is the one with lower resilience enhancement, this lasts almost not increase resilience due to floods. They used as resilience measure the EENS. Their model used some assumptions to obtain all the data necessary to run.

The study (FU et al., 2017), used the resilience assessment methodology based on Monte Carlo simulation to evaluate effects of extreme windstorms together with evolution on demand, supply and development policies, and the resilience was measured by LOLP, LOLE, and EENS. They evaluated four future scenarios of the Grand Britain transmission network:

1. Low cost and centralized generation;
2. Low cost and distributed generation;
3. High cost and centralized generation;
4. High cost and distributed generation.

They concluded that only the scenario 4 high cost and distributed generation increases the system resilience, achieving a combined effect of reducing the impact of generators loss and increasing network redundancy. Moreover, for all scenarios, an increase of 10% of intensity and frequency of weather severity already significantly impact the network resilience, and further increases exponentially affect the system resilience.

Panteli et al. (2017b) present the fundamental concepts of power transmission resilience and a quantitative resilience framework is proposed. It was used to evaluate the strategies of hardening and using smart operational features to improve transmission systems resilience. They used the Grand Britain transmission networks and investigated the resilience improvement strategies in a scenario of extreme windstorms. Again, the

increase in the robustness of system elements by hardening resulted in the higher resilience improvement, and the restoration of damaged elements was the step that more affects the test case resilience. They also evaluated the use of defensive islanding during extreme windstorms, and they noticed that defensive islanding enhances resilience during the start of damages by reducing the number of lines that are tripped by the protection, and reducing the number of faulted lines during the restoration stage.

Fang e Sansavini (2017) proposed an optimization algorithm to increase power transmission systems resilience after attacks considering an expansion scenario. The used optimization model minimizes operational costs, investments, and performance loss after attacks, and was applied to the IEEE 14-bus test system. They concluded that small investments to enhance transmission line switching and installing selected transmission lines enhance resilience. They performed a sensitivity analysis due to uncertainty in attack scenarios. The consideration of large-scale attacks results in the higher resilience enhancement but with the need for a large budget.

Another study about power transmission resilience optimization against attacks is (OUYANG; FANG, 2017), where a decomposition algorithm finds the best pre-event defense strategy, hardening elements and increasing redundancies by building new transmission lines, the worst-case attack scenario, and the post-attack repair strategy for the system damaged elements. They applied the algorithm in the IEEE RTS 24 and IEEE RTS 48 and used the DC power flow model. They concluded that even small pre-event defense strategy is significant for resilience enhancement, especially under massive attacks, the defenses strategies efficiency is dependent on the attack scenario, and an optimized recovery strategy can enhance resilience, being necessary the consideration of both, pre-event defense and post-event repair optimize resilience.

In (KIM et al., 2017), the South Korean power transmission grid resilience was analyzed using Complex Networks metrics together with the Crucitti-Latora-Marchiori cascading model (CRUCITTI; LATORA; MARCHIORI, 2004a). The performance of the system is quantified by the global network efficiency[2] They first compared the Korean system with some CN models [3]. The analysis was divided into two aspects, robustness, by investigation of how damaging events reduce the system performance, without accounting damage accommodation and recovery capability, and resilience by assessing the dynamic system performance after damages. They concluded that the Korean system is most vulnerable to betweenness-based[4] attacks and their recommended to the system evolve to a system with distributed generation and homogeneous load reduction by demand management. They also noticed that an early and fast recovery is fundamental to the

[2] It is the inverse of the harmonic mean of the shortest path between all nodes, see Section 2.2.1.
[3] To more about CN models see Section 2.2.2
[4] A vertex betweenness is the sum of the ratio of all-pairs shortest paths that pass through it, see Section 2.2.1

system resilience.

Fang, Pedroni e Zio (2016) presented a resilience-based component importance measures. The first is a measure of repair and re-install priority, and the second is a measure of the potential loss due to a delay in the recovery of a damaged element. They used a Monte Carlo simulation to obtain the probability distribution of the two metrics for all the components of the IEEE 30-bus test system, and the elements were ranked using a stochastic ranking approach. The final rank is compared with three classical CN centrality measures[5]. They conclude that the CN metrics and reliability component importance metrics are not appropriate for resilience component importance since these do not account the recovery of damaged elements.

2.1.1.1 Power Distribution Systems Resilience

Maliszewski e Perrings (2012) used outages duration from the residential DS in part of the City of Phoenix, Arizona, US, together with spatial models to investigate the relation between the DS infrastructure and the environment. They pointed out that the vegetation plays a significant role in PDSs resilience, and that the resilience of customers electricity is proportional to the proximity with high priority loads. In (KWASINSKI, 2016), a framework to quantify resilience using historical data was proposed, which was applied to data describing natural disasters over different PDSs. The metrics proposed by Kwasinski provided a coherent quantification of the different aspects of resilience: robustness, resources, recovery, and adaptation.

Chanda e Srivastava (2016) proposed a methodology to quantify DS topological resilience using a set of CN metrics, they also presented a decision-making approach to numerically interpret the factors that affect DS resilience (topology, flow, constant failure rate and damaging events), which result in a composite resilience index. Such methodology was applied in two different DS: two micro-grids, and a real large DS in Pullman, Washington. They compared the resilience with and without Distributed Generator (DG) units and noticed that an increase in reconfiguration possibilities and the location of DG units near critical loads enhances the resilience.

Similarly, Bajpai, Chanda e Srivastava (2016) presented an algorithm to provide a view of all feasible configurations of a DS with their resilience, focusing on high priority loads and minimizing the number of switching operation. Resilience was measured using information related to system topology and operation, which were computed by CN metrics and information about the reconfiguration resources. The algorithm was applied in two micro-grids operating together and a modified IEEE 123 node DS. They concluded that DSs resilience is dependent on the number of paths that can connect the sources to the

[5] Such measures are presented in Section 2.2.1.

loads and the ration between the number of sources and number of critical loads for both cases.

Micro-grids as a resilience resource during extreme weather events is evaluated in (SCHNEIDER et al., 2017). They used the Washington State University (WSU) micro-grid in Pullman and evaluated the operational feasibility of three configurations. The WSU micro-grid was supplying only the loads owned by the micro-grid operators (local resource), the micro-grid supplying critical loads outside of it (community resource), and the micro-grid as a power source to start-up power plants facilities (black start operations). They concluded that a micro-grid could enhance resilience during such extreme weather events as local and community resource, and resilience enhancement for black start operations is dependent on the distance and power of the power plant.

The study (LLORET-GALLEGO et al., 2017) proposed a methodology for evaluating the ICT system of DSs. They used the Smart Grid Architecture Model (SGAM) together with an Entity Relationship Model (ERM), where the functionalities and technical features are represented, and evaluated the ICT platform of a local energy market with prosumers, i.e., consumers that play an active role in the distribution system due to the use of renewable energy generators. Several resilience indicators were presented for the physical infrastructure, the ICT system, and the socio-economical dimension by the identification of elements requirements and potential disruptions. They concluded that the Smart Energy Service Provider, which is responsible for the control and operation of different units such local energy markets, is the critical ICT element for a resilient local energy market.

In (BIE et al., 2017), Bie presented a general view of DS resilience and proposed a reconfiguration algorithm for DS considering different operational scenarios:

1. Without reconfiguration switches and DG;
2. Without reconfiguration switches but with DG;
3. With reconfiguration switches and without DG;
4. With reconfiguration switches and DG, where each DG forms one island;
5. With reconfiguration switches and DG, where islands were optimally formed;

The algorithm was tested on the IEEE 33-bus system, and a real urban DS located in China and resilience was measured as total load not supplied. They verified that the reconfiguration capacity together with DGs is important for resilience increase, which allows the formation of island partition supplied by DG sources, and the optimization of the number of islands enhances the tested DSs resilience.

Another study that analyzed DSs resilience is (MOUSAVIZADEH; HAGHIFAM; SHARIATKHAH, 2018), where the optimal formation of micro-grids, energy storage

technologies, demand-side management, and DGs were investigated. They modeled such dynamics by mixed-integer linear programming together with two-stage stochastic programming to handle the uncertainty of renewable energy resources. Such approach was tested on the modified 118-bus test system and also on a distribution network of Sa'adat-Abad district of Tehran, Iran. They agree with (BIE et al., 2017) that formation of micro-grids enhances resilience, and also shown that load control in specific nodes can significantly improve the system recovery after faults, and the uncertainty on renewable energy sources can decrease system resilience.

In (YAO; WANG; ZHAO, 2018), the effect of transportable energy storage on DSs with multiple micro-grids in system resilience during large area blackouts is evaluated. A restoration scheme with network reconfiguration that minimizes the customer interruption cost, generation cost, and the transportable energy storage cost is proposed. They tested the approach in a modified 33 bus test system with three micro-grids and four transportable energy storage and observed that the use of transportable energy resulted in a more resilient DS compared to a conventional energy storage system. This was due to the total cost reduction and the flexibility and transportability of energy storage to handle critical loads.

2.2 Complex Networks

In the 90's (WATTS; STROGATZ, 1998; BARABÁSI; ALBERT, 1999), CN field had evolved from the use of statistical physics approach and graph theory together with the crescent amount of data describing different real-world technological and biological systems (CUI; KUMARA; ALBERT, 2010). CN are related to graph theory (BOCCALETTI et al., 2006), which is used to represent structural aspects of systems and phenomena. The elements, or agents, are represented as vertices of a graph, and the interaction between them are represented as edges. The graph can embed different characteristics as the direction, strength, and features of such interactions. CN theory aims to provide a comprehension of the global attributes of a system that cannot be solely described by its connected elements (AMARAL; OTTINO, 2004), as non-linear dynamics, emerging properties, and self-organization.

2.2.1 Complex Networks Characterization

In this Subsection, the main concepts regarding complex networks characterization are presented. For an in deep view of such concept see the following survey (COSTA et al., 2007) or the book (NEWMAN, 2010). A graph G is defined as $G = (V, E)$, where V is a set of N vertices $(v_1, v_2, ..., v_n)$, E is a set of M edges $(e_1, e_2, ..., e_m)$. N and M are respectively the *Order* and *Size* of G. In an *undirected graph*, each edge links two vertices of V and is represented by an unordered pair of vertices $\{v_i, v_j\} = \{v_j, v_i\}$. If G is a *directed graph* (also known as digraph) the vertices are represented as ordered pairs,

and $\{v_i, v_j\} \neq \{v_j, v_i\}$. G can be a *weighted graph*, i.e., for each edge (e_i) in E exists an associated weight - w_i. G is called a *planar graph* if it can be drawn in a plane without crossing edges.

The *neighbourhood* of a vertex v_i, $\Gamma(i)$, is the set of vertices that have an edge connecting them to v_i, and $v_i \in \Gamma(i)$ if and only if exists a reflexive edge $\{v_i, v_i\}$. The number of neighbouring vertices is known as vertex *degree* k_i, if G is directed, the vertex v_i has an *in-degree* k_i^{in} and an *out-degree* k_i^{out}. If G is weighted, v_i connectivity to neighbours is described by the sum of the connected edges weights and is called *strength* s_i. A *path* from v_i to v_j in G is a sequence of edges beginning at v_i and ending at v_j, where its *length* is the number of edges in the path, and if G is *weighted*, the path *length* is the sum of each edge weight in the path. If the path exists, v_i and v_j are *connected*. It is a *simple path* if no vertex is repeated. The shortest path between v_i and v_j is known as *geodesic path* $(d_{i,j})$.

A *cycle*, or *loop*, is a path that starts and ends at the same vertex, and a cycle of order 3 is known as a *triangle*. G is called *acyclic* when it does not have any loop, i.e., is impossible to start from a vertex of G and reach the same vertex by a set of unique edges in G. If for all G vertices pairs exists a path connecting them, G is called *Connected*. Every graph G have an associated *Adjacency matrix* (A), where $a_{ij} = 1$ if exists an edge linking i to j, and 0 otherwise. If G is undirected $a_{ij} = a_{ji}$, and A is a symmetric matrix, and if G is weighted, it also has a *Weight matrix* W, containing the weight of each edge. In the case of a directed G, A will be an asymmetric matrix.

Given a graph $G = (V, E)$ and using the taxonomy presented in the previous paragraphs, some measures to characterize its topological structure can be introduced:

- *Density* (δ): the ratio between the Size of G and the maximum possible Size (the number of combinations of vertices pairs) (NEWMAN, 2010),

$$\delta(G) = \frac{M}{\binom{N}{2}}, \tag{2.2}$$

  A graph with $\delta(G) = 1$ is called *complete*.

- *Diameter* (D): the length (number of edges) of the longest geodesic path between any two vertices in G (NEWMAN, 2010)

$$D = \max_{ij} d_{ij}; \tag{2.3}$$

- *Average Geodesic Path* (L): the average geodesic distance among all pairs of network vertices. It is also known as the *Characteristic Path Length*;

- *Clustering Coefficient* (C): the density of triangles in a undirected unweighted network (COSTA et al., 2007), it is related with local redundancy. It can be calculated

by two different equations, The first gives the same weight to each triangle in the network:

$$C = \frac{3N_\Delta}{N_3}, \tag{2.4}$$

where N_Δ is the number of triangles, and N_3 is the number of length 3 paths in G, such values can be calculated using the elements of the adjacency matrix $a_{i,j}$ as follows:

$$N_\Delta = \sum_{k>j>i} a_{ij}a_{ik}a_{jk} \tag{2.5}$$

$$N_3 = \sum_{k>j>i} (a_{ij}a_{ik} + a_{ji}a_{jk} + a_{ki}a_{kj}) \tag{2.6}$$

The factor 3 in (2.4) is to normalize C in the interval $[0, 1]$.

The second ($\widehat{C}$), which gives the same weight to each vertex, is presented as an average of the clustering coefficient of each vertex $C(i)$:

$$\widehat{C} = \frac{1}{N}\sum_{i\in V} C(i), \tag{2.7}$$

and $C(i)$ is calculated as follows:

$$C(i) = \frac{N_\Delta(i)}{N_3(i)}, \tag{2.8}$$

where $N_\Delta(i)$ is the number of triangles that contains v_i and N_3 is the number of length 3 paths containing v_i. Such values also can be calculated directly from A elements:

$$N_\Delta(i) = \sum_{k>j} a_{ij}a_{ik}a_{jk} \tag{2.9}$$

$$N_3(i) = \sum_{k>j} a_{ij}a_{ik} \tag{2.10}$$

- *Average Degree* ($\overline{k}$): the average value of all network vertices degree (NEWMAN, 2010).

$$\overline{k} = \sum_{i\in V} k_i, \tag{2.11}$$

if G is directed, an average in-degree and out-degree can also be calculated:

$$\overline{k}^{in} = \sum_{i\in V} k_i^{in}, \tag{2.12}$$

$$\overline{k}^{out} = \sum_{i\in V} k_i^{out}. \tag{2.13}$$

- *Degree Probability* ($p(k)$): indicates the probability of randomly choosing a vertex of degree k (COSTA et al., 2007), $p(k)$ can fully describes the range of degrees in a network and their frequencies of occurrence. $p(k)$ can also be defined for directed networks: $p(k^{in})$ and $p(k^{out})$.

- *Shannon Entropy of the Degree Distribution* (H): entropy is a concept used in thermodynamics, statistical mechanics, and information theory. It measures the magnitude of disorder in a system. Following the information theory approach, the entropy measures the presence of randomness in a random event (COVER; THOMAS, 2012). Considering a CN, the entropy of $p(k)$ is a measure of heterogeneity on a network (COSTA et al., 2007).

$$H = -\sum_{k} p(k) \log p(k) \tag{2.14}$$

  The degree distribution entropy is equal to zero only if all the network vertices have the same degree, and is maximum for a uniform degree distribution.

- *Assortativity coefficient*(r): Assortativity is quantified by the connected degree-degree function correlation (NEWMAN, 2002), which indicates how the vertices are connected, e.g., vertices with high degrees can be connected with others with high degree. This can be analyzed by the correlation among the network vertices and their neighbours average degree, and the joint probability $P(k'/k)$ also can represent such relation. To calculate r, a matrix E, where e_{ij} is the fraction of edges connecting vertices of type x to vertices of type y, can be used. It respect the following sum rules:

$$\sum_{xy} e_{xy} = 1, \quad \sum_{y} e_{xy} = a_x, \quad \sum_{x} e_{xy} = b_y, \tag{2.15}$$

  where a_x and b_y are the fraction of edges starting and ending at vertices with values x and y, respectively. Considering the matrix E is possible to calculate the assortativity by using the Pearson correlation (NEWMAN, 2003a):

$$r = \frac{\sum_{xy} xy(e_{xy} - a_x b_y)}{\sigma_a \sigma_b}, \tag{2.16}$$

  where σ_a and σ_b are the distributions a_x and b_y standard deviations. A positive r indicates that vertices of same type are connected, e.g., high degree $\rightarrow$ high degree, and a negative r indicates that vertices of different types are connected, e.g., high degree $\rightarrow$ low degree.

- *Network Efficiency* (E): is a measure of how efficient the network elements exchange information (LATORA; MARCHIORI, 2001). It is calculated as:

$$E = \frac{1}{N(N-1)} \sum_{i \neq j} \frac{1}{d_{ij}}, \tag{2.17}$$

  where d_{ij} is the geodesic path between vertices i and j. Its assumes that flow takes the geodesic paths, and $0 \leq E \leq 1$, where $E = 1$ is the case of a complete graph with all the $N(N-1)/2$ edges.

Another useful kind of CN metric are the centrality ones, which tries to measure the vertices importance to the connectivity of the network. Besides the k and $C(i)$ already presented, some others metrics can be used:

- *Betweenness Centrality* (C_B): the importance of a vertex v_i is quantified by the sum of the ratio of all-pairs shortest paths that pass through v_i (COSTA et al., 2007), calculated as follows:
$$C_B(i) = \sum_{j,k \in V} \frac{\sigma(j,k|i)}{\sigma(j,k)}, \tag{2.18}$$
where V is the set of network vertices, $\sigma(j,k)$ is the quantity of geodesic paths between vertices v_j and v_k, and $\sigma(j,k|i)$ is the quantity of geodesic paths between the vertices that pass through the vertex v_i; C_B is higher for vertex that are more important to the existence of a geodesic path between other vertices, and consequently may be more important for the network. Betweenness can also be calculated for edges in a similar way.

- *Closeness centrality* (C_C): the importance of a vertex v_i is defined as the inverse of the average distance between it and all the other network vertices (BOCCALETTI et al., 2006)
$$C_C(i) = \frac{1}{\frac{1}{N}\sum_{j=1}^{N} d_{ij}}, \tag{2.19}$$
where d_{ij} is the geodesic path between the vertices v_i and v_j. Vertices that have an smaller average distance to the others are more important to the network.

- *Eigenvector centrality* (C_E): account the importance of a vertex in respect to the ones it is connected (NEWMAN, 2010). Given A and its eigenvalues λ and their respective eigenvectors $\mathbf{x}$, that satisfies $\lambda\mathbf{x} = A\mathbf{x}$, the eigenvector centrality of a vertex v_i ($C_E(i)$) is calculated as:
$$C_E(i) = \frac{1}{\lambda}\sum_{i=1}^{j} a_{ij}x_j, \tag{2.20}$$
where x_j is the j-th element of the eigenvector $\mathbf{x}$ associated to the largest eigenvalue.

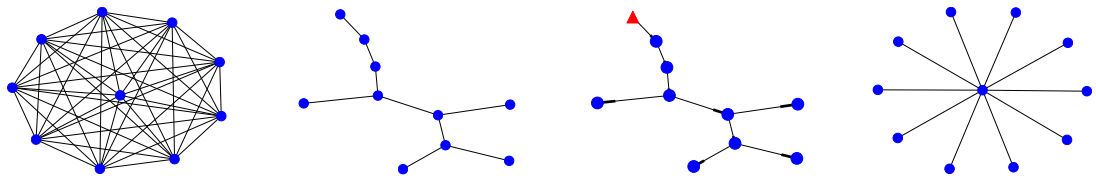
- *Random Walk centrality* (C_R): The facility of a random walker arrive or pass through a vertex is related to it centrality on the network (NEWMAN, 2005). The C_R is defined as the number of visits a vertex have by a random walker starting at vertex s and walking during L fixed steps, performed with all possible vertex s. The random walk is a stochastic process described by transitions probabilities among the network vertices (NOH; RIEGER, 2004). It is a simulation of a walker randomly choosing the path it will make over the network. A random walker at a vertex i and step s can stochastically move to any of its neighbors by some transition probability, defined as:
$$P_{ij} = \frac{A_{ij}}{k_i} \tag{2.21}$$

2.2.2 Complex Networks Models

Before the data describing real-world networks became abundant, abstract theoretical graph models were studied, and some regular networks were examined and used in different fields, as material science and parallel computing (CUI; KUMARA; ALBERT, 2010). Some of these are listed below:

- *Complete*: A network with all the possible edges between N vertices, $M = N(N-1)/2$ - see Figure 3a;
- *Tree*: A network with the minimum number of edges to make it connected, i.e., $M = N - 1$, and consequently without cycles - see Figure 3b;
- *Rooted Tree*: A *directed* Tree network with a root vertex v_s, which has $k_s^{in} = 0$ - See Figure 3c;
- *Forest*: A set of *disconnected* Trees
- *Star*: A network were a single vertex is connected to all the other vertices - see Figure 3d.

Figure 3 – Examples of Regular networks with $N = 10$ (a) Complete ($M = 25$), (b) Tree ($M = 11$), (c) Rooted Tree, the red triangle is the root vertex ($M = 11$), and (d) Star ($M = 10$).



(a) (b) (c) (d)

Source: Author

An important model was the one proposed by the mathematicians Erdös and Rényi (ERDOS; RÉNYI, 1960), which is a model for random networks and is named the ER model. It consists of defining the number of vertices N and a probability of connecting each pair of vertices p. Such model results in a degree probability distribution following a Poisson distribution with the peak at $\overline{k}$ for the generated network. For $N \to \infty$, $\overline{k}$ is calculated as:

$$\overline{k} = p(N-1) \tag{2.22}$$

In practical applications, $\overline{k}$ is fixed and p is chosen depending on N values:

$$p = \frac{\overline{k}}{N-1}. \tag{2.23}$$

In the 90's, the early CN studies were related to the topology of different self-organizing systems, as genetic networks, the World Wide Web, and social networks. The findings were related to how the networks elements were connected and resulted in two important models capable of reproducing such systems topology. The first is known as *Small-World* (SW) model, the SW concept emerged from a sociology experiment (TRAVERS; MILGRAM, 1969), also known as six degrees of separation, in the experiment was shown that in average the individuals in our society are far away from each other by six handshakes. In the seminal paper (WATTS; STROGATZ, 1998), a mathematical formulation for such model was presented, which is between regular and random networks.

The SW model is generated by starting with a regular network with N vertices, where each one is connected to the $\mathcal{K}$ nearest neighbors, resulting in $2k$ edges, with $\mathcal{K} \gg \ln(n)$ to guarantee a connected random graph. The regular network edges are rewired at random with probability p. $p = 0$ results in the original regular network with long distances and many triangles, and with $p = 1$ generates a random network. For a long interval of p, the resulting network presents small distances due to the addition of some edges connecting distant vertices, and the number of triangles remains almost the same. The SW model also results in networks with a degree probability distribution following a Poisson distribution with the average value equal to $\overline{k} = 2\mathcal{K}$.

Considering the real world large networks where some vertices are highly connected, while others have few connections, resulting in a power law degree probability distribution, (BARABÁSI; ALBERT, 1999) proposed a network model named *Scale-Free* (SF) networks. For SF networks, the degree *complementary cumulative distribution function*, or the tail function, follows (2.24) for large k values.

$$P(K > k) \sim k^{-\gamma}, \tag{2.24}$$

which is known as a Power Law (CLAUSET; SHALIZI; NEWMAN, 2009), or Pareto distribution. This is a "heavy-tailed" distribution, which indicates high values are present in the data (ALSTOTT; BULLMORE; PLENZ, 2014). It is possible that the data only follows a power law after a lower bound, named x_{min}. This result in the following :

$$P(X > x) = \left(\frac{x}{x_{min}}\right)^{(-\alpha+1)} \tag{2.25}$$

SF networks are generated by two simple mechanisms (BARABÁSI; ALBERT, 1999), growth and preferential attachment. Starting with a number N_0 of vertices, after a time step adds $n \ll N_0$ vertices, the new vertices will be connected with the other vertices

with a preferential attachment behavior, the probability that the new vertex be connected to another vertex i is proportional to the degree of i:

$$p(\{i,j\}) = \frac{k_i}{\sum k}, \tag{2.26}$$

where $\sum k$ is the sum of all vertices' degrees before the new vertex is connected.

2.2.3 Spatial Distribution Networks

Spatial Distribution Networks (SDN) are a specific case responsible for the flow of goods and services from a source element to end users at sink nodes (GASTNER; NEWMAN, 2006) and are physically dependent on the geography of the embedding space (BARTHÉLEMY, 2011). They normally have a Tree topology, with a single source vertex feeding the network flow (NEWMAN, 2010; VIANA et al., 2013), including engineered systems as Gas (CARVALHO et al., 2009) and Power (DELBEM; CARVALHO; BRETAS, 2005) Distribution Systems. These engineered distribution systems are connected with meshed Transmission Networks, which are responsible for dispatching large flows of commodities from generating units located at long distances from the consumer centers to the Distribution Networks (CARVALHO et al., 2009; SCALA et al., 2014).

Spatial, or Geographical, Networks can be represented as a graph $G = (V, E, D)$, where D is a set of vectors $D = (\overrightarrow{g_1}, \overrightarrow{g_2}, ..., \overrightarrow{g_N})$, with $\overrightarrow{g_i}$ indicating the spatial position of the Graph vertex i (COSTA et al., 2011). The edges in such networks are also physically located, as cables on electric power systems, and pipelines on water and gas systems. Such spatial networks should be efficiently designed, as they need to present a short distance between the source vertices and the other ones, and the total length of edges should be low, reflecting on building and maintenance costs (GASTNER; NEWMAN, 2006).

A metric useful to characterize SDNs is *Route Factor* (q) (BLACK, 2003). It compares the network with a Star graph, which is the case where all vertices are directly connected to the source vertex. It was used by (GASTNER; NEWMAN, 2006) and (YAZDANI; JEFFREY, 2011) on the characterization of some real-world SDNs. The *Route factor* (2.27) is a relation between the spatial (Euclidean) distance between the vertices and the source vertex, and the distance by the connection along the network edges:

$$q = \frac{1}{N_0} \sum_{i=1}^{N_0} \frac{l_{i0}}{d_{i0}}, \tag{2.27}$$

where N_0 is the number of vertices connected to the source element, l_{i0} is the spatial distance by considering the shortest path between vertex i and the source element (labeled as 0), and d_{i0} is the direct Euclidean distance between vertex i and the source. The smallest value of q is equal to 1 and occurs when all the vertices are directly connected to the source and the network forming a Star Graph (GASTNER; NEWMAN, 2006).

They argue that a "good" SDN needs to have relatively short paths from each vertex to the source vertex (star graph is the optimal solution), and the sum of the length of the edges should be low to an economical network build and maintenance (minimum spanning tree is the optimal solution). Based on this, they proposed a model to growth SDN accounting such aspects, the Route factor, and the average edge length.

Gastner e Newman (2006) evaluated the efficiency and spatial topology of the following real-world SDNs:

1. *Sewer system* in the City of Bellingham, Washington;
2. *Natural gas pipelines*, the first in Western Australia (WA) and the second in the south-eastern part of the US state of Illinois (IL);
3. *Commuter rail system* operated by the Massachusetts Bay Transportation Authority in the city of Boston, MA.

They argue that the real-world networks examined presented a good resulted, giving nearly optimal values for both metrics.

Yazdani e Jeffrey (2011) investigated four real Water Distribution Networks that were characterized in a similar way to (GASTNER; NEWMAN, 2006), the networks were:

1. *East-Mersea* in the UK;
2. *Colorado Springs* in the United States;
3. *Kumasi* in Ghana, Africa;
4. *Richmond* in Yorkshire, UK.

Table 1 presents the *Order* and the *Route Factor* obtained for the networks investigated in (GASTNER; NEWMAN, 2006) and (YAZDANI; JEFFREY, 2011). The Water Distribution Networks share a very similar q, and the Sewer System is in the same range of values. The Gas WA and Rail networks have the lower values. The *Route Factor* will be used to characterize the Brazilian DS samples

2.3 Vulnerability Analysis

Vulnerability Analysis history is intimately related with military operations research (ALDERSON et al., 2013), as the study of the Soviet Railway System (HARRIS; ROSS, 1955) that investigated what link should be removed from the network to decrease the most of its flow capacity. Since the availability of large amount of data describing different real-world systems (PAHWA; SCOGLIO; SCALA, 2014), Vulnerability Analysis could

Table 1 – *Route Factor* obtained for real-world spatial distribution networks. N is the Order of each network and q is the *Route Factor*.

Network	N	q
Sewer System (GASTNER; NEWMAN, 2006)	23992	1.59
Gas WA (GASTNER; NEWMAN, 2006)	226	1.13
Gas IL (GASTNER; NEWMAN, 2006)	490	1.48
Rail (GASTNER; NEWMAN, 2006)	126	1.14
East -Mersea (YAZDANI; JEFFREY, 2011)	755	1.54
Colorado Spings (YAZDANI; JEFFREY, 2011)	1786	1.45
Kumasi (YAZDANI; JEFFREY, 2011)	2799	1.46
Richmond (YAZDANI; JEFFREY, 2011)	872	1.67

Source: Author

be performed in a range of systems, as Transportation (HONG et al., 2017), Power (ROSAS-CASALS; VALVERDE; SOLÉ, 2007; KIM et al., 2017), and Biological (LUSSEAU, 2003; COOK; FRANKS; ROBINSON, 2014; KUNERT-GRAF; SAKHANENKO; GALAS, 2017).

Vulnerability Analysis aims to understand the consequences of different types of events on systems performance. The Vulnerability can be interpreted as intolerance to damaging events, either random, as malicious, to a system (ALBERT; JEONG; BARABÁSI, 2000). In general, such events are investigated separately: Random events are related with errors, as parts removal by failures and environmental interventions, like blizzards, storms, and extreme temperature variations; Malicious events are interpreted as intentional attacks with interventions planned to remove or damage vital parts of a system, as terrorist attacks.

The earlier studies of Vulnerability Analysis using CN theory are related to analytical results on how removals of elements tend to affect the overall network connectivity, which is analyzed by using percolation theory. Percolation theory is linked with a critical threshold, which defines the ratio of removals, due errors or attacks, that leads to the breakdown of the network connectivity (COHEN; HAVLIN, 2010). Callaway et al. (2000) presented a percolation study on random graphs using a general connectivity probability distribution that reflects real-world networks and found exact solutions for the percolation problem. In (COHEN et al., 2000), and (COHEN et al., 2001), the Internet network had its vulnerability investigated by percolation theory due to errors and attack, and they obtained exact solutions for both cases.

Vulnerability Analysis is performed by investigating the consequences of such disruptive events by measuring their *Impact* on the System performance (CUADRA et al., 2015). The evaluation of such impacts enables estimation of damaging events effects, and also how different systems behave. Given a performance metric (P), the Impact (I) of an event ($\mathbf{j}$) can be estimated by quantifying the caused system performance drop (OUYANG

et al., 2014), as shown in the following equation:

$$I = \frac{P_0 - P_{\mathbf{j}}}{P_0}, \tag{2.28}$$

where $\mathbf{j}$ is a set containing the system damaged parts, P_0 is the system original performance value, and $P_{\mathbf{j}}$ is the new performance after damages. I is defined in the interval $[0, 1]$.

A variety of performance metrics already had been proposed and applied to different systems and phenomena. The most used ones, which are based only on CN topological characteristics, are presented below:

- *Average Geodesic Path* (l): defined in Section 2.2.1;
- Diameter (D): defined in Section 2.2.1, and used in (ALBERT; JEONG; BARABÁSI, 2000);
- *Network Efficiency* (E): defined in 2.2.1. Used in (TRAJANOVSKI et al., 2013);
- *Relative Order of the Largest Connected Component* (LCC): which is the fraction of nodes that belongs to the Connected Component with higher Order after a damaging event,

  $$LCC = \frac{N_c}{N}, \tag{2.29}$$

  where N_c is the largest Component Order after the event, and N is the network original Order. Used in (TRAJANOVSKI et al., 2013; IYER et al., 2013).

Vulnerability Analysis can be performed by simulations of both types of disruptive events (OUYANG et al., 2014), errors and attacks. Errors, which are related to the stochastic nature of a system' elements failures, is simulated by sequential, random removals of system parts, and assuming a uniform probability of failure for all system' elements. Such removals are performed until a maximum impact is reached ($I = 1$), i.e., total system' collapse. Due to the stochasticity, the simulations need to be repeated to generate a set of significant samples of the possible system performance loss. Such trials provide an average and standard deviation value of I.

On the other hand, attacks are simulated by parts removal respecting some estimated importance of network elements, trying to mimic a planned intervention to cause high impacts as terrorist attacks. CN centrality measures (COSTA et al., 2007), which quantify the topological importance of vertices in a network, .e.g., the Degree (k_i) and the Betweenness Centrality (C_B) (see Section 2.2.1) are usually used as an importance measure to perform attacks simulations (BOCCALETTI et al., 2006). Similar to errors simulation, the parts are removed sequentially until the system suffers the maximum impact.

The seminal paper (ALBERT; JEONG; BARABÁSI, 2000) presented a numerical analysis using a uniform random removal to simulate errors, and removal of vertices with the higher number of connections to emulate attacks over networks. Such study was performed to compare the Vulnerability of two network models, respectively the ER and SF network models (previously defined on Section 2.2.2), and also using a sample of the Internet routers network, and a sample of the World Wide Web which follows SF model. Albert, Jeong e Barabási (2000) noticed that ER, which is a model of random networks, where each node has approximately the same k, tends not to support both types of removals, errors, and attacks. On the other hand, SF networks, which presents few vertices with high k values, presented a different behavior during simulations. They showed a higher Robustness to random errors than the ER models while being more Vulnerable to directed attacks, the removal of a smaller fraction of the most connected nodes collapses the SF network.

Another parameter related to topological vulnerability is the Assortativity (see Section 2.2.1). In (TRAJANOVSKI et al., 2013), synthetic networks following ER and Albert-Barabasi SF models had their Vulnerability investigated. The networks' topology was changed by degree-preserving rewiring (each network vertex still have the same degree, but their neighboring were changed), resulting in only modification of their assortativity. They showed that the assortativity reflects directly on the Vulnerability to errors and attacks. High assortativity reduces the vulnerability to attacks while the vulnerability to errors increases and the converse is also true.

The mentioned studies are related to the Static Vulnerability, which investigates the impacts regarding connectivity of networks and without considering the network dynamics. This type of analysis uses removals simulation and accounting some topological metric as a performance measure. For both types of disruptive events, the critical fraction (f_c) (COHEN et al., 2000; WU et al., 2011), which is the threshold of the ratio of removed vertices (f) by some strategy that will collapse the entire network, can be numerically or analytically estimated. If $f < f_c$ the network will still have a Connected Component containing a part of the original network.

Another possibility of vulnerability assessment is to perform a Dynamic Vulnerability Analysis (BOCCALETTI et al., 2006), which accounts the interplay between network structure and dynamics. The dynamics of a network naturally presents challenges, since the components can present different capacities and the load uncertainty is directly related to time and space. Avalanche, or cascade, failures are linked with overloads due to flow redistribution over a network (MIRZASOLEIMAN et al., 2011), and it can be cited as an example, cascading on electric power systems (PAHWA; SCOGLIO; SCALA, 2014), congestions on communication networks (XIA; HILL, 2008), and impact diffusion in financial networks (SILVA; SOUZA; TABAK, 2017). Another dynamic related with vulnerability

is the capacity of a network to use backup connections to deal with damaging events or recovery a damaged element, this is known as *Self-Healing* (QUATTROCIOCCHI; CALDARELLI; SCALA, 2014; MAJDANDZIC et al., 2014).

The paper (WATTS, 2002) proposed a general binary model related to cascading events, as collective action, diffusion of norms or innovations, and load redistribution. They argue that an initial event increases the likelihood of subsequent events, and their model defines that probability of a vertex change its state is based on the amount of its neighbor that already changed their states. Other studies investigated the Vulnerability of CN due to cascading events. (MORENO; GÓMEZ; PACHECO, 2002) investigated connectivity loss due to load demand increase followed by load redistribution, which can generate new failures due to new overloads. (MOTTER; LAI, 2002) considered the flow along shortest paths and defined a *Capacity* (C_j for vertex v_j) that is proportional to its initial load:

$$C_j = (1+\alpha)L_j, \quad j = 1, 2, ..., N, \tag{2.30}$$

where $\alpha \geq 0$ is a tolerance parameter, and N is the network Order. The removal of elements change the shortest paths and consequently redistributes the flow. They considered that vertices loads are equals to the vertices k, and investigated errors and attacks into single vertices. They noticed that attacks cause severe consequences, and the α parameter is fundamental for a low vulnerability.

Vertex (HOLME; KIM, 2002) and edge (HOLME, 2002) overload in evolving networks also were investigated, these studies adopted the betweenness centrality as vertices loads. For edges overload, the ER model resulted in more robust networks than the SF model. In the case of vertices overload, they observed that vertices capacity must follow network growth to avoid cascades failures. In (MORENO et al., 2003), the average load effect on cascade failures is investigated, and they showed that above a critical average load a single failure could cause cascading failures over the entire network. They investigated the specific case of SF models focusing on communication networks, and they also used the betweenness centrality as load values, which is coherent in communication networks. All the cited CN Vulnerability Analysis studies use the average and standard deviation impact of damaging events after the simulation trials to perform the analysis.

A recent study proposed the use of some unique Robustness measures, called as the $R-index$ (SCHNEIDER et al., 2011):

$$R = \frac{1}{N}\sum_{i=1}^{N} P(i) \tag{2.31}$$

where $P(i)$ is a performance metric, as LCC, given the removal of i elements following a specific removal strategy. The values of R are in the interval $1/N$ (for a Star network) to $(1-1/N)/2$ (for a Complete network), for $N \to \infty$, $R \in [0, 0.5]$. Considering the $R-index$,

a $V - index$ is straightforward:

$$V = \frac{1}{2} - R. \tag{2.32}$$

In (IYER et al., 2013), they proposed a rewiring strategy to reconfigure networks connections by preserving topological features and increasing the R value, which was performed by changing the networks assortativity.

Recently, some studies investigated the robustness of complex systems by accounting both damages and the process of network "healing". Farr et al. shows that instead of redundancy, a network can withstand damages by repairing damaged elements and reconnecting them to the system. (FARR; HARER; FINK, 2014). In (BÖTTCHER et al., 2017), a model to describe the failures process together with repair is presented, showing that systems under such dynamics tend to coexists in two states, and the transitions between these states are dependent on the model control parameters. Shang analyzed the improvement on the robustness due to repair dynamics of different networks models (SHANG, 2015).

In (QUATTROCIOCCHI; CALDARELLI; SCALA, 2014), the healing of the network is obtained by using fixed backup connections to reconfigure the system and reduce its performance loss. Robustness is evaluated under such dynamic in different networks models using a routing algorithm to activate the backup connections. A similar approach is used in (MORONE et al., 2016), with the addition of a mathematical model of the simulated robustness. The latter work considers only a single system with a tree topology, where a single element is the flow source. However, such studies do not consider the capacity constraints related to using the backup connections. Moreover, there is a need for understanding dynamic aspects, such as reconfiguration, in interconnected systems (SHEKHTMAN; DANZIGER; HAVLIN, 2016). Such need is related to even more complex human-made, data-intensive systems, like smart grids and smart cities.

2.3.1 Power Systems Vulnerability Analysis

Power Systems are networked system responsible for transmitting electrical energy from generating units to final consumers. Generating units provide electric power that is transmitted in high-voltage by Transmission Networks to the demand centers, where the Distribution Systems (DSs) deliver medium and low-voltage electrical energy to end customers (CHOWDHURY; KOVAL, 2011). A high-voltage Transmission Network is, in general, represented as a graph with vertices representing the generation, transmission and distribution stations, and edges are the transmission lines (PAGANI; AIELLO, 2013). The network can be represented as an undirected or a directed graph, and also can have weights representing the physical features of the system (BOMPARD; LUO; PONS, 2015).

The first studies regarding Power Systems and CNs were related to describing their topological organization. (WATTS; STROGATZ, 1998) analyzed the US Transmission

Network and noticed that it follows an SW model. In (BARABÁSI; ALBERT, 1999), they argue that the electrical power grid of western US follows an SF model. However, such finding was not supported by subsequent studies. The US grid topology was investigated in (AMARAL et al., 2000) and (ALBERT; ALBERT; NAKARADO, 2004), they both found that the US grid follows the SW model by describing its degree probability distribution. In (ROSAS-CASALS; VALVERDE; SOLÉ, 2007) the EU grid also resulted in a similar degree distribution and average values, reflecting similarities on requirements and technological considerations in such systems development.

The high-voltage Transmission Network vulnerability already had been extensively investigated (ALBERT; ALBERT; NAKARADO, 2004; DOBSON et al., 2007; SOLÉ et al., 2008; WANG; RONG, 2011; PAHWA; SCOGLIO; SCALA, 2014; OUYANG et al., 2014; KIM et al., 2017). Vulnerability Analysis of Power Transmission Networks is related to the occurrence of large-scale failures (DOBSON et al., 2007; PAHWA; SCOGLIO; SCALA, 2014), affecting a significant part or even the entire system. Such severe outages, or blackouts, normally occur in a fast manner that does not allows operational intervention, resulting in serious problems, as economic and social losses (AMIN, 2005). Examples include the 2003 blackouts in North America and Europe (LISCOUSKI; ELLIOT, 2004; ANDERSSON et al., 2005). Blackouts already had been studied using CN Vulnerability Analysis (ALBERT; ALBERT; NAKARADO, 2004) and provided interesting insights about vulnerabilities of Transmission Networks (CUADRA et al., 2015).

The first Vulnerability analysis using real electric power system data was performed on the US Transmission Network in Albert, Albert e Nakarado (2004), where vertices were removed randomly, and also respecting decreasing degree values. A cascade failure model was also applied, and they noticed that the US power grid is robust to most of the removals. However, the removal of some specific vertices produces high impacts, the removal of 4% of high degree vertices causes around 40% of connectivity loss. They also investigated the removal of vertices with higher loads, and in such scenario, the removal of 2% of higher load vertices causes an even higher impact, near to 60% of connectivity loss. The scenario with load redistribution resulted in the higher performance loss. They argue that besides the system redundancy in generation and distribution substations, the system is highly dependent on the transmission substations.

In (CRUCITTI; LATORA; MARCHIORI, 2004b; CRUCITTI; LATORA; MARCHIORI, 2005) the European Transmission Network was also investigated, specifically the French, Italian and Spanish networks. These studies focused on investigating the elements that removals may cause severe connectivity loss. Such grids were also investigated considering specific vertices removals in (ROSATO; BOLOGNA; TIRITICCO, 2007), and their results were consistent with the previously obtained by Crucitti et al., all these studies considered only topological features of analyzed grids. (ROSATO; BOLOGNA;

TIRITICCO, 2007) and (SOLÉ et al., 2008) investigated the European national grids individually, inferring that the grids can be classified into two groups, vulnerable and robust, due to their topological differences described by them $\overline{k}$. These results were also compared with conventional Reliability indices as energy not supply, total loss of power, and average interruption time, indicating a correlation between such topological vulnerability provided by each grid and their reliability indices.

Hybrid Approaches

Those cited studies used a purely topological approach, by applying general CN concepts to electric power systems Vulnerability Analysis. However, electric power systems have some particularities that should be considered (PAGANI; AIELLO, 2013; BOMPARD; LUO; PONS, 2015), as the current flow described by the Kirchoff's laws, and the variety of types of elements, transformers, cables, switches, and capacitors. Similar to the topological metrics used to describe a CN structure and nodes importance, some studies proposed specific metrics regarding the particularities of electric power systems (BOMPARD; LUO; PONS, 2015). Such metrics are known as extended topological measures, or simple hybrid approaches (CUADRA et al., 2015) since they combine CN and Electrical Engineering concepts.

An electric power system can be represented as a graph with three types of vertices: *i)* Generation buses, which inject power in the network; *ii)* Transmission buses, which only transmits the power over the network; *iii)* Load buses, where the power is delivered to the loads. The electric connection between two buses i and j is physically governed by an Impedance ($Z_{ij} = R_{ij} + jX_{ij}$, where R is the resistance, and X is the reactance), which describes the opposition to current flow (I) due to an applied electric potential difference (V_{ij}). Similar to an Adjacency matrix, electric power systems also have an Impedance matrix ($\mathbf{Z}$), describing the impedance values of the network connections, matrix element (i, j) refers to the Z_{ij} of the connection between buses i and j. The electrical connections admittance is the inverse of their impedance $Y_{ij} = Z_{ij}^{-1}$.

A electric power system operates in a sinusoidal steady state (GLOVER; SARMA; OVERBYE, 2012), and each vertex i have an associated $\widetilde{V}_i$, which is a complex voltage ($\widetilde{V}_i = |V_i|\measuredangle\delta_i.$), and the current flowing through the network is related with the electrical connections complex admittance ($\widetilde{Y}_{ij} = |Y_{ij}|\measuredangle\theta_{ij}$). It can be represented as:

$$\mathbf{I} = \mathbf{Y}\,\mathbf{V}, \tag{2.33}$$

where $\mathbf{V}$ is an N-dimensional vector of the complex voltages at the network vertices, and $\mathbf{I}$ is an N-dimensional vector of complex currents injected into the network at each vertex. The $\mathbf{Y}$ elements are defined as follows:

- Y_{kk}: sum of admittances connected to vertex k - named *self admittance*;

- Y_{kn}: negative sum of admittances connected between vertices k and n - named *mutual admittance* or *transfer admittance*,

and $Y_{ij} = |Y_{ij}|e^{j\theta_{ij}} = G_{ij} + jB_{ij}$, G and B are named as conductance and susceptance, respectively. From (2.33), is possible to write the current equation for a bus v_i:

$$I_i = \sum_{n=1}^{N} Y_{in} V_n, \tag{2.34}$$

and knowing that the power S is equal to $S = VI^*$, the (2.33) can be rewritten as an equation for power flow, rather than current flow:

$$\mathbf{S} = \mathbf{V} \circ (\mathbf{Y}\mathbf{V}^*), \tag{2.35}$$

where $\circ$ indicates element-wise vector multiplication, and $\mathbf{S} = \mathbf{P} + j\mathbf{Q}$ is a vector of complex power injection at each vertex (P - active power and Q - reactive power). At each vertex i, the total injected power is the difference between the generation and the load power, S_i^G and S_i^L respectively:

$$S_i = P_i + jQ_i = (P_i^G - P_i^L) + j(Q_i^G - Q_i^L) = V_i I_i^* \tag{2.36}$$

Using (2.34) in (2.36):

$$P_i + jQ_i = V_i \left[\sum_{n=1}^{N} Y_{in} V_n \right]^*, \tag{2.37}$$

and using the polar notation, (2.37) became:

$$P_i + jQ_i = V_i \sum_{n=1}^{N} Y_{in} V_n e^{j(\delta_i - \delta_n - \theta_{k,n})}, \tag{2.38}$$

which can be decomposed in the real and imaginary parts:

$$P_i = V_i \sum_{n=1}^{N} Y_{in} V_n \cos(\delta_i - \delta_n - \theta_{k,n}) \tag{2.39}$$

$$Q_i = V_i \sum_{n=1}^{N} Y_{in} V_n \sin(\delta_i - \delta_n - \theta_{k,n}) \tag{2.40}$$

Each v_i at a electric power system with N vertices will have four electrical variables: P_i, Q_i, V_i and δ_i, and for power flow calculation, two of these variable can be fixed by using the knowledge about the system. In general, three types of buses are used (FRANK; REBENNACK, 2016):

1. *Slack bus*: The V and δ are known, while P and Q are unknown. Normally, only one vertex is the slack bus, providing a single reference for the entire system ($V = 1.0$ p.u. and $\delta = 0°$);

2. *Load bus*: The P_i and Q_i are known - PQ buses, normally represents generators and loads;

3. *Voltage-Controlled Bus*: The P_i and V_i are known - PV buses, corresponds to a local source or reactive power to regulate its voltage to a desired value.

The solution of the n equations (2.39) and (2.40) provides the power flow over the entire network. An way to simplify the power flow calculation is the use of some approximations (FRANK; REBENNACK, 2016):

- Line resistances (active power losses) are negligible, i.e., $R \ll X$;
- Voltages absolute values are set to one per unit ($V_i = 1$ p.u., $\forall i.$);
- Voltage angle differences are assumed to be small, $\sin(\theta) = \theta$ and $\cos(\theta) = 0$;

Such approximations make the power flow accounts only the active power, and result in the solution of the following linear equation for each vertex:

$$P_i = \sum_{n=1}^{N} B_{in}(\delta_i - \delta_n), \tag{2.41}$$

which is known as the DC power flow. A variety of hybrid approaches already had been performed on different Transmission Networks, using both, AC and DC power flow. The electrical features are considered as edges weights, e.g., the impedance and admittances. The power flow is also used as direction of edges, resulting in *directed* and *weighted* graphs representation.

The studies that used the electrical features of electric power systems also proposed some "electrical metrics" inspired on conventional CN metrics to perform structural and vulnerability analysis of electric power systems. Since the use of purely topological metrics can lead to misleading results (HINES; COTILLA-SANCHEZ; BLUMSACK, 2010), such metrics are capable of better describing the importance of a Transmission Network elements criticality (BOMPARD; LUO; PONS, 2015). One metric is based on the concept of electrical distance, which describes the electrical connectedness, and in (HINES et al., 2010) the inverse of the system Admittance matrix $\mathbf{Y}$, is used as electric distance matrix $\mathbf{E}$, with each element $e_{ij} \in \mathbf{E}$ describes the relation between V and I for the electrical connection, or edge, between a nodes pair. Using $\mathbf{E}$, a connectivity distance is calculated as:

$$\overline{e_i} = \sum_{j=1, j\neq i}^{N} \frac{e_{ij}}{N-1}, \tag{2.42}$$

and its inverse is known as electrical centrality (HINES et al., 2010):

$$c_i = \frac{1}{\overline{e_i}} \tag{2.43}$$

The main findings of using electrical centrality are that buses that do not are physical hubs (high degree value) showed to be electrical hubs (high electrical centrality), which serve many loads, and by using the **E** matrix to construct the network, its results in properties as scale-free degree distribution (WANG et al., 2012).

(DWIVEDI; YU; SOKOLOWSKI, 2009) proposed to use the reactance X_{ij} of the transmission lines as edges weights, and consequently, the shortest paths will be the ones with lower reactance, where more power can be transmitted, they define the efficiency of an edge as $\epsilon_{ij} = X_{ij}^{-1}$. The weights were used to calculate a line betweenness, which was used to simulate directed attacks and were compared with random errors. The impact of such events was estimated by using the average of the edges efficiency after removals:

$$J = \frac{1}{N(N-1)} \sum_{i \neq j \in V} \epsilon_{ij}. \tag{2.44}$$

In (NASIRUZZAMAN; POTA; MAHMUD, 2011; NASIRUZZAMAN; POTA; ANWAR, 2012; NASIRUZZAMAN et al., 2012), the power flow values were used to find the critical elements in a power transmission grid by a series of hybrid centrality measures, the transmission lines weights are their admittance. The two metrics that provided the better results according to Cuadra et al. (2015) were *electrical degree centrality* and *electrical betweenness centrality*. The *electrical degree centrality* $C_D^E(i)$ is calculated as follows:

$$C_D^E(i) = \frac{\sum_{i \sim j} P_{ij}}{N-1}, \tag{2.45}$$

where $i \sim j$ indicates a edge connecting vertex v_i and v_j, and P_{ij} is the power flowing through the electrical connection between v_i and v_j.

The *electrical betweenness centrality* $C_B^E(i)$ is similar to the topological betweenness centrality (Section 2.2.1):

$$C_B^E(i) = \sum_{j \neq k \neq i \in V} \frac{P_{jk}(i)}{P_{jk}}, \tag{2.46}$$

where $P_{jk}(i)/P_{jk}$ is a ratio between the amount of edges transmitting power from v_j to v_k that needs v_i along the shortest path, which uses the admittance as edges weight. These metrics were tested in different IEEE Test Systems (30, 57, 118, and 300 bus), and observed results showed that such metrics are feasible to highlight the criticality of vertices in a Power Transmission Network.

(WANG; SCAGLIONE; THOMAS, 2010) also proposed an extension of centrality metrics to embed the electrical features of electric power systems. Considering the Admittance matrix (**Y**), they defined the *electrical degree centrality* as:

$$C_D^E(i) = \frac{\|\mathbf{Y}(ii)\|}{N-1}, \tag{2.47}$$

The use of the C_D^E proposed in (WANG; SCAGLIONE; THOMAS, 2010) resulted in a change in the degree distribution when compared with the pure topological k, resulting

in a different node importance rank. Their results were obtained using the NYISO-2935 (New York Independent System Operator's Transmission Network) and the IEEE-300 bus test system.

In (KOÇ et al., 2014; WANG et al., 2015), they proposed a metric to evaluate Vulnerability of transmission networks to cascading failures, named *Graph Resistance* R_G. It is calculated by using the weighted Laplacian matrix L[6], where weights are the edges susceptance. Considering the eigenvalues (λ) of L, R_G i calculated as follows:

$$R_G = N \sum_{i=1}^{N-1} \frac{1}{\lambda_i}. \tag{2.48}$$

The R_G value was used during an optimization process to reduce the transmission systems vulnerability, and it helps to deal with the Braess's paradox[7] (BRAESS; NAGURNEY; WAKOLBINGER, 2005). The R_G value indicates if a new edge will increase or reduce the network vulnerability to cascading failures.

Bompard, Napoli e Xue (2009) proposed the use of an equivalent impedance Z^e, which is equal to the voltage between i and j when $I = 1$, as the weight describing the electrical connections over the network. Using such weights (BOMPARD; NAPOLI; XUE, 2009) introduces a new vertex connectivity measure, named *Entropic Degree*. Consider a random variable X that can assume different values x with $p(x)$ describing $\Pr\{X = x\}$. The Entropy (H) (COVER; THOMAS, 2012), which describes a measure of uncertainty of random variables, is defined as:

$$H(X) = -\sum_{x \in X} p(x) \log_2 p(x), \tag{2.49}$$

its describes the random variable X by considering its distribution probability instead of the variable values.

In (BOMPARD; NAPOLI; XUE, 2009), a normalized edge weight is calculated as:

$$p_{ij} = \frac{w_{ij}}{\sum_j w_{ij}}, \tag{2.50}$$

where w_{ij} is the edge $\{i, j\}$ weight and $\sum_j w_{ij}$ is the strength of vertex v_j. The normalization results in $\sum_j p_{ij} = 1$, and can be used as a probability distribution. By using p_{ij}, the *Entropic Degree* of a vertex i is calculated as:

$$g_i = \left(1 - \sum_j p_{ij} \log_2 p_{ij}\right) \sum_j w_{ij}, \tag{2.51}$$

[6] The Laplacian Matrix is defined as $L = D - W$, where D is a diagonal matrix with d_{ii} elements equal to the v_i weighted degree, or strength, and W is the weight matrix.

[7] The Braess's paradox is related to the possibility of performance decrease due to a new link added to a network. It is originate from transportation networks studies.

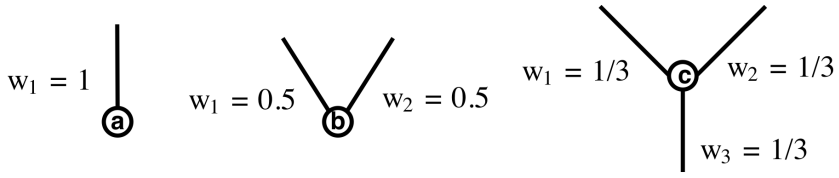
which indicates a vertex importance accounting the total strength of its connection together with the distribution of edges weights.

Consider the three vertices in the Figure 4. They degrees, strengths, and entropic degree are:

$$k_a = 1; \quad k_b = 2; \quad k_c = 3;$$
$$s_a = s_b = s_c = 1;$$
$$g_a = 1; \quad g_b = 2 \quad g_c = 2.59.$$

The values obtained are interesting, while the k represents only the amount of connections, and s accounts only the connections weights, the g deals with both informations and also with the distribution of weights among the edges.

Figure 4 – Example of vertices with different number of edges and edges weights.



Source: Author

In addition to the impedance, (BOMPARD; NAPOLI; XUE, 2009) also proposed a power transmission capacity, C_g^d, defined as the maximum power injected at bus g tolerated by all the edges in the path connecting the generating bus v_g to the load bus v_d, i.e.:

$$C_g^d = min\left(\frac{P_{ij}^{max}}{|f_{ij}^{gd}|}\right), \tag{2.52}$$

where f_{ij}^{gd} is the power on path $\{i,j\}$ caused by a unit power injected at v_g ($g \in G$) and withdraw at v_d ($d \in D$), and G and D are respectivelly the set of generation and load vertices. f_{ij}^{gd} can be calculated using the Power Transmission Distribution Facotrs (PTDF) matrix (FRADI; BRIGNONE; WOLLENBERG, 2001), where the PDTF element ij represents the change in the power in edge i for a unit change of power injection at vertex j.

Using the power transmission capacity, (BOMPARD et al., 2013) proposed an electrical betweenness for edges that accounts the power flowing on the edges:

$$B_e(\{ij\}) = max\left(B_e^p(\{ij\}), |B_e^n(\{ij\})|\right), \tag{2.53}$$

where

$$B_e^p(\{ij\}) = \sum_{g\in G}\sum_{d\in D} C_g^d f_{ij}^{gd}, \quad \text{if} \quad f_{ij}^{gd} > 0$$
$$B_e^n(\{ij\}) = \sum_{g\in G}\sum_{d\in D} C_g^d f_{ij}^{gd}, \quad \text{if} \quad f_{ij}^{gd} < 0$$

A electrical betweenness for vertices was also proposed:

$$B_e^p(v) = \frac{1}{2}(\sum_{g\in G}\sum_{d\in D} C_g^d \sum_{\{ij\}\in E^v} |f_{ij}^{gd}|), \tag{2.54}$$

where E^v is the set of edges connected with vertex v. These metrics were used to evaluate the Europe power transmission network and compared with the purely topological degree and betweenness. The results indicated that the hybrid metrics proposed are better in indicating elements criticality.

Recently, some studies have proposed the consideration of the time domain for Vulnerability Analysis, specifically for attacks against electric power systems (ZHU et al., 2014; YAN et al., 2015; YAN et al., 2017). The time variable is used to perform Sequential Attacks (SA) and are compared with simultaneous, or Concurrent Attacks (CA), The comparison was performed considering a DC power flow with cascading failures. A SA is formulated as a set S of 2-tuples ordered by time:

$$S = \{(a_1, t_1), (a_2, t_2), ..., (a_k, t_k)\}, \quad k \leq N \tag{2.55}$$

where a_i is the i-th attack launched at time t_i. The main finding was that an SA could produce more severe impacts than the same removals by a CA strategy. In (YAN et al., 2017), a reinforcement learning framework was proposed to obtain optimal SA strategies, and these studies used the IEEE test systems and the Polish transmission network.

The process of hidden failures also was addressed by using the load redistribution during cascading failures in (BILIS; KRÖGER; NAN, 2013; WENLI et al., 2016; YAN et al., 2017). The hidden failure is related to the flow redistribution dynamic during cascading failures that can lead to failures of protection or control elements. The results in (WENLI et al., 2016) indicate that the consideration of hidden failures leads to an observation of more severe damages during vulnerability analysis.

In (ZIO; GOLEA, 2012), a hybrid approach is proposed by considering the topological features together with electrical and reliability characteristics of power transmission networks. A weighted graph representation is used, and the weight is related to relevant electrical and reliability properties. Reliability properties of a transmission network was embedded by a reliability matrix $\{p_{ij}\}$, where each element p_{ij} indicates the probability of successful transmission through the edge $\{i, j\}$, and electrical connectivity was represented by the electrical distance (HINES; BLUMSACK, 2008), defined here as the impedance absolute value ($m_{ij} = |Z_{ij}|$). By considering both weights, vertex importance is measured by using a weighted degree.

In addition, an electrical-reliability degree was also proposed:

$$k^e r_i = \frac{1}{\sum_{j\in N} m_{ij} p_{ij}}. \tag{2.56}$$

The study was carried out using the IEEE RTS 96 system, and a ranking of the transmission network elements degrees can be used to identify the critical elements under the different perspectives, topology, reliability, electrical connectivity, and electrical-reliability. They showed that each degree indicates the importance of elements accounting specific characteristics. As low-reliability clusters, electric flow hubs, and project inconsistencies, as high power flow through low-reliability vertices.

Hybrid Performance Metrics

Besides the hybrid characterization and dynamic vulnerability analysis, some hybrid performance metrics also were proposed specifically for Power Transmission Networks Vulnerability Analysis (CUADRA et al., 2015; OUYANG et al., 2014):

- *Source-Demand Efficiency* (E_{SD}): the efficiency considering the Generation and Distribution buses of Transmission Networks,

$$E_{SD} = \frac{1}{N_G N_D} \sum_{i \in G_G} \sum_{j \in G_D} \frac{1}{d_{ij}}, \tag{2.57}$$

  where N_G is the number of Generation Substation and N_D is the number of Distribution Substation. Such metric was applied in vulnerability analysis of the North American high-voltage PG (KINNEY et al., 2005);

- *Connectivity Loss* (CL) quantify the ratio of Distribution buses that have a path to Generation buses (ALBERT; ALBERT; NAKARADO, 2004):

$$CL = 1 - \frac{1}{N_D} \sum_{i}^{N_D} \frac{N_G^i}{N_G}, \tag{2.58}$$

  where N_G is the number of Generation Substation, N_D is the number of Distribution Substation, and N_G^i is the number of Generation buses connected to the Distribution bus i. CL was applied to the North American high-voltage PG.

- *Net-Ability* ($\mathcal{A}$) Using the power transmission capacity, (ARIANOS et al., 2009) presents the concept of as performance measure for power transmission networks:

$$\mathcal{A} = \frac{1}{N_G N_L} \sum_{g \in G} \sum_{d \in D} \frac{C_g^d}{Z_g^d}, \tag{2.59}$$

  Used to perform vulnerability analysis of the interconnected European power transmission network in (BOMPARD; PONS; WU, 2013).

Power Distribution Systems Vulnerability

While Power Transmission Networks already had their Vulnerability widely investigated, the studies and approaches for Vulnerability analysis of DSs are sparse (CUADRA

et al., 2015). The majority of Complex Networks studies of Power Systems consider only the high-voltage Transmission Network (NEWMAN, 2010; PAGANI; AIELLO, 2013). The same also occurs for Vulnerability studies (CUADRA et al., 2015; PAGANI; AIELLO, 2013; NEWMAN, 2010). In the following paragraphs, the studies investigating DSs Vulnerability will be presented in detail.

A DS has a variety of elements, which are buses or branches of the system, and similar to Power Transmission Networks, a DS can also be represented as a graph, where the buses are the vertices, and the branches are the edges. For a more detailed view of such representation see (CAMILLO et al., 2016). The DS buses can be classified into four different types (ZHENG et al., 2012):

1. Buses without loads: poles sustaining overhead cables;
2. Buses with loads: pole-mounted transformers responsible for reducing the voltage to customers level;
3. Capacitor: used to reduce inductive loads effects on the power factor;
4. Bus in Substation: the source of electrical flow, it is a bus located on a substation, where the voltage is stepped down from transmission high-voltage to the distribution voltage level.

The branches, which are the electrical connections between the buses in a DS, also can be classified into four different types (ZHENG et al., 2012):

1. Cable or Line: conducts the power flow over the network;
2. Fuse: opens when it is overloaded to protect the system elements;
3. Switch: capable of opening or closing an electrical connection, it can be classified as:
    - Sectionalizing: isolate system elements, related to system protection;
    - Tie: reconnect system elements, related to load transfer during contingencies;
    - Breaker: responsible for cut the load on the circuit feeder.
        * Manual: needs a field crew to be operated;
        * Automated: is remotely operated from the operation center.
4. Voltage regulator: used to regulate the distributed electricity voltage under different load conditions.

In (PAGANI; AIELLO, 2011), they performed an investigation of the delocalized energy trading capability of the North Netherlands DS by using CN tools, including the system vulnerability. The motivation is the changing caused by the smart grid philosophy,

related to emerging of small-scale energy production. The used samples were modeled as weighted graphs, and the weight was chosen as the resistance of the cables. They characterized the samples by using the weighted degree, or strength, probability distribution, and found that low-voltage samples follow a sum of exponential decays, while medium-voltage samples were better described by a power-law, indicating an SF topology.

They also performed a Vulnerability Analysis, by using the strength and the betweenness centrality as metric to perform target attacks. The performance was measured by using the LCC. The samples are more vulnerable to targeted attacks than to errors, especially medium voltage samples, which is in agreement with the SF topology noticed by degree probabilities. They found that errors need the removal of a large ratio of vertices (90%) to cause an impact of 90%, while directed attacks cause the same impact by removing only the 10% most connected vertices. They also proposed a robustness index:

$$Rob_N = \frac{|LCC_{Random20\%}| + |LCC_{NodeDegree20\%}|}{2}, \tag{2.60}$$

where the LCC values are the average result from simulations and used values of random removals and node degree removal are the obtained when 20% of vertices are removed. Analysis regarding the energy exchanges by relating some economic aspects of the samples, as losses, capacity, redundancy, and limitations, was performed in the Dutch samples. Following the results in (PAGANI; AIELLO, 2011), they proposed a model in (PAGANI; AIELLO, 2013) to support smart grids design, and it was performed by thinking in the new profile of energy exchanges caused by renewable energy sources and micro-production.

After, in (PAGANI; AIELLO, 2014), they tested different network models and evaluated their characteristics by using metrics related to the generated networks topology, average geodesic path, clustering coefficient, betweenness average and variation coefficient, the vulnerability index Rob_N, and the redundancy cost. They argue that an increase on the $\overline{k}$ and moving for an SW topology can improve the robustness and reduce the electricity distribution costs. On the other hand, such improvements will result in investment costs on edges addition and protection schemes. They argue that the motivation of (PAGANI; AIELLO, 2014) is to develop CN based decision-support methods to allow DSs evolution to smart grids.

The Dutch samples were again evaluated in (PAGANI; AIELLO, 2015). In this study, the samples had their vulnerability investigated by vertices removals (errors and attacks), which results were similar to the presented in (PAGANI; AIELLO, 2011), the samples are vulnerable to attacks and robust to errors. The novelty in (PAGANI; AIELLO, 2015) is the vulnerability analysis due to edge removals. They used the second smallest eigenvalue of the network Laplacian matrix, named algebraic connectivity, which indicates the minimum number of edges necessary to split the network into two disconnected elements with similar order (ROSATO; BOLOGNA; TIRITICCO, 2007), named as *number of critical*

edges. They found that a small number of edge removals is enough to split the sample into two similar order networks. They repeated the experiment of (PAGANI; AIELLO, 2014) of using synthetic networks models with similar $\overline{k}$ to the Dutch samples, and with higher values of $\overline{k}$ ($\overline{k} = 4$ and $\overline{k} = 6$), but now considering the vulnerability to both, vertices and edges removals. They noticed that an increase of $\overline{k}$ also improves the robustness to edges removals.

In (NEGERI; KUIPERS; BAKEN, 2015), the low-voltage DS, which delivery the electricity in a suitable manner to end consumers (in Brazil 127 and 220 V), is investigated using CN theory. The authors used topological metrics (average geodesic path, diameter, clustering coefficient), together with hybrid metrics developed specifically to the low-voltage network:

- *Closeness to transform* (θ_i): Describe how close an vertex is to the transform providing flow to the low-voltage network, and is expressed in terms of the equivalent impedance between the transform (v_t) and the vertex (v_i):

$$\theta_i = z_{it} = \frac{(v_t - v_i)}{I_{unit}}, \tag{2.61}$$

  using θ_i, is possible to calculate the entire network closeness to transform:

$$\theta = \frac{\mu_\theta}{1 + \sqrt{\sum_{i \in N, i \neq t} (\theta_i - \mu_\theta)^2}}, \tag{2.62}$$

  where μ_θ is the average closeness of the vertices to transform.

- *Link betweenness to transformer* (β_{jk}): account the portion of current flow that pass through an edge $\{j, k\}$ when a unit current flows from the transform to v_i, while other vertices do not absorb or inject current in the network:

$$\beta_{jk} = \sum_{i \in N, i \neq t} \frac{f^{it}_{\{j,k\}}}{N - 1}, \tag{2.63}$$

  the link betweenness to transform of the entire network is calculated in the same way of the network closeness to transform.

- *Net-Ability to transformer* (η): measure the network capacity of transmission accounting it impedance, in a similar way to the Net-Ability presented in (2.59):

$$\eta = \frac{1}{N - 1} \sum_{i \in N, i \neq t} \frac{C_{it}}{z_{it}} \tag{2.64}$$

They also prosed two performance metrics, voltage feasibility ratio $R_{voltage}$ and load feasibility ratio R_{load}:

$$R_{voltage} = \frac{x}{N}, \tag{2.65}$$

$$R_{load} = \frac{y}{L}, \tag{2.66}$$

where x is the number of vertices with voltage in a acceptable boundary, and y is the number of vertices with load in a acceptable boundary.

They used synthetic networks (radial, binary tree, random networks, SF, and SW) as candidates for low voltage networks and calculated the structural and performance metrics for all the generated samples using three different load scenarios: a classical, a futuristic scenario, with electric vehicle, solar panels, and micro-CHP, and a worst-case where all consumers have the same constant load. They found that the performance is directly related to the structural metrics, and a structural improvement will improve the network feasibility.

They also investigated the vulnerability and found that the SF topology would provide higher robustness to low-voltage networks by account the LCC. The also proposed an optimization procedure to design low-voltage networks by accounting their structure and performance metrics and with costs related to cable lengths. They argue that networks with a low diameter will have better feasibility when consumer loads increase, but with a higher associated cost. An investigation related to the dependence on the communication network and the low voltage network was also performed. They found that the more the communication network is dependent on the low-voltage network electricity, the worst will be the voltage feasibility due to operational load actions guided by erroneous measures after low-voltage failure, and resulting in subsequent failures. They also presented an optimization procedure to design the interdependence between both networks, communication, and low voltage.

Another optimization approach is presented in (PAGANI; AIELLO, 2016), where the Dutch samples were used as base cases, and six different edges addition strategies were applied to each sample. The networks evolution by each strategy was evaluated considering both, topological properties and economic considerations, and applying the metrics presented in their early studies (PAGANI; AIELLO, 2011; PAGANI; AIELLO, 2013; PAGANI; AIELLO, 2014), including the vulnerability index Rob_N. The aim is to optimize the electricity transportation cost. They found that the strategies can decrease the losses by the addition of more edges to the network. In the Dutch samples, this is better performed by adding edges between the vertices with the smallest distance. The studies (PAGANI; AIELLO, 2011; PAGANI; AIELLO, 2013; PAGANI; AIELLO, 2014; PAGANI; AIELLO, 2016) are all related to assessing the economic aspects of electricity distribution and motivated by the coming change of passive end consumers to active prosumers on the smart grid.

The Dutch samples were also used in (CHAI et al., 2016). They are used to investigate the vulnerability of the interconnected medium voltage network and a communication network, similar to (NEGERI; KUIPERS; BAKEN, 2015). However, their focus was on the dynamics of a removal of a DS vertex cascading on the communication network elements.

They performed errors and attacks simulations and evaluated different topologies for the communication network. The numerically demonstrated that a medium voltage DS is less vulnerable when connected to an SW communication network.

(LUO; PAGANI; ROSAS-CASALS, 2016) investigate the spatial feature of cable lengths on power DSs by fitting heavy-tailed distributions (as the power law, exponential and lognormal), in the Dutch samples and also in two Spanish samples. They used two approaches for network rewiring, random vertex shuffling and random edge shuffling, that had their cost optimized using a simulated annealing technique. The cost was defined as the total network length, and they founded that all the samples can have their wiring cost optimized. They also performed a cascading failure model, using the Motter and Lai cascade model (MOTTER; LAI, 2002):

$$C(i) = (1 + \alpha)L(i), \tag{2.67}$$

where C is the vertex capacity, L is the load, and α is a tolerance parameter. A vertex i load was estimated as the total current passing through it, I_i. They used LCC to evaluate the performance of the network during removals. Their Vulnerability Analysis was performed by generating the load of each vertex following a normal distribution since they do not have access to generation and load data. They found that a low α value results in a higher vulnerability. They also correlated the vulnerability results with the available SAIDI[8] reliability index for the Spanish samples. They conclude that an optimal wiring strategy plays a fundamental role in DSs vulnerability.

2.4 Reliability Engineering

The history of Reliability Engineering is directly related to statistics and large-scale production (SALEH; MARAIS, 2006). In the 1920s, the Statistical Quality Control came, and in the 1950s the Reliability Engineering emerged due to the needs of reliable electronic components, which were extensively used during World War II, like radios, radars, and others. In 1954, the first conference on quality and reliability was held, which proceedings became the IEEE Transactions on Reliability. Later, the areas of system safety and software reliability emerged from the advances in electronics (large scale integration devices) and computation (increasing dependence on software). Reliability engineering still investigates single elements by using historical data and accelerate tests (SAHOO et al., 2004) and also deals with large-scale complex systems (WEBER; JOUFFE, 2006).

Reliability Engineering (ZIO, 2013) aims to model the failure process of systems or components by considering system configuration, redundancies, and historical data describing failures. Its accounts how the failure happens, the time to such failure happens, and also ways to mitigate the failures by improving the design or manufacturer

[8] SAIDI is the acronym for the *System Average Interruption Duration Index*, see Section 2.4.2.

processes (SALEH; MARAIS, 2006). The models try to infer the probability of proper functioning of such systems or components (GERTSBAKH; SHPUNGIN, 2016). Which can be a failure probability p_i for failure state and $1 - p_i$ for a working state or dynamic reliability where the failure probability is a function of time (t_i), which is modeled as a random variable $t_i \sim F_i(t)$. The learning of $F_i(t)$ is a fundamental aspect of Reliability Engineering since it allows the prediction of elements functioning during their uses.

The assumption of the time-to-failure as a random variable is also used to model different phenomena, as survival and recurrency time of patiants with a specific disease (MAZUCHELI; ACHCAR, 2011), and the time-to-occurrence of biological processess as neuronal spiking (LIMA et al., 2016), this type of application is called time-to-event, or Life Time Data, analysis (HOSMER; LEMESHOW; MAY, 2008). In the case of time-to-failure, the model is called as Reliability Function $R(t)$, which describes the probability of a correct functioning during a time interval t. It is represented as follows:

$$R(t) = P(T > t), \tag{2.68}$$

with $T > 0$ a random variable representing the time instant when a failure happens. Following that $R(t)$ is a *complementary cumulative probability function*, the *cumulate probability function* is defined as the probability of an individual fail until t:

$$F(t) = 1 - R(t) = \int_0^t f(s)ds, \tag{2.69}$$

where $f(t)$ is the *probability distribution function*.

$R(t)$ can be modelled as a parametric (ACHCAR; CEPEDA-CUERVO; RODRIGUES, 2012) or non-parametric (JAGER et al., 2008) probability distribution. The non-parametric Kaplan-Meier (KM) estimator (KAPLAN; MEIER, 1958) is used to obtain $R(t)$ from historical data, which is useful to time-to-event studies (JAGER et al., 2008). In this research, the historical data is complete, however in cases were incomplete observations are present, specific methods should be applyed to deal with such censoring, see (MEEKER; ESCOBAR, 2014) or (KLEIN; MOESCHBERGER, 2005). Consider a set describing the time-to-failure of n individuals, the KM estimator is obtained by sorting the times in ascending order ($\mathbf{t} = [t_1, t_2, ..., t_n], \quad t_i > t_{i-1}$), and $\widehat{R}(t)$ is estimated as:

$$\widehat{R}(t) = \frac{N_{obs} > t}{n}, \tag{2.70}$$

where $N_{obs} > t$ is the amount of individuals that do not suffer a failure in the instant t. The Equation (2.70) is also known as the empirical Reliability function.

Another useful metric is the Hazard rate ($h(t)$) (AALEN; BORGAN; GJESSING, 2008), which represents the conditional probability of an individual that have not experienced the event of interest by time t to experience its in a small time interval $[t, t + dt]$. $h(t)$ is formally defined in the following way:

$$h(t) = \lim_{\Delta t \to 0} \frac{1}{\Delta t} P(t \leq T < t + \Delta t | T \geq t) \tag{2.71}$$

Differently from $R(t)$ which is a strictly decreasing function, the $h(t)$ can be any non-negative function, and to estimate $h(t)$ the cumulative hazard rate ($H(t)$) needs to be calculated:

$$H(t) = \int_0^t h(s)ds \tag{2.72}$$

To estimate $H(t)$, the Nelson-Aalen (NA) estimator can be used (AALEN; BORGAN; GJESSING, 2008):

$$\widehat{H}(t) = \sum_{t_i \leq t} \frac{d_i}{n_i}, \tag{2.73}$$

where d_i is the quantity of events at t_i, and n_i is the number of individuals susceptible to the events at t_i.

Using (2.71) and (2.73), a connection between the Reliability function and the Hazard rate can be show:

$$\begin{aligned} H'(t) = h(t) &= \lim_{\Delta t \to 0} \frac{1}{\Delta t} \frac{R(t) - R(t + \Delta t)}{R(t)} \\ &= \frac{R'(t)}{R(t)} \end{aligned} \tag{2.74}$$

Considering that in the instant $t = 0$ all individuals are correctly functioning, i.e., $R(0) = 1$, and by integration the relation between $R(t)$ and $h(t)$ becomes:

$$\begin{aligned} -lnR(t) &= \int_0^t h(s)ds \\ R(t) &= exp\Big\{-\int_0^t h(s)ds\Big\} \\ R(t) &= exp\left\{-H(t)\right\} \end{aligned} \tag{2.75}$$

The Hazard rate is useful to understand the changes in the rates of the studied event; it can indicate if the Hazard rate change by time or is constant. Assuming a constant failure rate λ, it can be calculated as:

$$\lambda = \frac{number\,of\,failures}{total\,operation\,time\,of\,units}, \tag{2.76}$$

and using equation (2.75) $R(t)$ becomes:

$$R(t) = e^{-\lambda t}, \tag{2.77}$$

which is the exponential Reliability function, commonly used in Reliability Engineering, inclusive in electric power systems (BOLLEN, 2000), due to the following premise: After a failure, a component can be considered new due to maintenance or replacement, which is a two state model for the failure process, and the transition probabilities between states depend only on the actual state. It is also known as "lack-of-memory" (ZIO, 2013). From $R(t)$ is also possible to obtain the expected time to a failure happen, which is known as Mean Time to Failure (MTTF), or Mean Time between Failures (MTBF) for repairable elements. In the case of an exponential $R(t)$, MTBF is:

$$E[T] = \int_{-\infty}^{\infty} tf(t)\mathrm{d}t = \int_{-\infty}^{\infty} t\lambda e^{-\lambda t}\mathrm{d}t = \frac{1}{\lambda} \tag{2.78}$$

2.4.1 Systems Reliability

Using the $R(t)$ of the elements in a system, is possible to estimate its $R(t)$ and others quantities concerning its reliability, as the system failure rate (calculated in the same way as in (2.76), and system Availability (A) (SMIDT-DESTOMBES; HEIJDEN; HARTEN, 2004):

$$A = \frac{total\,time\,functioning}{total\,system\,operation\,time}, \tag{2.79}$$

Systems with serial or parallel connections can be solved by analytical methods. On the other hand, Complex Systems, which cannot be represented as serial or parallel systems, demand the use of more advanced techniques (KAPUR; PECHT, 2014), as state enumeration approach (KOŁOWROCKI, 2014; BHATT; SHAH; JANI, 2014), which already had been used for DSs (FALAHATI; FU; WU, 2012; FALAHATI; FU, 2014). Estate enumeration consists of listing all the states of a system and estimating the probability of occurrence of each one by using the system parts $R(t)$. Then, Reliability indices of interest can be calculated from the enumerated states, as loss of load probability and expected energy not supplied.

However, states enumeration becomes intractable for large-scale systems, since the combinatorial explosion (a system with n two-state elements and m two-state connections result on $2^{(m+n)}$ possible states) (AL-MUHAINI; HEYDT, 2013b). For large scale systems, the use of simulation approaches, as Monte Carlo Simulation (MCS) (BILLINTON; LI, 1994; ZIO, 2013), or using a Markov Model to sample the system behavior (AL-MUHAINI; HEYDT, 2013a). MCS consists of a virtual experiment where the stochastic behavior of system elements is emulated (respecting their $R(t)$), and a synthetic history of the system states is generated (CELLI et al., 2013). Using the synthetic history is possible to obtain estimations of reliability parameters. The convergence of MCS is related with the number of simulation trials (N) (THOMOPOULOS, 2012), as N increase, the average value of the estimated parameter approaches to the parameter real average value due to the *Central Limit Theorem*.

The aim of MCS is to estimate a quantity of interest by repeating the trials until obtain a confidence on the estimator (ZIO, 2013), which is proportional to the number of trials N. Since each trial results in a final value x_i, after N trials an expectation of x can be obtained from samples $\mathbf{x} = \{x_0, ..., x_N\}$:

$$\widehat{x} = \frac{1}{N}\sum_{i=1}^{N} x_i, \tag{2.80}$$

and the samples variance is:

$$V(x) = \frac{1}{N-1}\sum_{i=1}^{N}(x_i - \widehat{x})^2, \tag{2.81}$$

and a Coefficient of Variation (CV) for the MCS can be calculated as (BILLINTON; LI, 1994):

$$CV = \frac{\sqrt{\frac{V(x)}{N}}}{\widehat{x}}, \tag{2.82}$$

consequently, as N increases the CV of the MCS trial decreases. The quantity CV can be used to evaluate the convergence of the MCS, low values of CV indicates that the observed values of $\mathbf{x}$ presented a low dispersion around the expectation of x.

The use of MCS also has its variations. Exists the sequential, non-sequential, and the pseudo-sequential MCS (CELLI et al., 2013). Sequential MCS consists of repeating trials and use the historical sequence of events to estimate parameters of interest. Non-sequential is a state-based simulation and uses Markov models to states transitions, and the obtained states are evaluated without considering historical aspects. The pseudo-sequential MCS (SILVA et al., 2000) simulate specific states and then uses the sequential simulation approach to explore neighboring states through a forward/backward simulation to obtain a chronological history of the originally sampled state.

Another aspect of MCS is the possibility of exploring Rare Events (RUBINO; TUFFIN, 2009), which are events with a very low occurrence probability, but which can result in high consequences as multiple, or catastrophic, failures. Such Extremes and Rares Events (E&RE) occurrence is an essential part of risk analysis, and they forecasting is directly related to risk assessment and management (KOMLJENOVIC et al., 2016), where risk is defined as the effect of uncertainties on objectives achievements (AVEN; AVEN, 2015). Consequently (AVEN, 2015), the understanding of these events and their consequences is crucial to assess and manage risk, and are related to the knowledge or beliefs of its occurrence and consequence of who carries risk analysis and management. Therefore, identification, assessment, and management of such events are directly related to the resilience and robustness of services and companies (KOMLJENOVIC et al., 2016).

We can cite some approaches for MCS of rare events. The splitting method (KIM; BUCKLEW; DOBSON, 2013), which consists of splitting the simulations into stages where the number of occurrences defines the ends of each stage, and the other stage start from the trials that obtained the minimum number of occurrences, this process is performed on all the successive stages. Importance sampling (ZIO, 2013) consists of changing the probability distribution function that describes the simulated events to obtain more outputs with the occurrence of the rare event. The modification is performed by an importance sampling distribution that will generate a significant number of samples in the "important region", where the rare events are localized.

2.4.2 Power Distribution Systems Reliability

In the context of DS, reliability is concerned with the interruptions of electricity delivery to the final customers and is related to Quality of Service (QoS). In general, this is measured by standard reliability indices (IEEE PES, Transmission and Distribution Committee, 2012). Two conventional measures of reliability are the SAIFI (*System Average Interruption Frequency Index*) and SAIDI (*System Average Interruption Duration Index*) (HEYDT, 2010). SAIFI is calculated as follows:

$$\text{SAIFI} = \frac{\sum_i N_i}{N_T}, \tag{2.83}$$

where N_i is the number of customers interrupted in a fault event (i), and N_T is the total of customers served by the system. SAIFI indicates the expected amount of sustained interruption a regular customer suffers in a given time window, in general, a year ($interruptions/(customers * year)$). Similar to SAIFI, the others index that will be presented here are usually calculated for a time interval of a year.

SAIDI is concerned with the expected duration of interruptions for a standard customer in a period of time ($minutes/(customer * year)$, calculated as:

$$\text{SAIDI} = \frac{\sum_i N_i r_i}{N_T}, \tag{2.84}$$

where r_i is the restoration time experienced by the N_i consumers. In addition to SAIDI and SAIFI, several other reliability index already were proposed (ČEPIN, 2011):

- *Customer Average Interruption Duration Index* (CAIDI): the expected duration of a interruption experienced by a standard customer ($minutes/interruption$):

$$\text{CAIDI} = \frac{\sum_i N_i r_i}{\sum_i N_i} = \frac{\text{SAIDI}}{\text{SAIFI}} \tag{2.85}$$

- *Customer Average Interruption Frequency Index* (CAIFI): the average frequency of interruptions for customers that are experiencing interruptions ($interruptions/customer * year$):

$$\text{CAIFI} = \frac{\sum_i N_i}{N_c}, \tag{2.86}$$

  where N_c is the number of customers that experienced any interruption during the time interval.

- *Average Service Availability Index* (ASAI): the expected fraction of time the customers will receive power during a time interval:

$$\text{ASAI} = 1 - \frac{\sum_i N_i r_I}{T N_T}, \tag{2.87}$$

  where T is the total period of time reported. ASAI, or simply availability, can also be calculated from SAIDI: $\text{ASAI} = (T - \text{SAIDI})/T$.

- *Energy Not Supplied* (ENS): the expected energy that would be supplied during the interruptions (MWh):

$$\text{ENS} = \sum_i P_i r_i, \tag{2.88}$$

  where P_i is the load not supplied during interruption i. It is related with the system operation perspective.

- *Average Energy Not Supplied* (AENS): the average over customers of the ENS:

$$\text{AENS} = \frac{\sum_i P_i r_i}{\sum_i N_i}, \tag{2.89}$$

  AENS is more related with the QoS the customers are receiving.

Power distribution utilities use historical data describing the service interruptions to compute such indices. However, some investment scenarios, as expansion or upgrades, need to estimate such indices for different fictitious systems to support the decision making during projects. In this cases, the use of the methodologies presented previously, as MCS or Markov Models, are necessary to allow estimations considering the different possibilities.

Besides such indices, current DSs reliability research is focused on the emerging features related to the smart grid philosophy, as distributed generation (AL-MUHAINI; HEYDT, 2013a), the effects of automatic switches (ZHENG et al., 2012), support systems for operator decision making (ZIDAN et al., 2016), meshed networks reliability (AL-MUHAINI; HEYDT, 2013b), micro-grids with local and mobile generation (QUEVEDO et al., 2018), among others.

3 MATERIALS & METHODS

This chapter describes the materials and methods that were used in this research and also organizes the necessary analysis to achieve the research aim and objectives. The first Section provides an overview of the different DSs used during the research, and the last one describes the computational resources used.

3.1 Power Distribution Systems Used

During the development of this research, some DSs were used to evaluate the implemented methods and also to assess some important aspects related to this study aim. The two next subsections will briefly describe two systems presented in the literature that was used, and the Subsection 3.1.3 presents the used Brazilian DS.

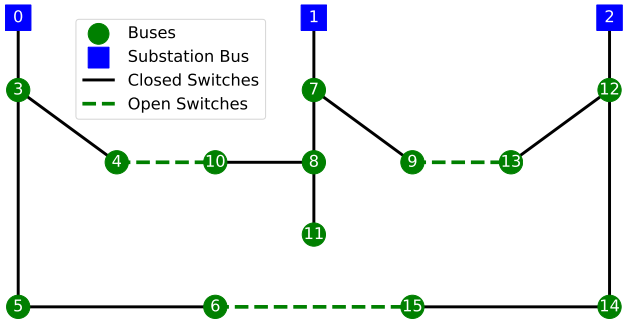
3.1.1 Civanlar's Power Distribution System

This is a test case system presented by Civanlar et al. (1988) and is shown in Figure 5. It is a three-feeder example distribution system, which full data is available in the Repository of Distribution Systems (REDS) (KAVASSERI; ABABEI, 2015). It consists of 13 buses, or vertices, three feeders, 13 sectionalizing switches and three tie-switches, as shown in Figure 5. It allows 15 feasible possibilities of topological reconfiguration (open a sectionalizing switch and closing a tie switch) respecting the system radiality, and without isolating any bus, the total number of possibilities of switching options is much larger than 15. Such system was used to evaluate the operator's response time effect on the reliability indices of a DSs with remotely controlled switches by MCS. This result will be presented in Section 4.1.

3.1.2 Taiwan Power Distribution System

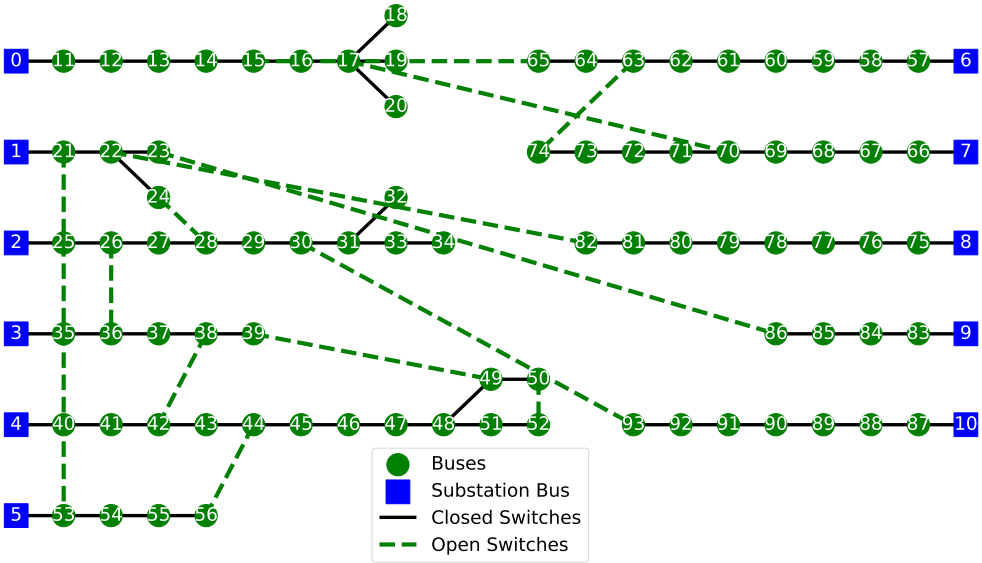
This is a practical DS of Taiwan Power Company presented by Su, Chang e Chiou (2005) and is shown in Figure 6. The system data is available in the REDS (KAVASSERI; ABABEI, 2015). It is a three-phase, 11.4 kV system and consists of 11 substation buses, and another and 83 buses, where 66 are load buses, 83 normally closed switches, 13 normally open switches. We used this system for assessing the effects of reconfiguration capability to reduce out-of-service loads after interruptions in DSs Vulnerability. This DS allows a high number of topological reconfiguration. Results about such analyzes will be presented in Section 4.7.

Figure 5 – Civanlar's system (CIVANLAR et al., 1988), which is a three-feeder DS, represented as a graph. It is a 3 feeder system, with 3 substation buses, and another 13 buses, 13 sectionalizing switches and 3 tie-switches which are the graph edges, and its data is available on the REDS (KAVASSERI; ABABEI, 2015).



Source: Author

Figure 6 – A practical DS of Taiwan Power Company (SU; CHANG; CHIOU, 2005) represented as a graph. It consists of 11 feeders, with a total of 83 nodes (buses), and 83 normally closed switches and 13 normally open switches that are the edges. Its data is available on the REDS (KAVASSERI; ABABEI, 2015).



Source: Author

3.1.3 Brazilian Power Distribution System

The Brazilian DS used in this study is managed by a Brazilian energy company. The DS is responsible for delivering electricity to a city with 558,439 inhabitants, which are in an area of 1,651 km^2, and operates with a nominal voltage of 13.8 kV. This city has both industrial and agriculture activities, which is reflected in dense urban centers and low population density zones. The remaining of this subsection will present the electrical characteristics of the system and the historical data describing the system's failures.

Topological and Electrical Features

The Brazilian DS have the following amount of each element (they were described in Section 2.3.1):

- Buses without loads: 32,312
- Buses with loads: 7,748
- Capacitors: 0
- Distribution feeders: 81
- Cables: 36,615
- Manual switches: 3,657
- Automated switches: 181
- Voltage regulators: 0

Regarding electrical features, the vertices have the following electrical informations:

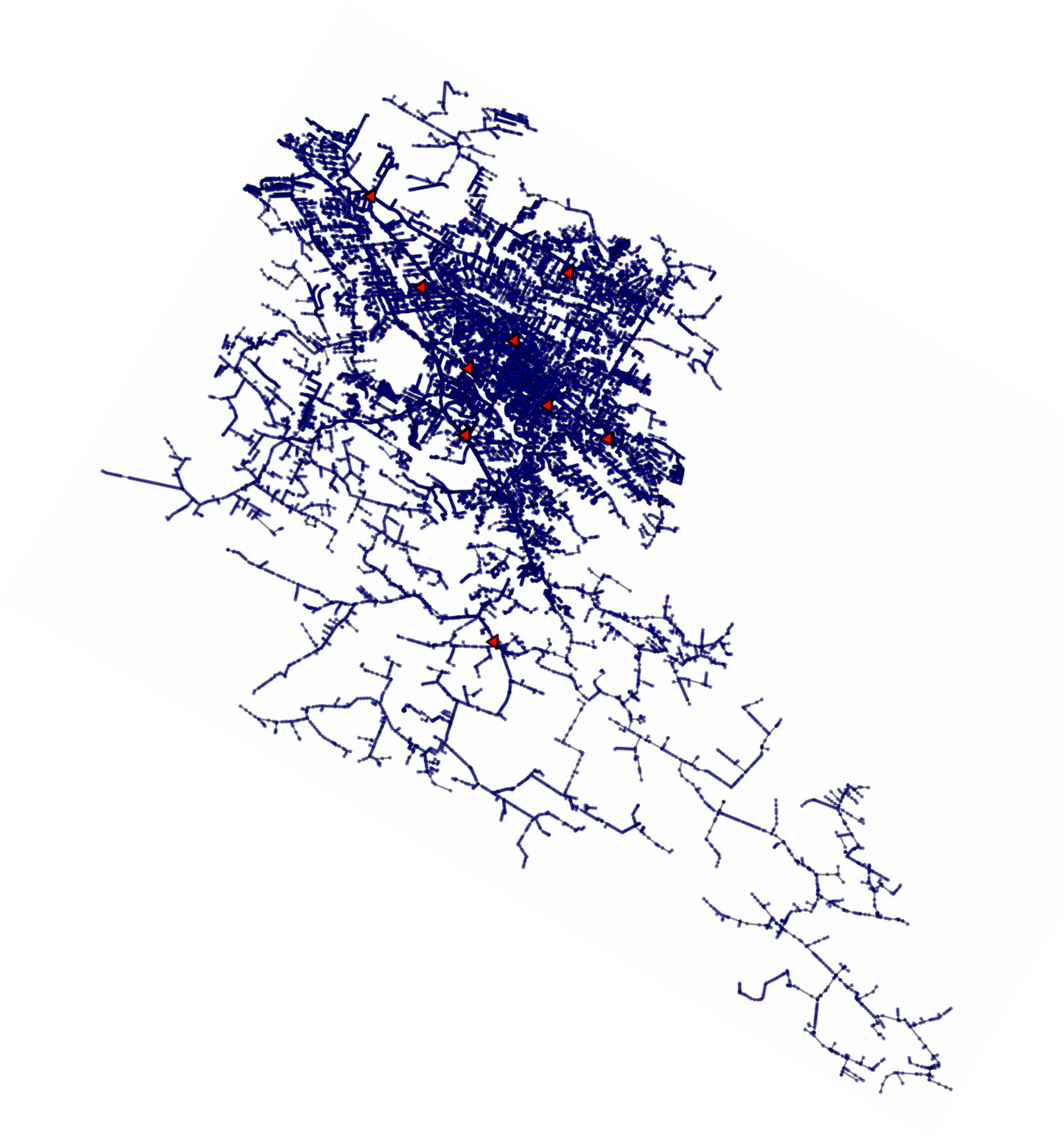
- Active power (P);
- Reactive power (Q);
- Amount of customer unites;
- Amount of standard customer unites;
- Amount of priority customer unites;

And edges have the following electrical informations:

- Switch type: operated with load, fuse, or short circuit;
- Resistence (R);
- Reactance (X);
- Ampacity.

The DS graph representation is displayed using geographical positions in Figure 7.

Figure 7 – Brazilian DS graph representation. The red triangles are the Substations where the distribution feeders are connected.



Source: Author

Historical Data

The historical data set contains 318,329 electricity interruptions records from January 2012 to September 2015. The interruptions were related to 53 different single causes, including the unidentified ones. A general view of the information described in the data set is presented in Table 2.

Table 2 – Description of information contained in historical data describing DS electricity interruptions.

Information	**Description**
Event	Unique number describing the event causing electricity interruption
Interruption	Unique number describing an electricity interruption caused by the Event
Type	Describes if the interruption was accidental, voluntary or programmed
Equipement	Unique identifier number of protection equipement that operated during the interruption
Feeder	Unique identifier number of the distribution feeder where the interruption happened
Start	Date and time of interruption start
Forecast	Date and time forecast of interruption finish
End	Date and time of interruption finish
kVA	Power not delivered during the interruption
Customers	Number of customers that suffered the interruption
Component Description	Description of how the interrupt occurred from a component viewpoint
Description Cause	Description of interruption cause
Interruption origin	Starter interruption, in case the interruption is consequence of another interruption in the system
X,Y coordinate	Geographical position X,Y of the protective equipment that operated
Substation	Unique substation identification number where the interruption occurred
Substation name	Substation name
Duration	Total interruption duration

Source: Author

3.2 Reliability Engineering

The methods chosen from Reliability Engineering concerns two aspects of failures: model failure dynamics, which includes the time-to-failure followed by the time-to-repair, and the Monte Carlo simulation to allow virtual experiments of the transitions between a working state to a failure state and also considering the time variable.

A variety of probability distributions can be used to model $R(t)$ (MEEKER; ESCOBAR, 2014), as the exponential (2.77), the normal, the lognormal, the smallest extreme value, and the Weibull distribution. To fit a $R(t)$ to reliability data the Maximum Likelihood Estimate (MLE) (MEEKER; ESCOBAR, 2014) was chosen. It consists on combining the model parameters with the data by a joint probability:

$$L(\mathbf{p}) = L(\mathbf{p}; \mathbf{t}) = \prod_{i=1}^{n} L_i(\mathbf{p}; t_i), \tag{3.1}$$

where $\mathbf{t}$ is the data set of observations, and $\mathbf{p}$ is the set of parameters for a $R(t)$ candidate function. The aim is to maximize the joint probability $L(\mathbf{p}; \mathbf{t})$, and in practice the log-likelihood is used:

$$\mathcal{L}(\mathbf{p}) = \ln L(\mathbf{p}) = \sum_{i=1}^{n} \ln L_i(\mathbf{p}; t_i), \tag{3.2}$$

it is related with the facility of sum over products, and since the log is a monotonically increasing function, the values of $\mathbf{p}$ that maximize $\mathcal{L}(\mathbf{p})$ will also maximizes $L(\mathbf{p})$. An way to maximize $\mathcal{L}$ is to find the $\mathbf{p}$ values that solves the following equation:

$$\frac{\partial \ln L(\mathbf{p})}{\partial \mathbf{p}} = 0, \tag{3.3}$$

if $R(t)$ have more than one parameter, is necessary to solve a system of equations for each partial derivate.

3.2.1 Failure Model

We choose to model the Failure process by using a count data regression for the failure rate with covariates for weather conditions. In general, the Poisson and Negative Binomial regression models, which are generalized linear models, are used in such type of problem (HILBE, 2014). The Poisson regression model assumes the modeled variable follows a Poisson distribution, which can be described as:

$$P(Y = y_i) = \frac{\exp(-\lambda)\lambda^{y_i}}{y_i!}, \tag{3.4}$$

where $\mathrm{P}(Y = y_i)$ indicates the probability of Y assuming y_i value, and λ is the occurrence rate. For the Poisson distribution the $E[Y]$ and $Var[Y]$ is equal to λ.

In the Poisson regression, λ is supposed to be related to a set of k predictors variables ($\boldsymbol{X} = \{x_1, ..., x_k\}$ by a log-linear relation., which is expressed as:

$$\ln \lambda = \boldsymbol{\beta}^t \boldsymbol{X} = \beta_0 + \beta_1 x_1 + \beta_2 x_2 + ... + \beta_k x_k, \tag{3.5}$$

where $\boldsymbol{\beta}^t$ is the regression coefficients vector with β_0 being the intercept, and $\boldsymbol{X}$ the available predictors vector.

The regression coefficients $\boldsymbol{\beta}^t$ are the values estimated from a data set. To estimate these coefficients, the MLE can be used. The log-likelihood function is as follows (SAFFARI; ADNAN; GREENE, 2011):

$$\mathcal{L}(\boldsymbol{\beta}) = \sum \{y_i \ln(\lambda_i) - \lambda_i - \log(y_i!)\}\,,\ \ln \lambda = \boldsymbol{\beta}^t \boldsymbol{X} \tag{3.6}$$

where y_i indicates the count value, and λ_i depends on the covariates $\boldsymbol{X}$ and the k predictors by (3.5).

The Negative Binomial regression is also a type of generalized linear model, which is indicated by the occurrence of overdispersion (HILBE, 2014), i.e., when the $Var[Y] > E[Y]$. The Negative Binomial distribution is defined as:

$$P(Y = y_i) = \frac{\Gamma(y_i + \frac{1}{\alpha})}{\Gamma(y_i + 1)\Gamma(\frac{1}{\alpha})} \left(\frac{1}{1 + \alpha\lambda}\right)^{\frac{1}{\alpha}} \left(\frac{\alpha\lambda}{1 + \alpha\lambda}\right)^{y_i}, \tag{3.7}$$

where Γ indicates the Gamma function, α the heterogeneity parameter related to the overdispersion, and λ follows the same modelling as presented for Poisson regression in (3.5). The regression coefficients' estimation can be made by MLE (HILBE, 2011):

$$\mathcal{L}(\alpha, \boldsymbol{\beta}) = \sum_{i=1}^{k} (y_i \ln(\alpha\lambda_i) - \left(y_i + \frac{1}{\alpha}\right) \log\left(1 + \alpha\lambda_i\right) + \log\Gamma\left(y_i + \frac{1}{\alpha}\right) - \log\Gamma\left(y_i + 1\right) - \log\Gamma\left(\frac{1}{\alpha}\right)) \tag{3.8}$$

Four estimation quality measures were chosen to evaluate the regression models:

1. *Akaike* Information Criterion (AIC): is a measure that allows estimating the quality of a regression model by accounting the information lost by using it. It is calculated as:

$$AIC = 2k - 2ln(L), \tag{3.9}$$

   where L is the model's likelihood function, and k is the number of estimated *regressors* (AKAIKE, 1974). When comparing models, the one with the minimum AIC value is the better model.

2. *Bayesian* Information Criterion (BIC): as AIC, the BIC is a criterion to select the model that better fits the observed data, where the preferred model is the one with the lowest BIC value. It is calculated as:

$$BIC = -2ln(L) + kln(n), \tag{3.10}$$

similar to AIC, L is the likelihood function of the model, k is the number of $regressors$ and n the number of observed values (SCHWARZ et al., 1978).

3. Wald test: is a parametric statistical test to verify if the parameter estimated by maximum likelihood is significant. It tests the null hypothesis, H_0, that the parameter is zero. Mathematically, it is represented as:

$$W = \frac{\hat{\beta}}{\hat{se}(\hat{\beta})}, \tag{3.11}$$

where $\hat{\beta}$ indicates the estimated coefficient value and $\hat{se}$, the standard error of the regression coefficient (HARRELL, 2015). Using the W value, the $z - value$ is obtained, and if it is less than 0.05 the null hypothesis can rejected and the coefficient is considered significant.

4. Cook's Distance: is a measure of the influence of an observed value in the regression model. The Cook's Distance value of the i observed value, D_i, is calculated as follows:

$$D_i = \frac{\sum_{j=1}^{n} \left(y_j - y_{j(i)}\right)^2}{\rho MSE}, \tag{3.12}$$

where y_j is the jth observation, $y_{j(i)}$ is the jth fitted response without considering the ith observation, MSE is the Mean Squared Error and ρ is the number of $regressors$ in the regression model. Thus, the Cook's Distance indicates a relation between the leverage and the residual of the observation (CHATTERJEE; HADI, 2015). An operational guideline of $D_i > 1$ is used to verify if the observed value is an influential point,

3.2.2 Repair Model

The outage duration in the data set refers to the total needed time to restore electrical energy to out-of-service customers. Given the occurrence of an interruption, the repair process is considered as the occurrence of the following steps (ROOS; LINDAH, 2004):

- Actuation of protection elements;
- Localization of the faulted component;
- Isolation of the faulted region;
- Repair or replacement of faulted component;
- Restoration of the isolated region.

The consideration of these steps naturally gives need to the use of a versatile probability distribution function. The Weibull distribution was chosen to model the repair time under different causes scenario. It is a parametric model widely used in data analysis (ACHCAR; CEPEDA-CUERVO; RODRIGUES, 2012), including survival (WANDEL et al., 2008) and reliability (MURTHY; BULMER; ECCLESTON, 2004) studies. A variation of the Weibull distribution is the Exponentiated Weibull (EW), which is part of the family of exponentiated exponential distributions introduced by Mudholkar and Srivastava (MUDHOLKAR; SRIVASTAVA, 1993). Its cumulative distribution function (CDF) (PAL; ALI; WOO, 2006) is defined as:

$$F(t;k;\lambda;\alpha) = \left[1 - exp\left\{-(t/\lambda)^k\right\}\right]^\alpha; \quad t > 0, \tag{3.13}$$

where $k > 0$ is the first shape parameter, $\alpha > 0$ is the second shape parameter, and $\lambda > 0$ is the distribution scale parameter. If we set $\alpha = 1$, (3.13) becomes the conventional two parameters Weibull, and with $k = 1$ it becomes the exponentiated exponential function.

The Reliability function is obtained from its CDF:

$$\begin{aligned} R(t) &= 1 - F(t) \\ R(t) &= 1 - \left[1 - exp\left\{-(t/\lambda)^k\right\}\right]^\alpha, \end{aligned} \tag{3.14}$$

differently from the exponential reliability function, the distributions following a Weibull distribution results in a variable hazard rate. For the EW, $h(t)$ is as follows (NASSAR; EISSA, 2003):

$$h(t) = \frac{R'(t)}{R(t)} = \frac{k\alpha}{\lambda^k} t^{(k-1)} exp\left\{-(t/\lambda)^k\right\} \frac{\left(1 - exp\left\{-(t/\lambda)^k\right\}\right)^{\alpha-1}}{1 - \left[1 - exp\left\{-(t/\lambda)^k\right\}\right]^\alpha} \tag{3.15}$$

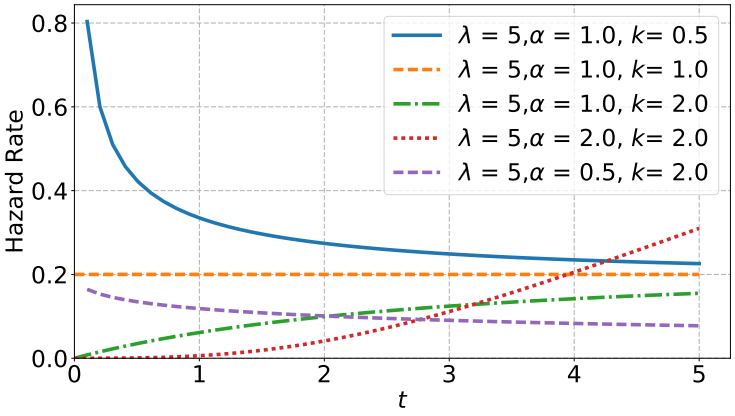
As a consequence, the EW can accommodate a variety of hazard rates behaviour, as constant, monotonically increasing and decreasing. In Figure 8, the $h(t)$ are presented for different parametrizations, including the exponential case and the two parameters Weibull.

In the case of the EW distribution the MLE can be performed in the following way. Let $t_1, t_2, ..., t_n$ be a random sample from a EW distribution as (3.13). The log-likelihood function is given in the following form:

$$\begin{aligned} \ln L(\alpha,\lambda,k) =& (\alpha-1)\sum \ln\left[1 - exp\left\{-(t_i/\lambda)^k\right\}\right] + \\ & (k-1)\sum \ln(t_i) - \sum (t_i/\lambda)^k + \\ & n\ln\alpha + n\ln k + nk\ln\lambda^{-1} \end{aligned} \tag{3.16}$$

Thus, the MLEs of α, λ, and k are solutions of the following equations obtained from the partial derivates:

Figure 8 – Different Hazzard Rates for the Exponentiated Weibull. For $\alpha = k = 1$, its shows a constant rate, for $k \neq 1$ and $\alpha = 1$ its presents the hazard equal to the two parameters Weibull, and for $\alpha \neq 1$ the rates becomes different from the 2-parameter Weibull.



Source: Author

$$\frac{\partial}{\partial \alpha} \ln L(\alpha, \lambda, k) = \frac{n}{\alpha} + \sum \ln \left[1 - exp(-(t_i/\lambda)^k))\right] = 0 \tag{3.17}$$

$$\begin{aligned} \frac{\partial}{\partial \lambda} \ln L(\alpha, \lambda, k) &= nk\lambda - k\lambda^{1-k} \sum t_i^k \\ &+ \frac{(\alpha - 1)k}{\lambda^{k-1}} \sum \frac{exp(-(t_I/\lambda)^k)}{1 - exp(-(t_I/\lambda)^k} t_i^k = 0 \end{aligned} \tag{3.18}$$

$$\begin{aligned} \frac{\partial}{\partial k} \ln L(\alpha, \lambda, k) &= \frac{n}{k} - n \ln \lambda - \lambda^{1-k} \sum t_i^k \ln(t_i/\lambda) \\ &+ \frac{(\alpha - 1)}{\lambda^k} \sum \frac{exp(-(t_I/\lambda)^k)}{1 - exp(-(t_I/\lambda)^k} t_i^k \ln(t_i/\lambda) \\ &+ \sum \ln t_i = 0 \end{aligned} \tag{3.19}$$

3.2.3 Monte Carlo Simulation

The Monte Carlo Simulation (MCS) is related to obtaining synthetic data from stochastic events where their probability distributions are known. Since probability distributions representing the failure and repair processes will be modeled, the MCS will be capable of generating the times-to-failure and times-to-repair of the system elements by computational trials.

To perform MCS is necessary to generate random numbers respecting an specific probability distributions which describes the simulated process or event. This can done by different methods (ZIO, 2013), and here the Inverse Transform Method was chosen. Knowing that $R(t)$ is defined as:

$$R(t) = P(T > t), \tag{3.20}$$

it is possible to obtain a cumulative distribution function as:

$$P(t) = P(T \leq t) = 1 - P(T > t) = 1 - R(t). \tag{3.21}$$

Since $P(t)$ is defined in the interval $[0, 1]$, it is possible to use the Inverse Transform Method (BILLINTON; LI, 1994) to sample from the image of $P(t)$, which is equivalent to get a sample from a uniform probability distribution defined in the interval $[0, 1]$. Using the exponential distribution as example, its $P(t)$ is as follows:

$$P(t) = 1 - R(t) = 1 - e^{-\lambda t}, \tag{3.22}$$

we can write:

$$U(r) = 1 - e^{-\lambda t}, \tag{3.23}$$

where U is the uniform distribution in the interval $[0, 1]$. Equation (3.23) can be rewritten as (3.24):

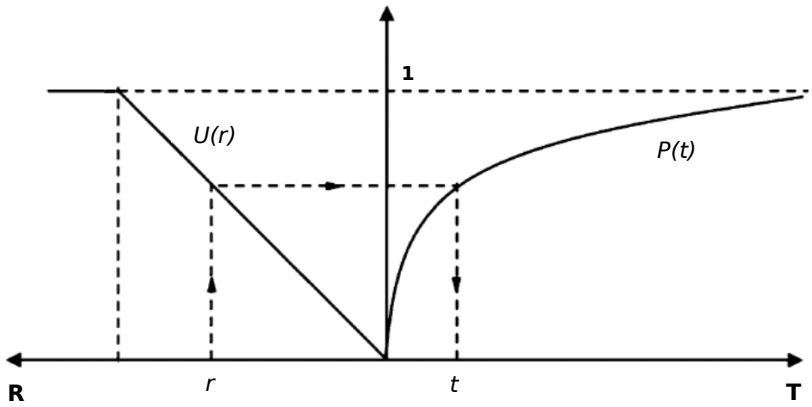
$$t = -\frac{1}{\lambda} \ln(1 - U), \tag{3.24}$$

using that $(1 - U)$ is also a uniform distribution between $[0, 1]$, (3.24) becames:

$$t = -\frac{1}{\lambda} \ln(U), \tag{3.25}$$

which shows how to obtain random samples following an exponential distribution by using random samples from an uniform distribution. Such methodology can be applied for different distribution, as the exponentiated Weibull presented previously. The Figure 9 illustrates the relations between uniform distribution and the sampled distribution.

Figure 9 – Illustration of the Inverse Transform Method. $U(r)$ is a uniform distribution with domain and image in the interval $[0, 1]$, and $P(t)$ represents the cumulative probability distribution that will be sampled, which also has the image defined in the interval $[0, 1]$.



Source: Adapted from Zio (2013)

In general, for Reliability Analysis, the MCS generates a state transition vector (BILLINTON; LI, 1994), which describes the transitions between the working and

failure states. It is obtained by using the sampling methodology previously presented. The state transition vector is a synthetic history of system failures and repairs respecting the failure rates and repair times of each system part, and is obtained using the following steps:

1. Define a duration length of the state transition vector (T) and start the transition vector at time 0 with the parts of interest functioning properly;
2. Sample a time to failure and add it to the vector;
3. Sample a repair time and add its duration to the vector;
4. Until the time T is reached repeat steps 2 and 3.

By generating N state transition vectors, it is possible to estimate the average values of the Reliability indices. MCS convergence is related with high values of N (THOMOPOULOS, 2012), as mentioned in Section 2.4.

As mentioned before, engineered systems had been integrated with communication and information technologies, resulting in Cyber-Physical Systems. The Cyber-Physical Power Systems is a particular case, related to the smart grid philosophy, including the Cyber-Physical Power Distribution Systems (CPPDS). It is already known that failures of the communication network are just as relevant as the electrical network's failures for CPPDS Reliability (KIRSCHEN; BOUFFARD, 2009). During power distribution systems contingencies, the system topology is dynamically changed to either solve or minimize contingency impacts, i.e., isolate the faulted parts and restore as many out-of-service healthy areas as possible (CAMILLO et al., 2014).

Such service restoration is performed in Distribution Operation Centers (DOCs), and the decision-making process is based on the expertise and knowledge of each human operator (CASTILLO, 2014). Consequently, the human operator's performance directly affects the network operation (AMIN, 2005). Decision-support systems (ARNOTT; PERVAN, 2008) have been proposed to improve operators performance during contingencies (CAMILLO et al., 2014; ZONOUZ et al., 2014). The CPPS real-time monitoring and physical measures allow the development of intelligent systems that can infer during a contingency situation and help the distribution operators decision-making process.

Current reliability analysis of CPPS contemplates the integration of communication in the electric power system (FALAHATI; FU; WU, 2012; CELLI et al., 2013; FALAHATI; FU, 2014) It is already known that cyber network failures directly reduces the reliability of the CPPS, e.g., increases the loss of load probability (FALAHATI; FU, 2014). During contingencies, the decision on service restoration is left to the human operators, who already have other obligations (AMIN, 2005). Their decision making varies in quality and

in time to be taken, and need to be embedded in modeling and simulation of CPS (AMIN, 2010).

In this sense, the MCS is used to evaluate how such operator decision affects the reliability indices of a CPPDS. The results regarding this are presented in Section 4.1. Such analysis was performed by an MCS methodology to evaluate CPPDS Reliability indices considering real-time network monitoring, operation, and incorporating the operators' response time, by incorporating such response time in the failures and repairs simulation. A probabilistic model was proposed to represent the response time of operation (t_{RTO}), which is assumed to follow a normal distribution:

$$t_{RTO} \sim \mathcal{N}(\mu_{RTO}, \sigma^2_{RTO}), \tag{3.26}$$

being μ_{RTO} the average operator response time, and σ^2_{RTO} represents the response time deviance, concerning both fast and delayed decision. Since data describing operators' response time are unavailable, the normal distribution was choose as it is a model that naturally fits processes that are smooth, without outliers, and with increasing entropy (KIM; SHEVLYAKOV, 2008), and it is a model widely used to describe different processes.

The Box-Muller method (BOX; MULLER et al., 1958) was used to obtain random samples from the normal distribution:

$$X = \sqrt{-2 \ln U_1} \cos(2\pi U_2), \tag{3.27}$$

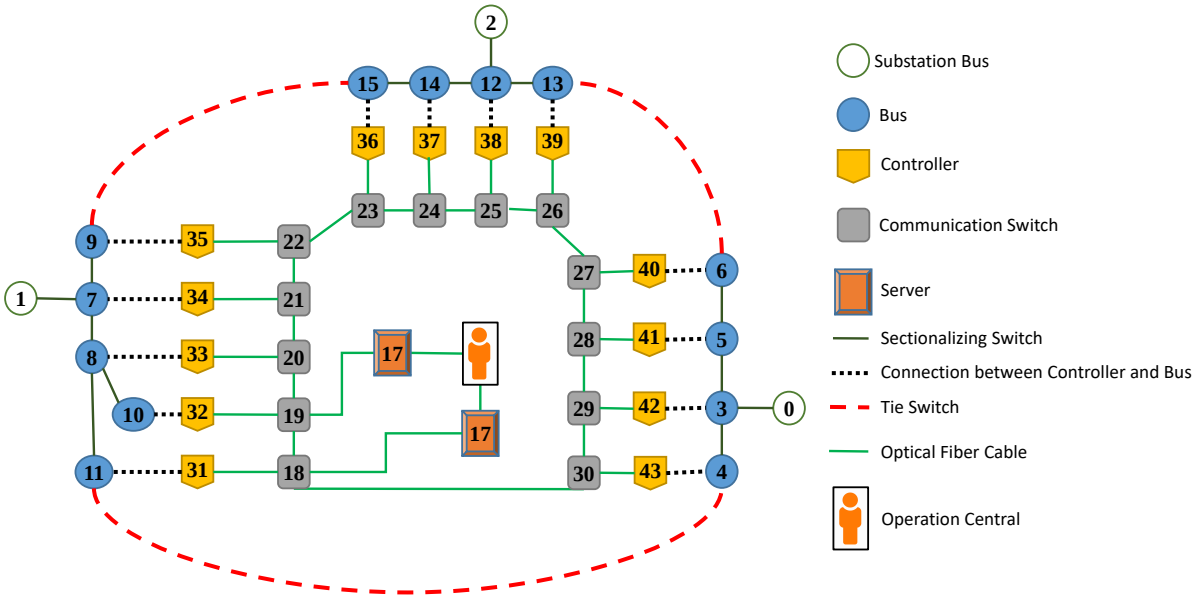
$$t_{RTO} = X\sigma_{RTO} + \mu_{RTO}, \tag{3.28}$$

where $X \sim \mathcal{N}(0, 1)$, and $t_{RTO} \sim \mathcal{N}(\mu_{RTO}, \sigma^2_{RTO})$ is obtained by applying both, the average and deviation on X.

A test case was used to evaluate the effects of t_{RTO} in the CPPDS Reliability, and it is based on Civanlar's distribution system, which is a three-feeder example distribution system previously presented in Section 3.1. A communication network was added to the Civanlar's DS following (FALAHATI; FU; WU, 2012) findings of communication networks for CPPS. The communication network topology follows a 1-ring topology and has 13 communication switches, 13 controllers, and two servers. We assumed that all the sectionalizing and tie switches are automated with time to reconfiguration equals to zero, and the controllers are responsible for monitoring the nodes and changing the states of the electrical switches. The final CPPDS system is presented in Figure 10.

Such response time model together with failure (Exponential) and repair (Normal) models for the electrical and communication elements was used to simulate different scenarios by applying the MCS methodology presented here. To evaluate the impact of μ_{RTO}, the following System Reliability indices were used: Failure Rate - Equation (2.76), Availability - Equation (2.79), represented by the *number of nines*: $N_9 = -\log_{10}(1 - A)$ (HEYDT, 2010), SAIFI - Equation (2.83), and SAIDI - Equation (2.84). The simulation

Figure 10 – Representation of the Cyber-Physical Power System simulated in this research. The Communication network has a 1-ring topology, and each communication switch is connected to two others, allowing network reconfiguration in case of failures.



Source: Author

approach, which deals with failures and repair for both electrical and communication elements, and the operator decision during system reconfiguration is presented in Figure 11. It presupposes that the distribution feeders are robust enough to handle the load transfer between each other during contingencies. All the MCS were performed with $T = 1000$ years and $N = 1000$ to estimate the steady-state of the reliability indices.

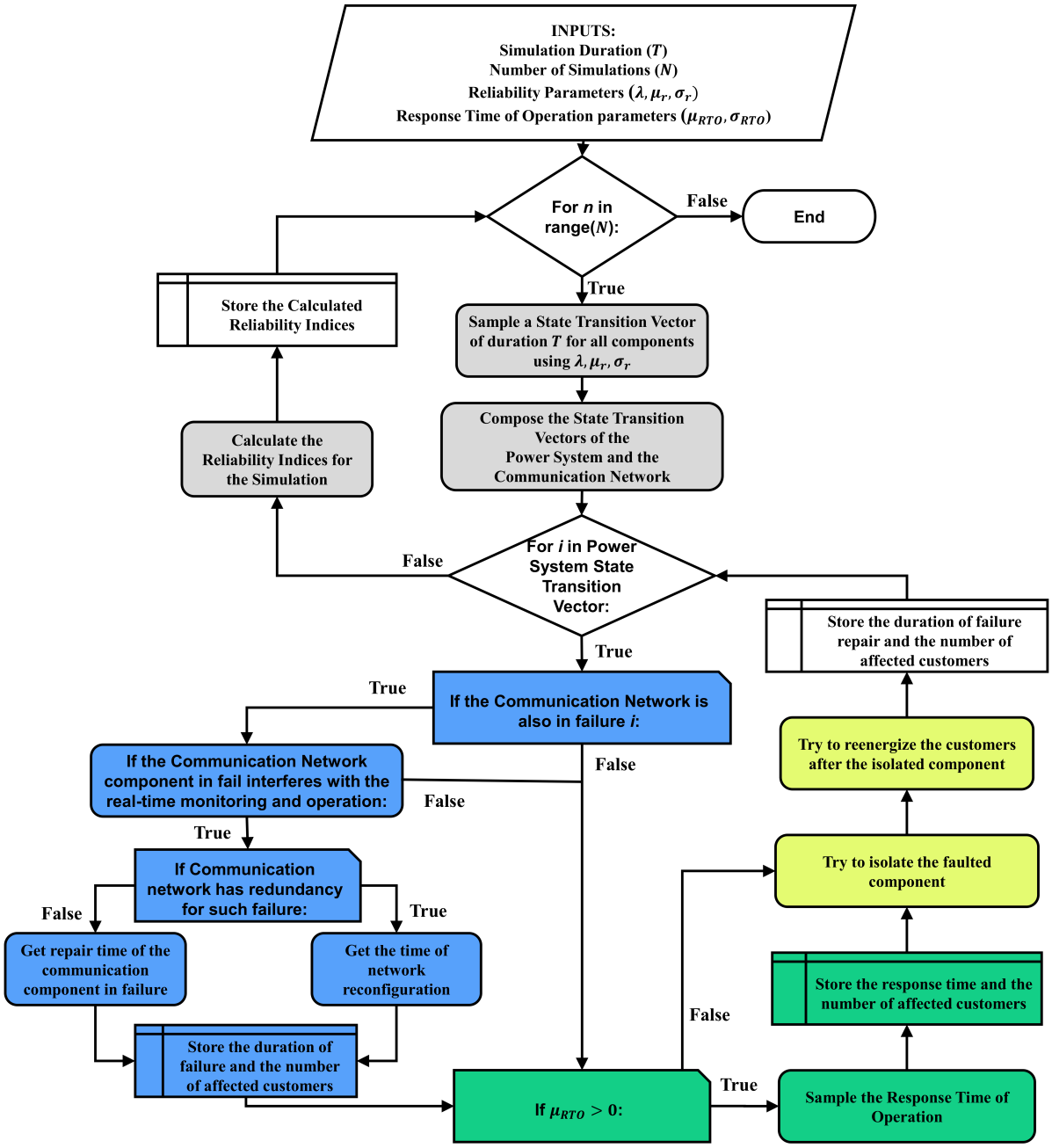
The quantities of customers assumed at each network bus are shown in Table 3. The failure rates used for system components are given in Table 4, and they were chosen respecting the typical distribution equipment outage statistics presented in (CHOWDHURY; KOVAL, 2011). The distribution feeders, fiber-optic cables, servers, and switches are assumed to be fully reliable.

The first test of our MCS methodology is to validate the capability of measuring the impact of communication network failures in the CPPDS reliability indices. Two different cases were used:

1. CPPDS with a fully reliable communication network and $\mu_{RTO} = 0$: The system has a fully reliable automated electrical switches and real-time monitoring, and the operator decision is instantaneous.

2. CPPDS with failures into communication network and $\mu_{RTO} = 0$: The same as the

Figure 11 – MCS to evaluate electrical and communication components failures and the operator response time impact on reliability indices of Cyber-Physical Power Distribution Systems. The yellow symbols represent the system topology reconfiguration for power restoration during contingencies. The blue symbols represent the communication networks failures. The green symbols compute the operation response time impacts.



Source: Author

case above, but communication network can fail, resulting in a delay effect in system operation, and the operator decision is instantaneous.

Following, different scenarios for the t_{RTO} were used to evaluate the impact of

Table 3 – Quantity of customers energized by each Cyber-Physical Power System bus.

Branch id	Customers	Branch id	Customers
3	3	10	1
4	5	11	7
5	3	12	1
6	2	13	1
7	6	14	1
8	8	15	3
9	1	-	-

Source: Author

Table 4 – Adopted failure rates (λ) in failures/year and repair time parameters (μ_r and σ_r) in hours.

Element	λ	μ_r	σ_r
bus	0,1	3	0,6
communication switch	0,005	3	0,6
controller	0,01	3	0,6

Source: Author - based on (CHOWDHURY; KOVAL, 2011)

operation performance on the Reliability of the CPPDS, they were simulated using the same assumption of failures in the Communication network case. The t_{RTO} parameters used are presented in Table 5, and they represent different performances of a human operator making a decision during a system contingency.

Table 5 – Values of μ_{RTO} and σ_{RTO} used to simulate the response time of operator.

μ_{RTO}	σ_{RTO}
0	0
1	0.2
5	1
10	2
20	4
40	8
60	12

Source: Author

3.3 Data Set Characterization

The Brazilian DS networks will be characterized using the topological CN metrics presented in Chapter 2.2, and also hybrid metrics using electrical characteristics for electric power systems. Here, some metrics developed during this research will be presented.

A metric related to the distribution nature of SDN is proposed. Such metric is called *Distribution Centrality*. In an SDN, the flow of goods and services are related to the connectivity of the vertices with the source element, or Tree root. To quantify the importance of a Spatial Distribution Network vertices, the *Distribution Centrality* measure of vertex importance (3.29) is introduced. It considers that vertex importance is proportional to its pertinence to the paths connecting the other network elements to the source vertex and is calculated as follows.

$$C_D(i) = \frac{\sum_{j \neq (i,0)}^{N} d_{0j}(i)}{N-1}, \tag{3.29}$$

where $d_{0j}(i)$ indicates that the path between the source vertex v_0 and v_j passes through v_i, and $N-1$ is the number of paths between elements and the Spatial Distribution Network source vertex v_0.

Distribution Centrality in (3.29) uses only the topological information about the SDN. It can be expanded by considering the network weights, named *Weighted Distribution Centrality*, and allowing the consideration of specific features. It is calculated as follows:

$$C_D^w(i) = \frac{\sum_{j \neq (i,0)}^{N} d_{0j}(i) l_{ij}}{N-1}, \tag{3.30}$$

where l_{ij} is the weighted path length from v_i to v_j in a weighted graph. In the context of Power DS, the weight can be related to different perspectives of the electricity distribution: the power flowing on the electrical connections, the edges impedance, the number of customers attached to the end of an edge, the power consumed at the end of an edge, and the current flow tolerance.

3.4 Vulnerability Assessment

The usually used *LCC* performance metric assumes that the ratio between the Connected Component with higher Order after elements removal and the original system Order can describe the system performance loss after disruptive events. Such assumption is coherent with many types of CN, like Social and Internet networks (ALBERT; JEONG; BARABÁSI, 2000). As an example, after an individual been removed/omitted from a Social network (LUSSEAU, 2003), the resulting components still can be considered functional Social networks.

The use of *LCC* metric in PG Vulnerability Analysis is relatively common (CUADRA et al., 2015) for both, Transmission Networks and DSs. In the case of Transmission Networks (see as an example (SOLÉ et al., 2008) and (ROSAS-CASALS; VALVERDE; SOLÉ, 2007)), which are composed of three types of buses: generation, transmission, and distribution (ALBERT; ALBERT; NAKARADO, 2004), the systems are capable of forming functional subnetworks, or islands, after parts removal (PAHWA et al., 2013; MUREDDU

et al., 2016). These islands may have the three kinds of buses interconnected, being capable of transmitting electrical energy from generation buses to distribution ones.

On the other hand, DSs are usually radial and characterized by having only one path for electricity flow from it distribution feeder bus to the customers at load buses (GRIGSBY, 2016). Such radial topology allows the representation of DS as trees (DELBEM; CARVALHO; BRETAS, 2005), where a DS root is the vertex corresponding to the bus of a feeder in the substation. After vertices removal from a Network corresponding to a DS, or another SDN, only one *connected component* will perform distribution, and this *connected component* contains the source element. Note that the *Largest Connected Component* metric will not necessary considers the Component that contains the source.

In such context, we introduce the *Sourced Connected Component* (SCC) performance metric (3.31). SCC Is the ratio between the Order of the Connected Component that contains the source element and the original Order of the system. SCC is calculated as follows:

$$SCC = \frac{N_S}{N}, \tag{3.31}$$

where N is the original network Order, and N_S is the Order of the Connected Component with the source vertex.

SCC is used to obtain an impact measure that considers the capacity of a Spatial Distribution Network to deliver services and goods to the end users. Based on the impact definition I (2.28), we define I_{SCC} as in (3.32), which is the impact caused by disruptive events considering SCC metric.

$$I_{SCC} = \frac{SCC_0 - SCC_{\mathbf{j}}}{SCC_0}, \tag{3.32}$$

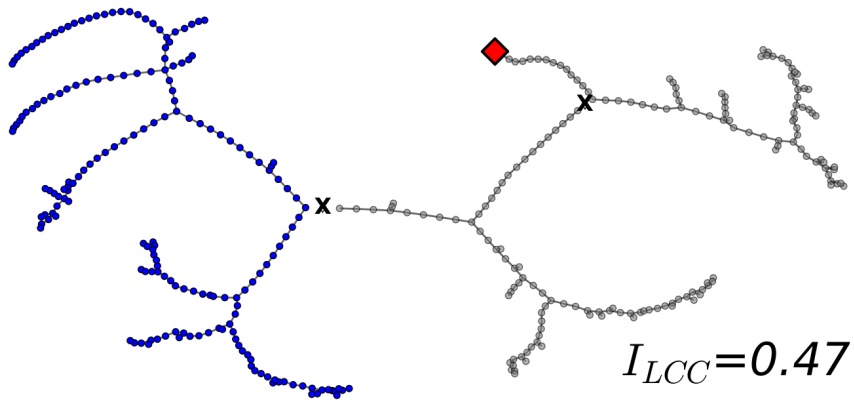
Figure 12 illustrates the main difference between both metrics, LCC and SCC. The first accounts the number of vertices in the *Largest Connected Component* after disruptive events and SCC considers the number of vertices that still are connected to the source after a disruptive event.

Similar to the *Distribution Centrality*, the SCC allows the account of specific properties of DS by using weight representations (SCC^w).

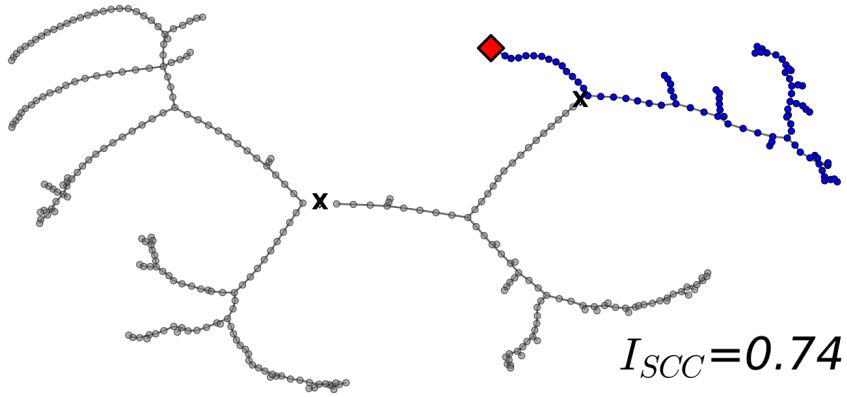
$$SCC^w = \frac{\sum_S w}{\sum_G w}, \tag{3.33}$$

where S represents the sourced connected component, G the system before damaging events, and w represent the adopted weights. For instance, the weight could be the load or the number of customers served by the DS.

Figure 12 – Example of impact calculated using both metrics, (a) *LCC* and (b) *SCC* after the removal of two vertices (marked with **X**) - $\boldsymbol{j} = [v_1, v_2]$. The Connected Component in blue is the one utilized by each metric to measure the impact. The red diamond represents the distribution feeder bus - source element - of the DS. Each subfigure shows the calculated impact.



(a) Impact calculated using *Largest Connected Component*.



(b) Impact calculated using *Sourced Connected Component*.

Source: Author

The use of SCC^w for DS with the weight as the power demand at each node results in the measure of the Power Not Delivered (PND) after a damage occurrence. This can be transformed to the Reliability index Energy not supplied by conversion of power to energy (Energy = Power $*$ Δt), defined previously in Section 2.4.2.

3.4.1 Cumulative Collapse Rate

Vulnerability studies have used the average, and the standard deviation of the impact obtained from simulations trials to describe systems vulnerability. Here, an analysis tool based on probability theory is introduced to better describes such stochastic phenomena of both random failures and attacks in CN. *Collapse Rate* (CR) is the conditional probability function, $P\{. \mid .\}$, representing the probability of a system that has not experienced a collapse with an amount of parts removal under a specific damage scenario to experience

a total system collapse with one more removals. CR is calculated as follows.

$$CR[n] = P\{I[n] = 1 \mid I[n-1] < 1\}, \tag{3.34}$$

where $I[n]$ is the impact with n parts removal, $n = \{x : x \in \mathbb{N}^*, \quad n < N\}$, and N is the system Order. Using the *Collapse Rate*, the *Cumulative Collapse Rate* (CCR) can be obtained, which is the probability of a number of removals less or equal to n to cause a total collapse. It is computed as follows:

$$CCR[n] = \sum_{i=1}^{n} CR[i] \tag{3.35}$$

where n is the number of parts randomly removed, and $n \leq N$. The CCR metric is a strictly increasing function. CR and CCR, are inspired in the Hazard Rate and the Cumulative Hazard Rate commonly used in time-to-event studies, as Survival (AALEN; BORGAN; GJESSING, 2008), and Reliability Analysis (ZIO, 2013).

3.4.2 Vulnerability Assessment using Reliability Failure model

An approach proposed in this study is the use of reliability models to perform vulnerability analysis to errors. The premise of equal failure probabilities does not contemplate the actual challenges of engineered systems modeling and analyzing (ZIO, 2016a; ZIO, 2016b), which have both structural and dynamic complexity. The use of reliability models naturally adds the time variable in the vulnerability analysis. The approach is organized in a hierarchical procedure, as presented in Figure 13.

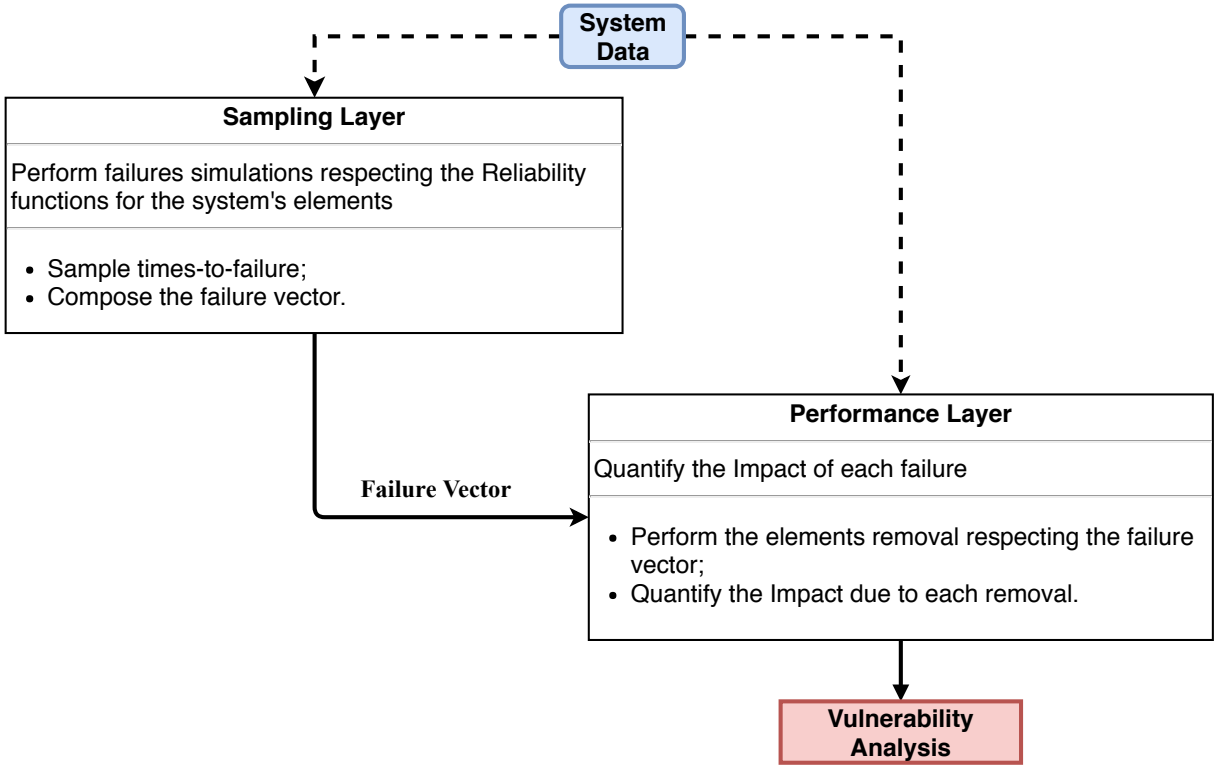
The necessary *System Data* are topological information, in the case of the Brazilian DS these are electrical connections and buses, and the types of elements including their reliability functions. The *Sampling Layer* uses the information about the system elements together with their respective $R(t)$ to simulate times-to-failure of each one. Given the $R(t)$ for each kind of element, the sampling layer generates a Failure Vector ($\boldsymbol{F}$) describing the order and time of elements failures, which are represented as:

$$\boldsymbol{F} = \{(f_1, t_1), (f_2, t_2), ..., (f_n, t_n)\} \tag{3.36}$$

where f_i is the i-th failure occurred at time t_i, and n is the number of susceptible elements.

Performance Layer considers the elements in $\boldsymbol{F}$ to perform elements removals and calculating the impact due to each removal. Such impact calculation can be considering topological, hybrid, or electrical metrics. With N repetitions, the framework can provide a general view of the system vulnerability, and also provide the impact average and standard deviation values together with the system Cumulative Collapse Rate. These metrics will also be related to the time variable given by the *Sampling Layer*.

Figure 13 – Hierarchical procedure for vulnerability analysis. The layers are all dependent on system data. Sampling Layer generates the time-to-failure data respecting the system's elements reliability models. Performance layer accounts the performance loss due to each sampled failure.



Source: Author

3.4.3 Vulnerability Assessment with Reconfiguration Dynamic

To perform vulnerability analysis of DSs with the reconfiguration dynamic is necessary to consider an important aspect. Knowing that a DS feeder, in general, has a radial topology, i.e., a rooted tree with the distribution feeder being the root, it is necessary to represent the capability of load transfer between neighbor feeders after a failure occurrence by operating the DS switches. The switches operation are related to the use of fixed back-up connections to heal, or recover, the network functionality after damaging events (QUATTROCIOCCHI; CALDARELLI; SCALA, 2014; GALLOS; FEFFERMAN, 2015; MORONE et al., 2016), which is a current research trend for vulnerability analysis (SHEKHTMAN; DANZIGER; HAVLIN, 2016). This dynamics can be interpreted as an interaction among the different distribution networks that compose the DS.

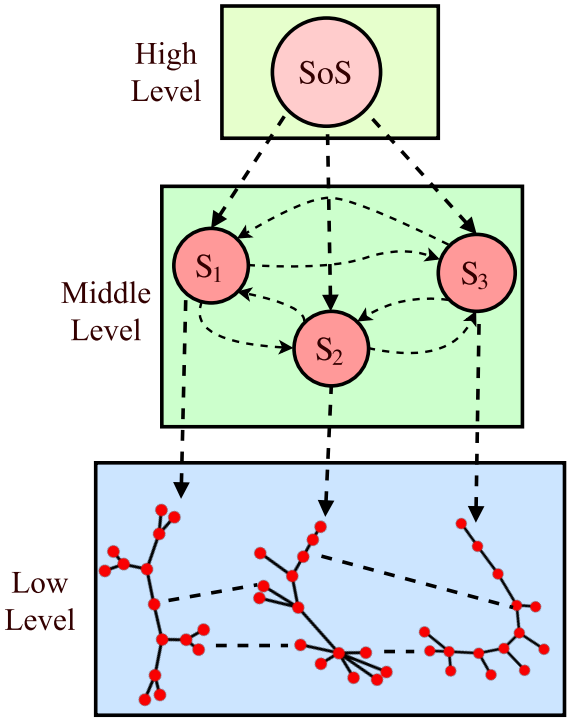
The DS reconfiguration capability interpretation as an interaction among the distribution networks allows the modeling of the DS as a System of Systems (SoS) (EUSGELD; NAN; DIETZ, 2011; THACKER; PANT; HALL, 2017), where each distribution network is a system, and the set of networks that can receive and transfer the load to the others

during reconfiguration forms the SoS. The SoS abstraction will need the consideration of three different levels:

1. Low level: the model of each system;
2. Middle level: the model of the interactions between systems;
3. High level: the global model of the SoS;

In the Figure 14, a representation of a SoS with the three levels is presented. The studies regarding DS Vulnerability showed in the Section 2.3.1, already focused on the low level model, and to account the capability of load transfer and topological reconfiguration is necessary to deal with the SoS middle level, where the interactions between the different distribution feeder networks can be modeled. By considering the load transfer and system reconfiguration, we can also evaluate the vulnerability of the high level layer, which accounts all the distribution feeder networks operating together and returns the vulnerability of the entire DS.

Figure 14 – System of Systems abstraction levels necessary to deal with DS Dynamic Vulnerability.



Source: Author

In addition to the SoS abstraction, it is also necessary to emulate the reconfiguration dynamics. A Multi-Agent model was chosen to emulate the reconfiguration of DSs during the vulnerability analysis. Multi-Agent Modeling and Simulation, in the context of complex systems, is a model that describes a system as a set of autonomous interactive agents,

where each type of agent has specific behaviors, and the global system's behavior emerges from the interactions among them (MACAL; NORTH, 2010). A typical multi-agent model is composed of:

- Agents: each type has its specific attributes and behaviors. The attributes can be static or dynamic, and the behaviors are rules that can modify other agents attributes or its attributes;
- Relationships: define which elements are interacting in the model;
- Environment: external factors that can affect or be affected by the agents.

The application of such modeling approach to the different elements that compose complex systems results in the emergence of system behaviors that are not necessarily, explicitly designed in the agents' behavior.

Several complex systems dynamics can be modeled using a multi-agent approach, such as ecological, economic and social dynamics (VESPIGNANI, 2012; MEI et al., 2015). This is also the case of smart grids, where multi-agent approaches have been applied for control, fault-management, and self-healing (MALIK; LEHTONEN, 2016). Besides this, there are also approaches using agents for emulation of smart-grids dynamics. For example, to describe prosumers' behaviours in local energy markets (SHA; AIELLO, 2016), and in decentralized scenarios of open energy markets (CAPODIECI et al., 2016).

The multi-agent model used to evaluate the reconfiguration dynamics during damages on DSs was implemented with three types of agents:

1. Topological agent: Stores topological information as connections status and unserved elements, it also receives the info about the occurrence of damages from protection devices;
2. Supply agent: Accounts the features related to a feeder total load, tolerance and capacity. Each distribution feeder is modeled as a supply agent;
3. Switch agent: Stores the status of switches, i.e., open or closed, and also verify if it can reconnect an unserved node. Each switch in the system is modeled as a switch agent.

The implemented multi-agent model runs the following procedure at each simulation step:

1. At each simulation step, a random node is damaged (feeders are fully reliable);
2. Topological agent detects the damaged node and informs its respective supply agent, so it can isolate the damaged node by informing the switch agents connected to such node to open the circuit;

3. Supply agent informs the other switch agents about the undamaged and unsupplied nodes (downstream to the damaged one), which verify if they can reconnect such unserved nodes to another supply agent;

4. If some supply agent can serve all the unserved nodes, the switch agent status becomes closed, connecting the nodes to the new supply agent;

5. In case of a higher unserved load than any supply agent can handle, the switch agents try to find a subset of unserved nodes that can be supplied after reducing its load, done by opening switch agents joining the unserved nodes;

6. If two or more switch agents capable of transferring a subset of unserved nodes, they divide the load among them maximizing the transferred unserved load.

Using such multi-agent model, we can evaluate the vulnerability of a DS under the reconfiguration dynamics. The multi-agent model was executed using varying values of feeders maximum capacities, which were modeled by the following equation:

$$C = (1 + \alpha)L_0, \tag{3.37}$$

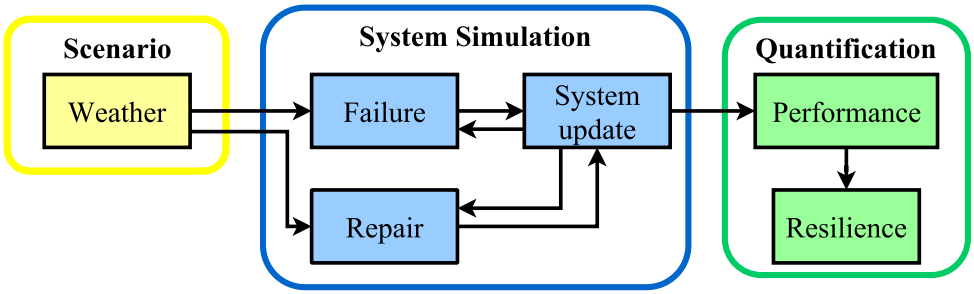
where L_0 is the initial load of each feeder in the DS default configuration, α is the tolerance parameter, and C is its maximum capacity. We use the following values of tolerance during vulnerability analysis: 5%, 10%, 50% , and 100%.

The system performance is quantified by the total power delivered. At each simulation step, the model returns the sum of the power delivered by all the feeders in the power distribution system after the load transfer using the switches to minimize the unserved loads. The process of damaging nodes is based on the error approach with equal failure probability for all susceptible elements. By repeating such process, an average and standard deviation of impact values versus the ratio of removals are obtained, which is used to analyze the DS vulnerability.

3.5 Resilience Assessment

The consideration of repair capacity is related to recovery in dynamical networks (MAJDANDZIC et al., 2014; FARR; HARER; FINK, 2014; SHANG, 2015; SHANG, 2016), where the time variable can be considered (MAJDANDZIC et al., 2014; SHANG, 2015). The reliability models were chosen to allow the consideration of the time during the dynamic process of damages and recoveries. By using such statistical models, it is possible to perform a probabilistic assessment of the system resilience. Moreover, such statistical models can embed the effects of covariables which are related to different scenarios, and in this study, they are weather variables. An estimation of the resilience under different

Figure 15 – Conceptual view of the resilience assessment under different weather scenarios. The scenario affects the failures and repairs which are used to simulate the synthetic dynamic performance. Resilience is quantified from such dynamic performance.



Source: Author

weather scenarios can be performed by MCS and using the time-to-event models under such scenarios. In Figure 15, a conceptual view of this methodology is presented.

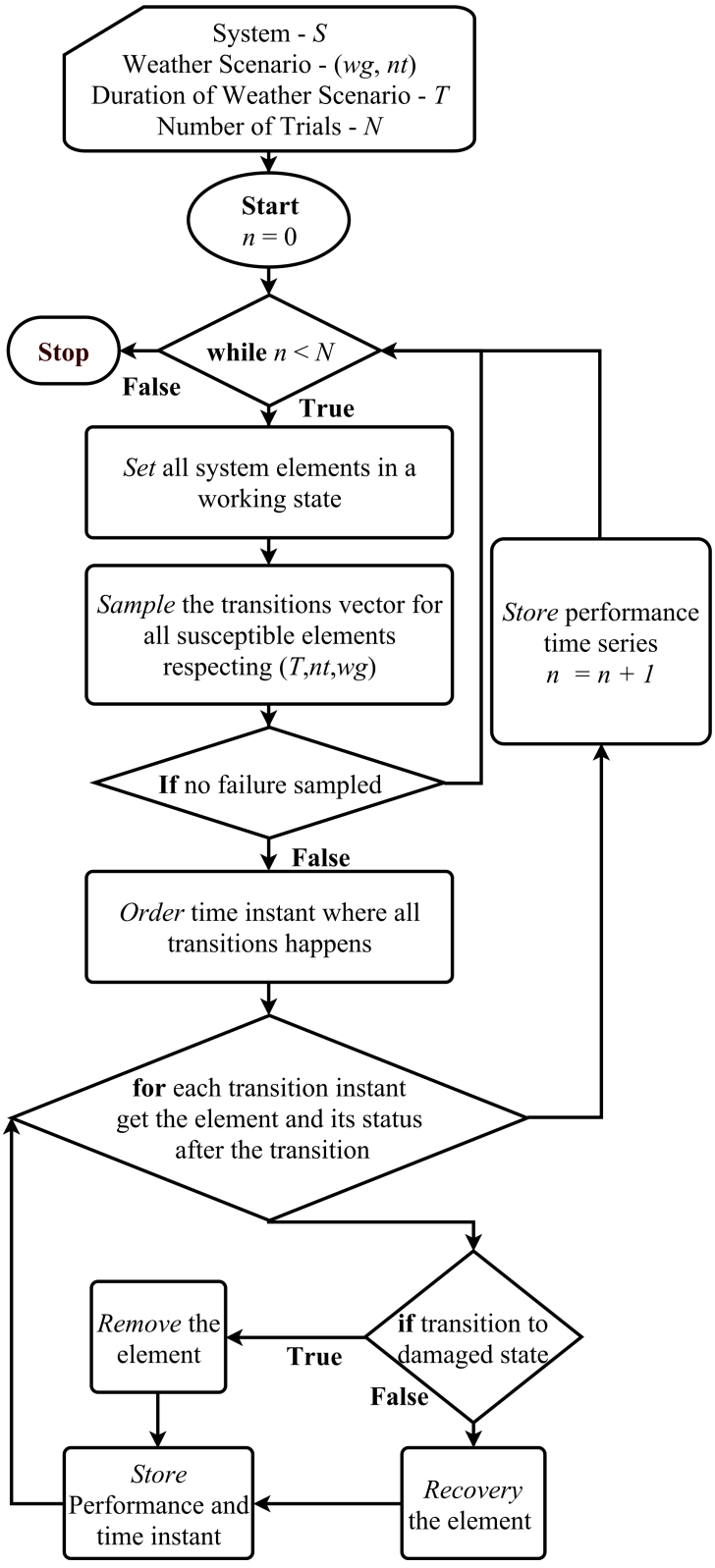
The weather scenario influences repair and failure models that are used to simulate the system elements transition between working and damaged states. Each state change is used to update the network topology, and the quantification measures the performance after such network update, i.e., elements failure or repair, generating a performance time-series. Such time-series are then used to calculate expected resilience. The failure and repair models used are obtained as described in Sections 3.2.1 and 3.2.2, respectively.

An MCS algorithm (see Section 3.2.3) is used to simulate states transitions and estimate resilience under a predefined weather scenario. It emulates the system failure and repair dynamics during a specified weather scenario by sampling the time instants where the system elements are damaged and then recovered. In Figure 16, a flow chart presents the simulation algorithm steps. The inputs to configure the simulation are a system (S), a weather scenario (wg, nt), the duration of the scenario T and the number of trials N. For each trial a transition vector for each susceptible element is sampled by the following steps. Given a susceptible element (e) and simulation conditions (T, nt, wg) do:

1. Start at $t = 0$ and with e in a working state;
2. Sample a time-to-failure t_f and $t = t + t_f$;
3. if $t < T$: $e \rightarrow$ damaged state;
4. Sample a time-to-repair t_r, $t = t + t_r$ and $e \rightarrow$ working state;
5. While $t < T$ return to Step 2:

If no failure is sampled in the time interval T, the simulation is restarted. Otherwise, the transition time instants are ordered in a crescent way, and for each transition, the respective element status is set to damaged or recovered, respecting its transition vector,

Figure 16 – Flow chart of the simulation algorithm. The setting of the simulation is defined by the inputs, system, weather scenario, weather adversity duration and number of trials.



Source: Author

and system performance is updated after each transition. The failures will be sampled only in the time interval T, but the repairs can happen at any time instant after T. After analysis of all transitions, the resulting time-series representing the dynamic performance of the system for such trial is stored, and the process is restarted until the realization of N trials. With the N time-series we can calculate the observed resilience values under the simulated scenario, and also the expected resilience.

Besides the estimation, features calculated from each distribution network (topological and hybrid ones) will be used to explore the associations among such features and the networks' expected resilience under extreme weather conditions. This will be performed by using Pearson and partial correlations. Although Pearson correlation does not implicate on independence and causality (VELICKOVIC, 2015), the absence of correlation can be interpreted as an independence indication. The Pearson correlation for two data sets ($\mathbf{X} = \{x_1, \ldots, x_n\}$ and $\mathbf{Y} = \{y_1, \ldots, y_n\}$) can be calculated as follows:

$$r_{xy} = \frac{\sum_{i=1}^{N}(x - \overline{x})(y - \overline{y})}{\sqrt{\sum_{i=1}^{N}(x - \overline{x})^2 (y - \overline{y})^2}} \tag{3.38}$$

where $\overline{x}$ and $\overline{y}$ are the average of $\mathbf{X}$ and $\mathbf{Y}$, respectively. The correlations will be calculated between each feature (topological and hybrid) and the networks expected resilience.

Partial correlation consists of estimating the Pearson correlation among two variables x and y by removing the linear effects of the control variables $\mathbf{z} = \{z_1, \ldots, z_n\}$ (FUENTE et al., 2004). Numerically, this is performed by first obtaining the residuals ϵ_{xi} and ϵ_{yi} for the N points in the data set from the following linear regressions:

$$x_i = \beta_0 + \beta_1 z_1 + \ldots \beta_n z_n + \epsilon_{xi}, \tag{3.39}$$

$$y_i = \beta_0 + \beta_1 z_1 + \ldots \beta_n z_n + \epsilon_{yi}, \tag{3.40}$$

which are solved by the least squares method.

The partial correlation between x and y given $\mathbf{z}$ ($r_{xy.\mathbf{z}}$) can be calculated by using (3.38) with the observed residuals $\boldsymbol{\epsilon_x}$ and $\boldsymbol{\epsilon_y}$ from the linear regressions. The general assumption is that a partial correlation near to zero is an indication that the variables can be conditionally independent given $\mathbf{z}$ (BABA; SHIBATA; SIBUYA, 2004). The partial correlations will be calculated between each feature and the networks expected resilience residuals obtained from the regression with the other features.

3.6 Computational Environment

All the methods presented in this Chapter were developed with the Python programming language (MILLMAN; AIVAZIS, 2011), a personal computer for code development, and a Beowulf cluster (STERLING, 2002) to run the computational experiments. The personal computer is an Intel Core i7-4500 (Intel Corporation, USA) CPU at 1.80 GHz, 8

GB RAM and Ubuntu operating system (Canonical Ltd., UK). The computers cluster is composed of 12 nodes connected to a host through a Gibagit ethernet switch. The nodes and host run Fedora OS and have an i7-4770 CPU @ 3.40 GHz with eight processing engines and 8 + 8 GB RAM (1333 MHz). During the development of the methodologies several python packages were used, and Table 6 lists and summarizes the application of these packages.

Table 6 – Python packages used in this study with a summary of their application in this research.

Package	Application
Matplotlib	Graphical visualization
Pandas	Handle data-structures
Numpy	Multi-dimensional arrays and matrices operations
IPython	Interactive python computing
IPyParallel	Python parallel and distributed computing
Scipy	Statistical functions
Networkx	Graphs representation and algorithms
Statsmodels	Estimation of statistical models
MESA	Framework for agent-based model and simulation
Powerlaw	Statistical methods to fit powerlaw distribution
Lifelines	Survival analysis
Sklearn	Metrics for models evaluation
Pandapower	Electric power system modeling and analysis

Source: Author

4 RESULTS & DISCUSSION

4.1 Operators' Response Time and DSs Reliability by Monte Carlo Simulation

Here, the results for the impact of operator performance into CPPDS Reliability (see Section 3.2.3) are presented. The first result is a validation of the capability of measuring the impact of communication network failures in the CPPDS reliability indices, and two different cases were evaluated:

1. CPPDS with a fully reliable communication network and assuming instantaneous operator response;
2. CPPDS with failures into communication network and assuming instantaneous operator response.

The estimated Reliability indices are presented in Table 7. These results show that our methodology correctly incorporates the communications failures impacts to the CPPDS reliability indices. The network reliability parameters are better in case 1 than 2 due to the assumption of a communication network fully reliable. The observed decline in reliability reflects the importance of integrating a reliable communication network into the Power System. A communication network failure can insert a delay during contingency situations, seeing that the distribution operation center will receive the information about contingency and properly reconfigure the system only if the communication network is functioning properly.

Table 7 – Reliability indices using two different cases to evaluate the impact of communication and electrical components failures into the reliability of the studied Cyber-Physical Power System.

Case	Availability	SAIDI	SAIFI	Failure Rate
Power Grid with a full reliable Communication network	3.386	0.457	0.152	1.200
Power Grid with failures into Communication network	3.203	0.953	0.318	1.831

Source: Author

Next, the results for different scenarios for the response time of operator - RTO are used to evaluate the impact of operation performance on the Reliability of the CPPDS, they were simulated using the assumption of failures in the Communication network case. The reliability indices estimated using our MCS considering the different values for t_{RTO} are presented in Table 8. The increase of the response time directly affects the reliability

indices that accounts failures durations – Availability and SAIDI, as the impact of a fast operation is related to the length of customers' electricity interruptions.

Table 8 – Reliability indices obtained for the CPPS with failures into Communication and Electrical components using the values described in Table 5.

μ_{RTO}	Availability	SAIDI	SAIFI	Failure Rate
0	3.203	0.953	0.318	1.831
1	3.202	0.956	0.336	1.900
5	3.198	0.969	0.336	1.900
10	3.194	0.984	0.336	1.900
20	3.185	1.014	0.336	1.900
40	3.167	1.075	0.336	1.900
60	3.151	1.136	0.336	1.900

Source: Author

For cases where $\mu_{RTO} > 0$, SAIFI and Failure Rate are affected because customers in the healthy out-of-service branches enter in failure state during the human operator's decision making. However, the impact is the same for any $\mu_{RTO} > 0$, since such indices account only outages occurrence, and are not influenced by their duration. In the case where $\mu_{RTO} = 0$, both system's Failure Rate and SAIFI do not account for the customers that are transferred to another energized feeder since the simulation assumes the transfer happens instantaneously after the failure.

Table 9 and Figure 17 present the percentage of these impacts. The indices that consider only failure occurrence are not affected by the response time since the number of failures is not either. It is important to highlight that this study investigates the response time of the operator's impact on CPPS reliability; the effects of the operator's decision quality were not investigated. The impact of considering $\mu_{RTO} = 1$ is less than 1% for both SAIDI and Availability. On the other hand, the effect of $\mu_{RTO} \geq 40$ in Availability is more than 1%, and the impact in SAIDI is greater than 1% for $\mu_{RTO} > 5$ minutes, and for $\mu_{RTO} = 60$, this is almost 20%. This result indicates that quick response time is essential to the CPPDS Reliability.

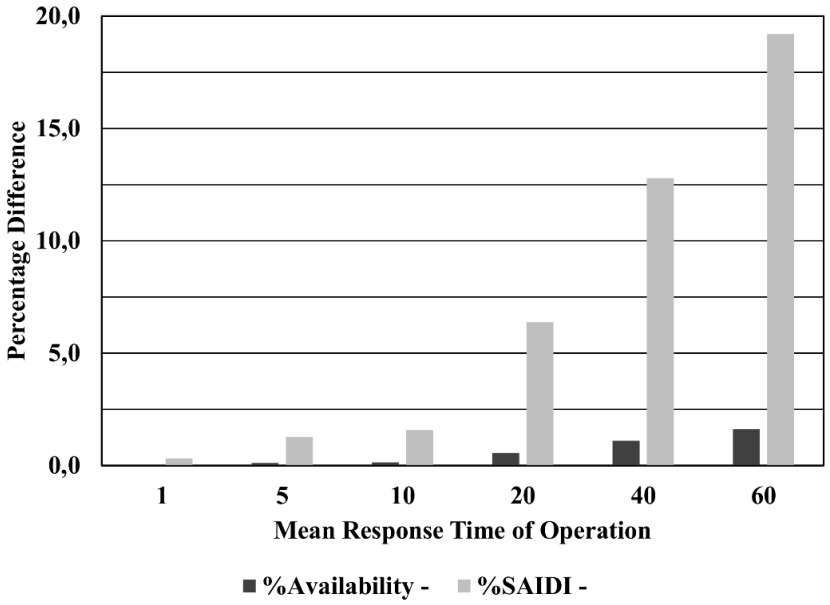
Besides the case study using the Civanlar's example distribution system, the results presented in this Section highlighted the importance of the operator's response time for DSs reliability. As the DSs are becoming even more integrated with ICT, as others engineered systems, these systems operation must also be in focus, inclusive the human operators. As shown in the paragraphs above, a delay in the decision making during contingencies in a CPPDS can expressively affect the system reliability, quantified by the worsening of the Availability and SAIDI metrics, which reflects the QoS perceived by consumers during interruptions. Such findings reinforce the need of decision support systems development to the operation of CPPS, as the integration of ICT aims to improve systems reliability

Table 9 – Percentage difference in Availability and SAIDI indices when increasing the μ_{RTO} parameter.

RTO	Availability	%Availability	SAIDI	%SAIDI
0	3,203	-	0,953	-
1	3,202	0,029	0,956	0,320
5	3,198	0,115	0,969	1,278
10	3,194	0,142	0,984	1,574
20	3,185	0,565	1,014	6,381
40	3,167	1,106	1,075	12,790
60	3,151	1,627	1,136	19,198

Source: Author

Figure 17 – Percentage difference in CPPS Availability and SAIDI indices by the μ_{RTO} used in each scenario. The greater the average response time values, the larger the effect on reliability indices



Source: Author

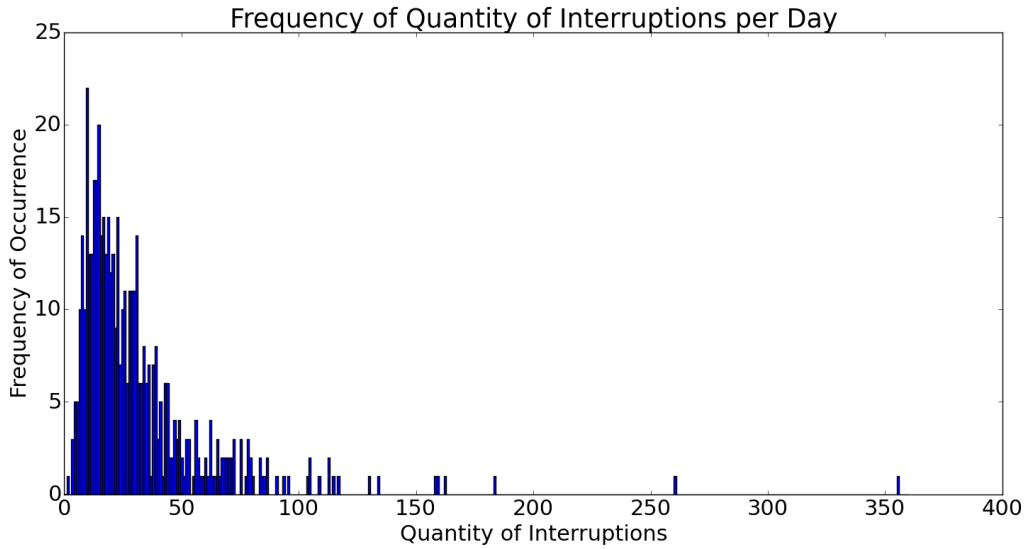
by real-time capabilities, the system reliability becomes more sensitive to human factors during contingencies.

4.2 Brazilian Power Distribution System Failure Model

The failure process was modeled by a regression for the failure rate, which is considered the daily quantity of outages per distribution network's kilometers with two predictors concerning atmospheric conditions: number of atmospheric discharge, and maximum wind gust speed in the day. The meteorological data is available from a weather station at the city airport, and it is the daily quantity of lightning and the maximum wind

gust speed in km/h. In Figure 18, a histogram shows the daily outages quantity, when at least one atmospheric discharge was detected, considering the historical data.

Figure 18 – Histogram of the daily outages when there is, at least, one atmospheric discharge.



Source: Author

Firstly, the Poisson Regression Model (Equation 3.4) was considered to predict the data set. In Table 10, the estimated coefficients are presented. The results (estimated values and the $p - values$) indicates that both factors are significant for the model. In addition, the intercept indicates the expect number of outages without the atmospheric events. The wind gust speed coefficient is greater than the number of atmospheric discharge coefficient, indicating that the number of outages is more influenced by the first one.

Table 10 – Poisson Regression Coefficients.

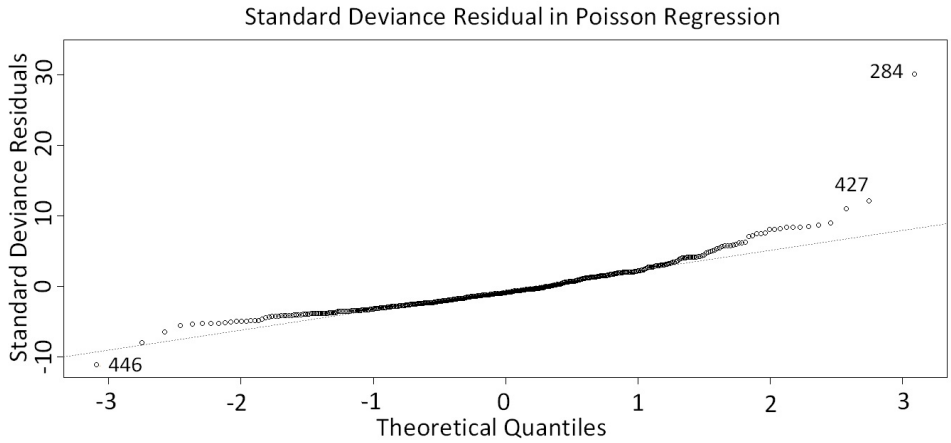
Coefficients	Estimated Value	Std Error	$\Pr(>\|z\|)$
Intercept	2.1435828	0.0224021	$< 2e^{-16}$
Number of Atmospheric Discharge	0.0007288	0.0000267	$< 2e^{-16}$
Wind Gust Speed	0.0314837	0.0005070	$< 2e^{-16}$

Source: Author

The residuals for the obtained model is presented in Figure 19. Besides the low residual, three samples presented large residuals, which are possibles *outliers*: 446, 427 and 284. These samples are related to extreme atmospheric events: the first one to the day with the higher quantity of atmospheric discharges, the second to a day where a storm strikes

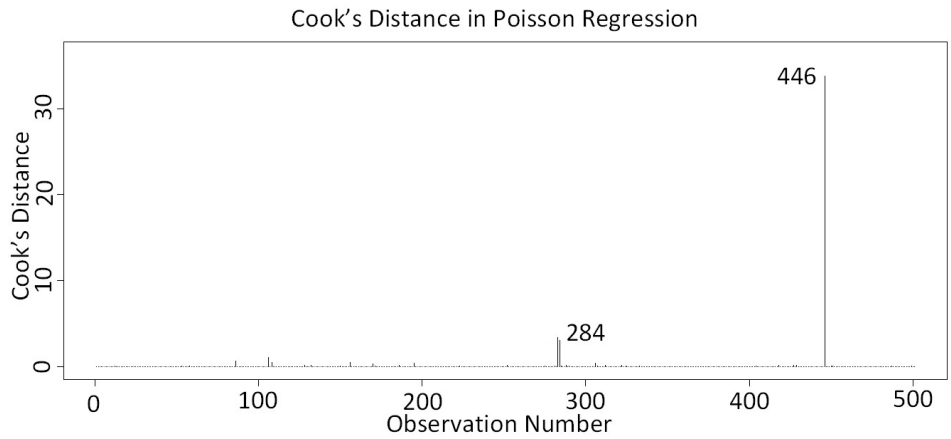
the city with many outages, and the last is the day following the one that occurred winds with the highest recorded speed in the data set. The Cook's Distance (Equation 3.12) is presented in Figure 20, the observations 446 and 284 presented a value greater than 1, indicating that both are possible influential points in the Poisson Regression Model.

Figure 19 – Standard Deviance Residual versus Theoretical Quantiles in the Poisson Regression.



Source: Author

Figure 20 – Cook's Distance for each predicted value in the Poisson Regression Model.



Source: Author

In Table 11, the coefficients obtained for the Negative Binomial Regression (Equation 3.7) are presented. The coefficients are similar to the ones acquired using the Poisson Regression (estimated values and $p - values$). However, the intercept and number of atmospheric discharges presented increased importance while the wind gust speed influence is lower than the Poisson regression.

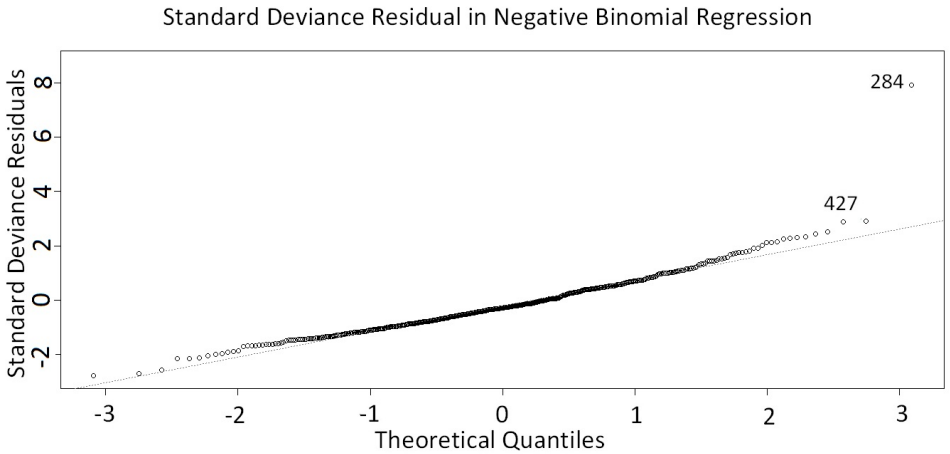
Table 11 – Negative Binomial Regression Coefficients.

Coefficients	Estimated Value	Std Error	Pr(> |z|)
Intercept	2.2507716	0.0864196	$< 2e^{-16}$
Number of Atmospheric Discharge	0.0011096	0.0001346	$< 2e^{-16}$
Wind Gust Speed	0.0274958	0.0023403	$< 2e^{-16}$

Source: Author

As in the Poisson Regression Model, the residuals are not normally distributed. However, the Negative Binomial Regression addresses a better response to the *outliers*, as we can observe in Figure 21. The samples 284 e 427 still presented larger residuals, but with lower values than in the Poisson Regression, indicating, as expected, that the Negative Binomial is better to deal with the *outliers*. The Cook's Distance for the Negative Binomial regression is presented in Figure 22 and all samples presented a distance lower than 1, reinforcing its better capability of dealing with the extreme events.

Figure 21 – Standard Deviance Residual versus Theoretical Quantiles in the Negative Binomial Regression.

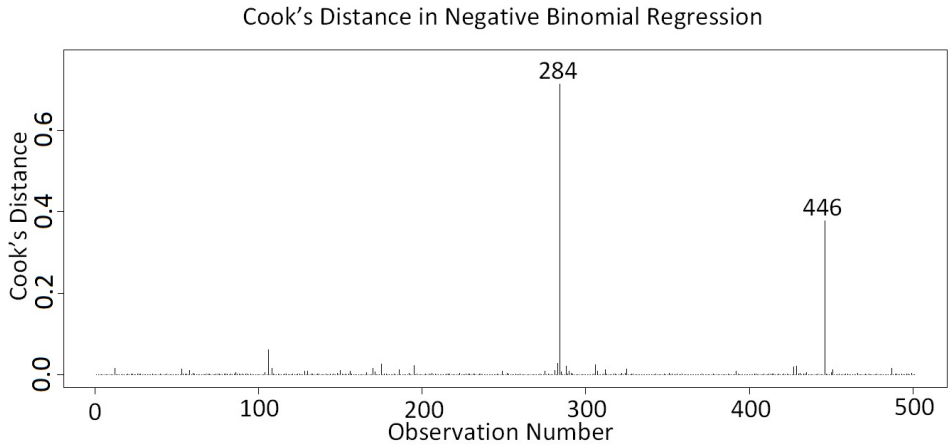


Source: Author

The AIC and BIC were used to compare the models, and the results are presented in Table 12. Such values are in agreement with the residuals and Cook's Distance presented previously, the lowest values of AIC and BIC are obtained using the Negative Binomial Regression. Then, if the total amount of overhead lines in the city is considered (in this case 3080 km), a final model can be defined as daily failure rate per kilometer, λ_d, as shown in (4.1).

$$\lambda_d = \frac{1}{3080} \left(\exp\left(2.2507716 + 0.0011096nt + 0.0274958wg\right)\right), \tag{4.1}$$

Figure 22 – Cook's Distance for each predicted value in the Negative Binomial Regression Model.



Source: Author

Table 12 – Akaike and Bayesian Information Criterion for both models, Poisson and Negative Binomial.

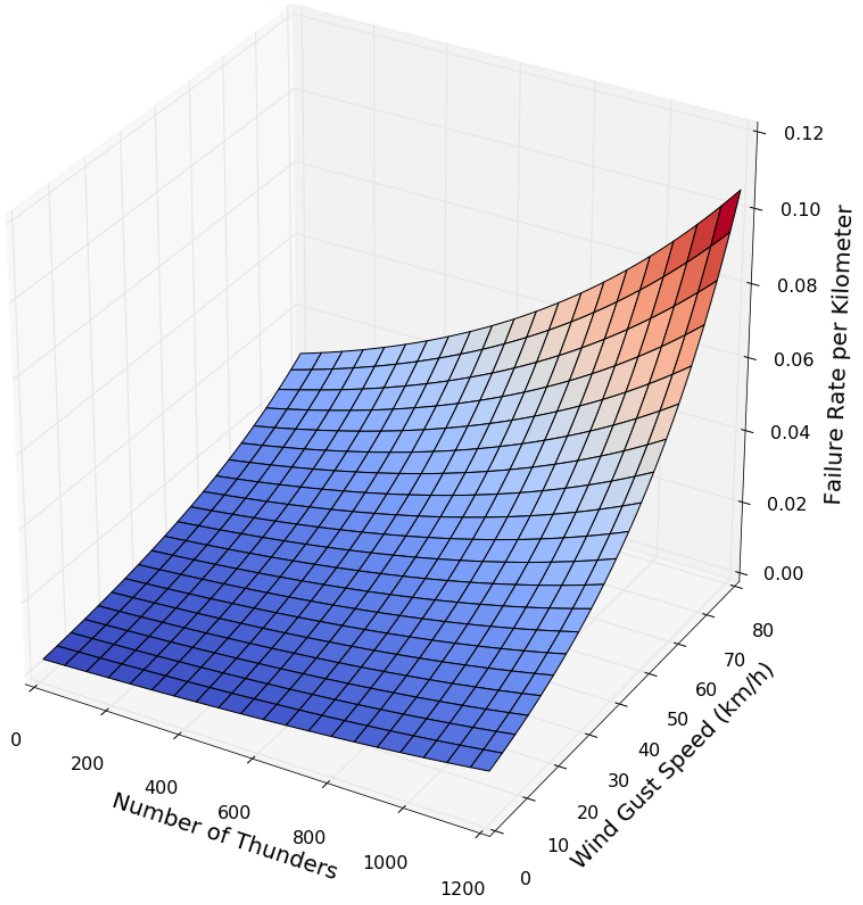
Model	AIC	BIC
Poisson	7925.59	7938.24
Negative Binomial	4124.65	4141.52

Source: Author

where nt is the occurred number of atmospheric discharges and wg is the maximum occurred wind gust speed in the day (km/h).

In Figure 23, the Equation (4.1) graphical representation is shown. It is possible to observe the greater influence of the wind gust speed relatively to atmospheric discharges on λ. Besides, it is possible to verify by the obtained model that there is an intrinsic failure rate for the Brazilian DS that is independent of the climatic covariates, this quantity, which is around 0.005 failures/(day.km), is obtained with $nt = wg = 0$. Such model can be useful to utilities locate and evaluate the need for more maintenance crews to restore the system by using atmospheric forecast information and consequently improving the QoS indicators. Moreover, the obtained final model, based on the Negative Binomial Regression, is capable of handling the extreme values, the *outliers* for the Poisson Regression model. This characteristic becomes important in the context of rare and extreme events, which is explored in the resilience analysis.

Figure 23 – Obtained Surface for Failure Rate per Kilometer in function of the Number of Thunders (Atmospheric Discharges) and Wind Gust Speed.



Source: Author

4.3 Brazilian Power Distribution System Repair Model

The electricity interruptions in the historical data have thirty-six single causes (they are presented in the Annex A) of service interruption which are grouped into five different categories: Atmospheric, Environmental, Urban, Operational Causes and Equipment Failure. They are exemplified in Table 13. Such grouping was performed to reflect the types of interactions between a distribution system and external agents. The Figure 24 presents a box plot of the repair time by the groups of causes.

First, a Survival data analysis was performed to explore the relations between the types of causes and the repair time, or outage duration. The Survival function ($S(t)$) describes the probability of having a failure with duration of length greater than t. The curves obtained using Kaplan-Meier estimator (Equation 2.70) are shown in Figure 25.

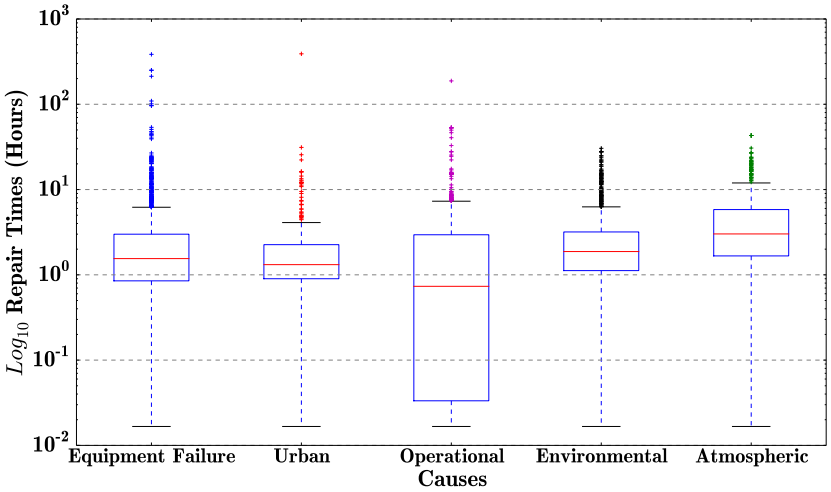
The Survival functions for Equipment Failure, Urban, and Environmental causes are very similar for all values of t. Operational causes have the Survival function with the

Table 13 – The five categories of outages causes assumed with some examples for each one.

Categories	Causes examples		
Atmospheric	thunders	wind	low temperature
Environmental	corrosion	tree fall	trapped animal
Urban	theft	flood	collision
Operational	load unbalance	load transfer	required shutdown
Equipment Failure	unidentified	damaged equipment	corrective maintenance

Source: Author

Figure 24 – Box plot of the Repair Time for Each Type of Causes. The y-axis is presented in log_{10} due to Large Variance in the Data Set.

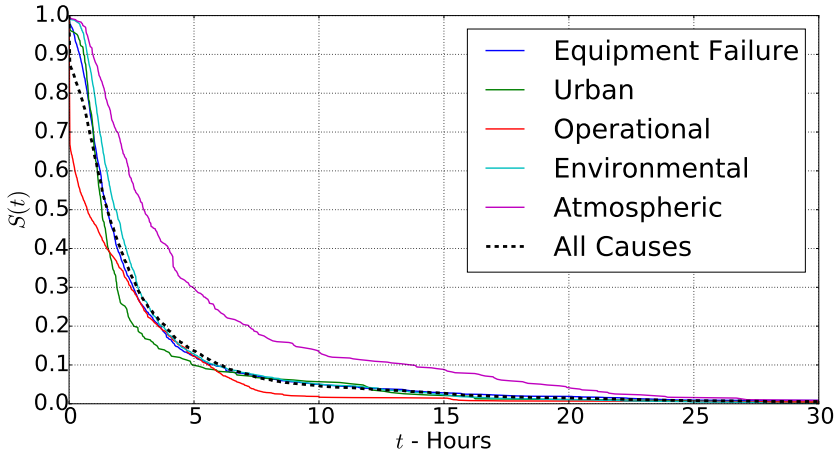


Source: Author

lower probabilities. In the opposite, Atmospheric causes have the higher probabilities. To summarize such differences, the following times to repair were calculated: Median Time to Repair (MTTR - $S(t) = 0.5$), and the 1st ($S(t) = 0.75$) and 3rd ($S(t) = 0.25$) quartiles from the KM estimation for the five types of causes. Such values are presented in Table 14, and reflect the differences in the $S(t)$ functions presented in Figure 25.

In addition to the Survival function, we also estimated the cumulative Hazard rate using the Nelson-Aalen estimator (Equation 2.71). The Figure 26 shows the results. In our context, the hazard rate represents the conditional repair rate. The cumulative Hazard rate increases for all types of outage causes, the Operational is the one with the faster increase. On the other hand, the Atmospheric causes are the one with the slower increase in the repair rate. For the Equipment Failure, Urban and Environmental causes, the Hazard rate increase in a similar manner. Such results are in agreement with the Survival function in Figure 25 and the Times to Repair of Table 14.

Figure 25 – Survival Function obtained using the Kaplan-Meier Estimator for the data set Describing Outages Duration and Causes for each Cause Category and considering the Duration of all Causes.



Source: Author

Table 14 – First ($S(t) = 0.75$) and Third ($S(t) = 0.25$) Quartiles Times to Repair and the Median Time to Repair obtained from the Kaplan-Meier estimator

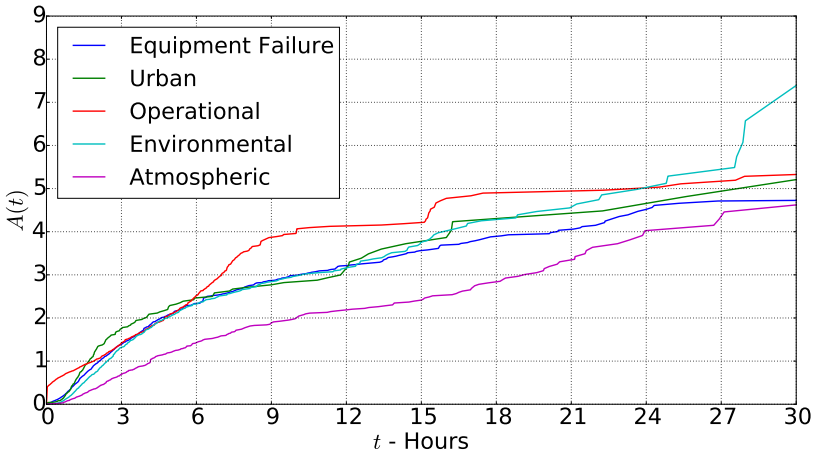
Outage Type	$S(t) = 0.75$	MTTR (hours)	$S(t) = 0.25$
Equipment Failure	0.867	1.550	3.000
Urban	0.916	1.317	2.300
Operational	0.034	0.733	2.967
Environmental	1.134	1.867	3.184
Atmospheric	1.667	3.017	5.834

Source: Author

The Survival analysis showed that the group of causes directly impact in the repair time of the studied Substation. Atmospheric causes are the one that can lead to the higher values of time to repair. The second type of outage cause with the higher value of MTTR is the Environmental, which is related to animals and trees interacting with the system. Urban and Equipment failure results in repair times statistically similar. The outage duration caused due to Operational needs represents the lower MTTF. To model such repair processess, an EW model was obtained from the data set. The parameters estimated using the MLEs are presented in Table 15, and the respective curves are shown in Figure 27.

The model was tested using Error Measures (Mean Squared, Mean Absolute, and Standard Deviation errors) to understand how well it can describe the outage durations. The values are presented in Table 16. The error values reveal that the EW is a good model to describe the outage duration, and its can be useful in answering questions about the probability of outages duration under specific scenarios. Additionally, it allows the

Figure 26 – Accumulative Hazard rate for each type of cause calculated using the Nelson-Aalen estimator.



Source: Author

Table 15 – Parameters estimated for the Exponentiated Weibull using the Maximum Log-likelihood.

Causes	$\widehat{\alpha}$	$\widehat{k}$	$\widehat{\lambda}$
Environmental	6.6737	0.3923	0.1873
Atmospheric	8.4298	0.3744	0.1210
Equipment Failure	1.1243	0.4828	0.9711
Operational	7.8570	0.4913	0.3165
Urban	7.4547	0.4502	0.4579

Source: Author

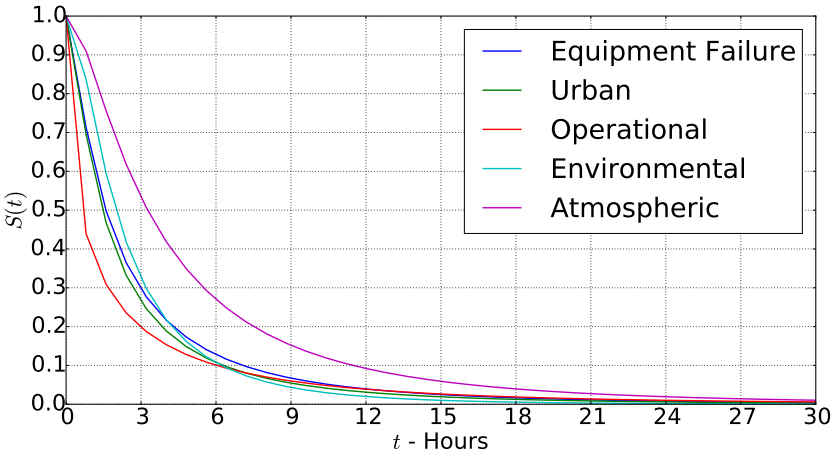
inference about the expected repair time, and can be used to provide restoration prediction.

Table 16 – Error measures for each Cause Group calculated from the EW models fitted and the K-M estimator

Causes	Mean Squared Error	Mean Absolute Error	Standard Deviation Error
Urban	0.0055	0.0627	0.0701
Operational	0.0025	0.0401	0.0472
Atmospheric	0.0006	0.0207	0.0230
Environmental	0.0011	0.0283	0.0298
Equipment Failure	0.0012	0.0291	0.0301

Source: Author

Figure 27 – Curves Obtained using the Estimated Parameters Presented in Table 15 for each Cause Group.



Source: Author

4.4 Brazilian Power Distribution System Characterization

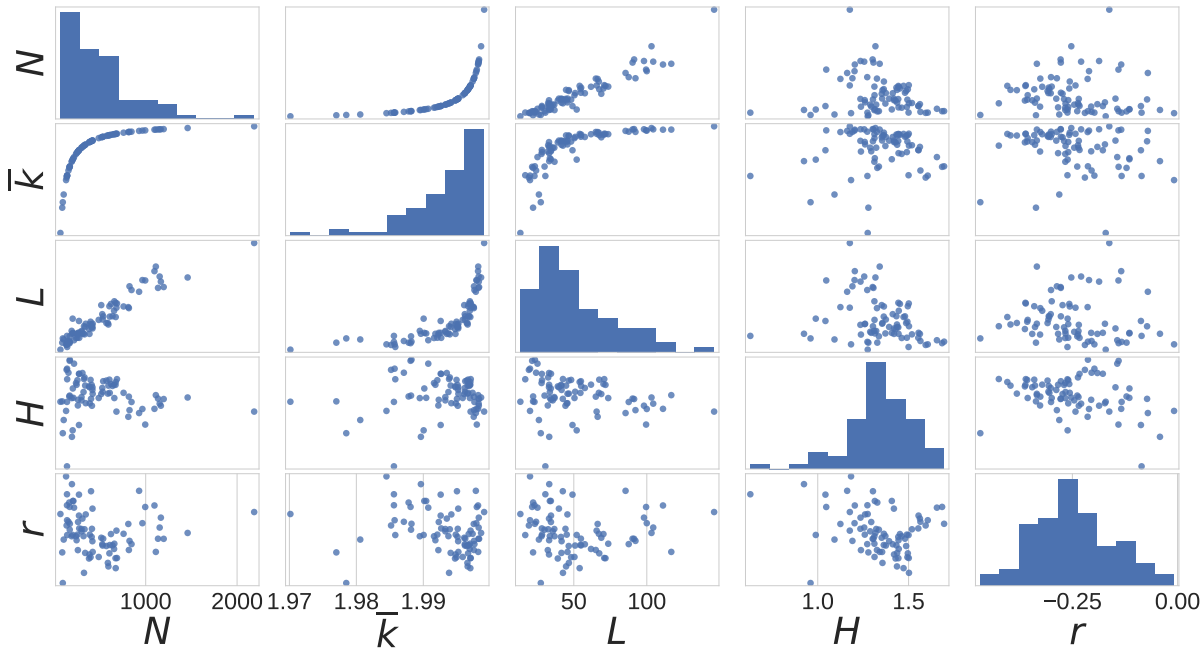
In this Section, different features of the Brazilian DS are presented, using both, topological and hybrid metrics. In Figure 28, a scatter matrix plot[1] presents the topological features calculated for the 81 distribution networks. All the networks share a similar value of $\overline{k}$ around 2, and the other features presented a higher variability. By inspecting the scatter plots, is possible to note that bigger networks have a higher L, reflecting that the average shortest path among the vertex increases with the distribution networks N. The H values shows that the uncertainty on the number of connections is low for such radial networks, and the $r \leq 0$ for all the networks indicates that most of the vertices are connected with lower degree ones.

Similarly, the Figure 29 presents the weighted version of such metrics, being the edges' weight equal to the power flowing through them. Using such hybrid features is possible to observe information about how the electricity flow is distributed over the networks structures. The first difference is that some relationships presented in Figure 28 are not present in the weighted features. The H^W resulted in higher values than H, indicating a higher uncertainty about the vertices weighted degree. Moreover, by inspecting the scatter plot of N x H^W is possible to see a tendency of higher weighted entropy for networks with higher Order.Another remarkable difference is the r^W that presented only positive values, related to the connection between only vertices with a similar weighted degree.

Such features presented in Figures 28 and 29 will be explored in the Section 4.8,

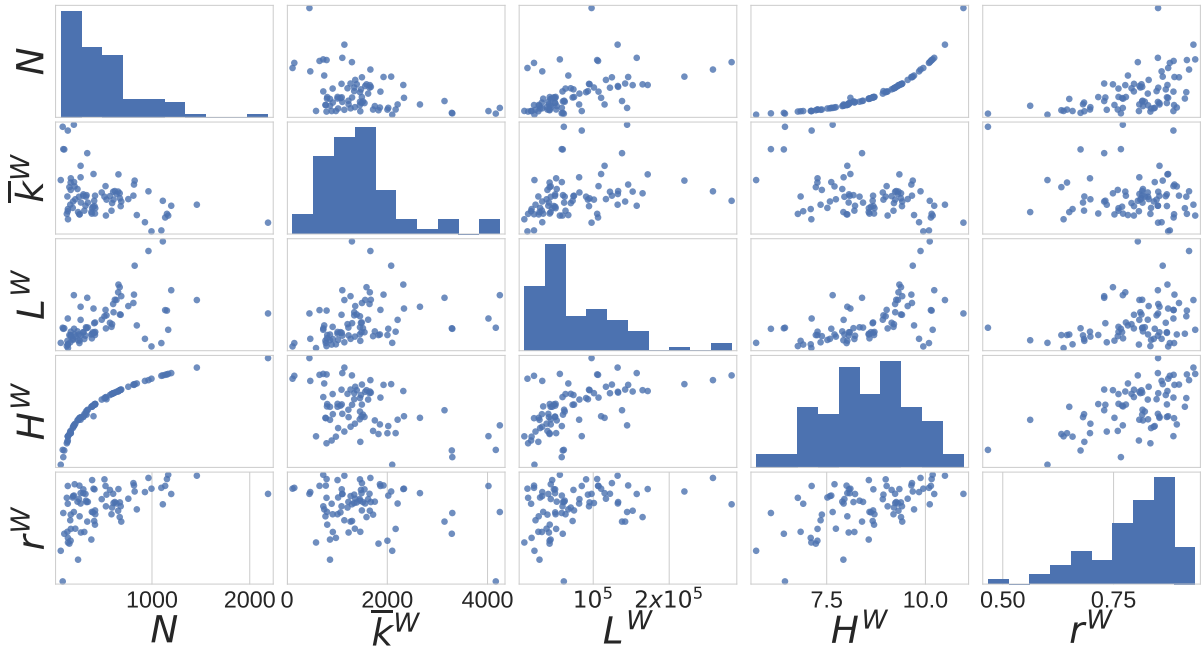
[1] In such matrix, the diagonal presents a histogram of the data, and the i, j element is a scatter plot of the i-th row by the j-th column.

Figure 28 – Scatter matrix presenting the topological features of the 81 distribution networks used in this study.



Source: Author

Figure 29 – Scatter matrix presenting the hybrid features of the 81 distribution networks, where the edges weights are the power flowing through them.

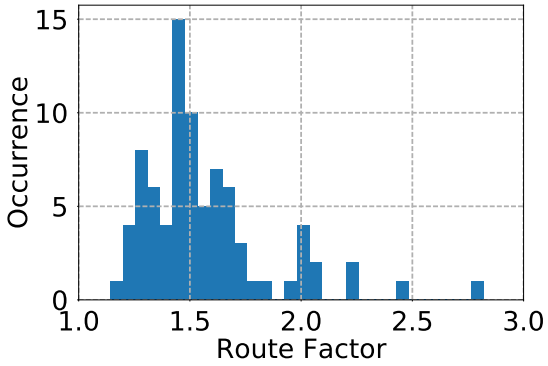


Source: Author

where the resilience assessment results will be presented under different weather scenarios for all the 81 distribution networks. In such Section, the association among these features

and the estimated resilience in the extreme weather scenario also will be investigated, as mentioned in the Section 3.5. The Route Factor (see Section 2.2.3) was also calculated for all the samples and is presented in Figure 30. The values range from 1.14 to 2.82, reflecting the heterogeneity of the Brazilian samples. The higher Route Factor values are very different from the values obtained for other types of SDN in (GASTNER; NEWMAN, 2006) and (YAZDANI; JEFFREY, 2011) (see Table 1). Since the Route Factor account the ratio between the Euclidean distance of a straight line between vertices on the 2-d embedding space and the path length by using the network edges, this probably is related to geographical circumstances.

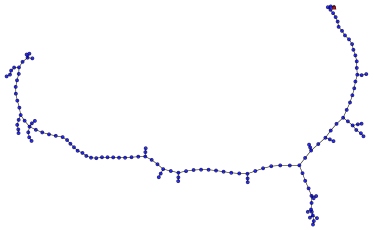
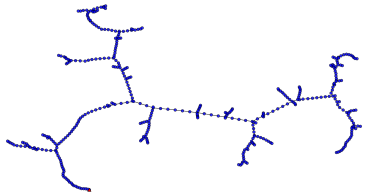
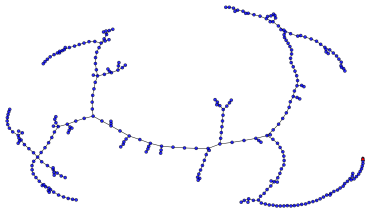
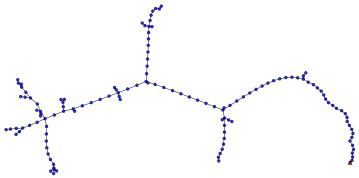
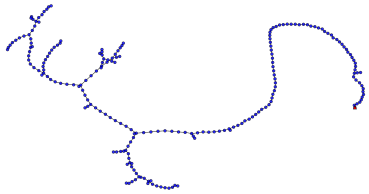
Figure 30 – Histogram for the Route Factor (see Section 2.2.3) calculated for all the 81 distribution networks of the Brazilian DS.



Source: Author

The results that will be presented in the next section, related to the vulnerability analysis, were obtained using five distribution networks. The Table 17 presents such networks with their topological characterization metrics and *Route Factor* (q) values. The values of q are in a range similar to the other spatial distribution networks q presented in Table 1. Samples 1, 4 and 5 have a similar *Route Factor* value, 1,21, 1,29 and 1,27 respectively. Samples 2 and 3 have a higher value, 1,45 and 1,64 respectively. Comparing the graphs displayed in Table 17 and the *Route Factor* values, is possible to notice that the samples that are more overspread presented a higher value of *Route Factor*.

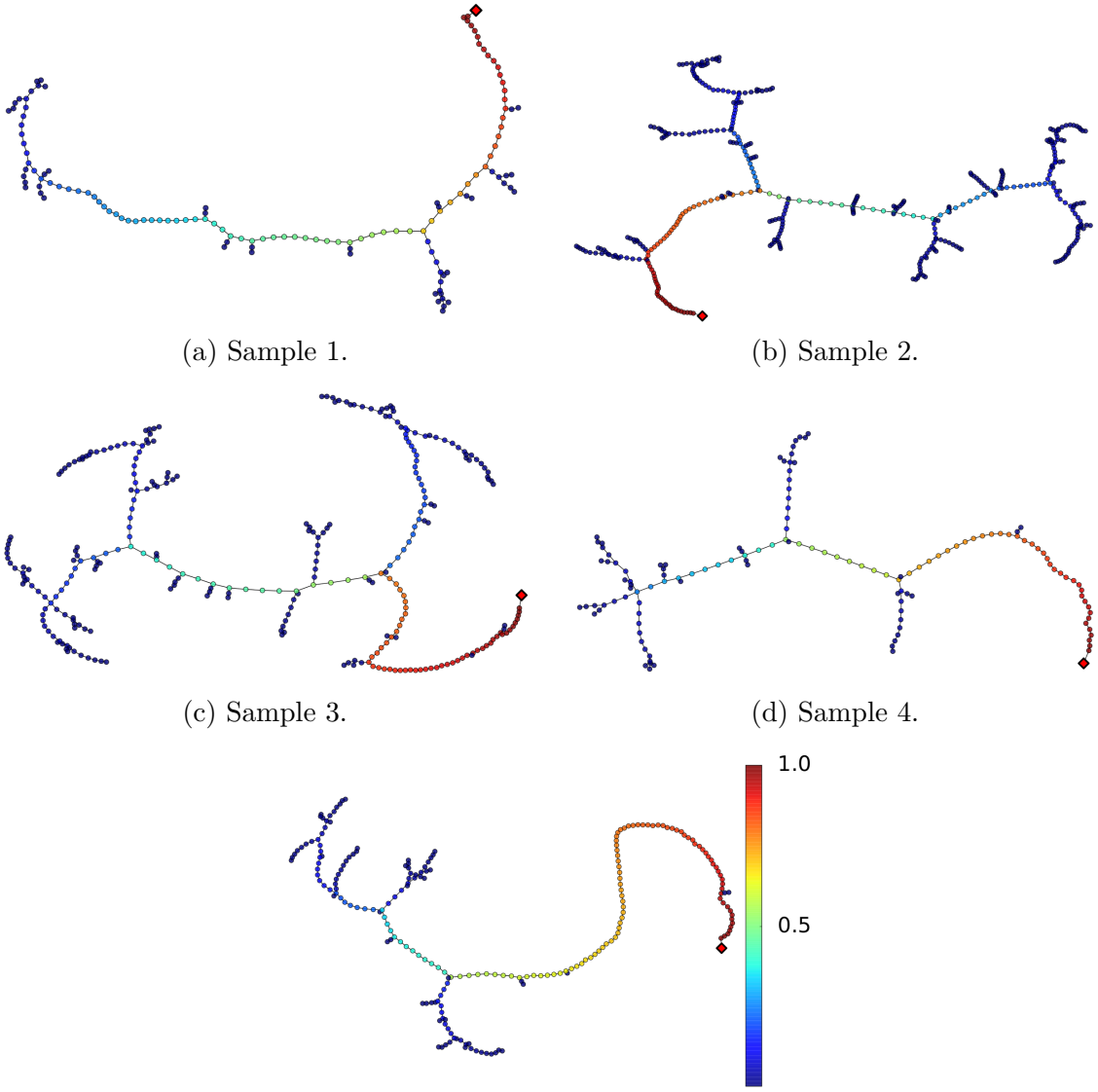
Table 17 – Features of used Brazilian DS samples. The metrics used to describe they topological structure are Order (N), Size (M), Density (δ), Average Degree ($\overline{k}$), Average Geodesic Path (l) and Diameter (D). All samples present a Clustering Coefficient (C) equal to zero. Such metrics were defined in Section 2.2.

Graph	Sample	N	M	δ	$\overline{k}$	l	D	H	E	r	q
	1	134	133	0.015	1.99	28.9	83	1.298	0.083	-0.293	1.21
	2	412	411	0.005	2.00	44.3	117	1.235	0.045	-0.234	1.45
	3	295	294	0.007	1.99	36.4	94	1.33	0.055	-0.233	1.64
	4	133	132	0.015	1.98	23.2	66	1.31	0.091	-0.163	1.29
	5	220	219	0.009	1.99	44.3	129	1.03	0.057	-0.313	1.27

Source: Author

These five samples were also characterized by using the proposed C_D. The Figure 31 displays the five samples graph representation with the vertices colored respecting their values of *Distribution Centrality*. The distribution of vertices C_D is not similar for all samples. While Samples 1, 4 and 5 have a considerable amount of high C_D vertices, Samples 2 and 3 have a relatively lower proportion of high C_D vertices.

Figure 31 – Graph representation using the *Distribution Centrality* (C_D). The color of vertices are displayed as a "heat map" of C_D values, which ranges from 0 to 1 and represents the pertinence ratio of a vertex to paths connecting the other vertices to the source one.



(a) Sample 1.

(b) Sample 2.

(c) Sample 3.

(d) Sample 4.

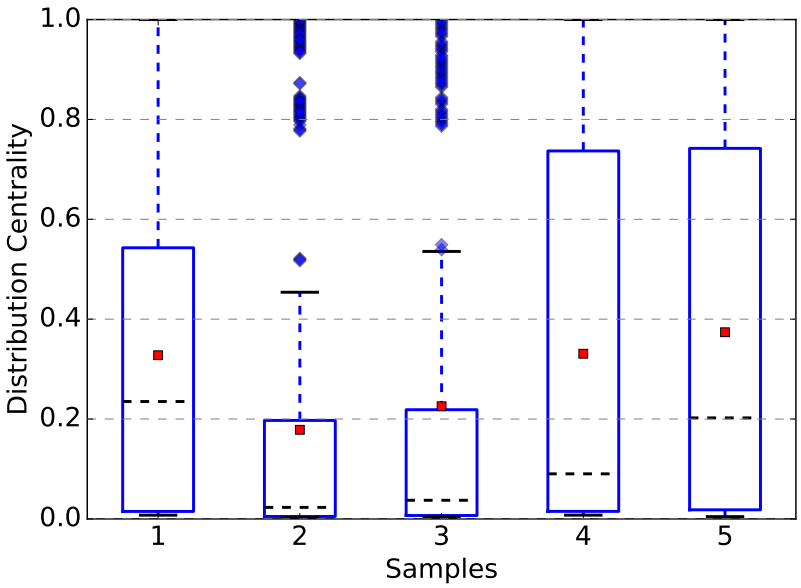
(e) Sample 5.

Source: Author

The samples C_D metric were characterized by fitting their distribution using the Power Law distribution (see (2.25)). First, the Figure 32 shows the C_D values box-plot, indicating that the Samples 2 and 3 have a very similar distribution of C_D values, with a

left fat-tailed distribution, with a low median and average values. The higher values of C_D are displayed as outliers in the box plot. The Samples 1, 4 and 5 have a higher median and average values, and without outliers in the box plot representation.

Figure 32 – Box plot of the *Distribution Centrality* values for each Brazilian DS sample. The red square represents each Sample Average C_D value.



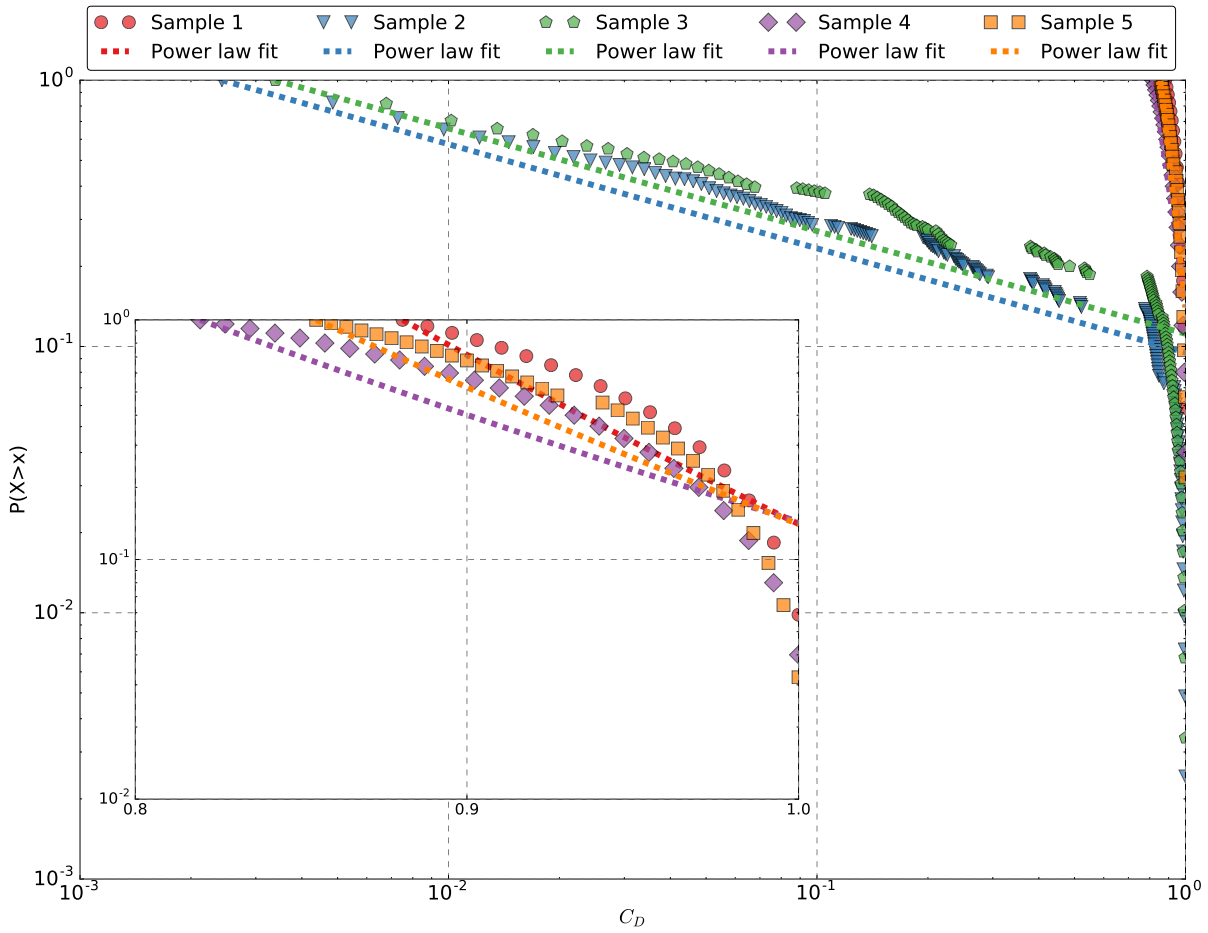
Source: Author

In Figure 33, the $P(X > x)$ values together with the fitted Power Law distributions are presented. The differences highlighted in the box-plot are reinforced by the Power Law fit. The Samples 2 and 3 resulted in a different distribution fit. In Table 18 the data parameters (average and standard deviation) together with the Power Law estimated parameters (x_{min} and α) are presented. The values of the lower bound x_{min} and the exponent presented a high variety. The Sample 1 has the higher exponent value and lowers bound, followed by Samples 5 and 4. The Samples 1 and 2 resulted in similar values for both parameters.

Table 18 – Distribution of the C_D values and the Power Law fitted parameters. $< x >$ is the average, σ is the standard deviation, $\widehat{x}_{min}$ is the estimated lower bound, and $\widehat{\alpha}$ is the estimated exponent.

Sample	$< x >$	σ	$\widehat{x}_{min}$	$\widehat{\alpha}$
1	0.328	0.336	0.881	16.422
2	0.178	0.305	0.002	1.391
3	0.226	0.336	0.003	1.386
4	0.331	0.367	0.820	10.741
5	0.374	0.366	0.855	13.493

Figure 33 – Power Law Fit for the Distribution Centrality considering the five Brazilian DS feeders. The smaller plot is a more detailed representation of Samples 1, 4 and 5.



Source: Author

The C_D metric will be used to discuss some differences among the Brazilian DS samples Vulnerability. Samples 1, 4 and 5 have a long path with higher C_D values, while Samples 2 and 3 have the shorter path with higher C_D values. Such difference is the same direction with the *Route Factor* values (see Table 17). The interpretation of such characteristics is that Samples 2 and 3 have more ramifications from the path connecting these systems sink vertices to the source one. This characteristic will be more explored in the following sections.

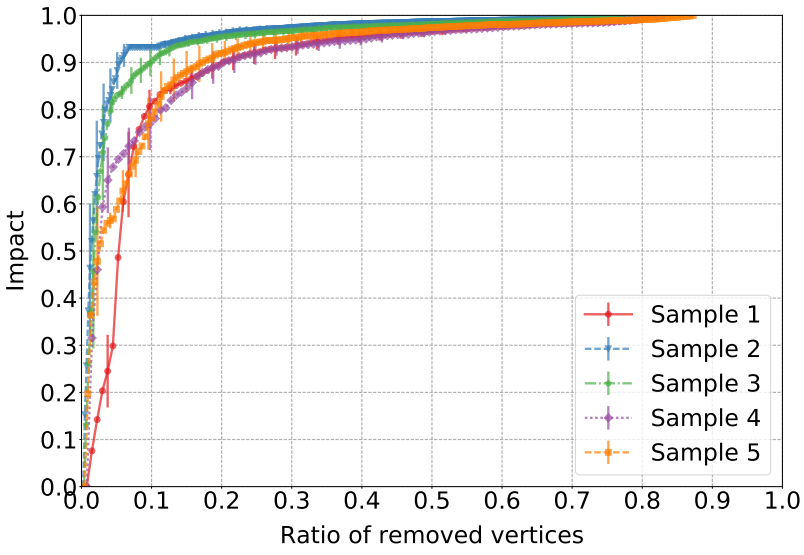
4.5 Static Vulnerability Analysis

In this Section, the static vulnerability analysis results are presented to the Brazilian samples. Firstly, vulnerability analysis to vertices attacks is performed by using the vertices degree as importance measure and the LCC and SCC as performance metrics. The relative impacts are compared by using their average and standard deviation, and by the CCR. The *Distribution Centrality* is also used to perform directed attacks. In sequence, Vulnerability Analysis to random errors is carried out assuming only vertex errors, and the achieved impacts are compared in a similar way as for directed attacks.

4.5.1 Attacks

Attacks were simulated by considering the vertices degree as importance measure. Since the samples have vertices with the same maximum degree value ($k_{max} = 4$), the simulation was repeated 50 times to allow the observation of variations in the elements removal order while respecting the degree as importance measure. The obtained average and standard deviation impact using the LCC performance metric are presented in Figure 34 for each sample. All samples are very vulnerable to directed attacks, the removal of a small fraction of the systems vertices is enough to cause a significant impact.

Figure 34 – Attacks impact obtained for the five samples of Table 17 using the metric LCC. The solid lines are the averages impact, and the error bars are the standard deviations obtained from trials.



Source: Author

The samples 2 and 3 are the more vulnerable, Sample 2 experiences an average impact of 0.9 with the removal of 5% of the higher degree vertices, Sample 3 experiences the same impact with the removal of 10% of its higher degree vertices. The other samples

experience the same impact with the removal of around 20% of their higher degree vertices. In Table 19, a summary of the average impact versus the number of necessary removals is presented. The values equal to zero indicate that a single removal causes an impact higher than 0.1. When compared with the Dutch medium voltage samples analyzed in (PAGANI; AIELLO, 2015), which need the removal of 10% of the higher degree vertices to suffer an impact of 0.9, the Brazilian samples provide a different result. Only two samples resulted in a similar vulnerability, Samples 2 and 3, the other three samples needs more than 10% of removals to suffer the same 0.9 impact.

Table 19 – Summary of the average impacts ($\overline{I}(j)$) for attacks considering the degree as importance metric and using the LCC performance metric for the five samples. The values equal to zero indicate that a single removal causes an impact higher than 0.1.

$\overline{I}(j)$	Number of removed elements (%)				
	S 1	S 2	S 3	S 4	S 5
0.1	1(0.75%)	1(0.24%)	1(0.34%)	0(0.00%)	1(0.45%)
0.5	6(4.47%)	5(1.21%)	5(1.69%)	2(1.50%)	5(2.27%)
0.9	26(19.40%)	22(5.33%)	28(9.49%)	26(19.55%)	37(16.82%)

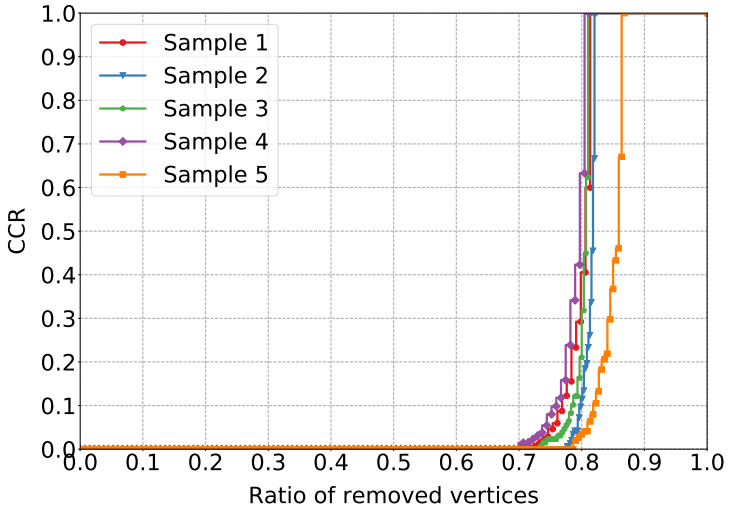
Source: Author

By using the cumulative collapse rate, CCR, it is possible to look at the collapse occurrence during the trials. In Figure 35, the CCR is presented considering the LCC as performance metric. All the samples presented a similar behavior, being the Sample 4 the one with higher rates in all the intervals of removals. This result is different when compared with the average impact, where Sample 4 is one of the less vulnerable. On the other hand, Sample 5 is the less vulnerable to collapses. Besides the average impact, the collapse rate provided another type of analysis, since all samples were investigated using the same strategy. All samples experienced collapses only with the removals of 70% or more of their higher degree vertices.

In Figure 36, the result of attacks is presented by considered the proposed metric for SDN, the SCC. It shows a higher vulnerability of the samples to attacks. All the samples suffer an average impact of 0.9 with the removal of less than 20% of the higher degree vertices. The Sample 5, which was one of the less vulnerable became highly susceptible. Another difference is the higher deviation when considering the SCC. Table 20 summarizes the results of attacks using the SCC performance metrics. The higher average and standard deviation of the impact considering the SCC indicates that parts removal can cause a more significant impact if the source vertex connectivity is considered.

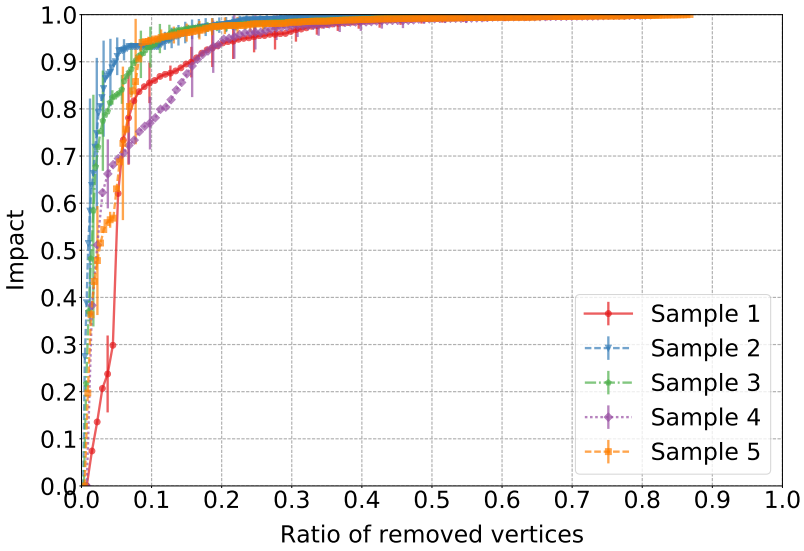
In Figure 37, the CCR for attacks using the SCC metric is presented. The differences between the average impact using LCC and SCC metrics (Figures 34 and 36) are highlighted by the CCR metric. All the samples experience collapses with the removal

Figure 35 – *Cumulative Collapse Rate* for attacks impact obtained for the five samples of Table 17 using the metric *LCC*.



Source: Author

Figure 36 – Attacks impact obtained for the five samples of Table 17 using the metric *SCC*. The solid lines are the averages impact, and the error bars are the standard deviations obtained from trials.



Source: Author

of only 10% of the higher degree vertices. By using the *SCC*, all the samples have a significant collapse probability for an even small ratio of removals. Sample 5 is the less vulnerable, similar to the results using *LCC* metric.

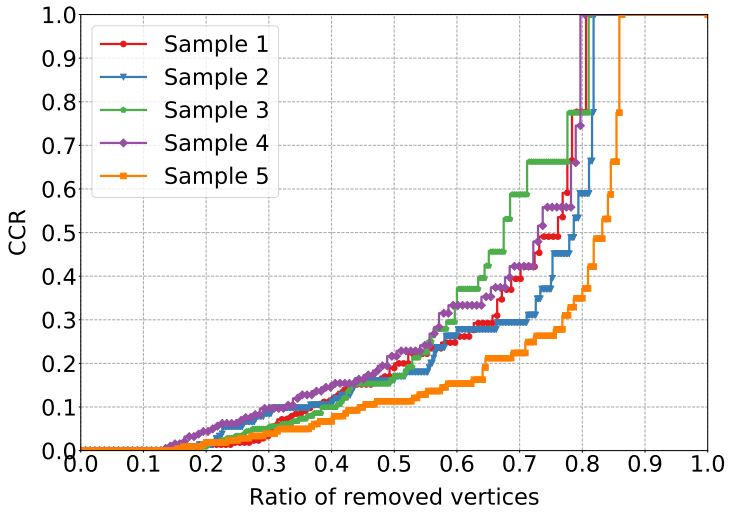
In Table 21, the $V - index$ (see Section 2.3) was calculated for all samples and considering both performance metrics. The higher the value of $V - index$, higher is the network Vulnerability. The $V - index$ is higher for *SCC* than for *LCC* for all samples,

Table 20 – Summary of the average impacts ($\overline{I}(j)$) for attacks considering the degree as importance metric and using the SCC performance metric for the five samples. The values equal to zero indicate that a single removal causes an impact higher than 0.1.

$\overline{I}(j)$	Number of removed elements (%)				
	S 1	S 2	S 3	S 4	S 5
0.1	1(0.75%)	0(0.00%)	0(0.00%)	0(0.00%)	1(0.45%)
0.5	6(4.47%)	3(0.73%)	3(1.02%)	2(1.50%)	5(2.27%)
0.9	20(14.93%)	19(4.61%)	21(7.12%)	21(15.79%)	17(7.73%)

Source: Author

Figure 37 – *Cumulative Collapse Rate* for directed attacks impact obtained for the five samples of Table 17 using the metric SCC.



Source: Author

corroborating with the previous results, indicating that the consideration of the source connectivity highlights a higher vulnerability.

Table 21 – $V - index$ calculated for all the samples considering both metrics, LCC and SCC, and the attack scenario. The higher the index, more vulnerable the sample is.

Attacks	$V - index$				
	S 1	S 2	S 3	S 4	S 5
LCC	0,41	0,46	0,45	0,42	0,43
SCC	0,43	0,47	0,47	0,44	0,46

Source: Author

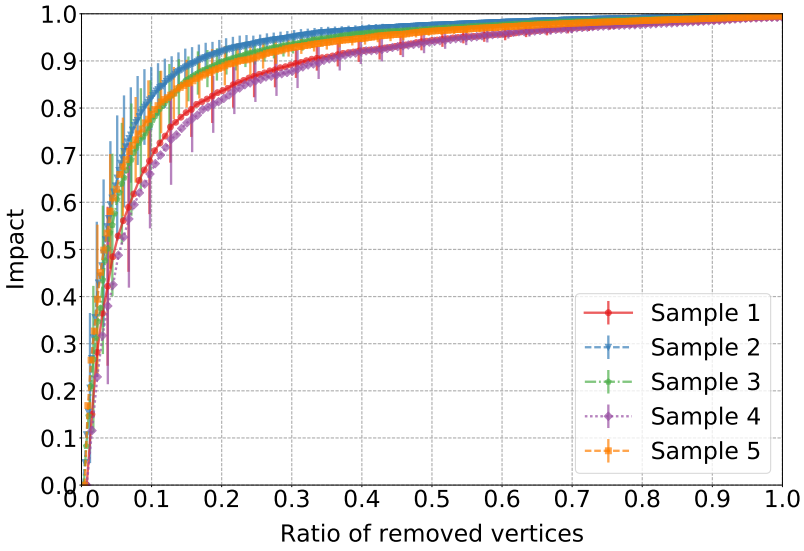
If the Distribution Centrality (C_D) is used to perform attacks and considering the SCC performance metric, the removal of the vertex with higher C_D value always result in system collapse, since the samples (See Figure 31) have a unique path connecting the

source element to the rest of the systems. This result is in agreement with such measure that accounts the importance of connecting other vertices to the source one.

4.5.2 Errors

The Vulnerability analysis to errors is performed following the assumption of equal removals probabilities. The simulations were repeated 100 times. In Figure 38, the result obtained using the LCC performance metric for the five samples is presented. The Table 22 summarizes the values obtained. The samples showed to be less vulnerable to errors when compared with the results of attacks with LCC. As for degree based attacks, the chosen samples provided a result different from the one presented for Dutch medium voltage DS samples (PAGANI; AIELLO, 2015), Brazilian ones showed to be less robust to random errors. Dutch samples suffer an impact of 0.9 when 40% of vertices are randomly removed, while Brazilian samples experiment the same impact with values less than 34%, the most vulnerable sample needs the removal of 16.26% of vertices to experience an impact of 0.9.

Figure 38 – Errors impact obtained for the five samples of Table 17 using the metric LCC. The solid lines are the averages impact, and the error bars are the standard deviations obtained from trials.



Source: Author

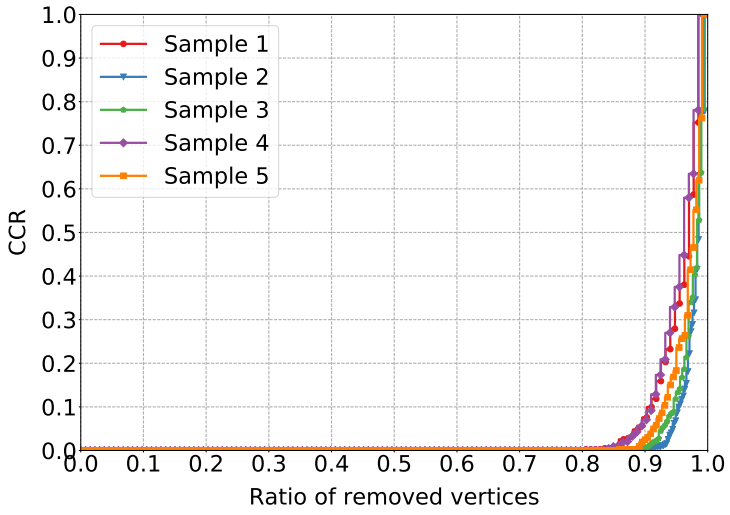
In Figure 39, the CCR is presented for random removals with the LCC performance metric. The less Vulnerability to errors, when compared with attacks and using the LCC, is highlighted by the CCR. The samples only experienced a collapse with more than 80% of random removals. For errors, Sample 3 is the less vulnerable, while Sample 4 is the most vulnerable, which is the inverse of the results obtained for attacks and using LCC.

Table 22 – Summary of the average impacts ($\overline{I}(j)$) for errors and using the LCC performance metric for the five samples.

$\overline{I}(j)$	Number of removed elements (%)				
	S 1	S 2	S 3	S 4	S 5
0.1	1(0.75%)	2(0.49%)	1(0.34%)	1(0.75%)	1(0.45%)
0.5	5(3.73%)	12(2.91%)	10(3.39%)	6(4.51%)	6(2.73%)
0.9	42(31.34%)	67(16.26%)	59(20.00%)	45(33.83%)	49(22.27%)

Source: Author

Figure 39 – Cumulative Collapse Rate for errors impact obtained for the five samples of Table 17 using the metric LCC.



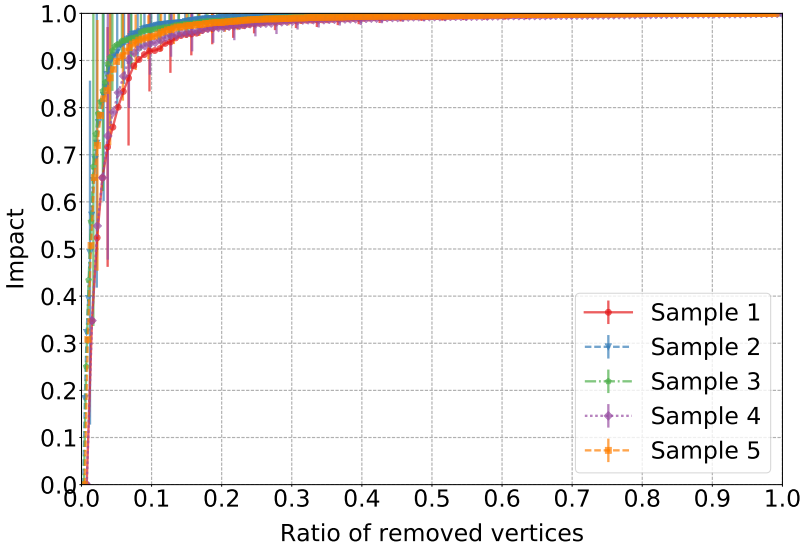
Source: Author

The same experiment was repeated but using the proposed SCC performance metric. The result is presented in Figure 40, and the Table 23 provides a summary of such results. When the source connectivity is considered by using the SCC performance metric, the random removals provide a very different impact. The analysis of all the samples indicates that they are very vulnerable to errors, the random removal of less than 10% of their vertices causes an impact of 0.9. Another important point is that a single failure results in an impact equal or higher than 0.1 for all samples.

In Figure 41, the CCR is presented, and the higher vulnerability to errors exposed previously is reinforced. The samples can experience collapses for any ratio of random removals. Sample 1, which is the most vulnerable have a collapse probability of 50% for the removal of approximately 40% of its vertices. The CCR shows an inherent vulnerability to random errors of the DS samples used.

In Table 24, the $V - index$ is presented for the five samples and using the LCC and SCC performance metrics. The $V - index$ is higher when considering the SCC metric than for the LCC, which reinforces that the consideration of the source connectivity

Figure 40 – Errors impact obtained for the five samples of Table 17 using the metric SCC. The solid lines are the averages impact, and the error bars are the standard deviations obtained from trials.



Source: Author

Table 23 – Summary of the average impacts ($\overline{I}(j)$) for errors and using the SCC performance metric for the five samples. The values equal to zero indicate that a single removal causes an impact higher than 0.1.

$\overline{I}(j)$	Number of removed elements (%)				
	S 1	S 2	S 3	S 4	S 5
0.1	0(0.00%)	1(0.24%)	0(0.00%)	0(0.00%)	0(0.00%)
0.5	2(1.49%)	4(0.97%)	3(1.02%)	2(1.50%)	2(0.91%)
0.9	10(7.46%)	16(3.88%)	11(3.73%)	8(6.02%)	10(4.55%)

Source: Author

exposes the vulnerability of DSs. Moreover, our analysis indicates that the DS samples are more vulnerable to errors than to attacks.

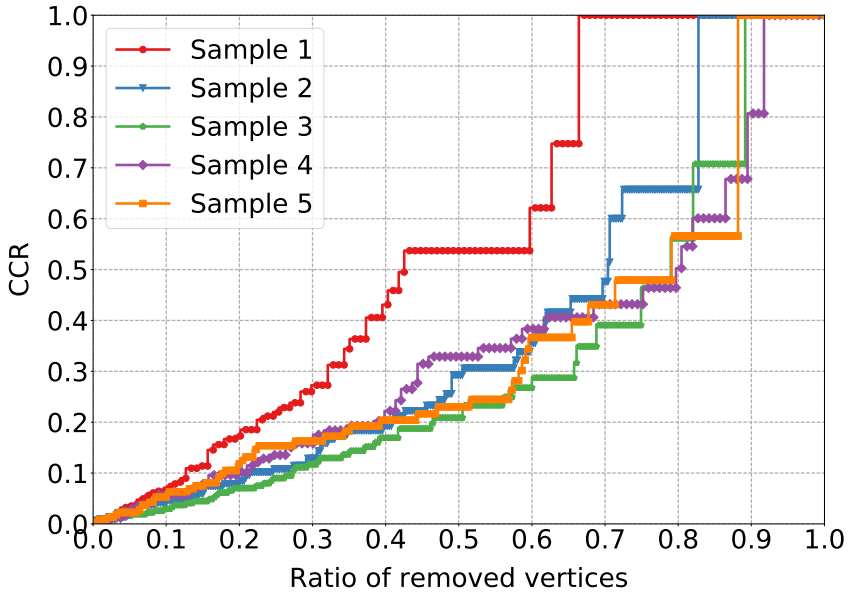
Table 24 – $V - index$ calculated for all the samples considering both metrics, LCC and SCC, and the errors scenario.

Errors	$V - index$				
	S 1	S 2	S 3	S 4	S 5
LCC	0,38	0,43	0,41	0,37	0,41
SCC	0,46	0,48	0,48	0,46	0,47

Source: Author

The use of SCC, which accounts the distribution source, together with CRR exposed a higher vulnerability than the usual analysis using the average impact calculated

Figure 41 – Cumulative Collapse Rate for errors impact obtained for the five samples of Table 17 using the metric *SCC*.



Source: Author

by the *LCC* metric. Moreover, consideration of the source connectivity will allow the examination of essential features of Distribution Networks, as the number of customers still receiving the goods, or services, and the amount of delivered goods, or services, after damaging events.

The results presented here for attacks and errors indicated that the Samples 2 and 3 are the most vulnerable to both. These Samples were also characterized by smalls lower bound and exponent for the fitted power law in the previous Section, see Figure 33. Such correlation should be better investigated in future research.

4.6 Vulnerability Analysis using Reliability Model

Here, the results obtained by using the method to perform vulnerability analysis by sampling from reliability models instead of using the hypothesis of equals failure probabilities are shown. The analysis was performed in the same five samples presented previously in Table 17 but assuming that both, vertices and edges are susceptible to errors. In Table 25, the amount of each type of element for the five samples is presented. The vertices and edges are divided into two groups, buses with and without load, and cables and switches. Besides the similarity due to topological radiality, each sample has a different proportion of vertices with load and switches. Such difference is related to variances in operational planning and needs, and also highlights the necessity to account the distribution networks heterogeneity. First, the results using the equal failure probabilities hypothesis is presented, and then the results using the reliability models during errors

sampling.

Table 25 – The amount of each component' type present in the DS samples. Buses with load are the vertices that have consumer units attached.

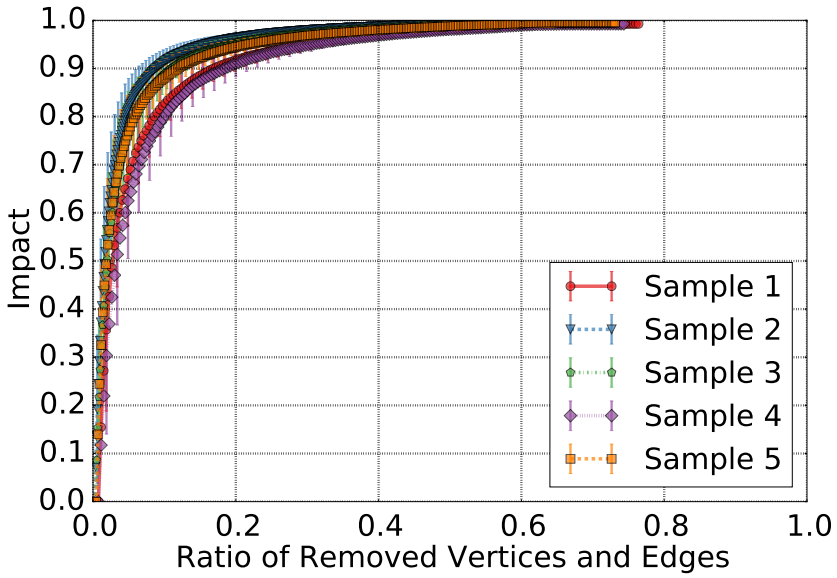
Sample	Vertices (Buses)		Edges	
	Load	Without Load	Cables	Switches
1	27	107	118	15
2	80	332	374	37
3	63	232	263	31
4	18	115	119	13
5	29	191	205	14

Source: Author

4.6.1 Equal Failure Probabilities

We performed the standard vulnerability analysis assuming that vertices and edges are susceptible to errors with equal probabilities. In Figure 42, the $\overline{I}(j)$ and $\sigma_I(j)$ due to errors on both, vertices and edges, are presented. The main difference with the result considering only vertices errors (see Section 4.5.2) is that the Samples cannot tolerate more than the removal of 80% of its vertices and edges. The Samples 1 and 4 still are the most robust, similar to the results for only vertices errors in the previous section.

Figure 42 – Impact due to vertices and edges errors using equal failure probabilities. The symbols mark the average values, and the vertical bars indicate the standard deviation. Similar to the result with only vertices errors, Sample 4 is the most robust, and Sample 2 is the least robust (see online version for colors).



Source: Author

In Table 26, a summary of the average impact values is presented. If the number of elements is considered instead of the ratio, the difference between only vertex and vertex and edges removals is low, the random removal of the same amount of elements causes a similar average impact for all Samples. The differences appear only for high numbers of removals, where the removal of vertices and edges require more removals to cause the same 0.9 average impact.

Table 26 – Summary of the vulnerability analysis considering average impacts ($\overline{I}(j)$) with equal failure probability for vertices and edges errors on the five samples.

$\overline{I}(j)$	**Number of removed elements (%)**				
	S 1	S 2	S 3	S 4	S 5
0.1	1(0.4%)	1(0.1%)	1(0.2%)	1(0.4%)	1(0.2%)
0.5	5(1.9%)	11(1.3%)	10(1.7%)	7(2.6%)	6(1.4%)
0.9	43(16.1%)	70(8.5%)	62(10.5%)	47(17.7%)	50(11.4%)

Source: Author

4.6.2 Failure Probabilities from Reliability Models

The methodology presented in Section 4.6.2 is dependable of the Reliability functions for each type of element present in the system to perform failures sampling. The Exponential Reliability function (Chapter 2.4) was adopted, and the chosen failure rates are given in Table 27. The values reflect that a bus with load is more susceptible to failures since it has more components in the same pole. The cables failure rate is proportional to their length, and switches are the most reliable element with lower failure rates.

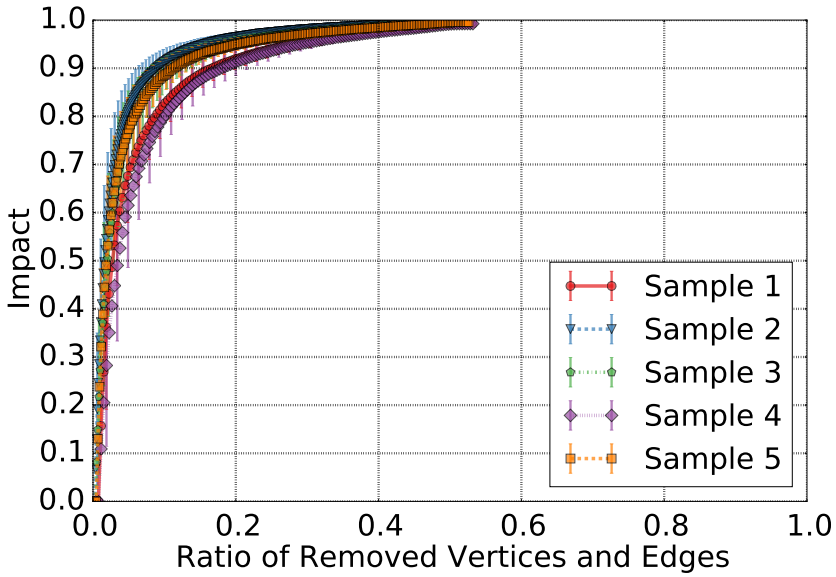
Table 27 – Failure rates adopted for each type of element present in the DS samples.

Element	**Failure Rate**
Load Bus (λ_{bl})	1.212 $failures/year$
Bus without load (λ_{bw})	0.606 $failures/year$
Cables (λ_c)	0.606 $failures/(year * mile)$
Switches (λ_s)	0.05 $failures/year$

Source: Author

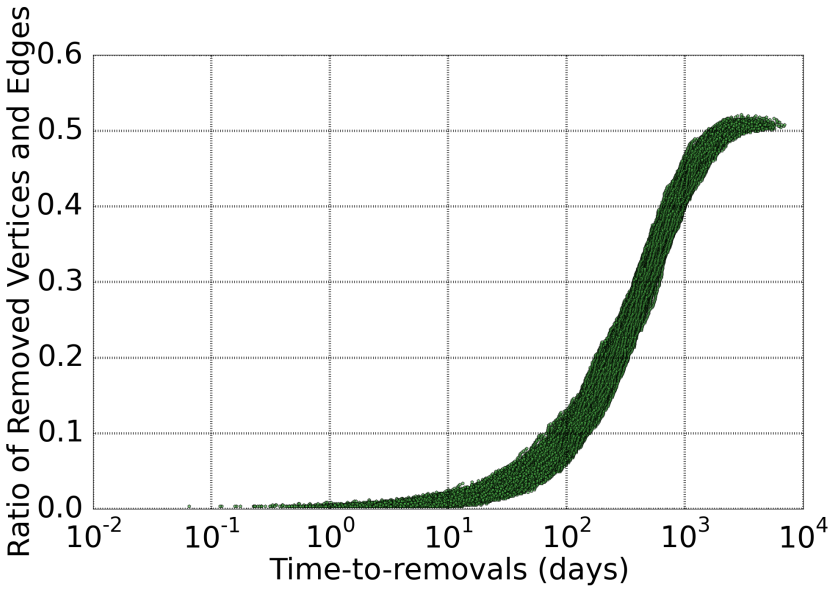
The values for average impacts - $\overline{I}(j)$ and standard deviation of impacts - $\sigma_I(j)$ assuming that both vertices and edges are susceptible to errors and following the λ values of Table 27 are presented in Figure 43. The shape of $\overline{I}(j)$ is very similar to the analyses presented before. Sample 4 still is the more robust, and Sample 2 the more vulnerable. The difference appears for the maximum ratio of removals tolerated, and this value is higher for the equal failure assumption than for the case where the Reliability function was used to sample the errors.

Figure 43 – Impact due to vertices and edges errors using the Reliability functions. The symbols mark the average values, and the vertical bars indicate the standard deviation. Similar to the previous results the Sample 4 is the most robust, and Sample 2 is the least robust. However, all the samples presented a lower maximum removal tolerance when the Reliability functions are considered.



Source: Author

Figure 44 – The relation between time-to-removals and % of removed parts obtained for Sample 3. The values presented are from all repetitions using the proposed framework.

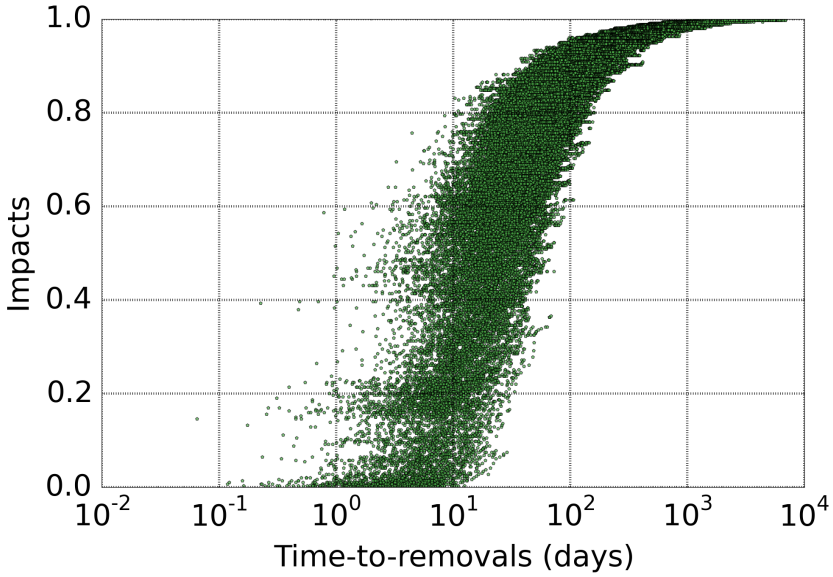


Source: Author

In addition to $\overline{I}(j)$ and $\sigma_I(j)$, this methodology also allows the consideration of the time variable. As an illustration, the Figure 44 presents the sampled times-to-removals

and the ratio of removed parts obtained for Sample 3. It allows the evaluation of the removals dynamic over the time domain. Another way to look at the data generated by the proposed framework is the relation between times-to-removals and the impact. The Figure 45 presents the values obtained in each simulation for Sample 3.

Figure 45 – The relation between time-to-removals and impacts obtained for Sample 3. The values presented are from all repetitions using the proposed Hierarchical Framework.



Source: Author

The results in Figure 44 and 45 highlight the dispersion of the simulated data in the time domain. The time variable is ranging from 10^{-2} to almost 10^{4} days. Although such variability, a specific time window can be investigated. The Table 28 presents the minimum, average, and maximum impact values when considering only the time window of a single day for all samples. It is important to note the impact variability, ranging from 0.002 to 0.586. Besides the similarity of the maximum and minimum values, the average value is very different between the samples. Sample 1 which was one of the most robust in the previous analysis, here present the higher average impact for the single day time window, 0.206.

All the five samples share similar intervals of impacts in the time window of a single day. Such a result leads to a slightly different perspective of the samples vulnerabilities when compared with the previous analysis of $\overline{I}(j)$, which indicates that Sample 2 is the most vulnerable, and Sample 4 the most robust to errors. When considering the events that happen in a single day time window, we can affirm that samples have a similar vulnerability, and Sample 1 becomes the most vulnerable, followed by Samples 4 and 5. This result is in agreement with the CCR obtained for errors in Section 4.5 Figure 41, which showed that these samples tend to suffer high impacts with few vertices errors.

Table 28 – Average, minimum and maximum impacts obtained considering a single day horizon.

Sample	Minimum I	Average I	Maximum I
1	0.007	0.206	0.500
2	0.002	0.094	0.492
3	0.003	0.084	0.586
4	0.007	0.158	0.436
5	0.005	0.125	0.431

Source: Author

When the time variable is considered during the vulnerability analysis by using reliability models, it allows reaching different interpretations. As an example, if just the number of removed elements is considered, the samples present a difference in the average impact caused by the same amount of random removals. However, when the time-to-removals are considered, and the same time window is used to compare samples vulnerability, the results become different since only the sampled removals in such a time window are considered. For instance, the Samples 2 and 3, which were the most vulnerable to errors in the static vulnerability analysis presented in the previous section, in the analysis with a single day horizon became the least vulnerable.

4.7 Vulnerability Analysis with Reconfiguration Dynamic

In this Section, the dynamic vulnerability analysis by considering the reconfiguration during the occurrence of failures presented in Section 3.4.3 is shown. Figure 46 illustrates a step of the reconfiguration process by the implemented multi-agent model using the Taiwan DS of Figure 6 in Section 3.1. The node 88, represented with a diamond shape, is the one damaged. The *topological agent* informs about the damage to the *supply agent* 10 that in turn informs the *switch agents* connected to node 88 to isolate it by becoming open. The *supply agent* informs the other *switch agents* that the nodes 89, 90, 91, 92 and 93 have become unserved. To transfer that load to another feeder, the *switch agent* between nodes 91 and 90 was opened, reducing the load transferred to the *supply agent* 2 by the *switch agent* between nodes 30 and 93. The *switch agent* 90-91 opens to allow the transfer of a load that respects the *supply agent* 2 load tolerance. In this example, the feeders' tolerance was set to 30 %.

For a better understanding of the effects of reconfiguration dynamics on the vulnerability of the used DS, its vulnerability without considering the reconfiguration is evaluated. The result of this analysis is presented in Figure 47 as the average and standard deviation of the impact versus the ratio of the removed nodes, such values were obtained from 100 trials and using the power delivered as the performance metric. The average impact due to faults and without reconfiguration causes an impact of around 40% for

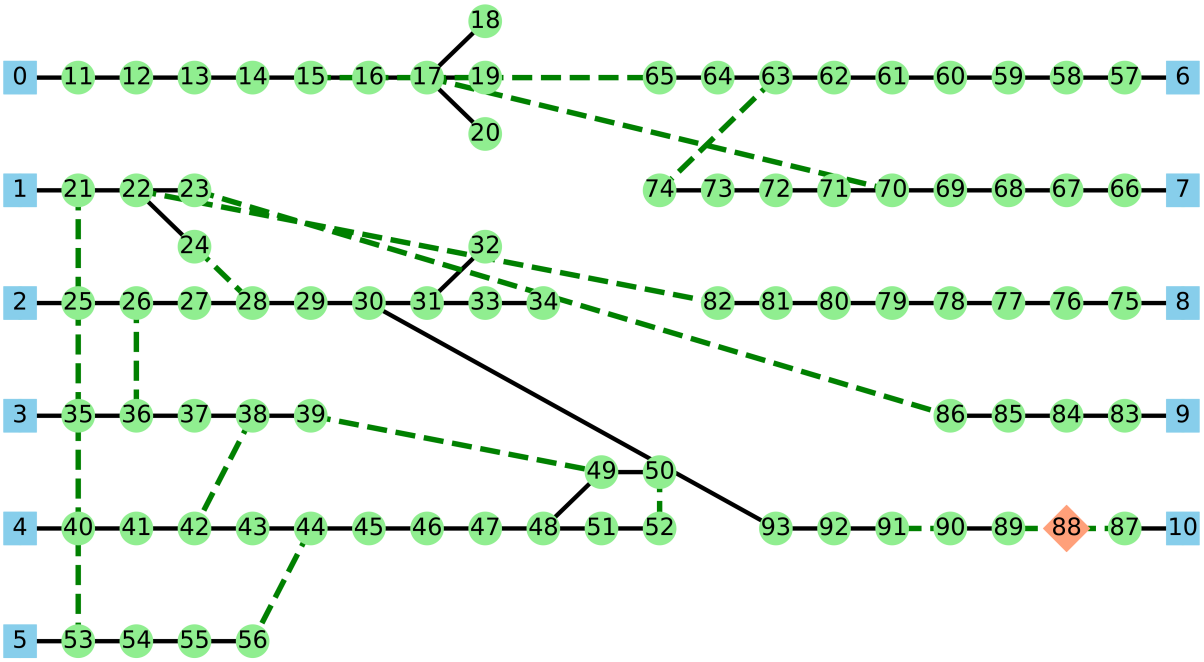


Figure 46 – Example of a time step in the multi-agent model during the simulation of errors. The diamond is the damaged node, and the unserved nodes were separated (switch 90-91 open) to allow a load transfer respecting the maximum capacity of feeder 2.

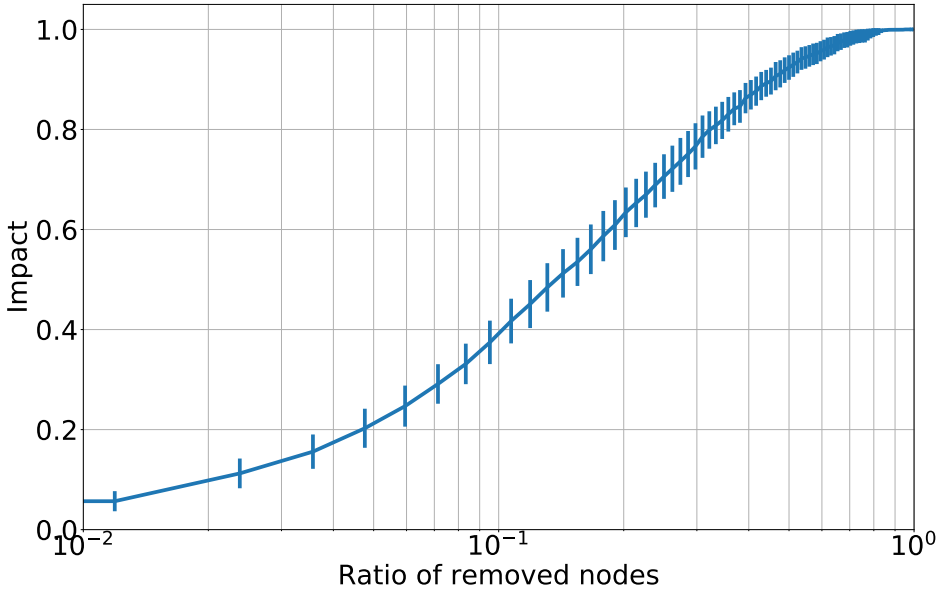
the removal of only 10% of its nodes, decreasing the power delivered to 17.000 kW. With removal of 20% of nodes, the impact is of 60%, only 11000 kW, and with the removal of 50%. of its vertices, the impact is around 90%, indicating delivery of only 2800 kW.

Figure 48 presents the average impact of different values of tolerance: 5%, 10%, 50%, and 100%, respectively. The values were obtained with 100 trials and using the power delivered as a performance metric. We also executed the simulations with higher values of tolerance, though the obtained values are all similar to the result presented for the 100% of tolerance case, indicating that higher tolerances do not necessarily provide better results, a consequence of the fixed number of switches as backup connections.

The results show that, as tolerance increases, the average impact decreases. For the tolerances of 50% and 100%, the impact for 10% of removed nodes is around 20%, that is, half the impact without reconfiguration. For the 20% of removals, the impact for all the values of tolerance is still lower than the case without reconfiguration, and in the case with 100% of tolerance, the impact is around 40%. Such robustness enhancement was expected since the reconfiguration dynamics simulated here aims at improving the system response to damaging events.

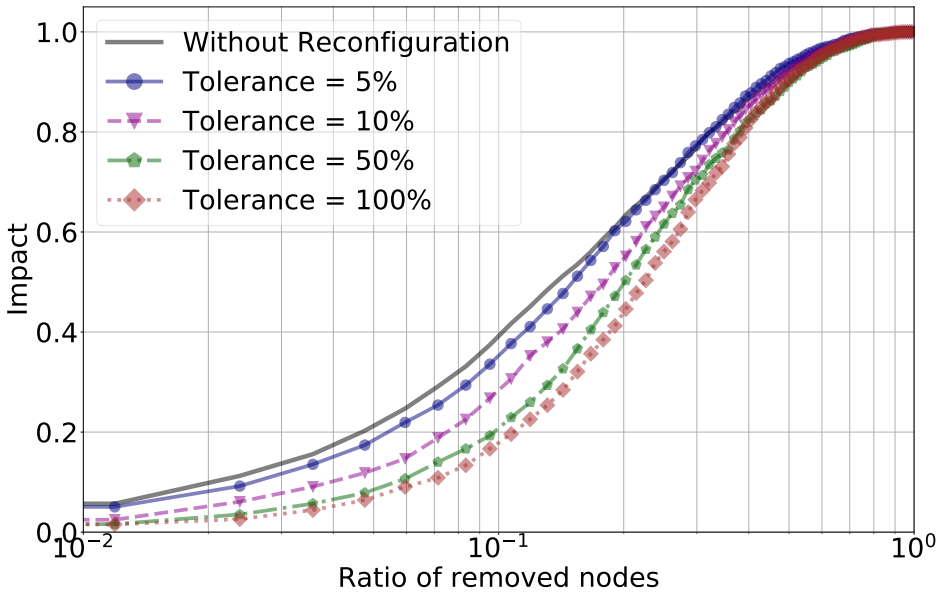
The values of tolerance also affected the running time of the simulations. In Figure 49, the average and standard deviation of a complete simulation running time, i.e., random removal of all susceptible nodes versus varying values of tolerance is shown.

Figure 47 – Impact average and standard deviation for the used power distribution system under errors without considering the reconfiguration dynamics.



Source: Author

Figure 48 – Impact average under faults for the used power distribution system under the reconfiguration dynamics with varying values of tolerance.

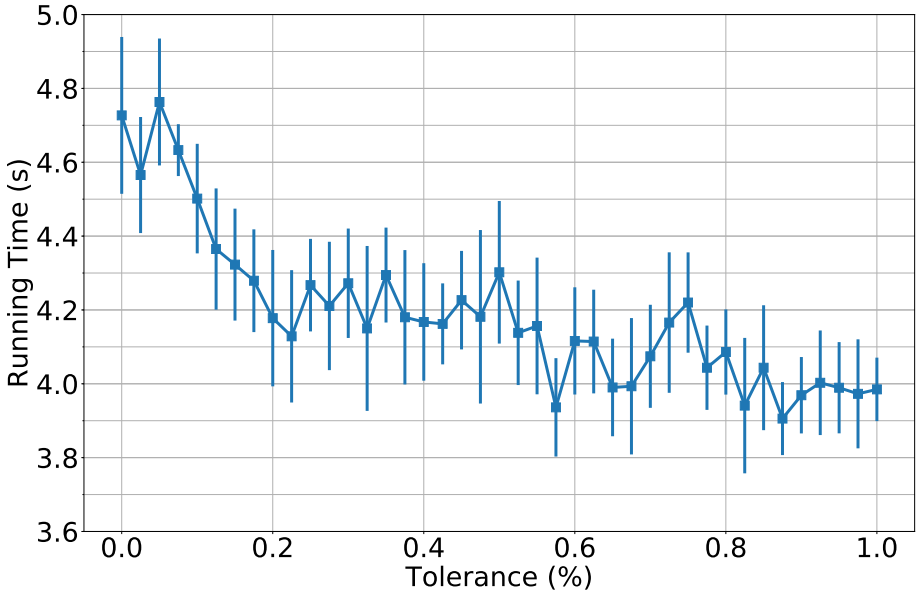


Source: Author

These values were obtained in a personal notebook: Intel Core i7-4500 (Intel Corporation, USA) CPU at 1.80GHz, 8 GB RAM and Ubuntu 17.04 operating system (Canonical Ltd., UK). For small values of tolerance, the running time of a complete simulation of faults is

around 4.7 s. As the tolerance value increases, the running time decreases. Such behaviour is related to the difficulty of agents to solve the reconfiguration problem when the system is functioning near to its load limits. For higher values of tolerance, the reconfiguration problem is solved more rapidly.

Figure 49 – Average running time of a single trial calculated from the 100 repetitions of different values of tolerance.



Source: Author

The observed impacts under the reconfiguration dynamic are directly related to the assumed tolerances, and the higher the tolerance, higher is the robustness enhancement compared with the system without reconfiguration. The observed values seem to be lower bounded by the fixed amount of switches among the distribution networks, which indicates that the number of switches to transfer load among distribution networks is a key aspect in the context of system reconfiguration during contingencies. Such robustness enhancement was expected since the capability of transferring undamaged nodes among power distribution networks is related to mitigating failures consequences in such systems.

4.8 Scenario-Based Probabilistic Resilience Assessment

The MCS to estimate resilience under different scenarios, presented in Section 3.5, were executed on each of the 81 distribution networks that composes the Brazilian DS. The networks resilience was estimated using two perspectives, one reflecting the structural resilience, by quantifying performance using the LCC metric, and the other measures the service resilience, with performance quantified as the power delivered. The simulation used the failure model with the wind gust speed (wg) and the number of atmospheric

discharges (nt) as covariates of the failure rate, presented in Section 4.2, and the repair model for typical equipment failures and with atmospheric causes, presented in Section 4.3. The following weather scenarios were considered

1. Scenario 1: Without weather adversities ($nt = wg = 0$);
2. Scenario 2: Adverse weather ($nt = 3000, wg = 50$);
3. Scenario 3: Extreme weather scenario ($nt = 5500, wg = 80$).

Those values were chosen considering historical information about such variables.

Such weather variables have a multiplicative effect on the nominal failure rate (λ_0) of the system elements, given by:

$$\lambda(nt, wg) = \lambda_0 exp(0.0011nt + 0.0275wg), \tag{4.2}$$

An advantage of using a parametric failure model is the capability of distinguishing between the different types of elements present in such networks. It was performed by specifying the failure rates by type of element, buses without loads, buses with loads, distribution feeders, cables, and switches. The adopted values of nominal failure rates for such types of elements follow (CHOWDHURY; KOVAL, 2011) and are shown in Table 29.

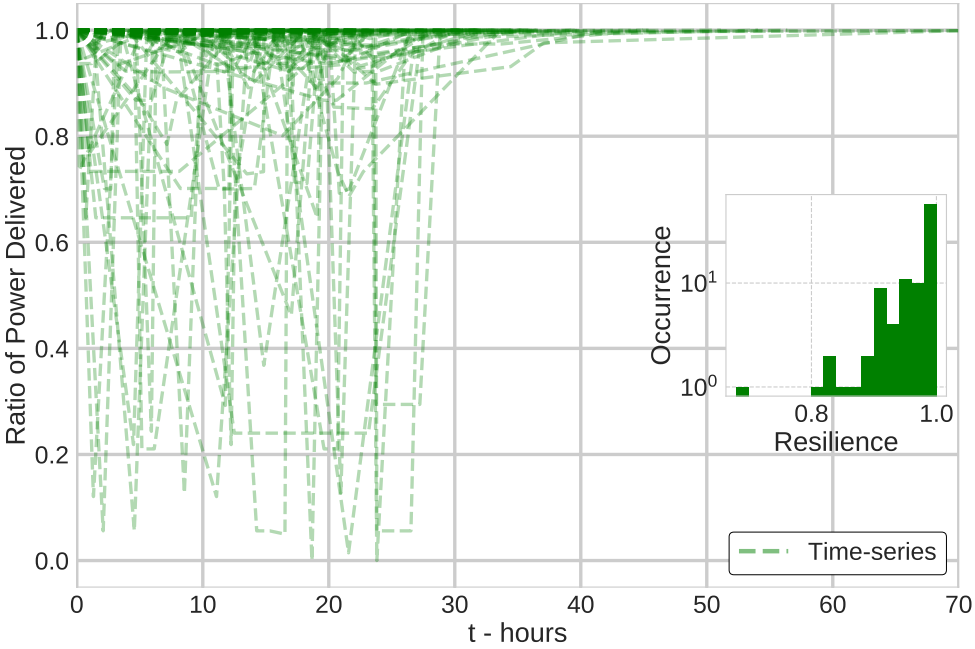
Table 29 – Failure rates adopted for each type of element present in the distribution networks.

Element	**Failure Rate**
Bus with load (λ_{bl})	0.012 $failures/year$
Bus without load (λ_{bw})	0.006 $failures/year$
Cables (λ_c)	0.009 $failures/(year * km)$
Switches (λ_s)	0.001 $failures/year$

Source: Adapted from (CHOWDHURY; KOVAL, 2011)

The simulation was set up with $N = 500$ and assuming weather scenario duration as $T = 24$ hours, reflecting the occurrence of a single day with adverse weather condition. All the simulations resulted in small coefficients of variation ($CV \leq 0.029$). The synthetic time-series generated by the MCS were used to calculate the $Я(T)$ using Equation (2.1), presented in Section 2.1. As an illustration of the MCS output, the Figure 50 presents 100 time-series obtained for a distribution network assuming the Scenario 2 together with a histogram of the calculated resilience values for service resilience. The time-series represent state changes during instants higher than $T = 24$ hours because the repairs can happen in t values higher than T. It is possible to observe that the simulations can reproduce the expected behavior, i.e., the system becomes damaged, and after some interval, the

Figure 50 – Hundred time-series representing the dynamic service performance of a power distribution network under the scenario 2. The time-series shows the performance behavior due to failures and repairs. The histogram within the figure represent the observed resilience figures.



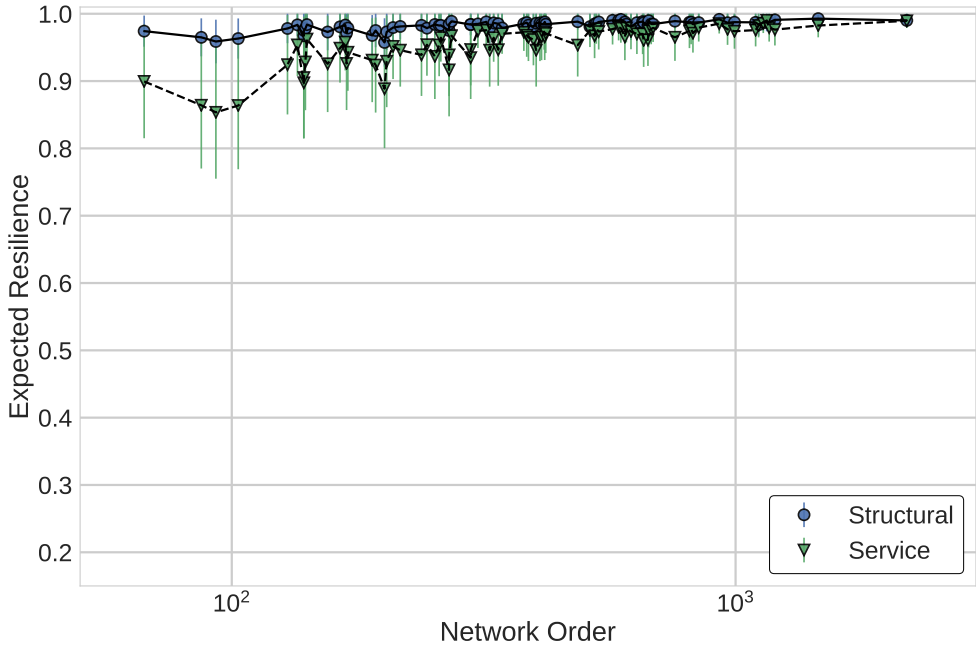
Source: Author

damaged elements are recovered. The histogram reflects the diversity of sampled resilience values.

Using the simulated performance time-series, the expected values of $\mathit{Я}(T)$ under the first scenario, i.e., without weather events, were calculated for all networks and they are presented in Figure 51, considering both resilience perspectives, structural and service. It shows that for a day without weather adversities all the networks presented high resilience values, as expected in an ordinary day for such type of system. The structural resilience is higher than service resilience in most of the networks, besides that the networks with lower Order seem to present smaller resilience values for both perspectives. In some cases, both metrics resulted in very similar values. The structural resilience ranges from 0.957 to 0.992, and service resilience from 0.853 to 0.991.

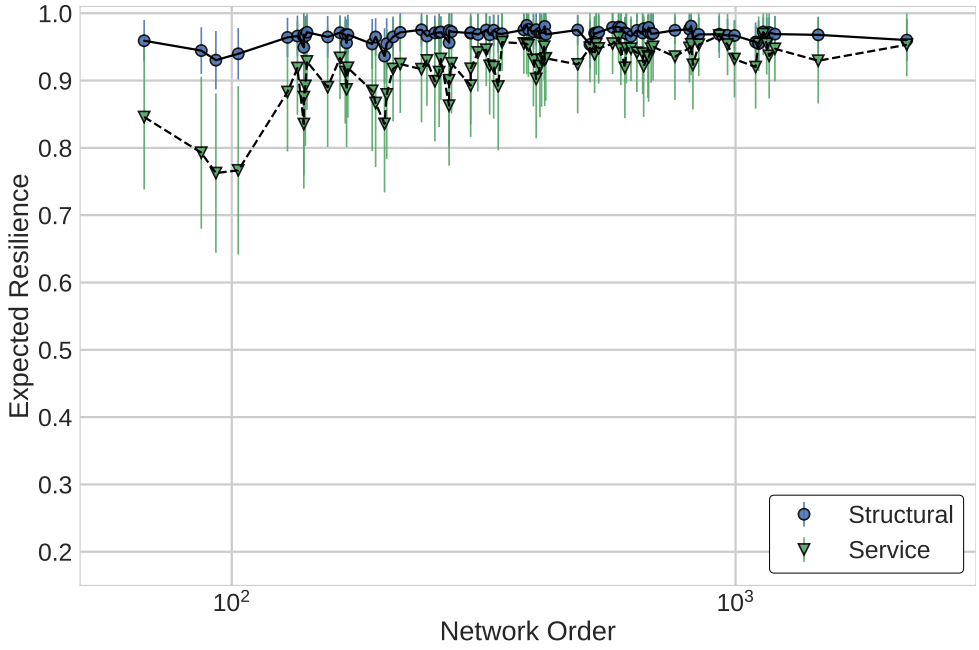
In Figure 52, the obtained expected values with their respective standard deviation of the networks resilience under the scenario 2, which is a day with severe weather scenario, are presented. All the networks presented a lower resilience if compared with the scenario 1 results, for both performance metrics, and similar to the scenario 1 results, the service resilience is equal or lower than the structural one for all the distribution networks. In such scenario, the structural resilience ranges from 0.931 to 0.982, while the service resilience from 0.763 to 0.968. The networks with low Order presented a propensity to have a smaller service resilience.

Figure 51 – Expected values and standard deviation of the power distribution networks under the Scenario 1, without weather adversity.



Source: Author

Figure 52 – Expected values and standard deviation of the power distribution networks under the Scenario 2, with an adverse weather scenario.

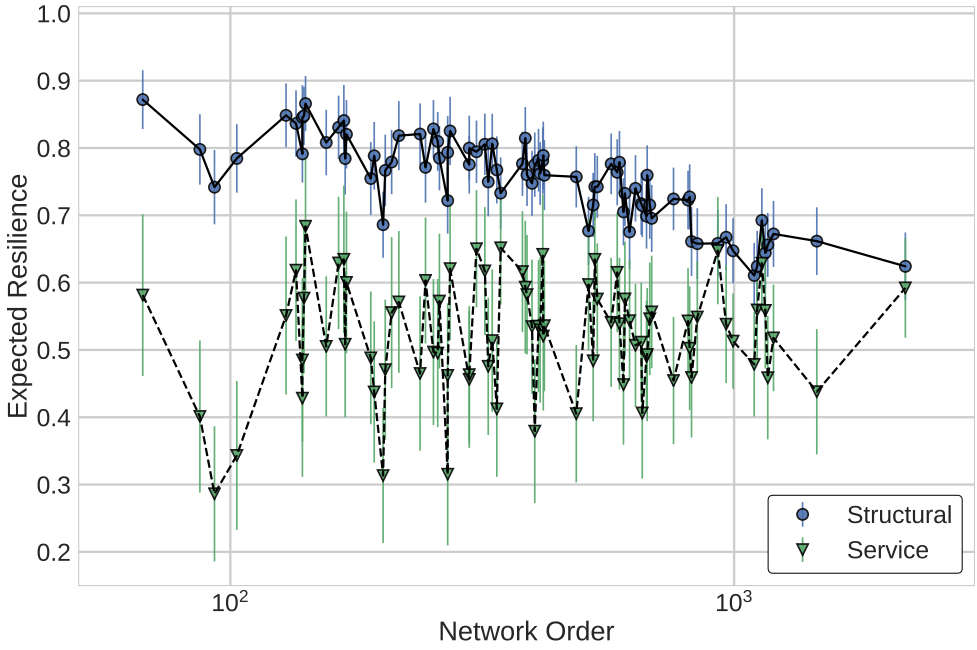


Source: Author

Figure 53 shows the results for the third scenario, where an extreme weather condition was considered. All the networks led to a lower expected resilience for both performance metrics. In such extreme scenario, we can note that structural resilience

appears to be linearly related to the networks Order, on the other hand, the service resilience seems not related to the network orders. The structural resilience ranges from 0.611 to 0.872, and service resilience from 0.286 to 0.684, indicating that while the networks can handle they connectivity, the delivery of electricity is very affected by such weather conditions. Another point is the standard deviation of the estimated service resilience, which is higher than the structural resilience in all scenarios.

Figure 53 – Expected values and standard deviation of the power distribution networks under the Scenario 3, with and extreme weather scenario.



Source: Author

Following these results, we performed an investigation of independence among the networks' features (presented in Figures 28 and 29, Section 4.4) and their expected resilience considering the values from scenario 3, which reflects an extreme weather condition. In Table 30, the absolute values of both correlations among the networks features and the expected structural resilience are presented. The displayed features are the four ones with the higher absolute partial correlation. An important point is the differences among the correlation and the partial correlation. For both average degrees (unweighted and weighted) the partial correlation is higher than the correlation. The p-values of the partial correlations reflect the significance of the relationship between the variables and serve as an indication of dependence.

Similarly, in Table 31, the correlations for networks expected service resilience is shown. Again, the values presented refer to the four features with the highest absolute partial correlation. The only feature that resulted in a lower partial correlation is $\overline{k}^W$, all the other features presented higher partial correlation than the Pearson correlation, and

Table 30 – Absolute values of correlation and partial correlation together with their p-values among the features and the structural resilience obtained for scenario 3.

Feature	**Correlation (p-value)**	**Partial Correlation (p-value)**
$\overline{k}$	0.665 (1.334e-11)	0.959 (4.759e-45)
L	0.938 (5.567e-38)	0.888 (2.365e-28)
N	0.818 (1.233e-20)	0.743 (2.084e-15)
$\overline{k}^W$	0.146 (0.195)	0.459 (1.646e-5)

Source: Author

the p-values of the partial correlation are all significant. Interestingly, the most correlated features are the average degree and assortativity, both unweighted and weighted values. These results presented in Tables 30 and 31 can be considered as evidence of associations between some topological and hybrid features of the assessed networks and their respective expected resilience on the extreme weather scenario considered. As mentioned previously, such correlations are indicative that there may be dependence.

Table 31 – Absolute values of correlation and partial correlation together with their p-values among the features and the service resilience for scenario 3.

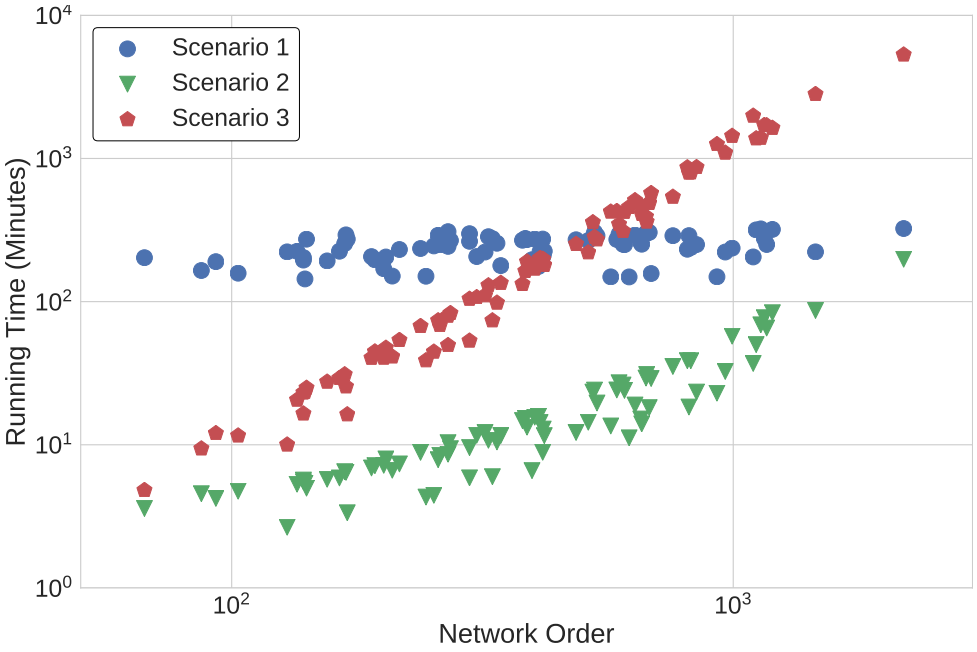
Feature	**Correlation (p-value)**	**Partial Correlation (p-value)**
$\overline{k}^W$	0.657 (2.661e-11)	0.550 (1.018e-7)
$\overline{k}$	0.154 (0.169)	0.528 (4.179e-7)
r^W	0.212 (0.057)	0.369 (6.902e-4)
r	0.081 (0.474)	0.250 (0.024)

Source: Author

In addition to the expected resilience, the weather scenario, and the power distribution networks size also affect the simulations running time. In Figure 54, the total running time of the simulation for each distribution network at each scenario is shown. For scenario 1, all the networks resulted in similar running time, and the ones with the lower order, resulted in higher running time for such scenario than for the others one. Such behavior is related to the low probability of observing the failures on a 24 hours time interval, requiring more sampling until the observation of a failure on the defined time interval. For scenarios 2 and 3, the running times are proportional to the networks' order. The increase in running time from scenario 2 to scenario 3 is related to the observation of more failures in the 24 hours time interval. The total running time in the used Beowulf cluster was 12 hours and 50 minutes, and the task parallelism was performed by sending each simulation (network, scenario and N) per processing engine.

The observed resilience loss of the distribution networks under the extreme weather scenario is in agreement with historical natural disaster data, as presented in (KWASINSKI,

Figure 54 – Log-log observed total simulation time for each distribution network at each scenario with $N = 500$.



Source: Author

2016). We observed that some features of the distribution networks are related to the structural and service resilience. For structural resilience, the features with higher linear correlation are all related to the topology of the networks, as the average degree and order of the networks. The weighted average degree presented only a higher partial correlation, which indicates an absence of linear association with the structural resilience. In the case of service resilience, the weighted average degree is the only features that are strongly associated by both correlations, Pearson and partial, indicating a high relation between the average power flowing over the networks with its service resilience. The other features presented only significant partial correlation: average degree, weighted and unweighted assortativity.

Both assortativities are related to the presence of lateral branches on such networks. In the case of lateral branches abundance, the probability of a network losing an element attending a high demand, and present in the main trunk, is reduced by the presence of other elements in the lateral branches which meets a lower demand. Such findings indicate that some topological and power flow features have a direct influence on the resilience of power distribution networks, and a better understanding of the extreme weather effect on the resilience of DSs can be achieved by investigating the association evidence highlighted in this study.

4.9 Doctoral Program

In This section, the results related to the doctoral program are presented. First, the ones related to the presented Thesis, followed by the collaborations unrelated to this research aim.

4.9.1 Related with Doctoral Research

Journals

- **Published**: Michel Bessani, Rodrigo Z. Fanucchi, Alexandre C. B. Delbem, Carlos D. Maciel: *Impact of Operators' Performance in the Reliability of Cyber-Physical Power Distribution Systems.* **IET Generation Transmission & Distribution**. v. 10, n. 11, p. 2640-2646, 2016.
- **Minor Review**: Michel Bessani, Júlio A.D. Massignan, Rodrigo Z. Fanucchi, Marcos H.M. Camillo, João B. London Jr., Alexandre C. B. Delbem and Carlos D. Maciel: *Probabilistic Assessment of Power Distribution Systems Resilience under Extreme Weather.* **IEEE Systems Journal**

Conferences

- **Published**: Michel Bessani, Rodrigo Z. Fanucchi, Jorge A. Achcar, Carlos D. Maciel: *Statistical Analysis and Modeling of Repair Data from a Brazilian Power Distribution System.* **Proceedings of 17th International Conference on Harmonics and Quality of Power - ICHQP 2016. IEEE.**
- **Published**: Rodrigo Z. Fanucchi, Michel Bessani, Marcos H.M. Camillo, Carlos D. Maciel: *Failure Rate Prediction Under Adverse Weather Conditions in an Electric Distribution System Using Negative Binomial Regression.* **Proceedings of 17th International Conference on Harmonics and Quality of Power - ICHQP 2016. IEEE.**
- **Published**: Michel Bessani, Rodrigo Z. Fanucchi, Júlio A.D. Massignan, Marcos H.M. Camillo, João B. London Jr. and Carlos Maciel. *A Hierarchical Framework for Complex Networks Robustness Analysis to Errors.* **11$^{\text{th}}$ Annual IEEE International Systems Conference - IEEE SysCon 2017** - *Best Student Paper - Honorable Mention.*
- **Accepted**: Michel Bessani, Rafael R.M. Ribeiro, Giuliano A. Pagani, Marco Aiello and Carlos D. Maciel: *Robustness of Reconfigurable Complex Systems by a Multi-Agent Simulation: Application on Power Distribution Systems.* **12$^{\text{th}}$ Annual IEEE International Systems Conference - IEEE SysCon 2018**.

4.9.2 Collaborations

Journals

- **Published**: Julio A. D. Massignan, João B. A. London Jr., Michel Bessani, Carlos D. Maciel, Alexandre C. B. Delbem, Marcos H. M. Camillo, Telma W. L. Soares: *In-Field Validation of a Real Time Monitoring Tool for Distribution Feeders*. **IEEE Transactions on Power Delivery**. (2017) DOI:10.1109/TPWRD.2017.2785044
- **Published**: Giovana Y. Nakashima, Theresa H. Nakagawa, Ana F. dos Santos, Fábio V. Serrão, Michel Bessani, Carlos D. Maciel: *Identification of directed interactions in kinematic data during running*. **Frontiers in bioengineering and biotechnology**. (2017) DOI:10.3389/fbioe.2017.00067
- **Published**: Araujo, R. B., Ribeiro, E. B., Campanari, D. D., Ramos, C. F., Bessani, M., Carlos D. Maciel, Vale, F. A. C.: *Components of metabolic syndrome, life habits and cognitive disorder in the elderly*. **Dementia & Neuropsychologia**, (2017).
- **Major Review**: Tadeu J. Gross, Renata B. Araújo, Francisco A.C. Vale, Michel Bessani and Carlos D. Maciel: *Dependence between Cognitive Impairment and Metabolic Syndrome Applied to a Brazilian Elderly Dataset*. **Artificial Intelligence in Medicine**

Conferences

- **Published**: M. H. M. Camillo; Marcel E. V. Romero; Rodrigo Z. Fanucchi; Telma W. de Lima; Bessani, M.; Carlos Dias Maciel; Julio A. D. Massignan; London Junior, J. B. A.; Anderson S. Soares. *Otimização do Processo de Restabelecimento de Energia em Sistemas de Distribuição de Larga Escala.* **VIII Congresso de Inovação Tecnológica em Energia Elétrica – CITENEL, 2015**
- **Published**: Darwin Junior, W.; Bessani, M.; M. H. M. Camillo; Tavares, D. M.; Maciel, C. D.. *Agrupamento de Relatórios Textuais de Falhas em Sistemas de Distribuição de Energia utilizando Divergência K-L.*. **XII Simpósio Brasileiro de Automação Inteligente (SBAI), 2015**.
- **Published**: Lima, D.; Bessani, M.; Newland, P.; Maciel, C. *Modeling of an Insect Proprioceptor System based on Different Neuron Response Times*. **9th International Joint Conference on Biomedical Engineering Systems and Technologies (BIOSTEC 2016), 2016**.
- **Published**: Camillo, Marcos H. M.; Fanucchi, Rodrigo Z.; Romero, Marcel E. V.; De Lima, Telma W.; Marques, Leandro T.; Massignan, Julio A. D.; Maciel, Carlos D.; Soares, Anderson S.; Delbem, A. B. C.; Bessani, Michel; London, Joao B. A. *Determination of switching sequence of Service Restoration in Distribution*

Systems: Application and analysis on a real and large-scale radial system. **IEEE/PES Transmission and Distribution Conference and Exposition (T&D), 2016**.

- **Published**: Rodrigo Z. Fanucchi; M. H. M. Camillo; Anderson S. Soares; Telma W. de Lima; London Junior, J. B. A.; A.C.B. Delbem; M. Bessani; Carlos Dias Maciel. *Inspeção de Alimentadores Utilizando Equipes de Campo com Recomposição Parcial de Trechos Entre Chaves Operáveis com Carga.* **Simpósio Brasileiro de Sistemas Elétricos (SBSE), 2016**.
- **Published**: Julio A. D. Massignan, Gustavo M. Hebling, Leandro T. Marques, Michel Bessani, Marcos H.M. Camillo, Carlos D. Maciel and João B. A. London Jr. *Modeling Issues on Load Flow Calculation for Meshed Distribution Systems.* **12$^{\text{th}}$ IEEE Power and Energy Society PowerTech Conference - PowerTech 2017**.
- **Published**: L.D. Neto; Bessani, M.; Rodrigo Z. Fanucchi; T. J. Gross; C.D. Maciel: *Otimização por exame de partículas aplicado ao roteamento de equipes de manutenção da rede elétrica.* **XIII Simpósio Brasileiro de Automação Inteligente - SBAI 2017**.
- **Published**: T. J. Gross; Bessani, M.; Dourado, J.R.; Lima, D.; C.D. Maciel . *Evaluation of Long-Term Feature Parameters for Noise-Tolerant Speaker Identification.* **XIII Simpósio Brasileiro de Automação Inteligente - SBAI 2017.**
- **Published**: M. H. M. Camillo; Rodrigo Z. Fanucchi; Telma W. de Lima; Anderson S. Soares; Bessani, M.; C.D. Maciel; Julio A. D. Massignan; Leandro T. Marques; A.C.B. Delbem; J. B. A. London Júnior. *Detecção, Isolamento, Inspeção e Restabelecimento de Energia em Sistemas de Distribuição de Distribuição em Larga Escala.* **IX Congresso de Inovação Tecnológica em Energia Elétrica – CITENEL, 2017.**

5 CONCLUSION

This doctoral research aimed to develop approaches to perform vulnerability and resilience assessment for power distribution systems capable of dealing with dynamic features, as the system reconfiguration during contingencies for vulnerability, and evaluate the effects of extreme weather scenarios on such systems resilience. A core tool of this research was the use of a simulation approach, which enabled the consideration of such features in both perspectives. The methods were applied in DSs from literature and also in a Brazilian DS.

The first result presented in Section 4.1 showed the capability of accounting different dynamics by applying Monte Carlo simulation, which was performed to evaluate the impact of operators' response time in DSs reliability indices considering the context of cyber-physical power distribution systems or smart distribution grids. These results reinforced the effectiveness of using the Monte Carlo simulation to address the effect of different dynamics in the context of reliability, and also for other analysis that also focuses on failures dynamics on complex systems. This result is directly related with the current changes, related to the integration with ICT, that DSs are facing to increase the quality of service delivered to final customers, highlighting the need of considering different factors that affect the proper functioning of such systems.

The following ones were the analysis of historical data describing interruptions suffered by the Brazilian DS. From such data set, two distinct models were obtained, the former describes how the weather variables (atmospheric discharge occurrence and daily maximum wind gust speed) affect such DS failure rate - Section 4.2. The latter is related to the time-to-repair due to different causes, urban, environmental, operational, and atmospheric, were the atmospheric causes resulted in the higher expected time-to-repair - Section 4.3. Those models are fundamental to characterize how climatic factors are related to the dynamics of failures and repairs of the Brazilian DS, and also to observe the specific effects of other external agents and urban and environmental ones.

Such information is supportive of the resources management in the maintenance planning of such systems, as the control of vegetation and readiness of maintenance crews to face days with adverse atmospheric events. Moreover, this also showed that a variety of factors, which surround and interact with these systems, can generate high variation on these essential parameters. As the failure rate model with the wind gust speed and atmospheric discharges as covariates, and the repair time that can be significantly increased depending on the nature of the failure cause. All this is directly related to the quality of service delivered to final consumers.

These results are related with the application of the simulation approach to deal with different dynamics, and also the analysis and modeling of external effects on the failure and repair dynamics from historical data describing how the failures are handled by the used Brazilian DS. In this sense, they are necessary results to achieve the aim of this study of deal with different dynamics during the assessment of vulnerability and resilience. Another necessary analysis was the characterization of the networks that form the Brazilian DS, which will provide features that were used to interpret the other results of this thesis better. The characterization presented in Section 4.4 brings a general view of how the distribution networks forming the Brazilian DS are different from each other. This is related to the different operational needs and spatial constraints related to such spatial distribution networks, and also highlights the high heterogeneity regarding their topological, spatial and electrical features.

Before the proper methodology to account variable failure rate and reconfiguration dynamics during vulnerability analysis, a conventional static vulnerability analysis was performed in five distribution networks from the Brazilian DS. These results were presented in Section 4.5 and some methods presented in this Thesis for support vulnerability analysis were applied in this static analysis. Also, the vulnerability of the five distribution networks was compared with the vulnerability results for the Dutch distribution networks. It was possible to conclude that the used Brazilian distribution networks are more vulnerable than the Dutch ones. This finding must be better explored in future studies.

The first result directly related with the aim of this doctoral research was presented in Section 4.6, where the results of using failure reliability models to sample errors are compared with the premise of equal failure probabilities generally used to perform vulnerability analysis of PS, and also of a variety of systems. The use of the failure reliability models allowed the consideration of the system heterogeneity, which is reflected by the use of specific failures rates for each type of element that composes the distribution networks used. This analysis was performed using the same five distribution networks used to do the static vulnerability analysis. The results here showed that the consideration of the type of elements that composes a system resulted in a higher vulnerability than the consideration of equal failure probabilities for all elements' type.

Such approach of using reliability models to sample errors also allowed the observation of the time variable during the vulnerability analysis, which enables different analysis, as the vulnerability in a specific time window, in our results we presented this analysis for a single day time window, but this can be performed for other time windows. Moreover, the use of reliability models opens the possibility of considering external factors that change the failure rates of the system elements, as the failure model obtained in the Section 4.2. Such possibility is in line with the current needs for reducing the current vulnerability of DSs to handle the new and old threats that they are exposed. Such approach can be

expanded to handle different threats in future research, as cyber and physical attacks.

Another result directly related to the research aim was the consideration of the reconfiguration dynamic, known as self-healing capability of smart grids, during the vulnerability analysis. This result was presented in Section 4.7 and such analysis were achieved by using a multi-agent model to emulate the operation of automatic switches after each element failure. These results were generated using the generally used premise of equal failure probabilities, but this not affects the findings regarding the influence of the reconfiguration in the vulnerability of DSs. The emulation showed that the higher the capability of load transfer among the interconnected distribution networks the higher would be the vulnerability reduction in the system-of-systems composed of the distribution networks connected by the switches, which are fixed back-up connections. However, the results showed that the robustness enhancement is limited by the number of such fixed back-up connections.

The main result presented in this Thesis was the one presented in Section 4.8, where the resilience of the 81 distribution networks that compose the Brazilian DS was assessed considering the dynamics of failure and repairs under different weather scenarios. The failure and repairs were modeled using the findings of the Sections 4.2 and 4.3, where a failure and repair models, respectively, were obtained from the historical data describing failures occurrences in the Brazilian DS. Such analysis showed that all the networks are remarkably resilient in the scenario without weather adversities, reflecting the readiness of such system to deal with everyday damaging events. The networks also resulted in high values of the estimated resilience in the scenario with weather adversities.

However, in the scenario with an extreme weather condition, reflecting the occurrence of low-probability high-intensity atmospheric events, the networks showed to loss resilience, principally in the context of service resilience, related to the delivery of electricity to the final users. Such resilience loss was further investigated by considering the features describing the different distribution networks that compose the Brazilian DS, which was presented in Section 4.4. This investigation, which used Pearson and partial correlation, was done to see if exists evidence of dependence among the features and the low resilience in the extreme weather scenario. The findings were that some topological and electrical features are strongly correlated with the resilience loss, such features are related with the presence of lateral branches connected to a central trunk, which is responsible by significant quantities of power flow over the network.

Such results about the association evidence between resilience loss in the extreme weather scenario and the topological and electrical features must be further explored in future studies. This type of information is of great value for decision making during extreme weather events, allowing, for example, allocation of resources as an increased amount of field crews and strategic placement of such crews. The possibility to infer the

resilience loss using the investigated features seems to be a promising path do perform DSs resilience-based investment as expansion planning and optimization. This possibility is directly related to the long-term resilience, where is necessary the learn of resilience-related aspects, resulting in improvements and adaptations to face future high impact events. This long-term resilience gain is related to the manner that the system decision makers treat the system' safety management.

The presented models and methods, which enable the assessment of reliability, vulnerability and resilience considering the dynamics of failure, repair, reconfiguration, operator decision, and external factors, allowing the evaluation of how old and new threads can affect such essential aspects of DSs, fits with this doctoral research aim and specific objectives. The different dynamics aspects and external factors modeled and evaluated during the performed analysis showed up relevant to the vulnerability and resilience of DSs, and the results presented here improves the knowledge about how the operator decision making, reconfiguration capability, and extreme weather affects the reliability, vulnerability and resilience of DSs.

All the methods presented in this study can also be improved by accounting other features related with the current upgrades and challenges that DSs are experiencing, as the cultural changes related with smart features and renewable energy sources penetration, and the transformation of passive consumer units to active prosumers. Moreover, the use of the different methods (Reliability models, Monte Carlo Simulation, Complex Networks, Multi-Agent models) showed to be a favorable approach to obtain a holistic view of DSs resilience and vulnerability. This view is a consequence of different perspectives consideration, related to the system' uncertainties and complexities as functioning, topology, operation, and dynamic characteristics.

The challenges of performing vulnerability and resilience analysis of such heterogeneous and complex systems are also the reality of different types of systems, as biological and engineered ones, and all we presented and mentioned can be expanded to other systems. In the context of CIs, that are fundamental systems for our modern society, and are all evolving to even more complex systems, like transportation, communication, and water systems, the methodologies can be adapted to handle these different systems. Moreover, they also can be used to investigate the interdependence among CIs, as energy and water, among others. This will need to use generalist approaches or the combination of the specific models related to each field to allow the consideration of the functioning, operation, and dynamics related to each of the analyzed systems in the context of interdependence.

In addition to such assessment methods, another aspect is the approach used to model the data of the Brazilian DS failures and repairs events. Another aspects can be explored in future research, as time-series analysis, Bayesian data analysis, investigation of non-homogeneity during the occurrence of failures, and spatial relationships among

the failure and repair data. These data modeling techniques can be useful to treat data describing similar temporal processes for other systems. In this manner, we can list some future research directions based on what was done in this doctoral research. They are divided in data modeling and system simulation and assessment.

- Data modeling:
  - Time-series analysis and modeling;
  - Spatial statistical analysis and modeling;
  - Bayesian approaches for data analysis and modeling;
  - Investigation of non-homogeneity during the occurrence of failures.
- System simulation and assessment:
  - Develop models to account other dynamic features related to smart grid features, like energy storage, distributed generation, micro-grids, and prosumers;
  - Estimate the resilience under different scenarios by using a probabilistic model capable of handling the uncertainties related to the features and scenarios;
  - Explore the effects of rare-events by using specific sampling methodologies;
  - Perform a single resilience assessment by accounting all the distribution networks as a single System-of-Systems by using the Multi-Agent model to emulate system reconfiguration during the assessment;
  - Better investigation of the differences among the Brazilian DS and the Dutch DS;
  - Expand the presented approaches to deal with interdependent systems, as energy and water;
  - Expand the resilience assessment methodology to evaluate long-term resilience investments;
  - Study how resilience can be embedded in the planning of DSs and other engineered systems.

BIBLIOGRAPHY

AALEN, O.; BORGAN, O.; GJESSING, H. **Survival and event history analysis: a process point of view**. [S.l.]: Springer Science & Business Media, 2008.

ACHCAR, J. A.; CEPEDA-CUERVO, E.; RODRIGUES, E. R. Weibull and generalised exponential overdispersion models with an application to ozone air pollution. **Journal of Applied Statistics**, Taylor & Francis, v. 39, n. 9, p. 1953–1963, 2012.

AIELLO, M.; PAGANI, G. A. How energy distribution will change: An ict perspective. In: **Smart Grids from a Global Perspective**. [S.l.]: Springer, 2016. p. 11–25.

AKAIKE, H. A new look at the statistical model identification. **IEEE transactions on automatic control**, Ieee, v. 19, n. 6, p. 716–723, 1974.

AL-MUHAINI, M.; HEYDT, G. T. Evaluating future power distribution system reliability including distributed generation. **IEEE transactions on power delivery**, IEEE, v. 28, n. 4, p. 2264–2272, 2013.

_____. A novel method for evaluating future power distribution system reliability. **IEEE transactions on power systems**, IEEE, v. 28, n. 3, p. 3018–3027, 2013.

ALBERT, R.; ALBERT, I.; NAKARADO, G. L. Structural vulnerability of the north american power grid. **Physical review E**, APS, v. 69, n. 2, p. 025103, 2004.

ALBERT, R.; JEONG, H.; BARABÁSI, A.-L. Error and attack tolerance of complex networks. **nature**, Nature Publishing Group, v. 406, n. 6794, p. 378–382, 2000.

ALDERSON, D. L. et al. Sometimes there is no most-vital arc: assessing and improving the operational resilience of systems. **Military Operations Research**, MORS, v. 18, n. 1, p. 21–37, 2013.

ALSTOTT, J.; BULLMORE, E.; PLENZ, D. powerlaw: a python package for analysis of heavy-tailed distributions. **PloS one**, Public Library of Science, v. 9, n. 1, p. e85777, 2014.

AMARAL, L. A.; OTTINO, J. M. Complex networks. **The European Physical Journal B-Condensed Matter and Complex Systems**, Springer, v. 38, n. 2, p. 147–162, 2004.

AMARAL, L. A. N. et al. Classes of small-world networks. **Proceedings of the national academy of sciences**, National Acad Sciences, v. 97, n. 21, p. 11149–11152, 2000.

AMIN, M. Energy infrastructure defense systems. **Proceedings of the IEEE**, IEEE, v. 93, n. 5, p. 861–875, 2005.

AMIN, S. M. Securing the electricity grid. **The Bridge, quarterly publication of the US National Academy of Engineering**, v. 40, n. 1, p. 13–20, 2010.

ANDERSSON, G. et al. Causes of the 2003 major grid blackouts in north america and europe, and recommended means to improve system dynamic performance. **IEEE Transactions on Power Systems**, IEEE, v. 20, n. 4, p. 1922–1928, 2005.

ANEEL, Brazilian Electricity Regulatory Agency. **Indicadores de Qualidade**. 2017. [Online; accessed 22-March-2018]. Disponível em: <http://www2.aneel.gov.br/aplicacoes_liferay/indicadores_de_qualidade/decFecEstAnual.cfm?anoInicio=2010&regiao=BR>.

ANJANA, K.; SHAJI, R. A review on the features and technologies for energy efficiency of smart grid. **International Journal of Energy Research**, Wiley Online Library, v. 42, n. 3, p. 936–952, 2018.

ARIANOS, S. et al. Power grid vulnerability: A complex network approach. **Chaos: An Interdisciplinary Journal of Nonlinear Science**, AIP, v. 19, n. 1, p. 013119, 2009.

ARNOTT, D.; PERVAN, G. Eight key issues for the decision support systems discipline. **Decision Support Systems**, Elsevier, v. 44, n. 3, p. 657–672, 2008.

AVEN, E.; AVEN, T. On the need for rethinking current practice that highlights goal achievement risk in an enterprise context. **Risk Analysis**, Wiley Online Library, v. 35, n. 9, p. 1706–1716, 2015.

AVEN, T. Implications of black swans to the foundations and practice of risk assessment and management. **Reliability Engineering & System Safety**, Elsevier, v. 134, p. 83–91, 2015.

BABA, K.; SHIBATA, R.; SIBUYA, M. Partial correlation and conditional correlation as measures of conditional independence. **Australian & New Zealand Journal of Statistics**, Wiley Online Library, v. 46, n. 4, p. 657–664, 2004.

BAEK, J. et al. A secure cloud computing based framework for big data information management of smart grid. **IEEE transactions on cloud computing**, IEEE, v. 3, n. 2, p. 233–244, 2015.

BAJPAI, P.; CHANDA, S.; SRIVASTAVA, A. K. A novel metric to quantify and enable resilient distribution system using graph theory and choquet integral. **IEEE Transactions on Smart Grid**, IEEE, 2016.

BARABÁSI, A.-L. **Network science**. [S.l.]: Cambridge university press, 2016.

BARABÁSI, A.-L.; ALBERT, R. Emergence of scaling in random networks. **science**, American Association for the Advancement of Science, v. 286, n. 5439, p. 509–512, 1999.

BARTHÉLEMY, M. Spatial networks. **Physics Reports**, Elsevier, v. 499, n. 1, p. 1–101, 2011.

BHATT, J.; SHAH, V.; JANI, O. An instrumentation engineer's review on smart grid: Critical applications and parameters. **Renewable and Sustainable Energy Reviews**, Elsevier, v. 40, p. 1217–1239, 2014.

BIE, Z. et al. Battling the extreme: A study on the power system resilience. **Proceedings of the IEEE**, IEEE, v. 105, n. 7, p. 1253–1266, 2017.

BILIS, E. I.; KRÖGER, W.; NAN, C. Performance of electric power systems under physical malicious attacks. **IEEE Systems Journal**, IEEE, v. 7, n. 4, p. 854–865, 2013.

BILLINTON, R.; LI, W. **Reliability assessment of electric power systems using Monte Carlo methods**. [S.l.]: Springer Science & Business Media, 1994.

BLACK, W. R. **Transportation: a geographical analysis**. [S.l.]: Guilford Press, 2003.

BOCCALETTI, S. et al. Complex networks: Structure and dynamics. **Physics reports**, Elsevier, v. 424, n. 4, p. 175–308, 2006.

BOLLEN, M. H. Effects of adverse weather and aging on power system reliability. In: IEEE. **Industrial and Commercial Power Systems Technical Conference, 2000. Conference Record. Papers Presented at the 2000 Annual Meeting. 2000 IEEE**. [S.l.], 2000. p. 63–68.

BOMPARD, E. et al. Classification and trend analysis of threats origins to the security of power systems. **International Journal of Electrical Power & Energy Systems**, Elsevier, v. 50, p. 50–64, 2013.

BOMPARD, E.; LUO, L.; PONS, E. A perspective overview of topological approaches for vulnerability analysis of power transmission grids. **International Journal of Critical Infrastructures 7**, Inderscience Publishers Ltd, v. 11, n. 1, p. 15–26, 2015.

BOMPARD, E.; NAPOLI, R.; XUE, F. Analysis of structural vulnerabilities in power transmission grids. **International Journal of Critical Infrastructure Protection**, Elsevier, v. 2, n. 1, p. 5–12, 2009.

BOMPARD, E.; PONS, E.; WU, D. Analysis of the structural vulnerability of the interconnected power grid of continental europe with the integrated power system and unified power system based on extended topological approach. **International Transactions on Electrical Energy Systems**, Wiley Online Library, v. 23, n. 5, p. 620–637, 2013.

BÖTTCHER, L. et al. Failure and recovery in dynamical networks. **Scientific Reports**, Nature Publishing Group, v. 7, p. 41729, 2017.

BOX, G. E.; MULLER, M. E. et al. A note on the generation of random normal deviates. **The annals of mathematical statistics**, Institute of Mathematical Statistics, v. 29, n. 2, p. 610–611, 1958.

BOYES, H. Trustworthy cyber-physical systems—a review. In: IET. **System Safety Conference incorporating the Cyber Security Conference 2013, 8th IET International**. [S.l.], 2013. p. 1–8.

BRAESS, D.; NAGURNEY, A.; WAKOLBINGER, T. On a paradox of traffic planning. **Transportation science**, INFORMS, v. 39, n. 4, p. 446–450, 2005.

BRIN, S.; PAGE, L. The anatomy of a large-scale hypertextual web search engine. **Computer networks and ISDN systems**, Elsevier, v. 30, n. 1, p. 107–117, 1998.

BRODER, A. et al. Graph structure in the web. **Computer networks**, Elsevier, v. 33, n. 1, p. 309–320, 2000.

BROWN, G. et al. Defending critical infrastructure. **Interfaces**, Informs, v. 36, n. 6, p. 530–544, 2006.

CALLAWAY, D. S. et al. Network robustness and fragility: Percolation on random graphs. **Physical review letters**, APS, v. 85, n. 25, p. 5468, 2000.

CAMILLO, M. H. et al. Combining exhaustive search and multi-objective evolutionary algorithm for service restoration in large-scale distribution systems. **Electric Power Systems Research**, Elsevier, v. 134, p. 1–8, 2016.

_____. Validation of a methodology for service restoration on a real brazilian distribution system. In: IEEE. **Transmission & Distribution Conference and Exposition-Latin America (PES T&D-LA), 2014 IEEE PES**. [S.l.], 2014. p. 1–6.

CAPODIECI, N. et al. An adaptive agent-based system for deregulated smart grids. **Service Oriented Computing and Applications**, Springer, v. 10, n. 2, p. 185–205, 2016.

CARVALHO, R. et al. Robustness of trans-european gas networks. **Physical review E**, APS, v. 80, n. 1, p. 016106, 2009.

_____. Resilience of natural gas networks during conflicts, crises and disruptions. **PloS one**, Public Library of Science, v. 9, n. 3, p. e90265, 2014.

CASTILLO, A. Risk analysis and management in power outage and restoration: A literature survey. **Electric Power Systems Research**, Elsevier, v. 107, p. 9–15, 2014.

CELLI, G. et al. Reliability assessment in smart distribution networks. **Electric Power Systems Research**, Elsevier, v. 104, p. 164–175, 2013.

ČEPIN, M. **Assessment of power system reliability: methods and applications**. [S.l.]: Springer Science & Business Media, 2011.

CHAI, W. K. et al. Resilience of interdependent communication and power distribution networks against cascading failures. In: IEEE. **IFIP Networking Conference (IFIP Networking) and Workshops, 2016**. [S.l.], 2016. p. 37–45.

CHANDA, S.; SRIVASTAVA, A. K. Defining and enabling resiliency of electric distribution systems with multiple microgrids. **IEEE Transactions on Smart Grid**, IEEE, v. 7, n. 6, p. 2859–2868, 2016.

CHATTERJEE, S.; HADI, A. S. **Regression analysis by example**. [S.l.]: John Wiley & Sons, 2015.

CHOWDHURY, A.; KOVAL, D. **Power distribution system reliability: practical methods and applications**. [S.l.]: John Wiley & Sons, 2011. v. 48.

CHU, C.-C.; IU, H. H.-C. Complex networks theory for modern smart grid applications: a survey. **IEEE Journal on Emerging and Selected Topics in Circuits and Systems**, IEEE, v. 7, n. 2, p. 177–191, 2017.

CIVANLAR, S. et al. Distribution feeder reconfiguration for loss reduction. **IEEE Transactions on Power Delivery**, IEEE, v. 3, n. 3, p. 1217–1223, 1988.

CLAUSET, A.; SHALIZI, C. R.; NEWMAN, M. E. Power-law distributions in empirical data. **SIAM review**, SIAM, v. 51, n. 4, p. 661–703, 2009.

COHEN, R. et al. Resilience of the internet to random breakdowns. **Physical review letters**, APS, v. 85, n. 21, p. 4626, 2000.

_____. Breakdown of the internet under intentional attack. **Physical review letters**, APS, v. 86, n. 16, p. 3682, 2001.

COHEN, R.; HAVLIN, S. **Complex networks: structure, robustness and function**. [S.l.]: Cambridge University Press, 2010.

COOK, Z.; FRANKS, D. W.; ROBINSON, E. J. Efficiency and robustness of ant colony transportation networks. **Behavioral ecology and sociobiology**, Springer, v. 68, n. 3, p. 509–517, 2014.

COSTA, L. d. F. et al. Analyzing and modeling real-world phenomena with complex networks: a survey of applications. **Advances in Physics**, Taylor & Francis, v. 60, n. 3, p. 329–412, 2011.

_____. Characterization of complex networks: A survey of measurements. **Advances in physics**, Taylor & Francis, v. 56, n. 1, p. 167–242, 2007.

COVER, T. M.; THOMAS, J. A. **Elements of information theory**. [S.l.]: John Wiley & Sons, 2012.

CRUCITTI, P.; LATORA, V.; MARCHIORI, M. Model for cascading failures in complex networks. **Physical Review E**, APS, v. 69, n. 4, p. 045104, 2004.

_____. A topological analysis of the italian electric power grid. **Physica A: Statistical mechanics and its applications**, Elsevier, v. 338, n. 1, p. 92–97, 2004.

_____. Locating critical lines in high-voltage electrical power grids. **Fluctuation and Noise Letters**, World Scientific, v. 5, n. 02, p. L201–L208, 2005.

CUADRA, L. et al. A critical review of robustness in power grids using complex networks concepts. **Energies**, Multidisciplinary Digital Publishing Institute, v. 8, n. 9, p. 9211–9265, 2015.

CUI, L.; KUMARA, S.; ALBERT, R. Complex networks: An engineering view. **IEEE Circuits and Systems Magazine**, IEEE, v. 10, n. 3, p. 10–25, 2010.

DAEMI, T.; EBRAHIMI, A.; FOTUHI-FIRUZABAD, M. Constructing the bayesian network for components reliability importance ranking in composite power systems. **International Journal of Electrical Power & Energy Systems**, Elsevier, v. 43, n. 1, p. 474–480, 2012.

DELBEM, A. C.; CARVALHO, A. P. L. de; BRETAS, N. Main chain representation for evolutionary algorithms applied to distribution system reconfiguration. **IEEE Transactions on Power Systems**, IEEE, v. 20, n. 1, p. 425–436, 2005.

DOBSON, I. et al. Complex systems analysis of series of blackouts: Cascading failure, critical points, and self-organization. **Chaos: An Interdisciplinary Journal of Nonlinear Science**, AIP, v. 17, n. 2, p. 026103, 2007.

DWIVEDI, A.; YU, X.; SOKOLOWSKI, P. Identifying vulnerable lines in a power network using complex network theory. In: IEEE. **Industrial Electronics, 2009. ISIE 2009. IEEE International Symposium on**. [S.l.], 2009. p. 18–23.

ERDOS, P.; RÉNYI, A. On the evolution of random graphs. **Publ. Math. Inst. Hung. Acad. Sci**, Citeseer, v. 5, n. 1, p. 17–60, 1960.

ESPINOZA, S. et al. Multi-phase assessment and adaptation of power systems resilience to natural hazards. **Electric Power Systems Research**, Elsevier, v. 136, p. 352–361, 2016.

European Commission. **Critical Infrastructure Preparedness and Resilience Research Network (CIPRNet) project**. 2017. [Online; accessed 30-March-2018]. Disponível em: <https://www.ciprnet.eu/home.html>.

EUSGELD, I.; NAN, C.; DIETZ, S. "system-of-systems" approach for interdependent critical infrastructures. **Reliability Engineering & System Safety**, Elsevier, v. 96, n. 6, p. 679–686, 2011.

FALAHATI, B.; FU, Y. Reliability assessment of smart grids considering indirect cyber-power interdependencies. **IEEE Transactions on Smart Grid**, IEEE, v. 5, n. 4, p. 1677–1685, 2014.

FALAHATI, B.; FU, Y.; WU, L. Reliability assessment of smart grid considering direct cyber-power interdependencies. **IEEE Transactions on Smart Grid**, IEEE, v. 3, n. 3, p. 1515–1524, 2012.

FANG, X. et al. Smart grid—the new and improved power grid: A survey. **IEEE communications surveys & tutorials**, IEEE, v. 14, n. 4, p. 944–980, 2012.

FANG, Y.; SANSAVINI, G. Optimizing power system investments and resilience against attacks. **Reliability Engineering & System Safety**, Elsevier, v. 159, p. 161–173, 2017.

FANG, Y.-P.; PEDRONI, N.; ZIO, E. Resilience-based component importance measures for critical infrastructure network systems. **IEEE Transactions on Reliability**, IEEE, v. 65, n. 2, p. 502–512, 2016.

FARHANGI, H. The path of the smart grid. **IEEE power and energy magazine**, IEEE, v. 8, n. 1, 2010.

FARR, R. S.; HARER, J. L.; FINK, T. M. Easily repairable networks: Reconnecting nodes after damage. **Physical review letters**, APS, v. 113, n. 13, p. 138701, 2014.

FIEDLER, M. Algebraic connectivity of graphs. **Czechoslovak mathematical journal**, Institute of Mathematics, Academy of Sciences of the Czech Republic, v. 23, n. 2, p. 298–305, 1973.

FLEMING, J.; LEDOGAR, R. J. Resilience, an evolving concept: A review of literature relevant to aboriginal research. **Pimatisiwin**, PMC Canada manuscript submission, v. 6, n. 2, p. 7, 2008.

FRADI, A.; BRIGNONE, S.; WOLLENBERG, B. E. Calculation of energy transaction allocation factors. **IEEE Transactions on Power Systems**, IEEE, v. 16, n. 2, p. 266–272, 2001.

FRANK, S.; REBENNACK, S. An introduction to optimal power flow: Theory, formulation, and examples. **IIE Transactions**, Taylor & Francis, v. 48, n. 12, p. 1172–1197, 2016.

FU, G. et al. Integrated approach to assess the resilience of future electricity infrastructure networks to climate hazards. **IEEE Systems Journal**, IEEE, 2017.

FUENTE, A. D. L. et al. Discovery of meaningful associations in genomic data using partial correlation coefficients. **Bioinformatics**, Oxford University Press, v. 20, n. 18, p. 3565–3574, 2004.

GALLOS, L. K.; FEFFERMAN, N. H. Simple and efficient self-healing strategy for damaged complex networks. **Physical Review E**, APS, v. 92, n. 5, p. 052806, 2015.

GAO, J.; BARZEL, B.; BARABÁSI, A.-L. Universal resilience patterns in complex networks. **Nature**, Nature Publishing Group, v. 530, n. 7590, p. 307–312, 2016.

GASTNER, M. T.; NEWMAN, M. E. Shape and efficiency in spatial distribution networks. **Journal of Statistical Mechanics: Theory and Experiment**, IOP Publishing, v. 2006, n. 01, p. P01015, 2006.

GERTSBAKH, I. B.; SHPUNGIN, Y. **Models of network reliability: analysis, combinatorics, and Monte Carlo**. [S.l.]: CRC press, 2016.

GHEDINI, C.; RIBEIRO, C. H.; SABATTINI, L. Improving the fault tolerance of multi-robot networks through a combined control law strategy. In: IEEE. **Resilient Networks Design and Modeling (RNDM), 2016 8th International Workshop on**. [S.l.], 2016. p. 209–215.

GHEDINI, C. G.; RIBEIRO, C. H. Rethinking failure and attack tolerance assessment in complex networks. **Physica A: Statistical Mechanics and its Applications**, Elsevier, v. 390, n. 23, p. 4684–4691, 2011.

_____. Improving resilience of complex networks facing attacks and failures through adaptive mechanisms. **Advances in Complex Systems**, World Scientific, v. 17, n. 02, p. 1450009, 2014.

GLOVER, J. D.; SARMA, M. S.; OVERBYE, T. **Power System Analysis & Design, SI Version**. [S.l.]: Cengage Learning, 2012.

GRIGSBY, L. L. **Electric power generation, transmission, and distribution**. [S.l.]: CRC press, 2016.

HARRELL, F. **Regression modeling strategies: with applications to linear models, logistic and ordinal regression, and survival analysis**. [S.l.]: Springer, 2015.

HARRIS, T.; ROSS, F. **Fundamentals of a method for evaluating rail net capacities**. [S.l.], 1955.

HEYDT, G. T. The next generation of power distribution systems. **IEEE Transactions on Smart Grid**, IEEE, v. 1, n. 3, p. 225–235, 2010.

HILBE, J. M. **Negative binomial regression**. [S.l.]: Cambridge University Press, 2011.

_____. **Modeling Count Data**. [S.l.]: Cambridge University Press, 2014.

HINES, P.; BLUMSACK, S. A centrality measure for electrical networks. In: IEEE. **Hawaii International Conference on System Sciences, Proceedings of the 41st Annual**. [S.l.], 2008. p. 185–185.

HINES, P. et al. The topological and electrical structure of power grids. In: IEEE. **System Sciences (HICSS), 2010 43rd Hawaii International Conference on**. [S.l.], 2010. p. 1–10.

HINES, P.; COTILLA-SANCHEZ, E.; BLUMSACK, S. Do topological models provide good information about electricity infrastructure vulnerability? **Chaos: An Interdisciplinary Journal of Nonlinear Science**, AIP, v. 20, n. 3, p. 033122, 2010.

HOLLING, C. S. Resilience and stability of ecological systems. **Annual review of ecology and systematics**, Annual Reviews 4139 El Camino Way, PO Box 10139, Palo Alto, CA 94303-0139, USA, v. 4, n. 1, p. 1–23, 1973.

HOLLNAGEL, E.; WOODS, D. D.; LEVESON, N. **Resilience engineering: Concepts and precepts**. [S.l.]: Ashgate Publishing, Ltd., 2006.

HOLME, P. Edge overload breakdown in evolving networks. **Physical Review E**, APS, v. 66, n. 3, p. 036119, 2002.

HOLME, P.; KIM, B. J. Vertex overload breakdown in evolving networks. **Physical Review E**, APS, v. 65, n. 6, p. 066109, 2002.

HONG, L. et al. Vulnerability effects of passengers' intermodal transfer distance preference and subway expansion on complementary urban public transportation systems. **Reliability Engineering & System Safety**, Elsevier, v. 158, p. 58–72, 2017.

HOSMER, D. W.; LEMESHOW, S.; MAY, S. **Applied Survival Analysis: Regression Modeling of Time to Event Data**. 2nd. ed. [S.l.]: Wiley, 2008.

HOSSEINI, S.; BARKER, K. Modeling infrastructure resilience using bayesian networks: a case study of inland waterway ports. **Computers & Industrial Engineering**, Elsevier, v. 93, p. 252–266, 2016.

HOSSEINI, S.; BARKER, K.; RAMIREZ-MARQUEZ, J. E. A review of definitions and measures of system resilience. **Reliability Engineering & System Safety**, Elsevier, v. 145, p. 47–61, 2016.

HUANG, C.-N.; LIOU, J. J.; CHUANG, Y.-C. A method for exploring the interdependencies and importance of critical infrastructures. **Knowledge-Based Systems**, Elsevier, v. 55, p. 66–74, 2014.

IEEE PES, Transmission and Distribution Committee. IEEE guide for electric power distribution reliability indices. **IEEE Std 1366™-2012**, 2012.

IYER, S. et al. Attack robustness and centrality of complex networks. **PloS one**, Public Library of Science, v. 8, n. 4, p. e59613, 2013.

IYER, S. M.; NAKAYAMA, M. K.; GERBESSIOTIS, A. V. A markovian dependability model with cascading failures. **IEEE Transactions on Computers**, IEEE, v. 58, n. 9, p. 1238–1249, 2009.

JAGER, K. J. et al. The analysis of survival data: the kaplan–meier method. **Kidney international**, Nature Publishing Group, v. 74, n. 5, p. 560–565, 2008.

KAPLAN, E. L.; MEIER, P. Nonparametric estimation from incomplete observations. **Journal of the American statistical association**, Taylor & Francis, v. 53, n. 282, p. 457–481, 1958.

KAPUR, K. C.; PECHT, M. **Reliability engineering**. [S.l.]: John Wiley & Sons, 2014.

KAVASSERI, R.; ABABEI, C. Reds: Repository of distribution systems. **On line]. Available: http://venus.ece.ndsu.nodak.edu/kavasseri/reds.html**, 2015.

KAVOUSI-FARD, A.; NIKNAM, T. Optimal distribution feeder reconfiguration for reliability improvement considering uncertainty. **IEEE Transactions on Power Delivery**, IEEE, v. 29, n. 3, p. 1344–1353, 2014.

KIM, D. H. et al. Network topology and resilience analysis of south korean power grid. **Physica A: Statistical Mechanics and its Applications**, Elsevier, v. 465, p. 13–24, 2017.

KIM, J.; BUCKLEW, J. A.; DOBSON, I. Splitting method for speedy simulation of cascading blackouts. **IEEE Transactions on Power Systems**, IEEE, v. 28, n. 3, p. 3010–3017, 2013.

KIM, K.; SHEVLYAKOV, G. Why gaussianity? **IEEE Signal Processing Magazine**, v. 2, n. 25, p. 102–113, 2008.

KINNEY, R. et al. Modeling cascading failures in the north american power grid. **The European Physical Journal B-Condensed Matter and Complex Systems**, Springer, v. 46, n. 1, p. 101–107, 2005.

KIRSCHEN, D.; BOUFFARD, F. Keeping the lights on and the information flowing. **IEEE Power and Energy magazine**, IEEE, v. 7, n. 1, 2009.

KLEIN, J. P.; MOESCHBERGER, M. L. **Survival analysis: techniques for censored and truncated data**. [S.l.]: Springer Science & Business Media, 2005.

KOÇ, Y. et al. The impact of the topology on cascading failures in a power grid model. **Physica A: Statistical Mechanics and its Applications**, Elsevier, v. 402, p. 169–179, 2014.

KOŁOWROCKI, K. **Reliability of Large and Complex Systems**. [S.l.]: Elsevier, 2014.

KOMLJENOVIC, D. et al. Risks of extreme and rare events in asset management. **Safety Science**, Elsevier, v. 88, p. 129–145, 2016.

KOTT, A.; ABDELZAHER, T. Resiliency and robustness of complex systems and networks. **Adapt. Dyn. Resilient Syst**, v. 67, p. 67–86, 2014.

KOUTSOUKOS, X. et al. Sure: A modeling and simulation integration platform for evaluation of secure and resilient cyber–physical systems. **Proceedings of the IEEE**, IEEE, v. 106, n. 1, p. 93–112, 2018.

KRÖGER, W.; ZIO, E. **Vulnerable systems**. [S.l.]: Springer Science & Business Media, 2011.

KUNERT-GRAF, J. M.; SAKHANENKO, N. A.; GALAS, D. J. Complexity and vulnerability analysis of the c. elegans gap junction connectome. **Entropy**, Multidisciplinary Digital Publishing Institute, v. 19, n. 3, p. 104, 2017.

KWASINSKI, A. Quantitative model and metrics of electrical grids' resilience evaluated at a power distribution level. **Energies**, Multidisciplinary Digital Publishing Institute, v. 9, n. 2, p. 93, 2016.

LABAKA, L.; HERNANTES, J.; SARRIEGI, J. M. Resilience framework for critical infrastructures: An empirical study in a nuclear plant. **Reliability Engineering & System Safety**, Elsevier, v. 141, p. 92–105, 2015.

LANGSETH, H.; PORTINALE, L. Bayesian networks in reliability. **Reliability Engineering & System Safety**, Elsevier, v. 92, n. 1, p. 92–108, 2007.

LATORA, V.; MARCHIORI, M. Efficient behavior of small-world networks. **Physical review letters**, APS, v. 87, n. 19, p. 198701, 2001.

LI, F. et al. Smart transmission grid: Vision and framework. **IEEE transactions on Smart Grid**, IEEE, v. 1, n. 2, p. 168–177, 2010.

LI, X.; CHEN, G. Synchronization and desynchronization of complex dynamical networks: an engineering viewpoint. **IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications**, IEEE, v. 50, n. 11, p. 1381–1390, 2003.

LIMA, D. R. de et al. Modeling of an insect proprioceptor system based on different neuron response times. In: INSTICC. **Bio-inspired Systems and Signal Processing, BIOSIGNALS 2016 - 9th International Conference on**. [S.l.], 2016. p. 219–226.

LISCOUSKI, B.; ELLIOT, W. Final report on the august 14, 2003 blackout in the united states and canada: Causes and recommendations. **A report to US Department of Energy**, v. 40, n. 4, 2004.

LIU, X. et al. Risk assessment in extreme events considering the reliability of protection systems. **IEEE Transactions on Smart Grid**, IEEE, v. 6, n. 2, p. 1073–1081, 2015.

LLORET-GALLEGO, P. et al. Methodology for the evaluation of resilience of ict systems for smart distribution grids. **Energies**, Multidisciplinary Digital Publishing Institute, v. 10, n. 9, p. 1287, 2017.

LUO, L.; PAGANI, G. A.; ROSAS-CASALS, M. Spatial and performance optimality in power distribution networks. **IEEE Systems Journal**, IEEE, 2016.

LUSSEAU, D. The emergent properties of a dolphin social network. **Proceedings of the Royal Society of London B: Biological Sciences**, The Royal Society, v. 270, n. Suppl 2, p. S186–S188, 2003.

MACAL, C. M.; NORTH, M. J. Tutorial on agent-based modelling and simulation. **Journal of simulation**, Springer, v. 4, n. 3, p. 151–162, 2010.

MAJDANDZIC, A. et al. Spontaneous recovery in dynamical networks. **Nature Physics**, Nature Research, v. 10, n. 1, p. 34–38, 2014.

MALIK, F. H.; LEHTONEN, M. A review: Agents in smart grids. **Electric Power Systems Research**, Elsevier, v. 131, p. 71–79, 2016.

MALISZEWSKI, P. J.; PERRINGS, C. Factors in the resilience of electrical power distribution infrastructures. **Applied Geography**, Elsevier, v. 32, n. 2, p. 668–679, 2012.

MAURER, M.; SCHNELLER, R.; OMER, M. A survey on complexity management in systems engineering. In: IEEE. **Systems Conference (SysCon), 2014 8th Annual IEEE**. [S.l.], 2014. p. 180–187.

MAZUCHELI, J.; ACHCAR, J. A. The lindley distribution applied to competing risks lifetime data. **Computer methods and programs in biomedicine**, Elsevier, v. 104, n. 2, p. 188–192, 2011.

MEEKER, W. Q.; ESCOBAR, L. A. **Statistical methods for reliability data**. [S.l.]: John Wiley & Sons, 2014.

MEI, S. et al. Complex agent networks: An emerging approach for modeling complex systems. **Applied Soft Computing**, Elsevier, v. 37, p. 311–321, 2015.

MILLMAN, K. J.; AIVAZIS, M. Python for scientists and engineers. **Computing in Science & Engineering**, IEEE, v. 13, n. 2, p. 9–12, 2011.

MIRZASOLEIMAN, B. et al. Cascaded failures in weighted networks. **Physical Review E**, APS, v. 84, n. 4, p. 046114, 2011.

MORENO, Y.; GÓMEZ, J.; PACHECO, A. Instability of scale-free networks under node-breaking avalanches. **EPL (Europhysics Letters)**, IOP Publishing, v. 58, n. 4, p. 630, 2002.

MORENO, Y. et al. Critical load and congestion instabilities in scale-free networks. **EPL (Europhysics Letters)**, IOP Publishing, v. 62, n. 2, p. 292, 2003.

MORONE, F. et al. Enhancing network resilience via self-healing. In: IEEE. **Environmental, Energy, and Structural Monitoring Systems (EESMS), 2016 IEEE Workshop on**. [S.l.], 2016. p. 1–5.

MOTTER, A. E.; LAI, Y.-C. Cascade-based attacks on complex networks. **Physical Review E**, APS, v. 66, n. 6, p. 065102, 2002.

MOUSAVIZADEH, S.; HAGHIFAM, M.-R.; SHARIATKHAH, M.-H. A linear two-stage method for resiliency analysis in distribution systems considering renewable energy and demand response resources. **Applied Energy**, Elsevier, v. 211, p. 443–460, 2018.

MUDHOLKAR, G. S.; SRIVASTAVA, D. K. Exponentiated weibull family for analyzing bathtub failure-rate data. **IEEE Transactions on Reliability**, IEEE, v. 42, n. 2, p. 299–302, 1993.

MUREDDU, M. et al. Islanding the power grid on the transmission level: less connections for more security. **Scientific Reports**, Nature Publishing Group, v. 6, 2016.

MURTHY, D. P.; BULMER, M.; ECCLESTON, J. A. Weibull model selection for reliability modelling. **Reliability Engineering & System Safety**, Elsevier, v. 86, n. 3, p. 257–267, 2004.

NASIRUZZAMAN, A.; POTA, H.; ANWAR, A. Comparative study of power grid centrality measures using complex network framework. In: IEEE. **Power Engineering and Optimization Conference (PEDCO) Melaka, Malaysia, 2012 Ieee International**. [S.l.], 2012. p. 176–181.

NASIRUZZAMAN, A. et al. Modified centrality measure based on bidirectional power flow for smart and bulk power transmission grid. In: IEEE. **Power Engineering and Optimization Conference (PEDCO) Melaka, Malaysia, 2012 Ieee International**. [S.l.], 2012. p. 159–164.

NASIRUZZAMAN, A.; POTA, H.; MAHMUD, M. Application of centrality measures of complex network framework in power grid. In: IEEE. **IECON 2011-37th Annual Conference on IEEE Industrial Electronics Society**. [S.l.], 2011. p. 4660–4665.

NASSAR, M. M.; EISSA, F. H. On the exponentiated weibull distribution. **Communications in Statistics-Theory and Methods**, Taylor & Francis, v. 32, n. 7, p. 1317–1336, 2003.

National Academy of Sciences, Engineering, and Medicine. **Disaster resilience: a national imperative**. [S.l.], 2012.

NEGERI, E.; KUIPERS, F.; BAKEN, N. Designing reliable and resilient smart low-voltage grids. **International Journal of Critical Infrastructure Protection**, Elsevier, v. 9, p. 24–37, 2015.

NEWMAN, M. **Networks: an introduction**. [S.l.]: OUP Oxford, 2010.

NEWMAN, M. E. Assortative mixing in networks. **Physical review letters**, APS, v. 89, n. 20, p. 208701, 2002.

_____. Mixing patterns in networks. **Physical Review E**, APS, v. 67, n. 2, p. 026126, 2003.

_____. The structure and function of complex networks. **SIAM review**, SIAM, v. 45, n. 2, p. 167–256, 2003.

_____. A measure of betweenness centrality based on random walks. **Social networks**, Elsevier, v. 27, n. 1, p. 39–54, 2005.

NICHOLSON, C. D.; BARKER, K.; RAMIREZ-MARQUEZ, J. E. Flow-based vulnerability measures for network component importance: Experimentation with preparedness planning. **Reliability Engineering & System Safety**, Elsevier, v. 145, p. 62–73, 2016.

NOH, J. D.; RIEGER, H. Random walks on complex networks. **Physical review letters**, APS, v. 92, n. 11, p. 118701, 2004.

OTTINO, J. M. Engineering complex systems. **Nature**, Nature Publishing Group, v. 427, n. 6973, p. 399–399, 2004.

OUYANG, M.; DUEÑAS-OSORIO, L. Time-dependent resilience assessment and improvement of urban infrastructure systems. **Chaos: An Interdisciplinary Journal of Nonlinear Science**, AIP, v. 22, n. 3, p. 033122, 2012.

OUYANG, M.; FANG, Y. A mathematical framework to optimize critical infrastructure resilience against intentional attacks. **Computer-Aided Civil and Infrastructure Engineering**, Wiley Online Library, v. 32, n. 11, p. 909–929, 2017.

OUYANG, M. et al. Correlation analysis of different vulnerability metrics on power grids. **Physica A: Statistical Mechanics and its Applications**, Elsevier, v. 396, p. 204–211, 2014.

PACHAURI, R. K. et al. **Climate change 2014: synthesis report. Contribution of Working Groups I, II and III to the fifth assessment report of the Intergovernmental Panel on Climate Change**. [S.l.]: IPCC, 2014.

PAGANI, G.; AIELLO, M. Modeling the last mile of the smart grid. In: IEEE. **Innovative Smart Grid Technologies (ISGT), 2013 IEEE PES**. [S.l.], 2013. p. 1–6.

PAGANI, G. A.; AIELLO, M. Towards decentralization: A topological investigation of the medium and low voltage grids. **IEEE Transactions on Smart Grid**, IEEE, v. 2, n. 3, p. 538–547, 2011.

_____. The power grid as a complex network: a survey. **Physica A: Statistical Mechanics and its Applications**, Elsevier, v. 392, n. 11, p. 2688–2700, 2013.

_____. Power grid complex network evolutions for the smart grid. **Physica A: Statistical Mechanics and its Applications**, Elsevier, v. 396, p. 248–266, 2014.

_____. A complex network approach for identifying vulnerabilities of the medium and low voltage grid. **International Journal of Critical Infrastructures 7**, Inderscience Publishers Ltd, v. 11, n. 1, p. 36–61, 2015.

_____. From the grid to the smart grid, topologically. **Physica A: Statistical Mechanics and its Applications**, Elsevier, v. 449, p. 160–175, 2016.

PAHWA, S.; SCOGLIO, C.; SCALA, A. Abruptness of cascade failures in power grids. **Scientific reports**, Nature Publishing Group, v. 4, p. 3694, 2014.

PAHWA, S. et al. Optimal intentional islanding to enhance the robustness of power grid networks. **Physica A: Statistical Mechanics and its Applications**, Elsevier, v. 392, n. 17, p. 3741–3754, 2013.

PAL, M.; ALI, M. M.; WOO, J. Exponentiated weibull distribution. **Statistica**, v. 66, n. 2, p. 139–147, 2006.

PANTELI, M.; MANCARELLA, P. Influence of extreme weather and climate change on the resilience of power systems: Impacts and possible mitigation strategies. **Electric Power Systems Research**, Elsevier, v. 127, p. 259–270, 2015.

_____. Modeling and evaluating the resilience of critical electrical power infrastructure to extreme weather events. **IEEE Systems Journal**, IEEE, 2015.

PANTELI, M. et al. Power system resilience to extreme weather: Fragility modeling, probabilistic impact assessment, and adaptation measures. **IEEE Transactions on Power Systems**, IEEE, v. 32, n. 5, p. 3747–3757, 2017.

_____. Power systems resilience assessment: hardening and smart operational enhancement strategies. **Proceedings of the IEEE**, IEEE, v. 105, n. 7, p. 1202–1213, 2017.

PASTOR-SATORRAS, R. et al. Epidemic processes in complex networks. **Reviews of modern physics**, APS, v. 87, n. 3, p. 925, 2015.

QUATTROCIOCCHI, W.; CALDARELLI, G.; SCALA, A. Self-healing networks: redundancy and structure. **PloS one**, Public Library of Science, v. 9, n. 2, p. e87986, 2014.

QUEVEDO, P. M. de et al. Reliability assessment of microgrids with local and mobile generation, time-dependent profiles, and intraday reconfiguration. **IEEE Transactions on Industry Applications**, IEEE, v. 54, n. 1, p. 61–72, 2018.

RAJKUMAR, R. R. et al. Cyber-physical systems: the next computing revolution. In: ACM. **Proceedings of the 47th Design Automation Conference**. [S.l.], 2010. p. 731–736.

RAMCHURN, S. D. et al. Putting the'smarts' into the smart grid: a grand challenge for artificial intelligence. **Communications of the ACM**, ACM, v. 55, n. 4, p. 86–97, 2012.

RAMIREZ-MARQUEZ, J. E. et al. Quantifying the resilience of community structures in networks. **Reliability Engineering & System Safety**, Elsevier, v. 169, p. 466–474, 2018.

REE, J. D. L. et al. Catastrophic failures in power systems: causes, analyses, and countermeasures. **Proceedings of the IEEE**, IEEE, v. 93, n. 5, p. 956–964, 2005.

REN, H.-P. et al. Cascade failure analysis of power grid using new load distribution law and node removal rule. **Physica A: Statistical Mechanics and its Applications**, Elsevier, v. 442, p. 239–251, 2016.

RIGHI, A. W.; SAURIN, T. A.; WACHS, P. A systematic literature review of resilience engineering: Research areas and a research agenda proposal. **Reliability Engineering & System Safety**, Elsevier, v. 141, p. 142–152, 2015.

RINALDI, S. M.; PEERENBOOM, J. P.; KELLY, T. K. Identifying, understanding, and analyzing critical infrastructure interdependencies. **IEEE Control Systems**, IEEE, v. 21, n. 6, p. 11–25, 2001.

ROOS, F.; LINDAH, S. Distribution system component failure rates and repair times–an overview. In: CITESEER. **Conf. Rec. the Nordic Distribution and Asset Management Conference**. [S.l.], 2004.

ROSAS-CASALS, M.; VALVERDE, S.; SOLÉ, R. V. Topological vulnerability of the european power grid under errors and attacks. **International Journal of Bifurcation and Chaos**, World Scientific, v. 17, n. 07, p. 2465–2475, 2007.

ROSATO, V.; BOLOGNA, S.; TIRITICCO, F. Topological properties of high-voltage electrical transmission networks. **Electric Power Systems Research**, Elsevier, v. 77, n. 2, p. 99–105, 2007.

RUBINO, G.; TUFFIN, B. **Rare event simulation using Monte Carlo methods**. [S.l.]: John Wiley & Sons, 2009.

SAFFARI, S. E.; ADNAN, R.; GREENE, W. Handling of over-dispersion of count data via truncation using poisson regression model. **Journal of Computer Science and Computational Mathematics**, v. 1, n. 1, p. 1–4, 2011.

SAHOO, R. K. et al. Failure data analysis of a large-scale heterogeneous server environment. In: IEEE. **Dependable Systems and Networks, 2004 International Conference on**. [S.l.], 2004. p. 772–781.

SALEH, J. H.; MARAIS, K. Highlights from the early (and pre-) history of reliability engineering. **Reliability Engineering & System Safety**, Elsevier, v. 91, n. 2, p. 249–256, 2006.

SCALA, A. et al. Power grids, smart grids and complex networks. In: **Nonlinear Phenomena in Complex Systems: From Nano to Macro Scale**. [S.l.]: Springer, 2014. p. 97–110.

SCHLÄPFER, M.; KESSLER, T.; KRÖGER, W. Reliability analysis of electric power systems using an object-oriented hybrid modeling approach. In: **Proceedings of the 16th power systems computation conference, Glasgow**. [S.l.: s.n.], 2008. p. 14–18.

SCHNEIDER, C. M. et al. Mitigation of malicious attacks on networks. **Proceedings of the National Academy of Sciences**, National Acad Sciences, v. 108, n. 10, p. 3838–3841, 2011.

SCHNEIDER, K. P. et al. Evaluating the feasibility to use microgrids as a resiliency resource. **IEEE Transactions on Smart Grid**, IEEE, v. 8, n. 2, p. 687–696, 2017.

SCHWARZ, G. et al. Estimating the dimension of a model. **The annals of statistics**, Institute of Mathematical Statistics, v. 6, n. 2, p. 461–464, 1978.

SELVAM, M. M.; GNANADASS, R.; PADHY, N. Initiatives and technical challenges in smart distribution grid. **Renewable and Sustainable Energy Reviews**, Elsevier, v. 58, p. 911–917, 2016.

SHA, A.; AIELLO, M. A novel strategy for optimising decentralised energy exchange for prosumers. **Energies**, Multidisciplinary Digital Publishing Institute, v. 9, n. 7, p. 554, 2016.

SHANG, Y. Impact of self-healing capability on network robustness. **Physical Review E**, APS, v. 91, n. 4, p. 042804, 2015.

_____. Localized recovery of complex networks against failure. **Scientific Reports**, Nature Publishing Group, v. 6, 2016.

SHAUKAT, N. et al. A survey on consumers empowerment, communication technologies, and renewable generation penetration within smart grid. **Renewable and Sustainable Energy Reviews**, Elsevier, 2018.

SHEKHTMAN, L. M.; DANZIGER, M. M.; HAVLIN, S. Recent advances on failure and recovery in networks of networks. **Chaos, Solitons & Fractals**, Elsevier, v. 90, p. 28–36, 2016.

SHIN, D. H.; HE, S.; ZHANG, J. Robust, secure, and cost-effective design for cyber-physical systems. **IEEE Intelligent Systems**, v. 29, n. 1, p. 66–69, 2014.

SHUANG, Q.; ZHANG, M.; YUAN, Y. Performance and reliability analysis of water distribution systems under cascading failures and the identification of crucial pipes. **PloS one**, Public Library of Science, v. 9, n. 2, p. e88445, 2014.

SILVA, A. L. D. et al. Pseudo-chronological simulation for composite reliability analysis with time varying loads. **IEEE Transactions on Power Systems**, IEEE, v. 15, n. 1, p. 73–80, 2000.

SILVA, T. C.; SOUZA, S. R. S. de; TABAK, B. M. Monitoring vulnerability and impact diffusion in financial networks. **Journal of Economic Dynamics and Control**, Elsevier, 2017.

SMIDT-DESTOMBES, K. S. de; HEIJDEN, M. C. van der; HARTEN, A. van. On the availability of a k-out-of-n system given limited spares and repair capacity under a condition based maintenance strategy. **Reliability engineering & System safety**, Elsevier, v. 83, n. 3, p. 287–300, 2004.

SOLÉ, R. V. et al. Robustness of the european power grids under intentional attack. **Physical Review E**, APS, v. 77, n. 2, p. 026102, 2008.

SONG, C.; HAVLIN, S.; MAKSE, H. A. Origins of fractality in the growth of complex networks. **Nature Physics**, Nature Publishing Group, v. 2, n. 4, p. 275–281, 2006.

SRA, Society of Risk Analysis. **Glossary of the specialty group on foundations of risk analysis**. 2015. [Online; accessed 21-November-2016]. Disponível em: <http://www.sra.org/news/sra-develops-glossary-risk-related-terms>.

STERLING, T. L. **Beowulf cluster computing with Linux**. [S.l.]: MIT press, 2002.

SU, C.-T.; CHANG, C.-F.; CHIOU, J.-P. Distribution network reconfiguration for loss reduction by ant colony search algorithm. **Electric Power Systems Research**, Elsevier, v. 75, n. 2, p. 190–199, 2005.

THACKER, S.; PANT, R.; HALL, J. W. System-of-systems formulation and disruption analysis for multi-scale critical national infrastructures. **Reliability Engineering & System Safety**, Elsevier, v. 167, p. 30–41, 2017.

THOMOPOULOS, N. T. **Essentials of Monte Carlo simulation: Statistical methods for building simulation models**. [S.l.]: Springer Science & Business Media, 2012.

TRAJANOVSKI, S. et al. Robustness envelopes of networks. **Journal of Complex Networks**, Oxford University Press, v. 1, n. 1, p. 44–62, 2013.

TRAN, H. T. et al. A framework for the quantitative assessment of performance-based system resilience. **Reliability Engineering & System Safety**, Elsevier, v. 158, p. 73–84, 2017.

TRAVERS, J.; MILGRAM, S. An experimental study of the small world problem. **Sociometry**, JSTOR, p. 425–443, 1969.

TUBALLA, M. L.; ABUNDO, M. L. A review of the development of smart grid technologies. **Renewable and Sustainable Energy Reviews**, Elsevier, v. 59, p. 710–725, 2016.

US DOE. **Transforming the Nation's Electricity System: The Second Installment of the Quadrennial Energy Review**. [S.l.], 2017.

VELICKOVIC, V. M. What everyone should know about statistical correlation. **American Scientist**, Sigma XI-The Scientific Research Society, v. 103, n. 1, p. 26, 2015.

VESPIGNANI, A. Modelling dynamical processes in complex socio-technical systems. **Nature physics**, Nature Research, v. 8, n. 1, p. 32–39, 2012.

VIANA, M. P. et al. The simplicity of planar networks. **Scientific reports**, Nature Publishing Group, v. 3, 2013.

WANDEL, S. et al. Duration from seroconversion to eligibility for antiretroviral therapy and from art eligibility to death in adult hiv-infected patients from low and middle-income countries: collaborative analysis of prospective studies. **Sexually transmitted infections**, v. 84, p. i31–i36, 2008.

WANG, J.-W.; RONG, L.-L. Robustness of the western united states power grid under edge attack strategies due to cascading failures. **Safety science**, Elsevier, v. 49, n. 6, p. 807–812, 2011.

WANG, S. et al. Vulnerability analysis and critical areas identification of the power systems under terrorist attacks. **Physica A: Statistical Mechanics and its Applications**, Elsevier, 2017.

WANG, X. et al. A network approach for power grid robustness against cascading failures. In: IEEE. **Reliable Networks Design and Modeling (RNDM), 2015 7th International Workshop on**. [S.l.], 2015. p. 208–214.

WANG, X. F.; CHEN, G. Complex networks: small-world, scale-free and beyond. **Circuits and Systems Magazine, IEEE**, IEEE, v. 3, n. 1, p. 6–20, 2003.

WANG, Y. et al. Research on resilience of power systems under natural disasters—a review. **IEEE Transactions on Power Systems**, IEEE, v. 31, n. 2, p. 1604–1613, 2016.

_____. Study on structural vulnerabilities of power grids based on the electrical distance. In: IEEE. **Innovative Smart Grid Technologies-Asia (ISGT Asia), 2012 IEEE**. [S.l.], 2012. p. 1–5.

WANG, Z.; SCAGLIONE, A.; THOMAS, R. J. Electrical centrality measures for electric power grid vulnerability analysis. In: IEEE. **Decision and Control (CDC), 2010 49th IEEE Conference on**. [S.l.], 2010. p. 5792–5797.

WANG, Z. et al. Cyber-physical systems for water sustainability: challenges and opportunities. **IEEE Communications Magazine**, IEEE, v. 53, n. 5, p. 216–222, 2015.

WATTS, D. J. A simple model of global cascades on random networks. **Proceedings of the National Academy of Sciences**, National Acad Sciences, v. 99, n. 9, p. 5766–5771, 2002.

WATTS, D. J.; STROGATZ, S. H. Collective dynamics of 'small-world'networks. **nature**, Nature Publishing Group, v. 393, n. 6684, p. 440–442, 1998.

WEBER, P.; JOUFFE, L. Complex system reliability modelling with dynamic object oriented bayesian networks (doobn). **Reliability Engineering & System Safety**, Elsevier, v. 91, n. 2, p. 149–162, 2006.

WENLI, F. et al. Cascading failure model in power grids using the complex network theory. **IET Generation, Transmission & Distribution**, IET, v. 10, n. 15, p. 3940–3949, 2016.

WOODS, D. D. Four concepts for resilience and the implications for the future of resilience engineering. **Reliability Engineering & System Safety**, Elsevier, v. 141, p. 5–9, 2015.

WU, J. et al. Spectral measure of structural robustness in complex networks. **IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans**, IEEE, v. 41, n. 6, p. 1244–1252, 2011.

XENIAS, D. et al. Uk smart grid development: An expert assessment of the benefits, pitfalls and functions. **Renewable Energy**, Elsevier, v. 81, p. 89–102, 2015.

XIA, Y.; HILL, D. J. Attack vulnerability of complex communication networks. **IEEE Transactions on Circuits and Systems II: Express Briefs**, IEEE, v. 55, n. 1, p. 65–69, 2008.

XU, L. D.; XU, E. L.; LI, L. Industry 4.0: state of the art and future trends. **International Journal of Production Research**, Taylor & Francis, p. 1–22, 2018.

YAMIJALA, S.; GUIKEMA, S. D.; BRUMBELOW, K. Statistical models for the analysis of water distribution system pipe break data. **Reliability Engineering & System Safety**, Elsevier, v. 94, n. 2, p. 282–293, 2009.

YAN, J. et al. Q-learning-based vulnerability analysis of smart grid against sequential topology attacks. **IEEE Transactions on Information Forensics and Security**, IEEE, v. 12, n. 1, p. 200–210, 2017.

_____. Smart grid vulnerability under cascade-based sequential line-switching attacks. In: IEEE. **Global Communications Conference (GLOBECOM), 2015 IEEE**. [S.l.], 2015. p. 1–7.

YANG, Y.; HUANG, A.; GUAN, W. Statistic properties and cascading failures in a coupled transit network consisting of bus and subway systems. **International Journal of Modern Physics B**, World Scientific, v. 28, n. 30, p. 1450212, 2014.

YAO, S.; WANG, P.; ZHAO, T. Transportable energy storage for more resilient distribution systems with multiple microgrids. **IEEE Transactions on Smart Grid**, IEEE, 2018.

YAZDANI, A.; JEFFREY, P. Robustness and vulnerability analysis of water distribution networks using graph theoretic and complex network principles. **Proceeding of Water Distribution System Analysis 2010**, p. 12–15, 2010.

_____. Complex network analysis of water distribution systems. **Chaos: An Interdisciplinary Journal of Nonlinear Science**, AIP Publishing, v. 21, n. 1, p. 016111, 2011.

YODO, N.; WANG, P.; ZHOU, Z. Predictive resilience analysis of complex systems using dynamic bayesian networks. **IEEE Transactions on Reliability**, IEEE, v. 66, n. 3, p. 761–770, 2017.

YUSTA, J. M.; CORREA, G. J.; LACAL-ARÁNTEGUI, R. Methodologies and applications for critical infrastructure protection: State-of-the-art. **Energy Policy**, Elsevier, v. 39, n. 10, p. 6100–6119, 2011.

ZECHMAN, E. M. Agent-based modeling to simulate contamination events and evaluate threat management strategies in water distribution systems. **Risk Analysis**, Wiley Online Library, v. 31, n. 5, p. 758–772, 2011.

ZHENG, H. et al. Impact of automatic switches on power distribution system reliability. **Electric Power Systems Research**, Elsevier, v. 83, n. 1, p. 51–57, 2012.

ZHU, Y. et al. Resilience analysis of power grids under the sequential attack. **IEEE Transactions on Information Forensics and Security**, IEEE, v. 9, n. 12, p. 2340–2354, 2014.

ZIDAN, A.; EL-SAADANY, E. F. A cooperative multiagent framework for self-healing mechanisms in distribution systems. **IEEE transactions on smart grid**, IEEE, v. 3, n. 3, p. 1525–1539, 2012.

ZIDAN, A. et al. Fault detection, isolation, and service restoration in distribution systems: State-of-the-art and future trends. **IEEE Transactions on Smart Grid**, IEEE, 2016.

ZIO, E. Reliability analysis of complex network systems: research and practice in need. **IEEE Reliability Society Annual Technology Report**, 2007.

_____. Reliability engineering: Old problems and new challenges. **Reliability Engineering & System Safety**, Elsevier, v. 94, n. 2, p. 125–141, 2009.

_____. **The Monte Carlo simulation method for system reliability and risk analysis**. [S.l.]: Springer, 2013.

_____. Challenges in the vulnerability and risk analysis of critical infrastructures. **Reliability Engineering & System Safety**, Elsevier, v. 152, p. 137–150, 2016.

_____. Some challenges and opportunities in reliability engineering. **IEEE Transactions on Reliability**, IEEE, 2016.

ZIO, E.; GOLEA, L. R. Analyzing the topological, electrical and reliability characteristics of a power transmission system for identifying its critical elements. **Reliability Engineering & System Safety**, Elsevier, v. 101, p. 67–74, 2012.

ZIO, E.; SANSAVINI, G. Component criticality in failure cascade processes of network systems. **Risk Analysis**, Wiley Online Library, v. 31, n. 8, p. 1196–1210, 2011.

ZONOUZ, S. et al. Socca: A security-oriented cyber-physical contingency analysis in power infrastructures. **IEEE Transactions on Smart Grid**, IEEE, v. 5, n. 1, p. 3–13, 2014.

Appendices

APPENDIX A – BRAZILIAN POWER DISTRIBUTION SYSTEM INTERRUPTION CAUSES

Table 32 – Causes of service interruption classified as atmospheric causes

Atmospheric discharge
Wind / Gale
Frost / snow / low temp / hail

Table 33 – Causes of service interruption classified as environmental causes

Corrosion / oxidation / pollution
Tree branches touching the net (pruning)
Tree fell on the net
Erosion
Peels / twigs thrown in the rd
Animals / Insects / Birds
Flood / flood

Table 34 – Causes of service interruption classified as urban causes

Car collision
Third party knocked down tree in the net
Replace stolen network component
Burns / fire
Vandalism / Thefts
Foreign objects in the network
Unpredictable factors / public calamity

Table 35 – Causes of service interruption classified as operational causes

Load / voltage unbalance
Supervision failure
Load transference / return to original configuration
Human failure of a contracted company
Shutdown by security
Accidental interference by the maintenance team
Network recomposition
Human failure of the company
Load shedding
Improper maneuver on the transmission
Tension / frequency oscillation

Table 36 – Causes of service interruption classified as equipment failures

Unidentified
Component broken / deregulated
Corrective maintenance
Component protection failure
Replacement / withdrawal / installation
Installation defect
Preventive maintenance
Manufacturing failure or defect