TÉCNICO LISBOA

Failure Modes and Effects Analysis (FMEA) for Smart Electrical Distribution Systems

Alexandre Neves Silvestre Baleia

Thesis to obtain the Master of Science Degree in

Electrical and Computer Engineering

Supervisor(s): Prof. Paulo José da Costa Branco
Prof. João Filipe Pereira Fernandes

Examination Committee

Chairperson: Prof. Rui Manuel Gameiro de Castro
Supervisor: Prof. Paulo José da Costa Branco
Member of the Committee: Prof. Pedro Manuel Santos de Carvalho

November 2018

“People do not lack strength, they lack will”

– Victor Hugo

Declaration

I declare that this document is an original work of my own authorship and that it fulfills all the requirements of the Code of Conduct and Good Practices of the Universidade de Lisboa.

Acknowledgments

First of all, I would like to express my gratitude to my thesis supervisor, Professor Paulo José da Costa Branco of the Electrical and Computer Engineering Department at Instituto Superior Técnico. From the great and innovative ideas to the urge motivation, his passion for science and knowledge inspired me to embrace this dissertation. His guidance and support made this work possible. I also want to address an acknowledgment to my co-supervisor, Professor João Filipe Pereira Fernandes. His readiness in helping me to solve the apparently unsolvable problems made me believe that I was able to perform this work. I would also like to thank Andrés Alejandro Zúñiga Rodríguez. The door to Andrés' office was always open whenever I needed some help with challenges on my research or with problem resolution.

I would also like to show my sincere gratitude to Luísa Jorge and Maria Inês Verdelho, from DAPR department at EDP Distribuição, for having received me in their offices and clarified, with patience, my doubts and problems. A special thanks to Fernando Carvalho, from AmberTREE, who made this contact possible.

I must express my gratitude to my family, specially to my parents and sister, for all the unfailing support and continuous motivation through all my life and my study years. Without their support I would never be the person I am today. This accomplishment would not have been possible without you.

Finally, I would like to thank Inês, my friend, my companion, my lover, my inspiration, for being alongside me, supporting me whenever I needed and celebrating with me in all of my achievements.

Resumo

A avaliação de fiabilidade em sistemas de distribuição tradicionais tem desempenhado um papel fundamental no planeamento, design e operação de sistemas de potência.

Recentemente, novas tecnologias de informação e comunicação têm sido introduzidas na automação de sistemas de potência e gestão de ativos, tornando a rede de distribuição ainda mais complexa. De modo a alcançar uma gestão eficiente de energia, a rede de distribuição terá de adoptar uma nova configuração que irá mudar o paradigma da rede elétrica, que tem de enfrentar inúmeros desafios técnicos e económicos.

A emergência do conceito de redes inteligentes ou *smart grids*, de modo a corresponder às necessidades energéticas futuras, requer abordagens alternativas na avaliação de fiabilidade dos novos sistemas de distribuição. Na presente dissertação, uma abordagem que faz uso dos modos de falha dos principais equipamentos de potência e de comunicação é proposta uma abordagem para a avaliação da análise de risco de sistemas de distribuição inteligentes.

Este trabalho introduz a aplicação da metodologia FMEA de modo a estabelecer os impactos de diferentes modos de falha na performance da rede inteligente. Um sistema de teste é definido e modos de falha e suas respetivas consequências no sistema serão estudadas. Medidas de manutenção preventiva são propostas e sistematizadas de modo a minimizar o impacto de falhas com alto índice de criticidade e melhorar a fiabilidade do sistema considerado.

Palavras-chave: análise de risco, fiabilidade, FMEA, modo de falha, redes inteligentes, taxa de falha.

Abstract

Reliability assessment in traditional power distribution systems has played a key role in power system planning, design and operation.

Recently, new information and communication technologies have been introduced in power systems automation and asset management, making the distribution network even more complex. In order to achieve efficient energy management, the distribution grid has to adopt a new configuration and operational conditions that will change the paradigm of the actual electrical system which has to face numerous technical and economic challenges.

The emergence of the smart systems concept to face future energetic needs requires alternative approaches for evaluating the reliability of modern distribution systems, especially in the smart grids environment. In this thesis, a reliability approach that makes use of failure modes of power and cyber network main components is proposed to evaluate risk analysis in smart electrical distribution systems.

This dissertation introduces the application of Failure Modes and Effects Analysis (FMEA) method in future smart grid systems in order to establish the impact of different failure modes on smart grid performance. A smart grid test system is defined and failure modes and their effects on the system are studied. Preventive maintenance tasks are proposed and systematized to minimize the impact of high-risk failures and to increase reliability of the proposed test system.

Keywords: failure mode, failure rate, FMEA, reliability, risk analysis, smart grid.

Contents

List of Tables

List of Figures

List of Acronyms and Symbols

List of Acronyms

AFR	Annual Failure Rate
CB	Circuit Breaker
DET	Detection
DEEI	Direct Element-Element Interdependency
DNEI	Direct Network-Element Interdependency
EB	Energy Box
EMS	Energy Management System
FMEA	Failure Modes and Effect Analysis
FTP	File Transfer Protocol
HMI	Human-Machine Interface
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Device
IEEI	Indirect Element-Element Interdependency
INEI	Indirect Network-Element Interdependency
LAN	Local Area Network
MAN	Metropolitan Area Network
MTBF	Mean Time Between Failures
OCC	Occurrence
PM	Preventive Maintenance
PrM	Proactive Maintenance

PTI	Predictive Testing and Inspection
RBD	Reliability Block Diagram
RCM	Reliability-Centered Maintenance
RM	Reactive Maintenance
RPN	Risk Priority Number
SCADA	Supervisory Control And Data Acquisition
SEV	Severity
SV	Server
SW	Ethernet Switch
WAN	Wide Area Network

List of Symbols

λ	Failure rate

Chapter 1

Introduction

In this chapter, a brief overview about the addressed problem will be presented.

It will be firstly introduced the motivation underlying to this work, referring the importance of FMEA in reliability assessment in smart electrical distribution systems.

Secondly, some of the relevant works and researches on reliability assessment and risk analysis in power networks and smart grids will be reviewed. Then, the main objectives of this thesis will be stated, and finally a brief outline of the present work will be presented.

1.1 Motivation

It is undeniable that electricity plays a crucial role in today's society. It is the most versatile and easily controlled form of energy, and welfare, comfort and health of world communities depends on the delivery of electricity. It is involved in almost all aspects of society's daily routine.

It is fair to recognize that electrical energy means economic, technological, social and cultural development. In turn, society's development brings more electricity needs, leading to the increase in electricity demand. Besides that, electricity demand has been accentuated in recent decades and it is expected an increase in world's population in the forthcoming years, alongside with the increasing access to electricity in developing countries, will trigger a strong demand of energy [1, 2]. It urges the necessity to introduce new ways of generating electrical energy from renewable resources [3] by decreasing the dependence from conventional and pollutant energy resources, thus promoting human development in a more sustainable way [1].

The transition from conventional to renewable forms of energy poses numerous challenges. Energy becomes available everywhere from dispersed sources, and it must be integrated in every points in the grid. Associated with the growth of mobile loads and the increasing number of energy storage equipment [4, 5], new technological functionalities are required to provide energy management in a more reliable and effective way. Some of them, such as real-time distributed intelligence and a new level of controllability, are a decisive factor for ensuring stable, cost-effective and resource-efficient energy supply, and robust and complex cyber-physical systems able to meet future needs concerning sustainability

and electricity commitment must be developed [4–6].

The impact of having a smart grid is evident: instead of having a passive and rigid grid determined by predictable flow directions, conventional energy sources and expected load profiles, one has an active grid, with constant fluctuations due to inconstant generating resources like solar or wind, total unexpected load profiles and unpredictable power flow directions, making a more dynamic grid. Consumers participation in demand response and in electricity markets are also expected to play an important role in energy efficiency [5, 6].

However, new problems arise [2, 7]:

- the increased complexity of the electrical system creates a considerable number of barriers that can difficult the development of such system, regarding technical and non-technical challenges;
- the correct operation of every single equipment in a smart grid is direct or indirectly dependent on the correct behaviour of other equipment;
- an absolute interdependence between cyber and power system is needed to endow the grid of such intelligence and robustness, and a malfunction, even in the most insignificant equipment, can put in danger the efficiency and reliability of system's performance.

The lack of adequate control and management strategies can lead to power outage of parts of the grid, and if taken into account an inability to face threats that can compromise system's security, a complete outage of the grid can happen in an ultimate perspective.

The reliability assessment in traditional power distribution systems considers reliability probability-modelling for power components such as electrical lines, circuit breakers or transformers [8]. However, it is important to evaluate reliability and security of a smart system through alternative reliability approaches that take into account the complexity previously described [9–15]. The relevance of these tools in such complex systems like future smart grids allows not only the development of maintenance strategies to create a safe and secure system but also the optimization of installation and maintenance costs, in order to create a high-reliable system with low-risk failures.

When considering reliability tools, a methodology called Reliability Centered Maintenance (RCM) arises as one of the most important ones. The benefits of an RCM approach far exceed those of any type of maintenance program, and it has long been accepted by the aircraft, spacecraft or nuclear industry [16] but it is a relatively new way of approaching maintenance for the majority of facilities outside of these areas. RCM strategies impact on energy field is still undefined, due to the lack of evidences, and the application of RCM as a useful tool for a smart grid reliability analysis must be studied.

In this context, Failure Modes and Effects Analysis (FMEA) is a RCM technique used to define, identify and eliminate known and/or potential failures, problems and errors from the system, design, process and/or service [17]. FMEA is generally good for exhaustively identifying and recording the local effects that arise from component failures and then inferring the effects of those failures at the system level.

FMEA has been extensively used in aerospace, automotive, nuclear, electronics, chemical, mechanical, and health care [17] as a powerful tool for safety and reliability analysis with proven results.

As a RCM technique, FMEA methodology will then be used in a smart grid test system to evaluate smart grid risks and to study FMEA contributions for reliability assessment in energy systems.

1.2 Topic Overview

A few studies concerning reliability analysis in energy systems had been developed throughout the years.

Concerning reliability analysis in power systems, one can found works applying reliability methodologies in power grids. In [9], a first attempt for an RCM application in Turkish National Power Transmission System is presented. The transmission system were decomposed into sub-systems and failures of each sub-system was held individually to attain a reasonable maintenance program for the transmission system. For each sub-system, failure modes were defined with their respective failure causes and effects. Decision tree diagrams for the sub-systems were constructed, and RCM management program was developed by formulating the most appropriate maintenance procedures from those decision tree diagrams. The survey displayed failure modes with lower impact on the system that do not need proactive maintenance, while unexpected phenomena like atmospheric conditions cannot be economically minimized by periodic and predictive maintenance. The authors concluded that the resulting maintenance procedure determined by the applied RCM methodology greatly depends on the system data and on the models held for the sub-systems and failures previously defined.

In [10], RCM methodologies are applied in more than 90 high-voltage stations operated by a generating and transmission company in Brazil. Several power system performance indexes and results were modeled and compared with the company operating data. The study provided an optimization of maintenance activities, which allowed the company a more effective-cost maintenance strategy. In another survey, reference [11] proposes a reliability model based on a combination of fault tree analysis and FMEA, both combined with dynamic power system simulations as used for probabilistic analysis of power system reliability in the Finnish 400kV transmission system.

A method based on condition-based maintenance (preventive maintenance) and system's reliability assessment was proposed in [12] to model the quantitative relationship between monitoring data of overhead lines and failure rates, as well as system reliability in overhead lines in a 182-bus, considering 5474 MW of the transmission system in southwest China. A maintenance strategy that is based on the monitoring data and impacts of line maintenance on system reliability is also proposed. With this approach, the authors achieved significant maintenance cost savings when compared to two traditional maintenance strategies previously in used, while increasing lines reliability.

Focusing on communication architecture and redundancy of system functionality, authors in [13] use Markov state model for reliability analysis of various substation automation system architectures. A new approach for power system reliability analysis using the fault tree analysis approach was also developed in [14]. Reliability Block Diagram (RBD) and Monte-Carlo simulation methods were applied in [15] for reliability assessment in UPSs and the authors suggested its implementation on all system configurations.

Related to an introduction in reliability studies in future smart grids, recent approaches discussed new methodologies for assessing reliability performance of power systems in order to quantify in the most realistic manner standard set of indices for regulator requirements. In [18], an extensive study based on analytic and probabilistic reliability procedures is evaluated under various scenarios. In this turn, authors in [19] analyze the performance of smart grids with demand-side management, distributed generation and storage technologies. Adapted Monte-Carlo procedures were adopted in order to provide a more accurate assessment and reliability indices and quality of supply were evaluated.

In sum, several studies focused on RCM and alternative approaches to evaluate reliability assessment in energy systems, but none of them have considered FMEA as a reliable tool for risk assessment.

1.3 Objectives

In order to study reliability and efficiency performances of a smart grid system, this dissertation will emphasize failure modes impacts on the grid by identifying several failure modes in different smart grid's equipment. Information related to different equipment should be gathered from different sources in order to define a complete report of every weaknesses in a smart grid structure.

Then, identified failure modes allow the conduction of a risk analysis through the application of FMEA methodology by studying failure modes and their respective failure causes and effects in smart grid performance.

Hence, the main purpose of this dissertation is to understand FMEA as a utility tool for reliability analysis, where FMEA must be evaluated as a viable tool for a reliability assessment in modern smart grids.

Finally, this thesis also aims to evaluate FMEA as a feasible solution for the definition of maintenance strategies and optimization of installation and maintenance costs.

1.4 Thesis Outline

The work developed in this dissertation is organized into six different chapters.

In the first chapter, the circumstance that led to the study of reliability analysis in smart grids is presented. Also in this chapter, some works related to the concerned topic are enumerated and briefly explained, and the objectives of this thesis are highlighted.

In chapter two, it is introduced the concept of microgrid as today's smart grids and some projects related to the concerned topic are enumerated. Then, a general characterization of the concept of a smart grid is presented, setting the current energy panorama in the need for technological evolution of the electrical grid.

In chapter three, a special focus is given to the FMEA methodology that will be used to address the problem. The basics of FMEA, including its fundamental concepts, development, implementing procedure and basic terminology, are herein introduced.

The fourth chapter describes the implementation of FMEA in a test system in order to evaluate FMEA methodology in a smart grid reliability study.

In chapter five, it will be presented the most relevant results obtained through the employment of FMEA in a smart grid environment. FMEA methodology and its application in a complex system such as a smart electrical distribution system are discussed.

Finally, a brief conclusion regarding main topics throughout this dissertation is dedicated in the last chapter. A deliberation about the achievement of the proposed objectives in the first chapter will be given, and final conclusions regarding FMEA as a useful tool for risk assessment will be given.

Chapter 2

Smart Grid Definition

In this chapter, a general characterization of the concept of a smart grid is presented, setting the current energy panorama in the need for technological evolution of the electrical grid.

In the first section, a general paradigm of today's smart grids is briefly explained. The concept of microgrid is explored and some recent projects in the field are presented.

In the second section, the definition of smart grid is introduced. The reasons for the need of a smart electrical system are enumerated, as well as technical challenges it has to face in future years are discussed. The two main layers of a smart grid – power and cyber network – are briefly explained.

In the third section, it is given a special focus concerning smart grid security, enumerating vulnerabilities that can compromises correct grid operation.

2.1 Today's Smart Grids

The interest in local connection of distributed electrical resources at the distribution network has gained lots of attention of the industry. Hence, small, modern and interconnected distribution systems – designated microgrids – have been integrated in the traditional distribution network [20].

A microgrid is defined as an interconnected network of distributed energy systems (loads and resources) that can function whether it is connected to or separate from the electricity grid – interconnected or islanded operation mode, respectively.

As shown in Figure 2.1, a microgrid incorporates high penetration of decentralized energy resources in medium or low voltage capable of meeting local demand as well as feeding the unused energy back to the utility grid. It services a variety of loads, including residential, commercial and industrial loads, making use of local and distributed power-storage systems to smooth out the intermittent performance of renewable resources. It also incorporates monitoring equipment such as smart meters and smart appliances capable of communicating their real-time status and accepting commands to adjust and control their performance [6, 20].

The application of energy management appliances and the embodiment of a communication infrastructure that enables system components to exchange information and commands improve efficiency

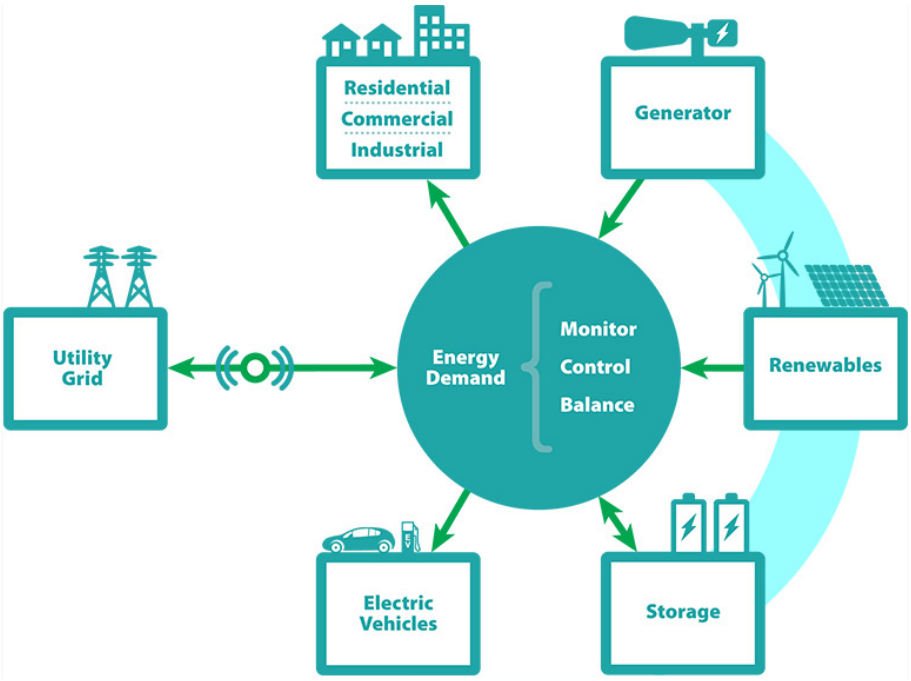

Figure 2.1: Illustration of a Microgrid (from [21])

and reliability comparing to traditional distribution networks, enhancing power quality and security in energy delivery.

Note that not all microgrids will be equally created. The diversity of load, the mix of primary energy resources and distinct geographic areas, among other factors, require different microgrids assets and structures [6].

Recent projects have been developed in order to test and validate their viability and some of them were considered a remarkable case study for testing and validating smart grid concepts.

In Italy, *Enel* implemented one of the first projects concerning smart grids. In operation since 2005, the company designed and manufactured their own meters and developed their own system software, making Telegestore project the first commercial scale grid that makes use of smart grid technology.

The United States of America have funded large smart grid programs, in which ARRA Smart Grid Program stands out. $9 billion were invested in technologies development like advanced metering infrastructures, customer interface systems, distribution and substation automation, cyber security projects, advanced distribution management systems, energy storage systems and renewable energy integration projects. In another projects, in Austin, Texas and in Boulder, Colorado, smart meters were introduced in order to control energy demand by controlling sockets and devices.

In Germany, E-Energy project comprises the creation of several utilities in six independent model regions. In the Netherlands, Bronsbergen Holiday Park is a large-scale project which will create a microgrid by integrating smart grid technologies, services and business cases. Test systems have also been implemented in Japan, in which Sendai Project is one of the well-known microgrid demonstration so far: in operation since 2005, the project achieved microgrid superstardom because of its excellent performance during the 2011 earthquake and tsunami.

Started in 2008, the InovGrid is a project headed by *EDP Distribuição* in the city of Évora, Portugal, with the aim of endowing the distribution network with information and intelligent equipment capable of integrating electrical vehicles and distributed energy resources and stimulating an active consumers participation in energy management through integrated technological platforms. It aspires the improvement of quality of service, as well as the increase of cost-effectiveness and sustainability by reducing grid operation costs and fomenting environmental responsibility and consciousness. InovGrid was part of a European project, the InSmart, whose goal was to replicate in other three cities the same sustainability target. The cities working together were, besides Évora, Cesena in Italy, Nottingham in the United Kingdom and Trikala in Greece.

In the long run, future smart grids are expected to emerge as a well-planned integration of microgrids that will be interconnected through dedicated highways for command, data and power exchange.

2.2 A Smart Grid Brief Description

Smart grid, also known as ”intelligent grid”, ”modern grid” or ”future grid”, is a cyber-physical system capable of integrating an information and communication technology (ICT) network with the existing power system infrastructure. A smart grid is a smarter version of its predecessor, the traditional power grid, which has to face the increased use of digital information and control technologies to improve reliability, security and efficiency of the grid [22].

Smart grid is envisioned to take advantage of all available modern technologies in transforming the current grid to one that functions more intelligently, meaning it has to face some requirements to meet the challenges of the 21st century needs. According to [5], a smart grid should:

- enable active participation by consumers in demand response;
- be self-healing;
- provide quality power that meets current needs;
- operate resiliently against both physical and cyberattacks;
- accommodate all generation and storage options;
- enable new products, services and markets;
- optimize asset utilization and operating efficiency.

The objective of transforming the actual power grid into a more intelligent one is to provide reliable, high-quality electric energy to digital societies in an environmentally friendly and sustainable way.

The transition from a traditional grid to a smart grid will change the design and the operational paradigm of the grid: while actual power grids have central and conventional resources and predictable unidirectional power flows, future smart grids will be characterized by distributed and renewable energy resources, alongside with unpredictable and bidirectional power flows; in a nutshell, a passive grid will

give rise to an active grid. Demand response and consumers participation in electricity markets are expected to play increasing roles in the modern smart grid environment.

In short, the grid will be more dynamic in its configuration and operational conditions, which will present many opportunities for optimization but also many new technical challenges, such as [4]:

- integration of renewable energy: energy from diverse renewable sources, in addition to traditional ones, must be combined to serve customer needs while minimizing the impact on the environment and maximizing sustainability; renewable sources will be found distributed in the grid;
- proliferation of energy storage: numerous energy storage centers must be used to buffer the impact of sudden load changes and fluctuations in renewable resources;
- growth of mobile loads and resources: the increase viability of electric vehicles means many loads and resources will no longer be stationary, which will represent both mobile loads and potential sources of power;
- the smart consumer and the grid-friendly appliance: end-user interactive and intelligent appliances will be able to interact with the grid by collecting and monitor information about consumption patterns, modulating power consumption to reduce stress on the system and to help preventing service disruptions;
- real-time distributed intelligence and a new level of controllability: advanced grid-monitoring, optimization and control applications will continuously monitor the operating conditions of grid assets and determine the best control strategies to maximize energy delivery efficiency and security in real time.

To provide all of these configurations and technical requirements, a smart grid demands the integration of an ICT network capable to autonomously control and operate the grid. These technologies enable the control of power demand and allow an efficient and reliable power delivery at reduced cost. Via digital two-way communications between consumers and control centers, the smart grid system provides the most efficient electric network operations based on the received consumer's information.

This way, the smart grid encompasses complex systems of power, control, sensors, computing and communication with critical interdependent sectors, creating a critical cyber-physical infrastructure.

According to [7], a smart grid must ensure the following requirements in order to reach its purpose:

- Reliability: ensure a high performance of the elements of the system resulting in power being delivered to consumers within accepted standards and in the desired amount;
- Security: withstand sudden disturbances or violations of its operating limits such as electric short circuits or non-anticipated loss of system components;
- Resiliency: recover from a failure after it has occurred;
- Efficiency: operate in the optimal conditions in what concerns of energy production, demand response, market prices, energy storage and electric transportation;

- Flexibility: supply the aggregate power and energy requirements at all times, taking into account the scheduled and unscheduled component outages;
- Survivability: ensure the operation of critical infrastructures even when components of the grid fail.

Figure 2.2 depicts a typical smart grid's cyber-physical structure as a set of correlated interacting layers.

At the bottom level, the physical layer incorporates physical systems and devices which participate in the generation, transmission, distribution and consumption sectors of the grid. At the top level, the cyber layer manages and operates the physical layer, providing local control and computation capabilities through cyber systems and enabling intra and inter-communication between physical and cyber systems [23].

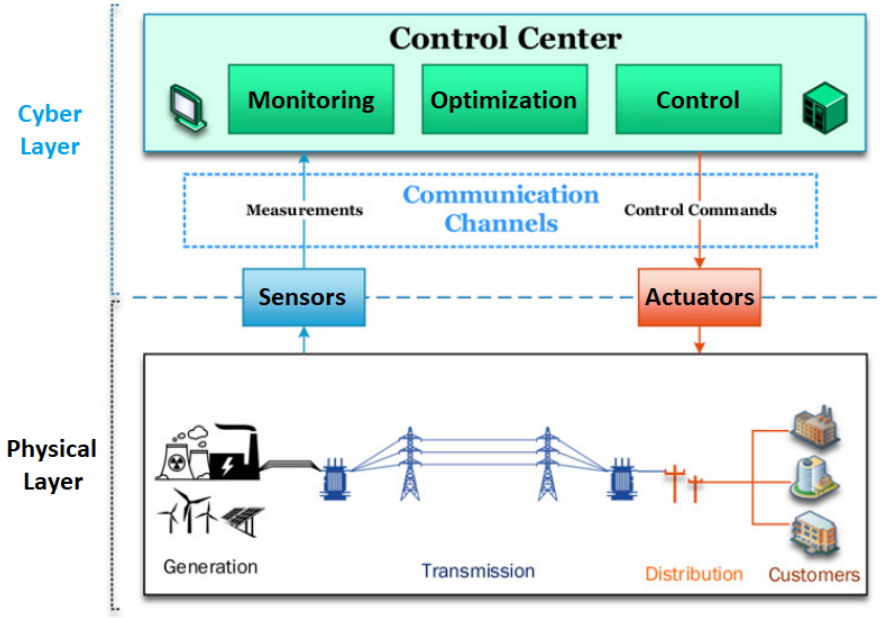

Figure 2.2: Typical cyber-physical structure in a smart grid (adapted from [24])

The physical layer is tightly coupled to the cyber layer. The smart electrical system is this way an integration of (i) electric power equipment responsible for delivering electricity from power generation sources to end-users and (ii) two-way digital communication networks between utilities and consumers that carry out network monitoring and control operations.

Power and cyber network are detailed introduced in the following subsections.

2.2.1 Power Network

The electrical network is an interconnected physical network responsible for delivering electricity from producers to consumers. A power network is usually divided into three hierarchical levels: generation, accountable for electrical power production; transmission, responsible for carrying power from distant sources to demand centers; and distribution, taking charge of connecting individual customers.

A power grid has its own physical laws and limitations due to its inherence. For instance, the power balance at each node and the relation between voltage and power through each line are two fundamental sets of equations that must be considered in a power study. Overloads and abnormal voltages must be avoided to preserve physical network integrity and to guarantee user's security, delivering reliable and stable electricity to customers [25]. Otherwise, possible destructive effects on power network could collapse the system, compromising society's comfort and welfare.

The integration of distributed generation from renewable resources, the proliferation of energy storage facilities and a new level of controllability will change today's electrical grid and new physical constraints will be considered in order to meet society needs.

2.2.2 Cyber Network

The cyber network is an ICT network accountable for performing a wide variety of tasks in order to successfully operate the power system. These tasks consist in monitoring, protecting and controlling the power system, making use of every kind of data collected in all devices [7, 24].

As seen in Figure 2.2, the cyber network is usually divided into two sub-layers: the communication layer, in which grid-status data are gathered in real-time synchronization and information is exchanged between devices; and the control layer, responsible for power system automation and other widespread control systems.

The typical communication framework of a smart grid is usually categorized in three levels: Local Area Network (LAN), Metropolitan Area Network (MAN) and Wide-Area Network (WAN).

In general, home appliances of consumers are connected to LAN, which report their need and usage pattern of electricity in real-time to control and monitor the real-time power consumption. Ethernet, Bluetooth and Wi-Fi are the most popular architectures of LANs, which cover buildings like single homes or shopping stores with limited distances between equipment. LANs are connected to a MAN which, in its turn, covers multiple LANs, substations and distribution systems. Finally, a WAN is a data communication network that covers a wide area and connects multiple MANs and LANs, also comprising power generation sites and transmission. Optical fiber networks are the most famous architectures in use. Thereby, a smart grid relies on wired and wireless communication networks, inheriting both their benefits and security vulnerabilities [26] and [25].

Communication is essential to support different smart grid functions such as self-healing, asset management and wide area integrity. The International Electrotechnical Commission (IEC) 61850 standard allows high-speed Ethernet communication at electrical substations and offers an international standardized configuration language and data model, providing interoperability, reliability and agility in the communication system [27] and [28]. IEC 61850 was designed to operate over modern networking technologies and delivers an unprecedented amount of functionalities and a variety of services which are time-critical and responsible for monitoring and controlling tasks. It provides significant benefits that are not available using legacy approaches such as DNP3 or TCP/IP, making it possible to implement new capabilities while eliminating ambiguities and reducing installation, equipment, commissioning and

integration costs [29].

Besides that, IEC 60870 standard defines communication protocols used for telecontrol – Supervisory Control And Data Acquisition (SCADA) control center application –, which in turn is used for power system automation and other widespread control systems, suiting the requirements for communication between control centers and substations [28].

Along with several benefits communication networks offer to smart grids, they bring the private power control systems to the public communication networks and associated security vulnerabilities [26]. Such a substantial dependence on ICT, alongside with the increasing complexity of the cyber network, require cybersecurity techniques in order to meet cybersecurity requirements.

2.2.3 Cyber-Power Network

Communication networks connect power and cyber layers with robust communication links, which perform two way communication between smart grid domains as shown in Figure 2.3. Electrical flows are also illustrated between power layer's domains.

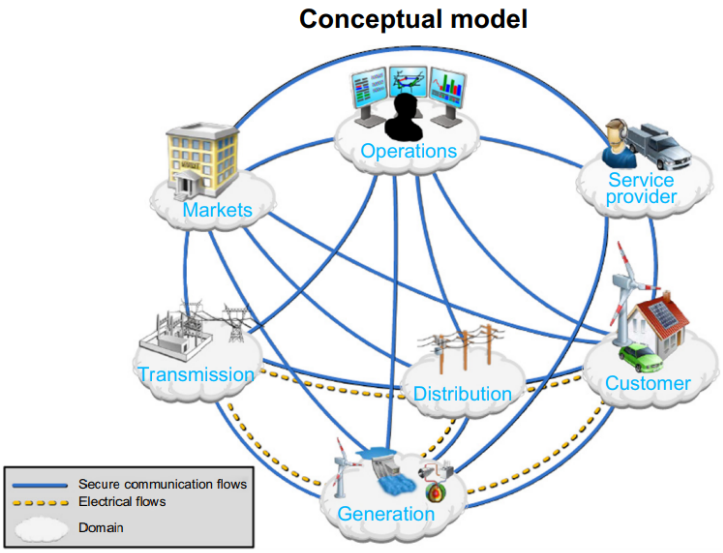

Figure 2.3: Conceptual model for a smart grid (from [30])

The cyber-power network is known as an interconnected network with interdependencies. Interdependency means that the correct and appropriate operation of one element of the grid depends on the existence and proper function of some other elements, whether or not they are part of the same network [31] and [32].

A failure in the cyber network may cause numerous effects on the power network. If taken into account a failure that withdraws from operation a cyber equipment, serious consequences may exist in the grid as far as the failure in a critical cyber equipment affects the appropriate monitoring, protection or control tasks due to the lack of information and/or communication. With this, power outages can possibly occur.

In the reverse direction, a failure in the power network does not affect the correct operation of the cyber network, as long as the cyber network still operates properly. However, if the failure occurs in a power critical component, the operation of the grid is not optimized, and energy may not be correctly delivered as desired.

Therefore, actual interdependencies inherent to the smart grid operation cover element-element and network-element interdependencies, as recognized in [31] as follow:

- Direct Element-Element Interdependency (DEEI): failures in a group of elements in one network either cause the failure or change the behavior of one element in the other network (is always found between cyber and power networks);
- Direct Network-Element Interdependency (DNEI): the performance on one network causes the failure or changes the behavior of the element in other network;
- Indirect Element-Element Interdependency (IEEI): failures in a group of elements in one network do not directly cause the failure or change the behavior of one element in the other network;
- Indirect Network-Element Interdependency (INEI): the performance on one network does not directly cause the failure or change the behavior of the element in other network.

In order to minimize negative effects of cyber-based failures on the power system, cyber network topologies must be optimized [33].

As long as numerous power applications rely upon increasingly complex cyber networks, the probability of failure in a smart grid also increases, and their impact on the power system become a serious concern. In general, the impact of non-ideal communication in the operation of the power grid can be categorized as follows [7]:

- Failure to send the correct control signal to a dispatchable energy resource;
- Failure to send the correct demand response signal to a controllable load;
- Failure to send the correct open/close command to breakers or tie-switches;
- Failure to send the correct measurement values (e.g. voltage, current, active power, reactive power, power factor, etc.) to the control center or any distributed function using those measurements;
- Failure to send the correct status data (e.g. breaker status, capacitor banks status, etc.) to the control center or any distributed function using those data.

In short, wrong operation and deficiency in cyber network applications, such as in control, monitoring and protection tasks, are decisive factors for the degradation of power grid's stability and efficiency, which ultimately may cause massive outages.

Weather conditions can also decrease the performance of the ICT network [7], causing some inherent delays in the communication network, thus in demand response in power applications.

2.3 Smart Grid Security

The vulnerability of future smart grids has been illustrated in today's electric grids, such as recent incidents in the USA and in Ukraine: in PG&E Metcalf Transmission Substation, in 2013, a sniper attack fired on 17 substation's transformers resulting in $15 million worth of equipment damage [34], luckily with little impact on energy supply in Silicon Valley; in this turn, in Ukraine power grid, in 2016, malware was injected from the communication channels and allowed the attacker to obtain illegal access to the control center. With the collected information, the attacker was able to determine critical lines in the regional grid leading to a widespread power blackout affecting 225,000 customers [35].

This clearly shows that knowledgeable attackers can directly exploit vulnerabilities of communication and control systems to exert immediate and significant impacts on the smart grid. Attackers could be elite hackers, terrorists, competitors or even employees or customers acting for different reasons: non-malicious attackers driven by intellectual challenge and curiosity; consumers or employees driven by vengeance; ill-trained employees causing unintentional errors; competitors attacking each other for the sake of financial gains; or terrorists who view the smart grid as an attractive target to affect millions of people making terrorists' cause more visible [36].

The security issues of a cyber-physical smart grid comprise the following issues: the physical components of the smart grid; control centres and control applications; the cyber infrastructures for stable, reliable, and efficient operation and planning; the correlation between cyberattacks and the resulting physical system impacts and protection measures to mitigate risks from cyber threats.

To properly secure the smart grid, it is of utmost importance to: a) understand its underlying vulnerabilities and associated threats, b) quantify their effects, and c) devise appropriate security solutions.

2.3.1 Physical Security

Power systems have inherent physical vulnerabilities. Besides that, the increase of the number of equipment strictly necessary for the correct operation of future smart grids enlarge insecure physical locations, making them vulnerable to physical access. An equipment could be damaged or even destroyed in an attempt to make the service unavailable.

Therefore, it is important to take some countermeasures in order to protect the system against physical attacks. Contingency analysis must evaluate power system security by developing security measures to ensure the survivability of power systems with minimal interruptions in the delivery of electricity.

2.3.2 Cybersecurity

The increasing complexity of the communication network and ICT strictly necessary for the control of a smart grid create new weaknesses in the cyber network. A great number of intelligent devices represents several points for external access in the cyber system, making the smart grid more vulnerable to different types of attacks which can compromise the correct operation of the grid.

There are many possible schemes for cyberattacks, which according to the authors in [7] they can be defined in:

- Device attack: the goal is to take control over a grid device;
- Privacy attack: the goal is to infer a user's private information by analyzing the load data;
- Data attack: the goal is to insert, manipulate or delete data or control commands in the communication network in order to mislead the smart grid controls towards performing wrong actions;
- Network availability attack: the goal is to create communication bottlenecks to overload computational resources in order to generate delays or even failures in the communication network (Denial-of-Service).

Such attacks can occur by malware spreading, false data injection or control system network access through database links. Communication equipment may be compromised, in the sense it can be directly damage or used as a backdoor to launch future attacks. Hence, sensitive information can be obtained and network availability is in danger, since attackers might attempt to delay, block or corrupt information transmission (and affect SCADA for instance) in order to make smart grid resources unavailable.

2.3.3 Cyber-Physical Security

A secure smart grid must combine the strength in both physical and cybersecurity against both inadvertent and malignant events [24]. The major challenges for making a smart grid more robust against physical attacks and more secure against cyberattacks have been widely discussed. A robust cyber-physical network must be able to detect, prevent and eliminate all kinds of external intrusions previously listed so that the smart grid may operate without external interference.

In order to achieve this goal, special focus in cyber-security threats and mitigation approaches have received much attention in the literature recently.

In [37], authors study the impacts of potential adversity based on hypothesized substations outages as the worst case scenario for an external attack event, proposing a new approach for impact analysis of critical cyber assets in substations based on historical load and topology conditions. Reference [38] discusses potential cyberattacks and their impacts on power grid operation and a general SCADA cyber-attack is hypothesized. Authors review major challenges and strategies to protect a smart grid against cyberattacks and propose a conceptual layered framework for protecting power grid automation. In addition, authors in [39] describe a focused literature survey of machine learning and data mining methods for cyber analysis of intrusion detection, recognizing the methods that are the most effective for cyber applications have not been established yet.

One general aspect recognized in every cybersecurity study is the importance of developing strategies to ensure several security requirements in order to protect a smart grid against cyberattacks or at least mitigate their actions. These requirements are listed in [7]:

- Privacy: a customer load data from smart meters should be maintained confidential;

- Availability: attackers cannot perform a denial of service attack or its impact must be mitigated;
- Integrity: data must not be manipulated by unauthorized users;
- Authentication: the identity of communication users must be validated;
- Authorization: unauthorized users cannot access the cyber system;
- Audibility: a system must record all kinds of actions made in the system (keep track of actions history for useful further investigations);
- Non-repudiability: a system must provide irrefutable proof to a third party on who started an action in the system.

If some of the previous security requirements are violated, adverse impacts on power supply can occur, and system's reliability drastically decreases.

On the one hand, data modified from smart meters in LAN communications can usurp collected data tripping the circuit breakers and leading to inadvertent operations in power grid [38] and [40].

On the other hand, in MAN and WAN communications, sensor data could be missed or misrepresented, or external control commands could be injected; data delay could compromise the effectiveness of SCADA, exchanged data between different cyber equipment could be modified and illegal access to price and cost information can occur.

This actions could cause adverse effects on power systems, such as false alarms, Energy Management Systems (EMS) applications failure – like state estimation and contingency analysis – shifting power transmission and distribution system from its optimal running point (non-optimal planning and asset management). The system can run exceeding its own limits and in the worst cases malicious actions leads to system outage and personnel injuries or death [38] and [40].

Since the smart grid is considered a critical infrastructure, all vulnerabilities should be identified and sufficient security strategies must be incorporated in the smart grid system to reduce the risks to an acceptable secure level. They must ensure the availability of uninterrupted power supply according to user requirements, the integrity of communicated information and confidentiality of user's data in order to make a smart grid more reliable.

Chapter 3

Reliability Assessment

In this chapter, it is introduced RCM methodolody as a reliability assessment application for risk analysis and maintenance strategies.

The importance of risk analysis in RCM is emphazised and FMEA is presented as a useful tool in the identification of failure modes in a system, in the sense that it allows the recognition of possible failure causes and studies their effects on system performance.

The basics of FMEA, including its fundamental concepts, development, implementing procedure and basic terminology, are finally introduced.

3.1 The RCM Approach

The RCM methodology is a systematic approach which determines maintenance requirements of a system or equipment in its operation with the aim of increasing cost effectiveness, reliability and a greater understanding of the level of risk of the analyzed system [41] and [16].

First adopted in 1978 in *Reliability-Centered Maintenance* to determine the optimum maintenance requirements in the aeronautic industry, F. Stanley Nowlan and Howard F. Heap took a different approach from maintenance methodologies at that time by developing a maintenance strategy based on system functions, consequence of failure and failure modes, in addition to the existing preventive maintenance techniques. This new approach combined proactive maintenance techniques, based on preventive maintenance in order to avoid the failure of an equipment or system or at least to decrease its probability of failure, and reactive techniques, related to maintenance techniques implemented after a failure occurs.

Nowadays, RCM integrates Preventive Maintenance (PM), Predictive Testing and Inspection (PTI), Repair (also called Reactive Maintenance (RM)) and Proactive Maintenance (PrM) to increase the probability a system or component will function in the desired manner over its design life-cycle with a minimum amount of maintenance and downtime.

PM consists of regularly scheduled inspections, adjustments, cleanings, lubrication and replacement of components and equipment, performed without regarding equipment condition. PM is also referred to as time-driven or interval-based maintenance since it schedules inspection and maintenance at prede-

fined intervals in an attempt to reduce equipment failures. PTI uses non-intrusive testing techniques to measure and trend equipment performance, replacing arbitrary timed maintenance tasks with scheduled maintenance only when warranted by equipment condition (with the help of real-time monitoring). In its turn, RM assumes that a failure is equally likely to occur in any part, and may ignore opportunities to influence equipment survivability. Finally, PrM is responsible for redesign the system or equipment in order to mitigate the failure.

Rather than being applied independently, these maintenance strategies are integrated to take advantage of their respective strengths in order to reduce the life-cycle cost to a minimum while continuing to allow the facility to function as intended with the required reliability and availability [41]. The components of RCM are shown in 3.1:

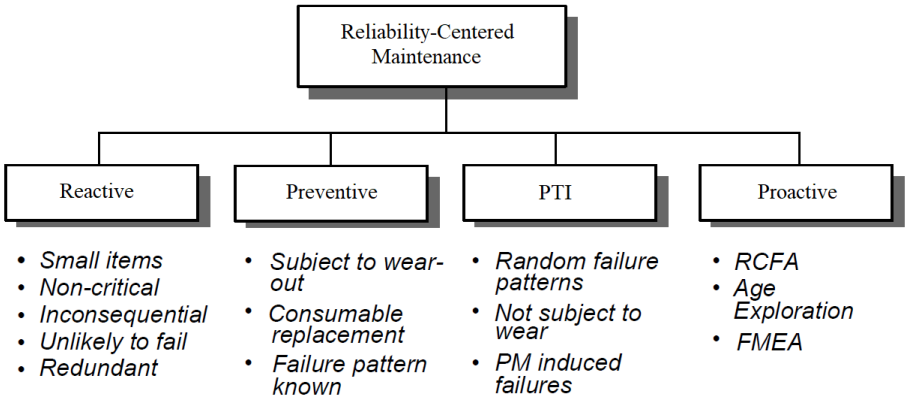

Figure 3.1: RCM methodology (from [16])

As stated by Nowlan and Heap, RCM objective is to ensure realization of the inherent safety and reliability levels of the system. If a deterioration occurs, RCM provides methodologies to restore the system to the inherent levels, and obtains the necessary information for design improvement of those items where their reliability proves to be inadequate.

The goal is to determine the most applicable cost-effective maintenance strategy (related to maintenance costs, support costs and economic consequences of operational failures) to minimize the risk of impact and failure and to create an hazard-free environment. To answer to this goal, RCM analysis carefully considers the following questions:

- What does the system or equipment do; what are its functions?
- What functional failures are likely to occur?
- What are the likely consequences of these functional failures?
- What can be done to reduce the probability of the failure, identify the onset of failure, or reduce the consequences of the failure?

RCM programs can be implemented and conducted in several ways and use different kinds of information, depending in which system RCM is applied. RCM output is a complete maintenance strategy

to ensure the inherent reliability of the equipment or system in the sense that RCM uses a structured decision process to determine a task to eliminate, detect, decrease the frequency of occurrences or the consequence of a specific failure mode.

A technique for risk analysis and for proactive maintenance that can be implemented in RCM is FMEA, which is a qualitative technique for reliability assessment and risk analysis. This approach is introduced in section 3.2.

3.2 FMEA Methodology

Failure Mode and Effect Analysis (FMEA), first developed in the 1960s by aerospace industry, is a systematic methodology designed to identify known and potential failure modes, their causes and effects on system performance [17] and [42].

In other words, FMEA is a proactive procedure for evaluating a process by identifying where and how it might fail and assessing the relative impact of different failures [43].

This methodology allows the identification of parts of the process that are most in need of repair and maintenance so that it is possible to carry out corrective actions for the most serious issues to enhance the reliability and safety of the analyzed system. FMEA aims to mitigate risk of a failure mode through a recommended action, without necessary elaborating a maintenance task. FMEA can be performed in the design phase of a project, in the hope of assessing risks and improving the reliability of the asset by optimizing the design of the system.

FMEA assigns a numerical value, in a qualitative way, to each risk associated with a causing failure, taking into account the risk factors for occurrence (OCC), severity (SEV) and detection (DET), and subsequently prioritizes the actions needed to counteract or avoid these failures. The line-up of failure modes in FMEA is determined by a risk priority number (RPN), made by the arithmetic product of the previous risk factors, as expressed in (3.1):

$$RPN = OCC \times SEV \times DET. \tag{3.1}$$

The higher the RPN of a failure mode, the greater the risk is for the system reliability. Proper actions should be preferentially taken on the high-risk failure modes so that the system should increase its performance.

An example of a FMEA worksheet can be consulted in Appendix A.

3.2.1 The Procedure of FMEA

In order to carry out an FMEA effectively, a systematic approach should be followed. FMEA is a dynamic document which suffers constant changes, always with the intent to make a deeper evaluation of the analyzed system. The general procedure for conducting an FMEA is shown in the flow chart of Figure 3.2 and is briefly explained in the following steps [17]:

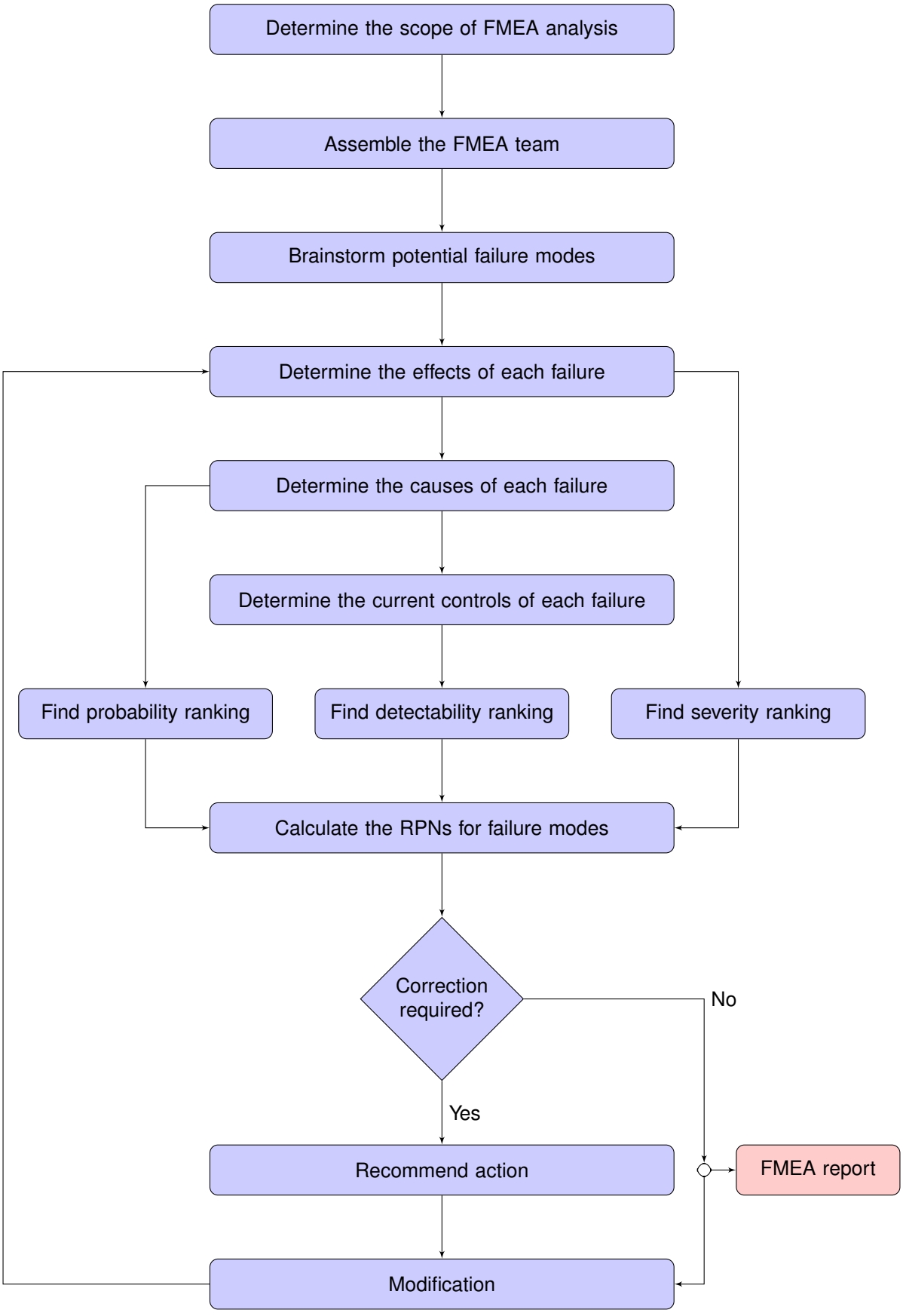

Figure 3.2: FMEA procedure (from [17])

- step 1: determine the scope of FMEA analysis in order to define boundaries approaches that are to be considered during the analysis;
- step 2: assemble the FMEA team in order to be cross-functional and multi-disciplined, forming a line-up of subject matter experts from a variety of disciplines with knowledge of the problem to be discussed;
- step 3: understand the problem to be analyzed by dividing the system into subsystems and/or assemblies and use schematics and flowcharts to identify components and relations among components;
- step 4: brainstorm failure modes that could affect the system quality and identify their causes and potential effects on the system;
- step 5: determine OCC, SEV and DET for failure modes and calculate their RPN;
- step 6: prioritize failure modes by ranking them in terms of the RPNs for preventive actions and recommend actions for the high-risk failure modes in order to eliminate them, increasing failure detectability and minimizing losses in the event a failure occurs;
- step 7: prepare FMEA report by summarizing the analysis results;
- step 8: calculate the revised RPNs as the failure modes are reduced or eliminated once the recommended actions have been taken to improve the system.

3.2.2 The Terminology in FMEA

Some of the terms commonly used in FMEA are introduced below. The definitions of terms used herein are in accordance with the definitions used in [17]:

- **Function:** task that the system, process or component must perform;
- **Failure mode:** manner in which a failure occurs; the way in which a component could fail to perform a required function;
- **Failure cause:** cause or sequence causes that initiate a process that leads to a failure mode over a certain time;
- **Failure effect:** adverse consequence of a failure in terms of the operation, function or status on a system. It can be addressed from two points of view: the first one is local, in which the failure is isolated and does not affect anything else so that it is considered the impact on a system element under consideration; the second one is global, in which the entire system is considered for the effect analysis;
- **Occurrence:** frequency that a root cause is likely to occur;
- **Severity:** magnitude of the end effect of a system failure;

- **Detection:** likelihood of not detecting a root cause before a failure can occur;
- **Recommended actions:** specific actions that can be implemented to reduce or eliminate the risk associated with a potential cause of each failure mode.

Note that the definitions of failure mode, failure cause and failure effect depend on the level of analysis and failure criteria. It is important to follow a constant evaluating pattern while doing the FMEA analysis.

3.2.3 FMEA ranking system

Ratings of OCC, SEV and DET are divided in a numerical representation, in a ranking system usually from 1 to 10 (or 5) in order to represent the risk level of a given failure, according to the respective rating.

In this dissertation, ratings are classified according to [17] which are portrayed in Tables 3.1, 3.2 and 3.3:

Table 3.1: Traditional ratings for occurrence (OCC) of a failure mode

Rating	Probability of failure	Possible failure rate
10	Extremely high	$\geq$1 in 2
9	Very high	1 in 3
8	Repeated failures	1 in 8
7	High	1 in 20
6	Moderately high	1 in 80
5	Moderate	1 in 400
4	Relatively low	1 in 2000
3	Low	1 in 15,000
2	Remote	1 in 150,000
1	Nearly impossible	$\leq$1 in 150,000

Table 3.2: Traditional ratings for severity (SEV) of a failure mode

Rating	Effect	Severity of effect
10	Hazardous without warning	Highest severity ranking of a failure mode, occurring without warning, and consequence is hazardous
9	Hazardous with warning	Higher severity ranking of a failure mode, occurring with warning, and consequence is hazardous
8	Very High	Operation of system or product is broken down without compromising safe
7	High	Operation of system or product may be continued, but performance of system or product is affected
6	Moderate	Operation of system or product is continued, and performance of system or product is degraded
5	Low	Performance of system or product is affected seriously, and the maintenance is needed
4	Very low	Performance of system or product is less affected, and the maintenance may not be needed
3	Minor	System performance and satisfaction with minor effect
2	Very minor	System performance and satisfaction with slight effect
1	None	No effect

Table 3.3: Traditional ratings for detection (DET) of a failure mode

Rating	Detection	Criteria
10	Absolutely impossible	Design control does not detect a potential cause of failure or subsequent failure mode, or there is no design control
9	Very remote	Very remote chance the design control will detect a potential cause of failure or subsequent failure mode
8	Remote	Remote chance the design control will detect a potential cause of failure or subsequent failure mode
7	Very low	Very low chance the design control will detect a potential cause of failure or subsequent failure mode
6	Low	Low chance the design control will detect a potential cause of failure or subsequent failure mode
5	Moderate	Moderate chance the design control will detect a potential cause of failure or subsequent failure mode
4	Moderately high	Moderately high chance the design control will detect a potential cause of failure or subsequent failure mode
3	High	High chance the design control will detect a potential cause of failure or subsequent failure mode
2	Very high	Very high chance the design control will detect a potential cause of failure or subsequent failure mode
1	Almost certain	Design control will almost certainly detect a potential cause of failure or subsequent failure mode

3.3 Failure Rate

Failure rate, denoted by λ, is the frequency in which an engineering system or component fails, expressed in failures per unit of time. The failure rate of a system usually depends on time, with the rate varying over the life cycle of the asset. The failure rate λ is expressed as (3.2), where Nf is the number of failures and Δt is the period of time:

$$\lambda = \frac{\text{Nf}}{\Delta t}. \tag{3.2}$$

Failure rate is often reported in Mean Time Between Failures (MTBF), whose value is denoted by (3.3), which is valid when the failure rate is assumed to be constant (see 3.3.1).

$$\lambda = \frac{1}{\text{MTBF}} \tag{3.3}$$

Sometimes, failure rate is indicated in annual failure rate (AFR) in order to illustrate the expected number of failures in one calendar year. This way, failure rate can be defined as in (3.4):

$$\lambda = \frac{\text{AFR[\%]}}{100} \tag{3.4}$$

3.3.1 The Bathtub Curve

The bathtub curve is the most common term used in reliability engineering to describe a particular evolution of the failure rate of a engineering system or component over time. The term ”bathtub” is used due to the shape of a bathtub form, which is a combination of a decreasing hazard of early failures, a

constant hazard of random failures and an increasing hazard of wear-out failures. This way, this type of hazard function can be characterized by three distinct parts, as presented in Figure 3.3:

- a first part, characterized by early or infant-mortality failures, where failure rate decreases over time as defective parts of a system or a component are identified and discarded or installation errors are rectified;
- a second part, known as random or constant failures, where failure rate remains low and quasi-constant during system or component useful life;
- a third part, known for the increasingly possibility of wear-out failures as the system or component exceeds its design lifetime, where failure rate increases.

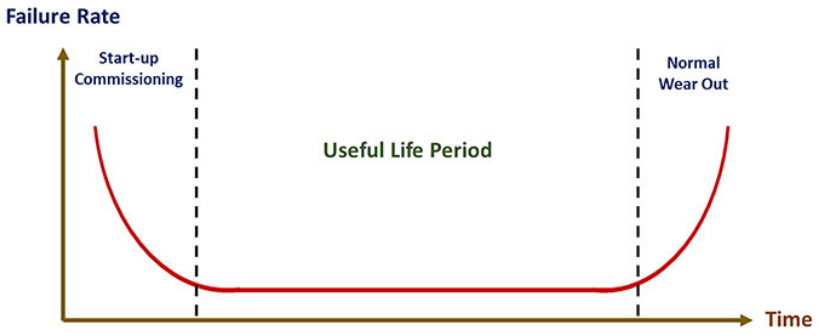

Figure 3.3: The bathtub curve [44]

Note that (3.3) is only valid for the flat region of the bathtub curve (as explained in section 3.3).

Power and cyber equipment are usually characterized by failure rates which behave in accordance with the bathtub curve.

For the purpose of this thesis, and bearing in mind the equipment which will be used in this dissertation for the FMEA analysis, future references of failure rate values will only refer to the useful life period of an equipment, thus when failure rate remains constant in time [45].

Chapter 4

FMEA Implementation

This chapter describes the implementation of FMEA in a test system in order to evaluate FMEA methodology in a smart grid's risk assessment study.

A case study is developed in order to demonstrate the application of FMEA in reliability analysis in a smart grid. The aim is to evaluate the impact of risks in the reliability analysis by identifying the source of failure of each equipment.

FMEA will be applied to each equipment taking into account the different manners in which a failure occurs, as described in section 4.2. Failure rates specified in Tables 4.1 and 4.3 will be partitioned and distributed according to each equipment's failure modes.

4.1 Description of the Test System

In order to evaluate the reliability of a smart grid using FMEA analysis, a test system is defined. The test system is designed in order to simulate a simple model of a smart electrical system. The assessment of failure rates for each equipment is a key issue.

4.1.1 Power Network Test System

Figure 4.1 presents the model of the 30kV simplified power distribution network considered for the test system.

The power network is a meshed grid consisted of four 30kV substations. One has admitted each bus is connected to each other through single 30kV aerial cables, this way with no redundancy. A 110MW conventional generation station is connected to B1, while distributed generation stations are referred to B2 and B4 – 130MW wind and 100MW solar energy, respectively. B3 is linked to a 50MW energy storage technology. Cables between generation or storage stations and the respective substations are ignored since they are of minimal length compared with the network. A total of four transformers and fifteen circuit breakers are also included in the grid.

Customers are referred as three load points LPB2, LPB3 and LPB4, in BUS2, BUS3 and BUS4, respectively. LPB2 is a 20MW residential area, while LPB3 and LPB4 are industrial and commercial areas

referred as 85MW and 40MW load points, respectively. These load points are illustrated as distribution feeders that represents the total customers connected to the grid.

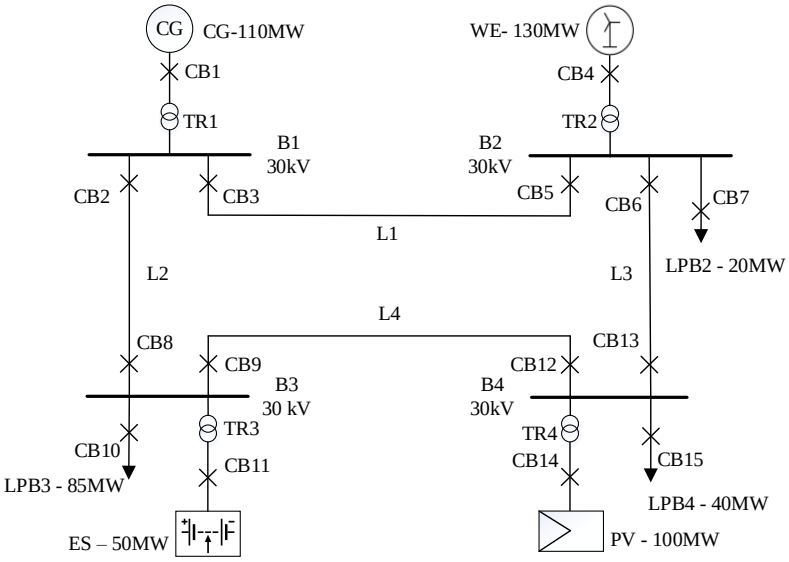

Figure 4.1: Power network test system

In this power test system, only bus bars, cables (aerial lines), circuit breakers (CB) and transformers are considered for reliability analysis. Storage facility and generation stations were not regarded into this reliability analysis, since it was considered that their failures don't compromise system's operation.

Failure rates for each component have been collected from different sources. Power components' reliability data is found in Table 4.1.

Note that related to aerial cables, and for simplification purposes, it was defined different substations are equally distanced between each other – about 2,5km.

Table 4.1: Power equipment's reliability data

Equipment	Failure rate [(f/yr)/km]	Length [km]	Failure rate [f/yr]	Source
Bus bar 30kV	-	-	0,01	[46]
Cable 30kV	0,054	2,5	0,135	EDP Distribuição
Circuit Breaker 30kV	-	-	0,023	EDP Distribuição
Transformer	-	-	0,01	EDP Distribuição

4.1.2 Cyber Network Test System

In order to create a smart electrical system, in Figure 4.2 a scheme of a communication network topology to integrate the power system defined in subsection 4.1.1 is proposed. Among all possible cyber network topologies, a cyber-ring topology was defined for the test model due to its elementary architecture.

The cyber-control network is a bus topology LAN-Ethernet and WAN-optical fiber network consisted

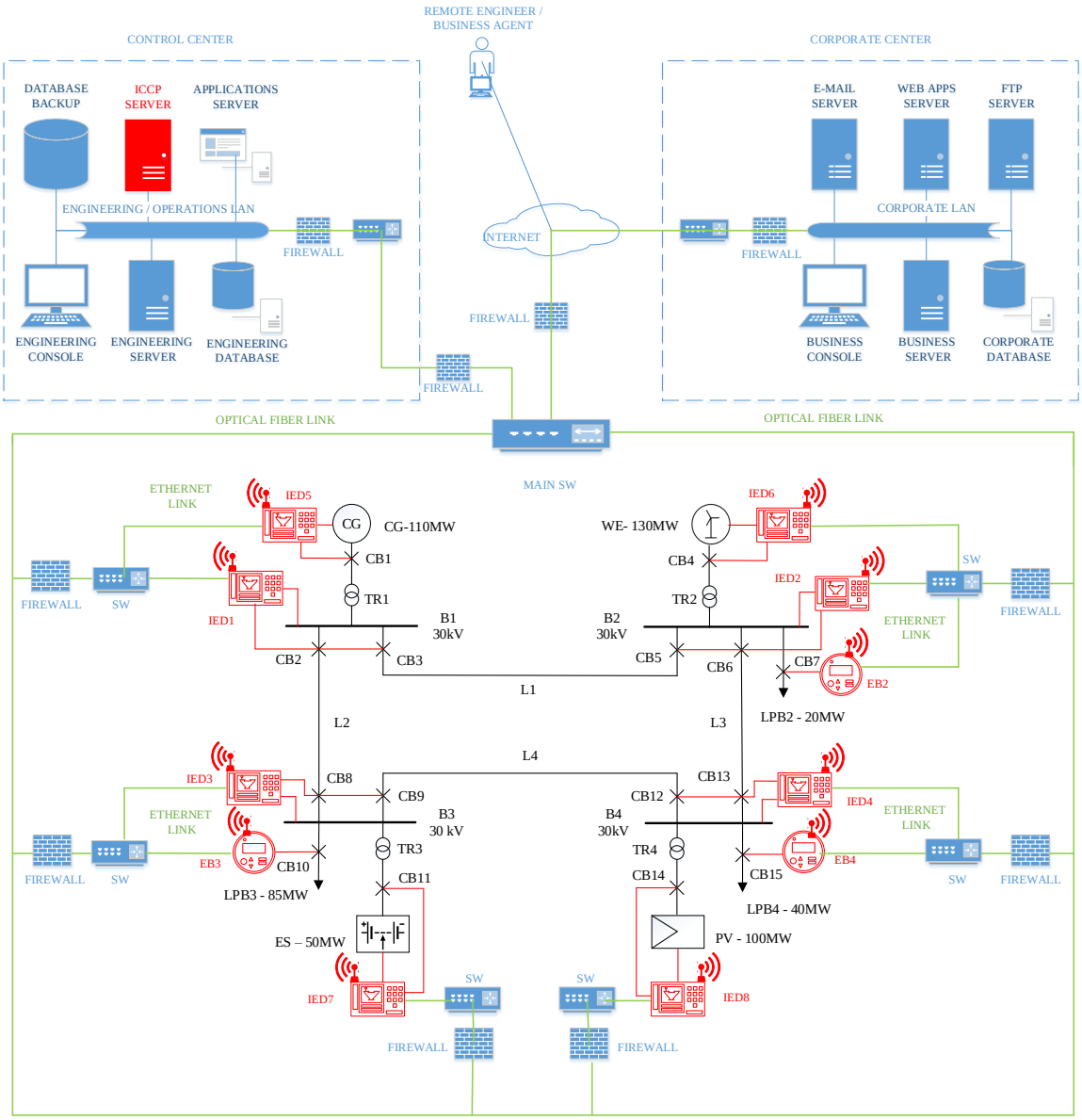

Figure 4.2: Cyber-Power network test system

of human-machine interfaces (HMIs), Ethernet switches (SWs), servers (SVs), energy boxes (EBs) – also designated as smart meters –, intelligent electronic devices (IEDs) and Ethernet and optical fiber links.

IEDs, acting as interface devices between power and communication network, include measuring units, protective relays and controllers. Each IED is responsible for monitoring, controlling and optimizing the effective utilization of energy between generation and load. It also applies the commands received from HMIs.

Cyber-power links between individual IED controllers and their corresponding power elements are given in Table 4.2.

Metering infrastructures, such as EBs (also called smart meters) are linked to load points in order to collect data concerning energy consumption. Note that it is assumed each customer is connected to a

Table 4.2: Cyber-power links between power and cyber network

Link	Linked Equipment
1	IED1:B1, IED1:CB2, IED1:CB3
2	IED2:B2, IED2:CB5, IED2:CB6
3	IED3:B3, IED3:CB8, IED3:CB9
4	IED4:B4, IED4:CB12, IED4:CB13
5	IED5:CG, IED5:CB1
6	IED6:WE, IED6:CB4
7	IED7:ES, IED7:CB11
8	IED8:PV, IED8:CB14

single EB, and in the model a general EB represents the whole EBs connected to the load point.

Each IED or EB is connected to a SW through a LAN-Ethernet communication which is responsible for redirecting information through the corresponding communication links. They are connected to each other through a ring topology towards WAN-optical fiber network links. A main SW is responsible for gathering information from all points of the communication network and send it to the corporate and control center.

In the control center, all data concerning power system status can be assessed and monitored. The control center is responsible for scheduling power generation to meet customer demand and for managing major system problems by executing manual instructions through the HMIs. Real-time data gathered from the power system are also displayed on the HMI allowing intelligent data handling and network status monitoring in real-time. The Inter-Control Center Communications Protocol (ICCP) server is specified to provide data exchange over WANs between utility control centers and substations. An applications server and an engineering server manage a large amount of data and information, which are stored in an engineering database, in order to efficiently operate the power system in a safer and more reliable and cost-effectiveness way.

The corporate center is responsible for managing a large number of markets which will compete with each other to provide the best power quality at the best price. Cost fluctuations on energy generation (due to different penetration levels of distributed generation and dynamic energy demand) are managed in the business server in order to optimize cost effectiveness operations and the balance between energy demand, storage and production. A corporate database is responsible for collecting and storing all markets information in the corporate center, while e-mail, web apps and File Transfer Protocol (FTP) servers make it accessible for all market stakeholders.

Table 4.3 summarizes the cyber equipment' data for the test system. The given values correspond to failure rate data found in some data sheets and reliability statistics and obtained using (3.2), (3.3) and (3.4). For Ethernet links, reliability data was not found. One has supposed it has a very low failure rate. Related to optical fiber links, it was supposed it has a total length of 10km in the communication network.

Table 4.3: Cyber-control equipment's reliability data

Equipment	MTBF [h]	AFR [%]	Failure rate [(f/yr)/km]	Failure rate [f/yr]	Source
HMI	50.000	-	-	0,172	EKE-Electronics
SW	390.190	-	-	0,0225	Cisco
SV	-	2,07	-	0,027	Backblaze
IED	166.440	-	-	0,0526	Schweitzer Engineering Laboratories
EB	-	0,5	-	0,005	Frontier Economics
Ethernet Link	-	-	-	$\leq$1E-6	-
Optical fiber Link	-	-	0,0044	0,0438	[47]

Sources: EKE-Electronics [48], Cisco [49], Backblaze [50], Schweitzer Engineering Laboratories [51], Frontier Economics [52]

4.2 Definition of Failure Modes

The application of the FMEA technique comprises the definition of failure modes that can be triggered in a given system, in order to evaluate their causes of failure and their impacts on the system.

This way, a study on potential failure modes of each equipment is going to be performed in this section.

Equipment are first categorized according to their type and a brief definition concerning their function in the test system is given. It is important to know their role in the smart grid operation so that the identification of failure modes and their impact in the grid may be studied.

For each equipment, several failure modes are finally defined and herein briefly described.

4.2.1 Failure Modes for Power Equipment

With respect to the power equipment, the following items describe the main function of each equipment:

- Bus: collect electric energy from the incoming feeders and distribute them to the outgoing feeders;
- Cable: carry load and fault current safely and reliably, without overheating or causing damage to the environment;
- Circuit Breaker: protect an electrical circuit from damage by interrupting current flow after a fault detection;
- Transformer: step up or step down voltage and provide a secondary output voltage which is within statutory limits.

The collection and selection of several failure modes for power equipment are presented below in more detail:

- Bus
  - Loss of structural integrity: the metallic strip can lose its mechanical integrity due to support insulators breakdown, cracking of welds and fracture of the copper bar;
  - Loss of electrical continuity: the occurrence of arc flashes degrades the copper bar;
  - Loss of electrical efficiency: moisture and humidity can lead to short circuits;
  - Electrical operation failure: short circuits between buses and harmonics can lead to ohmic heating.
- Cable
  - Insulation failure: the ageing process results in the eventual failure of the insulating and sheating materials;
  - Cable integrity defect: manufacturing imperfection, incorrect installation or hostile environments can result in cable breakdown;
  - Electrical operation failure: moisture, shield damage, overloads or short circuits can damage the cable.
- Circuit Breaker
  - Insulation failure: loss of dielectric properties can damage the CB;
  - Wrong operation: improper parameterization or manual installation leads to spurious opening or closures;
  - Bushing breakdown: lightnings or external short circuits can damage the bushing;
  - Bushing terminal hotspot: moisture can increase ohmic resistance in bushing terminals, resulting in bushing damage;
  - Loss of dielectric strength in bushings: heat, oxidation, acidity and moisture can lead to bushing degradation;
  - Mechanical failure in operating mechanism: lack of lubrification, contamination or corrosion prevent CB from acting when necessary;
  - Contacts degradation: contact wear and electrical treeing can damage the equipment.
- Transformer
  - Bushing breakdown: lightnings or external short circuits can damage transformers bushings;
  - Bushing terminal hot spot: moisture can increase ohmic resistance in bushing terminals, resulting in bushing damage;
  - Loss of dielectric strength in bushings: heat, oxidation, acidity and moisture can lead to bushing degradation;
  - Magnetic-core delamination: harmonics or corrosion can induce core degradation;

  - Tap changer mechanical failure in drive mechanism: corrosion, friction or contamination can lead to transformer unstable operation;
  - Tap changer contacts degradation: contact wear and electrical treeing can lead to transformer unstable operation;
  - Tank rupture: vibration-induced damage, corrosion or cracking of welds result in oil leakage and possible catastrophic event;
  - Windings isolation degradation or breakdown: oil contamination, oil moisture or short circuits and overloads can damage transformer windings;
  - Distortion, loosening or displacement of the windings can lead to short circuits;
  - Transformer explosion: internal short circuits or human sabotage can lead to catastrophic events;
  - Cooling system failure: damaged fans or cooling pipes obstruction can also lead to catastrophic events;

4.2.2 Failure Modes for Cyber-Control Equipment

Related to the cyber-control equipment, their functions in the communication network is described below:

- IED: to monitor, control and optimize the effective utilization of energy between generation and load;
- SV: to provide functionality for other programs and centralize grid information;
- HMI: to manually monitor and control the grid;
- SW: to centralize communications among multiple connected devices and select paths to transfer information through network connections;
- EB: to record and communicate electric energy consumption;
- optical fiber link: to assure the connection between two cyber equipment in long distances.
- ethernet link: to assure the connection between two cyber equipment in short distances.

In cyber network equipment, common failure modes were assigned to all equipment unless network links:

- HMI, SW, SV, EB and IED
  - Security failure: related to the susceptibility of cyber equipment to lose their integrity;
  - Power failure: related to the remote disconnection of power which affects the normal operation of cyber network.

Specific failure modes for each of the previous equipment are now enumerated:

- HMI
  - Operational failure: related to inherent problems in the HMI operation that compromises its function.
- SW
  - Performance decrease: congestion of packets in communication network can decrease the SW operational performance;
  - Operational failure: inherent problems in SW configuration or module failure can blackout the SW;
  - Network/Cyber storm: broadcast of excessive amount of messages in uncontrollable way can congestion SW operation.
- SV
  - Data overload: lower storage capacity or unexpected large amount of data to storage results in defective data storage;
  - Hardware crash: physical damage, overheating, humidity or hard drive crash result in loss of data;
  - Data error: inherent software errors can corrupt storaged data.
- EB
  - Communication error: poor signal with SV leads to no transmission data;
  - Power consumption misreading: manual manipulation or significant measurement error lead to incorrect data acquisition;
  - Operational failure: improper EB programming or defective installation result in incorrect data acquisition;
  - Catastrophic failure: temperature stress can severely damage the EB.
- IED
  - Defective communication: damaged transducers or poor signal can lead to poor communication between IED and remaining cyber-network;

Related to network links, two types were considered: optical fiber links, for communications in long distances, and Ethernet links, for short distances. Their inherent characteristics result in different failure modes:

- Ethernet link
  - Cross talk: excessive traffic of packets results in congestion and overload of data;

  - Integrity defect: manufacturing imperfection, incorrect installation or RJ45 degradation results in delays in data transmission, or even its interruption;
  - Link breakdown: cable breakdown due to external physical damage.

- Optical fiber
  - Fracture: stress, corrosion or fatigue can lead to microcracks, resulting in cable breakdown;
  - Lead-bonds degradation: temperature stress can damage in plated contacts;
  - Humidity induced: electro-chemical oxidation in transmitters and receivers

4.3 Application of FMEA

A study on the function of each power and cyber equipment in the operation of the smart grid and their inherent failure modes had been studied in the previous section (see section 4.2).

In section 2.2, it was introduced the smart grid as a complex and robust cyber-physical infrastructure able to incorporate power system, control appliances, sensors and ICTs. As also illustrated in subsection 2.2.3, this means a failure in a given equipment can affect the operation of other equipment and possibly the correct operation of the grid.

Therefore, in order to understand failure modes' impacts on the system, interdependencies between cyber-cyber, cyber-power and power-power must be examined.

The impact of cyber-physical intrusions, as demonstrated in section 2.3, must also be taken into account.

A FMEA report is presented in Table 4.4, in which an analysis of predictable impacts on the system as an effect of identified failure causes is evaluated.

Failure consequences are measured in: a local perspective, where the impact of a failure is locally evaluated considering the impact on the system element under consideration; and in a system's perspective, where the implications of given failures are globally inspected at the entire system.

In order to evaluate the likelihood of detecting a root cause, detection methods are also enumerated for each specific cause of failure.

Table 4.4: Failure modes, effects analysis and detection methods for the test system

Equipment	Function	Failure Mode(s)	Failure Cause(s)	Failure Effect(s)		Detection method
				Local Effect(s)	System Effects(s)	
Bus bar	Collect electric energy from the incoming feeders and distribute them to the outgoing feeders	Loss of electrical efficiency	Moisture, Humidity	Short circuits	Short circuits; decrease of power quality	Visual inspection
		Loss of structural integrity	Fracture of the copper bar	Bus bar break; no electrical connection	No energy supply from the faulty bus; possible unstable conditions in the power system	Infrared thermographic scanning
			Break of the support insulators			Infrared thermographic scanning
			Human sabotage			Physical surveillance
			Cracking of connection welds			Infrared thermographic scanning
		Loss of electrical continuity	Arc flash	Degradation of the physical structure	Possible unstable conditions in the power system; decrease of power quality	Infrared thermographic scanning (not the best solution)
		Electrical disturbances	Short circuits between bus bars	Short circuits	Short circuits; decrease of power quality	Power relays detection, signal analysis
			Harmonics	Increase of energy losses	Decrease of power quality	Signal analysis
			Ohmic heating (overload)			Signal analysis
Cable	Carry load and fault current safely and reliably, without overheating or causing damage to the environment	Insulation failure	Insulation aging	Short circuits	Grid operation outside of the optimal operating conditions; short circuits	Electrical test
		Cable integrity defect	Manufacturing imperfection	Decrease of power quality; no energy supply	Grid operation outside of the optimal operating conditions; power quality decrease; no energy supply from the faulty cable; short circuits; loss of efficiency	Electrical test and quality assessment
			Incorrect installation	Decrease of power quality; no energy supply		Visual inspection
			Lightnings	Excessive heat (saturation); line jumping; cable breakdown		Weather monitoring
			Cable breakdown (human sabotage)	Line jumping; cable breakdown		Weather monitoring

Equipment	Function	Failure Mode(s)	Failure Cause(s)	Failure Effect(s)		Detection method
				Local Effect(s)	System Effects(s)	
Cable (cont.)		Electrical operation failure	Overload	Excessive heat (saturation)	Grid operation outside of the optimal operating conditions; loss of efficiency; decrease of power quality	Electrical monitoring
			Short circuits transients			Power relays detection, signal analysis
			Shield damage	Loss of efficiency		Current signal analysis
			Moisture	Decrease of volume resistivity and dielectric strength in XLPE insulation		Visual inspection, electrical tests
CB	Protect an electrical circuit from damage; interrupt current flow after a fault is detected	Insulation failure	Loss of dielectric properties	Inability to open and/or close circuit with fault currents	Possible damage in other equipment; concerns about physical securities; grid operation outside of the optimal operating conditions	Electrical test
		Wrong operation (Spurious opening and closure)	Improper manual installation	Spurious or improper opening or closure; power quality decrease	Possible downstream grid disconnection; possible damage in other equipment; power system instability; power quality decrease	Inspection after installation
			Improper sizing			Visual inspection, operational test
			Overload	Wrong current cut	Possible downstream grid disconnection; power system instability	Signal analysis
		Bushing breakdown	Lightning	Phase to ground internal fault	Possible damage in other equipment; concerns about physical securities; grid operation outside of the optimal operating conditions	Weather monitoring
			External short circuit			Power relays detection, signal analysis
		Bushing terminal hot spot	Heat, oxidation, acidity and moisture	CB damage ; inability to open and/or close circuit with fault currents	Possible damage in other equipment; concerns about physical securities; grid operation outside of the optimal operating conditions	Periodic visual inspection
			Mechanical stress due to external short circuit conditions			Operational test
		Loss of dielectric strength in bushings	Heat, oxidation, acidity and moisture	Short circuits to ground; CB damage; inability to open and/or close circuit with fault currents	Possible damage in other equipment; concerns about physical securities; grid operation outside of the optimal operating conditions	Sensors for leakage currents, power factor and capacitance tests

Equipment	Function	Failure Mode(s)	Failure Cause(s)	Failure Effect(s)		Detection method
				Local Effect(s)	System Effects(s)	
CB (cont.)		Mechanical failure in operating mechanism	Corrosion	Inability to open and/or close circuit with fault currents	Possible damage in other equipment; concerns about physical securities; grid operation outside of the optimal operating conditions	Visual inspection, operational test
			Dirt/contamination			Visual inspection, operational test
			Lack of lubrication			Visual inspection, operational test
		Contacts degradation	Contact wear	CB damage; inability to open and/or close circuit with fault currents	Possible damage in other equipment; concerns about physical securities; grid operation outside of the optimal operating conditions	Visual inspection, operational test
			Electrical treeing (partial discharges)			Infrared thermographic scanning
Transformer	Step up or step down and provide a secondary output voltage which is within statutory limits	Bushing breakdown	Lightning	Phase to ground internal fault; transformer damage	Decrease of power quality; wrong output power; short circuits in power network	Weather monitoring
			External short circuit			Power relays detection, signal analysis
		Bushing terminal hot spot	Heat, oxidation, acidity and moisture	Internal short circuits; transformer damage	Decrease of power quality; wrong output power; short circuits in power network	Visual inspection
			Mechanical stress due to external short circuit conditions			Operational test
		Loss of dielectric strength in bushings	Heat, oxidation, acidity and moisture	Internal short circuits; transformer damage	System losses increase; decrease of power quality	Sensors for leakage currents, power factor and capacitance tests
		Magnetic-Core delamination	Harmonics	Degraded operation of the transformer	Power network operation outside of optimal operating conditions	Signal analysis
			Corrosion			Operational test
		Winding overheating	Overload	Overheating; loss of efficiency; explosion	Increase system losses; catastrophic event (fire, explosions, . . .)	Signal analysis;
		Tap changer mechanical failure in drive mechanism	Corrosion	Wrong output power	Power network operation outside of optimal operating conditions	Visual Inspection
			Dirt/contamination			Visual Inspection
			Friction			Visual Inspection

Equipment	Function	Failure Mode(s)	Failure Cause(s)	Failure Effect(s)		Detection method
				Local Effect(s)	System Effects(s)	
Transformer (cont.)		Tap changer contacts degradation	Contact wear	Wrong output power	Power network operation outside of optimal operating conditions	Operational test
			Electrical treeing (partial discharges)			Infrared thermographic scanning
		Tank rupture	Vibration-induced damage	Over-heating and damage in surronding components due to oil leakage; loss of transformer function	Possible downstream network disconnection; no energy supply	Sensor detection
			Corrosion			Visual Inspection
			Cracking of welds			Infrared thermographic scanning
		Windings isolation degradation or breakdown	Short circuits and overloads	Flash over of the windings	Power network operation outside of optimal operating conditions	Power relays detection, signal analysis, infrared thermographic scanning (thermal analysis)
			Oil contamination			Oil analysis
			Oil moisture			Oil analysis
		Distortion, loosening or displacement of the windings	Short circuits	Internal short circuits; transformer damage	Decrease of power quality; wrong output power; short circuits in power network; power network operation outside of optimal operating conditions	Power relays detection, signal analysis, capacitance change
		Transformer explosion	Human sabotage	Serious damage in the substation; personnel injuries or death	Possible downstream network disconnection; no energy supply	Physical surveillance
			Internal short circuit			Signal analysis
			Overheating			Infrared thermographic scanning
		Cooling system failure	Cooling pipes obstruction	Overheating; degraded operation of the transformer; possible transformer explosion	Possible downstream network disconnection; no energy supply	Infrared thermographic scanning
			Damaged fans			Infrared thermographic scanning

Equipment	Function	Failure Mode(s)	Failure Cause(s)	Failure Effect(s)		Detection method
				Local Effect(s)	System Effects(s)	
HMI	Primary tool by which operators coordinate and control the grid	Operational failure	Poor communication between HMI and other cyber components	Impossibility to monitor and/or control the grid in real-time via manual operation; wrong control commands	No system monitoring; corrective and/or preventive manual commands are not properly executed, or can't even be impossible to execute	Real-time monitoring
			Human error			–
			Poor software design			Software malfunctions detection; inability to execute manual actions
		Power outage	Remote disconnection of power	HMI disconnection from the communication network; impossibility to monitor and/or control the grid in real-time by manual operation	No system monitoring; corrective and/or preventive manual commands are not properly executed, or can't even be impossible to execute	Loss of power; HMI blackout
		Security failure	Direct human intrusion: faulty commands (cyberattacks)	Loss of integrity	EMS applications run under inadvertent commands; inadvertent operations in the power system, which can lead to partial losses of energy; possible blackout	Erroneous/illogical commands made without operator's consent; firewall block; attempt to pass the firewall
			Human Vengeance			–
SW	Hardware device that centralizes communications among multiple connected devices and select paths to transfer information inside the cyber network through network connections	Performance decrease	Multicast traffic	Communication network congestion; delays in data transfer	Delay in system response; EMS applications are compromised due to low communication performance	Network congestion
			Blocking (High traffic loads)			Inspection after installation
		Operational failure (SW blackout)	Bad SW configuration	Incorrect SW function or SW malfunction	Decrease in communication network performance; EMS applications fail or are compromised (non-optimal asset management)	Corrupted data; poor data processing; cyber-network system
			SW is locked up			Uncontrollable SW
			Module failure	Network congestion; loss of access to database (if central SW fails)		SW blackout

Equipment	Function	Failure Mode(s)	Failure Cause(s)	Failure Effect(s)		Detection method
				Local Effect(s)	System Effects(s)	
SW (cont.)		Network/Cyber storm	Broadcast of excessive amount of messages in uncontrollable way (misleading information)	Communication network becomes unavailable to redirect the important data for the system operation; large volume of data saturating the network capacity; major consumption of processor computation resources	EMS applications fail or are compromised (non-optimal asset management); decrease in communication network performance	Broadcast of excessive amount of data detection
		Power outage	Remote disconnection of power	Switch disconnection from communication network	EMS applications fail or are compromised	Loss of power; SW blackout
		Security failure	Faulty signal injections (cyberattacks)	Loss of data integrity	EMS applications run under fallacious information; inadvertent operations in the power system	Firewall block; attempt to pass the firewall; suspicious system behaviour; existence of corrupted data
SV	Computing system platform used for various network communication applications / computer program or device that provides functionality for other programs or devices	Data overload	Lower storage capacity or unexpected large amount of data to storage	Large amount of data is lost; defective storage of data	EMS applications are compromised	SV has low data storage capacity
		Hardware crash	Overheating and high humidity	Impossibility to access system's information	SCADA system failure; IT malfunction; EMS applications fail or are compromised	Temperature monitoring
			Hard drive crash			SV blackout
			Hardware sabotage			Physical surveillance
			Physical disaster (such as fire, earthquake, lightning or flooding)			Weather monitoring
		Data errors	Software malfunction	Impossibility to access system's information	IT malfunction; EMS applications fail or are compromised	Unexpected behaviour
		Power outage	Remote disconnection of power	Impossibility to access system's information	SCADA system failure; EMS applications fail or are compromised	Loss of power

Equipment	Function	Failure Mode(s)	Failure Cause(s)	Failure Effect(s)		Detection method
				Local Effect(s)	System Effects(s)	
SV (cont.)		Security failure	Denial of service attack (DoS)	Loss of data integrity; deleted or corrupted data	EMS applications run under fallacious information; inadvertent operations in the power system; loss of integrity	Firewall block; attempt to pass the firewall; suspicious system behaviour
			Hacking for sensitive information			Firewall block; attempt to pass the firewall; suspicious system behaviour
			Malicious software infection			Firewall block; attempt to pass the firewall; suspicious system behaviour
EB	Electronic device used to record and communicate electric energy consumption for monitoring and controlling purposes	Communication Error	Poor signal with SV	Defective or even no transmission of data	EMS applications run under lack of information (non-optimal asset management); inadvertent operations in the power system	Inability to get EB reading
		Power consumption misreading	Manual manipulation	Incorrect data acquisition	EMS applications run under lack of information (non-optimal asset management); loss of efficiency; loss of power quality	Record of abrupt drop in power supply; comparison between registered and expected load diagrams
			Significant measurement error, or even inability to measure power consumption			Comparison between registered and expected load diagrams
		Operation failure	Improper EB programming and parameterization	Incorrect data acquisition, or even no data acquisition	EMS applications run under lack of information (non-optimal asset management); inadvertent operations in the power system	Comparison between registered and expected load diagrams
			Erroneous installation			EB test and quality assessment
			Power supply failure	No data acquisition		–
		'Catastrophic' failure (burning, melting or explosion)	Temperature stress	Degradation of surrounding smart meter components; personnel injuries or death	EMS applications run under lack of information (non-optimal asset management)	Temperature monitoring

Equipment	Function	Failure Mode(s)	Failure Cause(s)	Failure Effect(s)		Detection method
				Local Effect(s)	System Effects(s)	
EB (cont.)		Security failure	Hacking for personnel sensitive information or faulty information injection (cyberattack)	Loss of data integrity	Energy management applications are based on fallacious information	Attempt to pass the SM security system; existence of corrupted data
IED	Interface device responsible for collecting data from the electrical equipment and receiving and applying a control command from the operator	Communication failure	Damaged transducers	Incorrect data processing due to erroneous or incomplete data acquisition; inadequate processing of data; inability to communicate with control center unit	Corrupted communications; EMS applications fail or are compromised (non-optimal asset management); decrease in communication network performance; SCADA system failure	Inability to establish communication with IED
			Poor communication between IED and remaining cyber-network			Inability to establish communication with IED
			Signal processing error (corrupted data)			Inability to establish communication with IED
			Network/Cyber storm	Communication network becomes unavailable to redirect the important data for the system operation; large volume of data saturating the network capacity; major consumption of processor computation resources		Broadcast of excessive amount of data detection
		Monitoring failure	I/O port damage	No power component status monitoring	EMS applications fail or are compromised (non-optimal asset management); SCADA system failure	Loss of data
			Significant measurement error	Error in monitoring power components		Incongruous or corrupted data
		Control failure	Inability to apply control commands	Inability to control power system operation	EMS applications fail or are compromised; SCADA system failure	Operational test
			Software error (Defective data processing)			Operational test
		Power outage	Remote disconnection of power	IED disconnection from cyber and power network; inability to communicate with control center unit.	EMS applications fail or are compromised; loss of control in the downstream network area; SCADA system failure	Loss of power

Equipment	Function	Failure Mode(s)	Failure Cause(s)	Failure Effect(s)		Detection method
				Local Effect(s)	System Effects(s)	
IED (cont.)		Security failure	Hacking for personnel sensitive information	Loss of integrity	EMS applications run under fallacious information; loss of integrity; SCADA system failure	Firewall block; attempt to pass the firewall; existence of corrupted data
			Faulty information injection (cyberattack)			Firewall block; attempt to pass the firewall; existence of corrupted data
Network link - Ethernet link	Physical component responsible for assuring a message is sent from one network node to another node (local distances)	Cross talk (overload)	Excessive traffic/ congestion of packets	Delays in data communication; corrupted signal	Deterioration of communication network performance; EMS applications are compromised	Deterioration in communication network performance
		Network link integrity defect	Manufacturing imperfection	Delays in data communication; no data transmission	EMS applications are compromised (non-optimal asset management); decrease in communication network performance	Electrical test and quality assessment
			RJ45 degradation			Visual inspection
			Incorrect installation			Inspection after installation
		Network link breakdown	External damage (accidents)	Cable break; loss of communication between cyber-equipment	EMS applications are compromised (non-optimal asset management); decrease in communication network performance	No communication
Network link - optical fiber	Physical component responsible for assuring a message is sent from one network node to another node (long distances)	Fracture	Stress, corrosion or fatigue due to microcracks	No data transmission	Deterioration of communication network performance; EMS applications fail or are compromised	No communication
		Lead-bonds degradation in plated contacts	Temperature stress	Delays in data communication; corrupted signal	Deterioration of communication network performance; EMS applications fail or are compromised	Visual inspection; communication problems
		Humidity induced	Electro-chemical oxidation of transmitters and receivers	Delays in data communication; corrupted signal; no data transmission	Deterioration of network performance; EMS applications fail or are compromised	No communication

4.4 Failure Rates of Failure Modes

In order to obtain the final FMEA table with obtained RPN for each failure mode, failure rates of power and cyber equipment must be distributed accordingly to each failure mode defined in section 4.2.

In the literature, it was verified the lack of this kind of data for power and cyber equipment. Even data found in *EDP Distribuição*, a company with interests in the field, was inconclusive. In this dissertation, to work around this problem, equipment's failure rates defined in Tables 4.1 and 4.3 are subjectively discriminated into failure modes' rates.

A failure rate distribution is proposed in Tables 4.5 and 4.6 for power and cyber equipment, respectively.

Table 4.5: Proposed failure rates for power equipment's failure modes

Equipment	Failure mode	Failure distribution [%]	Failure rate [f/yr]	OCC
Bus	Loss of electrical efficiency	25	0,0025	4
	Loss of structural integrity	50	0,005	5
	Loss of electrical continuity	10	0,001	4
	Electrical disturbances	15	0,0015	4
Cable	Insulation failure	10	0,0108	5
	Cable integrity defect	50	0,054	7
	Electrical operation failure	40	0,0432	6
Circuit Breaker	Insulation failure	10	0,0023	4
	Wrong operation (spurious opening or closing)	15	0,0035	5
	Bushing breakdown	5	0,0012	4
	Bushing terminal hot spot	10	0,0023	4
	Loss of dielectric strength	5	0,0012	4
	Mechanical failure in operating mechanism	35	0,0081	5
	Contacts degradation	20	0,0046	5
Transformer	Bushing breakdown	10	0,001	4
	Bushing terminal hot spot	15	0,0015	4
	Loss of dielectric strength in bushings	10	0,001	4
	Magnetic-Core delamination	7,5	0,00075	4
	Winding overheating	12,5	0,00125	4
	Tap changer mechanical failure in drive mechanism	5	0,0005	3
	Tap changer contacts degradation	2,5	0,00025	3
	Tank rupture	2	0,0002	3
	Windings' isolation degradation	15	0,0015	4
	Distortion, loosening or displacement of the windings	15	0,0015	4
	Transformer explosion	0,5	5E-05	1
	Cooling system failure	5	0,0005	3

Table 4.6: Proposed failure rates for cyber-control equipment's failure modes

Equipment	Failure mode	Failure distribution [%]	Failure rate [f/yr]	OCC
HMI	Operational failure	90	0,1577	8
	Power outage	10	0,0175	6
	Security failure	–	–	2
SW	Decrease of performance	60	0,0135	6
	Operational failure (SW blackout)	20	0,0045	5
	Network/Cyber storm	10	0,0022	4
	Power outage	10	0,0022	4
	Security failure	–	–	2
SV	Data overload	10	0,0021	4
	Hardware crash	65	0,0135	6
	Data error	15	0,0031	4
	Power outage	10	0,0021	4
	Security failure	–	–	2
EB	Communication error	20	0,001	4
	Power consumption misreading	55	0,0028	5
	Operation failure	20	0,001	4
	'Catastrophic' failure (burning, melting or explosion)	5	0,0003	3
	Security failure	–	–	1
IED	Communication failure	20	0,0105	5
	Monitoring failure	30	0,0158	6
	Control failure	40	0,0211	6
	Power outage	10	0,0053	5
	Security failure	–	–	3
Network link - Ethernet link	Cross talk (overload)	50	5E-07	1
	Network link integrity defect	30	3E-07	1
	Network link breakdown	20	2E-07	1
Network link - optical fiber	Fracture	34	0,0145	5
	Lead-bonds degradation in plated contacts	33	0,0145	1
	Humidity induced	33	0,0145	1

Note that, due to the lack of this kind of data, the assignment of OCC rating ends up being performed in a subjective manner. Besides discriminated failure rates are taken into account for the determination of OCC rating, a critical analysis on the obtained rating demands a revision in its ranking in accordance with specific failure causes which seems to be more or less likely to occur.

Chapter 5

Results

In this chapter, it will be presented the most relevant results obtained through the employment of FMEA in a smart grid environment.

The main goal is to assess the impact of FMEA on the present reliability analysis, emphasizing failure modes impact on the electric grid.

In the first section, the baseline solution of the implementation described in the previous chapter is presented. The final RPN obtained for each failure mode are presented in a table, where critical failure modes are identified and enumerated in accordance to their risk number.

In section two, risk analysis is performed in order to understand FMEA conclusions concerning reliability analysis of the presented case study.

Finally, FMEA methodology and its application in a complex system such as a smart electrical distribution system are discussed.

5.1 Baseline Solution

With respect to the equipment identified in chapter 4 and presented in Figure 4.2 as integral components of the test study in analysis, a FMEA analysis on a smart grid was fulfilled.

Bearing in mind FMEA procedure in Figure 3.2, failure modes of each power and cyber equipment were identified and briefly explained in the previous chapter. A FMEA table was created (see Table 4.4), where implied causes of failure of each equipment were deliberated and respective potential impacts on the smart grid were brainstormed, always taking into account power and cyber systems topology and their main interdependencies. Current controls of each failure were also conceived.

In order to evaluate risk analysis in the presented study, RPN for each failure mode must be calculated as determined in (3.1).

The three risk factors were determined for each failure cause according to Tables 3.1, 3.2 and 3.3: for DET assignment, it was taken into account the ability to detect the failure before the impact of the effect could be realized in the system; for SEV rating, the seriousness of the failure and its effects in the system is taken in consideration; in its turn, OCC rating is specified according to equipment's failure

rates specified in Tables 4.5 and 4.6. Note that the assignment of these ratings ends up being performed in a subjective manner, thus without precise determination. Even OCC rating, which seems to be the one whose assignment could be accurately performed, can be revised in accordance with specific failure causes which seems to be more or less likely to occur.

In sum, a failure mode is expected to be assigned with different DET and OCC ratings, depending on the causes that trigger the respective mode of failure, while SEV rating should be unique for each failure mode. This may lead to different RPNs inside of each failure mode, since each cause of failure has its own RPN. As a result, final RPN for failure modes corresponds to the highest RPN obtained between its respective failure causes.

The obtained FMEA table provided in Appendix B consists on the assignment of several RPN values for each failure cause identified in Table 4.4.

Table 5.1 presents the FMEA table resulted from the selection of the most relevant information from Table B.1, in which the failure cause with the highest RPN of each failure mode is highlighted in order to determine the failure mode's RPN.

Failure modes are ordered considering the highest RPN and high-risk failure modes for the present case study are identified. Preventive actions for high-risk failure modes are also suggested in order to minimize the impact of the given failures in the system.

Table 5.1: Final RPN obtained for each failure mode

Rank	Equipment	Failure Modes	Failure Causes	OCC	DET	SEV	RPN	Recommended action(s)
1	SV	Hardware crash	Hard drive crash	6	10	8	480	Install redundant SV
2	Transformer	Transformer explosion	Internal short circuit	5	10	9	450	Real-time signal analysis
3	HMI	Operational failure	Human error	8	10	5	400	Hire or educate qualified employees
4	IED	Control failure	Defective data processing (software error)	7	7	8	392	Periodic software update
5	Bus bar	Loss of structural integrity	Break of the support insulators	6	9	7	378	Implement hot spot alert strategies
6	Cable	Electrical operation failure	Short circuits transients	6	10	6	360	Real-time current analysis
7	SW	Operational failure (SW blackout)	SW is locked up	6	10	6	360	Periodic reboot
8	Bus bar	Loss of electrical continuity	Arc flash	4	10	8	320	Improve preventive maintenance actions
9	Bus bar	Electrical disturbances	Short circuits between bus bars	4	10	8	320	Real-time current analysis
10	Transformer	Distortion, loosening or displacement of the winding	Short circuits	5	9	7	315	Real-time current analysis
11	CB	Bushing breakdown	External short circuit	5	10	6	300	Real-time current analysis
12	SV	Data errors	Software malfunction	5	10	6	300	Periodic software update; periodic data backup
13	Transformer	Winding overheating	Overload	6	7	7	294	Real-time signal analysis
14	Cable	Cable integrity defect	Lightnings	7	5	8	280	Use of active lightning protection equipment
15	CB	CB contacts degradation	Electrical treeing (partial discharges)	5	9	6	270	Implement hot spot alert strategies

Rank	Equipment	Failure Modes	Failure Causes	OCC	DET	SEV	RPN	Recommended preventive action(s)
16	SW	Performance decrease	Multicast traffic	7	6	6	252	Establish optimized communication network topology for better performance; SW replacement
17	IED	Communication failure	Poor communication between IED and remaining cyber-network	5	8	6	240	Establish alternative paths for communication
18	Transformer	Winding isolation degradation or breakdown	Short circuits and overloads	4	10	6	240	Real-time current analysis
19	Transformer	Bushing breakdown	External short circuit	4	10	6	240	Real-time current analysis
20	Transformer	Tank rupture	Cracking of welds	3	9	8	216	Implement hot spot alert strategies
21	IED	Power outage	Remote disconnection of power	3	10	7	210	Install a capacity external battery for backup (UPS)
22	SV	Power outage	Remote disconnection of power	3	10	7	210	Install a capacity external battery for backup (UPS)
23	CB	Insulation failure	Loss of dielectric properties	5	7	6	210	Signal analysis optimization in order to find opening patterns
24	SV	Security failure	Denial of Service attack (DoS)	2	10	10	200	Enforce appropriate security policies
25	CB	Bushing terminal hot spot	Mechanical stress due to external short circuit conditions	4	8	6	192	Establish preventive cleaning and terminal squeeze routines
26	IED	Security failure	Faulty information injection (cyberattack)	3	7	9	189	Enforce appropriate security policies and configuration
27	IED	Monitoring failure	Significant measurement error	5	6	6	180	Cross data with other monitored data in the grid
28	HMI	Security failure	Human vengeance	2	10	9	180	Restrict access to specialist personnel and controlled by security check
29	SW	Power outage	Remote disconnection of power	3	10	6	180	Install a capacity external battery for backup (UPS); Install PLC system
30	SW	Network/Cyber storm	Broadcast of excessive amount of messages in uncontrollable way (misleading information)	4	7	6	168	Install higher-performance SWs; establish communication network topology for better performance

Rank	Equipment	Failure Modes	Failure Causes	OCC	DET	SEV	RPN	Recommended preventive action(s)
31	Transformer	Cooling system failure	Cooling pipes obstruction	3	7	8	168	Periodic cooling system maintenance (check for leaks, rust or accumulation of dirt)
32	CB	Wrong operation (Spurious opening and closure)	Overload	6	4	7	168	Real-time current analysis
33	Transformer	Magnetic-Core delamination	Harmonics	4	7	6	168	Real-time current analysis
34	Transformer	Bushing terminal hot spot	Mechanical stress due to external short circuit conditions	4	7	6	168	Establish preventive cleaning and terminal squeeze routines
35	Transformer	Tap changer contacts degradation	Electrical treeing (partial discharges)	3	9	6	162	Implement hot spot alert strategies
36	EB	Power consumption misreading	Significant measurement error, or even inability to measure power consumption	5	8	4	160	Correct smart meter calibration
37	HMI	Power outage	Remote disconnection of power	3	10	5	150	Install a capacity external battery for backup (UPS)
38	EB	Operation failure	Improper EB programming and parameterization	4	8	4	128	Good installation practice
39	Optical fiber link	Fracture	Stress, corrosion or fatigue due to microcracks	3	10	4	120	Increase cable robustness
40	Optical fiber link	Humidity induced	Electro-chemical oxidation of transmitters and receivers	3	10	4	120	Use hermetically sealed package
41	EB	'Catastrophic' failure (burning, melting or explosion)	Temperature stress	3	4	8	96	Develop protection strategies to limit EB operation in temperature stress situations
42	Transformer	Loss of dielectric strength in bushings	Heat, oxidation, acidity and moisture	4	4	6	96	Establish preventive maintenance routines
43	CB	CB mechanical failure in operating mechanism	Lack of lubrication	5	3	6	90	Establish preventive lubrication routines

Rank	Equipment	Failure Modes	Failure Causes	OCC	DET	SEV	RPN	Recommended preventive action(s)
44	Cable	Insulation failure	Insulation aging	5	3	6	90	Establish preventive maintenance routines
45	SW	Security failure	Faulty signal injections (cyberattacks)	2	5	8	80	Increase system's integrity and security through a new cyber security approach
46	Transformer	Tap changer mechanical failure in drive mechanism	Friction	3	4	6	72	Establish preventive maintenance routines
47	CB	Loss of dielectric strength in bushings	Heat, oxidation, acidity and moisture	4	3	6	72	Establish preventive maintenance routines
48	SV	Data overload	Lower storage capacity or unexpected large amount of data to storage	3	4	6	72	Install higher storage capacity SV
49	Bus bar	Loss of electrical efficiency	Moisture, Humidity	4	2	7	56	Establish preventive maintenance routines
50	Ethernet link	Network link breakdown	External damage (accidents)	1	10	4	40	Increase network link robustness
51	Optical fiber link	Lead-bonds degradation in plated contacts	Temperature stress	3	3	4	36	Use evaporated contacts
52	EB	Security failure	Hacking for personnel sensitive information or faulty information injection (cyberattack)	1	5	7	35	Enforce appropriate security policies; enforce intrusion detection strategies for EB
53	EB	Communication Error	Poor signal with SV	4	2	4	32	Periodic energy box reboot; periodic connected network links maintenance
54	Ethernet link	Cross talk (overload)	Excessive traffic/ congestion of packets	1	8	4	32	Establish optimized communication network topology for better performance;
55	Ethernet link	Network link integrity defect	RJ45 degradation	2	2	4	16	Improve maintenance in RJ45 connections

5.2 Risk Analysis

From Table 5.1, it is possible to conclude SVs and transformers are the equipment with the most critical failure modes, with RPNs of 480 and 450, respectively, meaning that their respective high-risk causes of failure compromises the correct grid operation. Bus bars failure modes are also identified as critical, in the sense that their impact of failure in the grid is significant (several failure modes with high RPN).

Related to cyber equipment, failure modes with the highest RPNs are those which express themselves as operational failures, verified in equipment like HMIs, SWs or IEDs. Concerning to power equipment, failure modes that tease unstable behaviors in system's power supply, possibly causing partial or total (less frequent) power outages in the grid, are also classified with high RPNs.

Table 5.1 also indicates Ethernet links, optical fiber links and EBs as the less critical equipment in the system, mainly due to their low failure rates.

In the domain of cyber equipment, failure modes concerning security reasons, despite the enormous impacts cyberattacks can cause in the system, are not considered as high-risk failure modes in the applied FMEA methodology. It can be explained due to low OCC ratings, in the sense that in spite of the expected increase of cyberattack attempts in future years, they will not be necessarily successful.

In this turn, power outages in each cyber equipment's power supply are expected to be less frequent, thus expressing themselves also with lower RPNs.

In general, it is possible to infer a pattern in high-risk failures, which are mainly determined by high DET and SEV ratings.

In fact, besides all ratings are treated as equals, one can see OCC rating remains with low variations between different failure modes with high and low RPNs, not being a decisive rating with impact on high-risk failures.

In its turn, failure modes characterized by high levels of unpredictability are more likely to be more critical, since these modes of failure occurs without early warning and are difficult to prevent, while strong negative impacts on the smart grid operation have also a repercussion in high SEV ratings.

Finally, a conclusion regarding human interference in future smart grids must be pointed out. In fact, HMI's operational failure due to human error proves to have negative impacts on the grid. This human error is unintentional, and its high probability of occurrence and unpredictability (as seen in Table 5.1) makes it a high-risk failure cause.

This way, it is expected main weaknesses in future smart grids are related to some tasks that demand human interference.

5.3 Discussion

In order to obtain the final result of FMEA, one has to take into account important information is lost during FMEA procedure. This situation can compromise final conclusions concerning high-risk failure modes and their impact on the reliability of the system.

As a matter of fact, Table 5.1 presents the final result of FMEA in the system, giving prioritization of high-risk failure modes with their respective high-risk causes of failure. This means that, according to FMEA, maintenance strategies should be prioritized from the highest RPN to the lowest in order to increase smart grids reliability. This implies it will be the origin of the failure which will receive special attention in its maintenance tasks in order to decrease or eliminate its risk of failure in the system and to reduce failure mode impact on the system. This is established with the aim of decreasing the number of times in which the respective failure manifests itself so that system reliability increases as pretended.

However, this also means numerous failure causes are herein discriminated as long as high-risk causes of failure of each failure mode are not taken into account for final FMEA analysis.

In fact, critical failure causes, sometimes with bigger RPN than certain failure causes and modes herein identified in Table 5.1, see their maintenance strategies being ignored.

Table 5.2 shows some failure modes with some high-risk failure causes that are not considered for final FMEA analysis.

Table 5.2: Some high-risk failure causes not considered for final FMEA analysis

Equipment	Failure Mode(s)	Failure Cause(s)	OCC	DET	SEV	RPN
Bus bar	Loss of structural integrity	Fracture of the copper bar	5	9	7	315
		Break of the support insulators	6	9	7	378
		Cracking of connection welds	5	9	7	315
Bus bar	Electrical disturbances	Short circuits between bus bars	4	10	8	320
		Harmonics	4	8	8	256
SW	Operational failure (SW blackout)	SW is locked up	6	10	6	360
		Module failure	5	10	6	300
IED	Communication failure	Poor communication between IED and remaining cyber network	5	8	6	240
		Signal processing error (corrupted data)	4	8	6	192
		Network/Cyber storm	5	7	6	210

For instance, as seen in Table 5.2, focusing on bus bar failure modes, this equipment can have electrical disturbances due to short circuits between bars with different phases or due to harmonics (also causing thermal losses). Applying FMEA methodology, these distinct failure causes, which express themselves in the system in the same way (same failure mode), obtained a RPN of 320 and 256, respectively (see Appendix B). Although harmonics still have a high RPN, meaning it is a high-risk cause of failure, its importance is neglected and maintenance strategies are not recommended for this cause in order to decrease its risk of failure.

From here, one can conclude that maintenance tasks are not efficiently applied in terms of risk decrease, therefore with implications in maintenance costs/risk-decrease ratio, bearing in mind the aim to execute a cost-effectiveness maintenance strategies.

Besides that, the relative importance among OCC, SEV and DET is not taken into account. The three risk factors are treated as equals, with the same weight in RPN calculation, and this may not be

the case when considering a practical application of FMEA in this dissertation.

As an illustration, as seen in Table 5.1, software errors in IEDs control applications have a larger negative impact on system performance (thus in terms of severity), when compared to unintentional human error in HMI operations (SEV rating is assigned with 8 and 5, respectively). However, one can see HMI operational failure due to human error is a higher-risk failure mode instead of IEDs control failure. The severity of the failure seems to be herein neglected.

Likewise, different combinations of OCC, SEV and DET may produce the same RPN rating, but their hidden risk implications may be different: for instance, wrong operation in CB due to overloads and magnetic-core delamination in transformers have the same RPN – 168 more precisely –, but their ratings are different. Their impacts on the system could be different, but FMEA cannot distinguish them.

The mathematical form adopted for calculating RPN is also strongly sensitive to the variation of risk factor evaluations. Small variation in one rating may lead to vastly different effects on the RPN value.

This clearly shows FMEA is limited in the prioritization of maintenance tasks. FMEA is not able to assign different weights for its ratings, leading to some misreadings concerning the risk of a failure mode.

For a correct application of FMEA, it is of utmost importance to assemble subject experts with a high level of knowledge of the smart grid operation. This condition is related to the fact that failure modes and failure causes must be enumerated and exhaustively detailed and discussed in order to evaluate, as accurately as possible, the impacts of failure in the system.

In the literature, it was verified the lack of failure rates information discriminated for each failure mode, either for power and cyber equipment. Even data found in *EDP Distribuição*, a company with interests in cost-effective maintenance methodologies, was inconclusive. In this dissertation, failure mode's rates were subjectively discriminated from equipment's failure rates, which may have led to some errors in RPN final calculation, specially for OCC rating, which seemed to cause low impact for RPN the way it was obtained (as noted in sections 5.1 and 5.2).

So that FMEA may be correctly applied, experimental failure rates for each mode of failure must be detailed. If possible, deeper researches would be useful to get experimental rates for each cause of failure.

Therefore, for a deeper understanding on the criticality of a certain failure, the collection of data on the frequency of failure for each power and cyber equipment, by specifying failure rates for each failure mode and their causes, would be profitable for reliability purposes. Knowing the frequency of a certain failure, as long as bearing in mind the real impact that that failure triggers in the smart grid, would make FMEA more efficient (more reliability of OCC rating) and maintenance strategies more precise (strategies based on maintenance frequency adjustments are improved).

Finally, in order to ensure system's high reliability level, a cost-effectiveness maintenance strategy must be achieve by prioritizing failure modes from the most critical to the lowest, as long as one has to take into consideration maintenance costs for each equipment and each failure mode.

This way, in what concerns the level of risk of the analyzed system (note that, concerning the economic side, it is not evaluated in the present study since it does not fall within the scope of this dissertation), it is of utmost importance to establish maintenance strategies according to their risk number.

Strategies with the aim of (i) mitigating or eliminating failure modes in order to decrease OCC rating, (ii) increasing failure detectability for the purpose of lowering DET rating and (iii) minimizing losses or negative impacts when a failure occurs in order to diminish SEV rating must be performed in order to increase reliability of the smart grid.

Chapter 6

Conclusions

In this chapter, the main conclusions of this dissertation regarding FMEA application for reliability assessment in a smart electrical distribution system are presented.

A deliberation about the achievement of the proposed objectives in the first chapter will be given, and final conclusions regarding FMEA as a useful tool for risk assessment will be given.

Finally, it will be enumerated some recommendations for future researches based on this work.

6.1 Achievements

This dissertation conducts an FMEA analysis in a smart grid environment. Smart grid concepts are enumerated in chapter 2, and a simple smart grid case study is defined in chapter 4, where fundamental failure modes and interdependencies between cyber and power equipment are identified. A qualitative assessment of reliability and risk analysis is performed on chapter 5, and a critical analysis of FMEA should be carried out.

In fact, despite FMEA is presented to be a useful risk assessment tool for reliability analysis in a lot of fields and one of the most important early preventive management initiatives, conclusions regarding its viability in complex systems such as smart electrical distribution systems must be pointed out. Applying FMEA as an RCM strategy to increase smart grid reliability turned out to be challenging.

FMEA is a powerful weapon used in risk analysis since main strength of FMEA allows an exhaustive failure modes and causes of failure identification, also analysing their impacts on the system.

Nonetheless, in a smart grid system, with such interdependencies between cyber-cyber, cyber-power and power-power equipment, FMEA proves to be limited at bearing in mind all interdependencies and not every possible effect on the system is taken into account.

FMEA is strongly used in other complex systems, such as nuclear power plants or in aerospace industry. However, in these systems, and contrary to the intended for a smart grid, FMEA is looking for a safety improvement instead of a reliability analysis.

For safety purposes, main contribution of FMEA is the identification of possible failure modes and their causes. No prioritization is evaluated, in the sense that all failure causes must be treated as equals

in order to ensure security of the system, ignoring economic constraints. In the presented case, FMEA is used as a reliability tool to study the delivery of electricity to the clients, therefore evaluating continuity of service, and maintenance strategies must be established in a cost-effective way, in which higher-risk failure modes must be mitigated taking into account economic restrictions.

Furthermore, a review on the determination of each risk number must be taken. Despite FMEA must be carried out by a team of subject matter experts which presupposes a weighted evaluation of each topic, the assignment of a value for each risk factor is uncertain and not consensual. It is based on different experiences and different levels on the knowledge of the target subject. A failure mode can be more critical to one team member, while another expert treats it as irrelevant.

Besides that, criticality of a failure mode depends on its penetration level on the system, and the manner in which a failure occurs could be seen in different perspectives, depending on the complexity of the system and where and how it expresses itself.

Additionally, the RPN method is only measuring from the risk viewpoint while ignoring the importance of corrective actions, then it cannot be used to measure the effectiveness of corrective actions. RPN calculation considers risk factors mainly in terms of criticality and other important risk factors such as economical impacts are ignored.

In a nutshell, FMEA is very successful in assemble failure modes and their causes of a given smart system. However, for a better reliability assessment and risk analysis of a smart grid using FMEA, one needs to adopt possible adjustments in FMEA technique in order to improve risk prioritization so that maintenance strategies can be efficiently applied.

6.2 Future Work

The final work of this dissertation serve as a basis for future researches to be developed in forthcoming works. Here is presented an enumeration of possible aspects that could be discussed and improved:

- Adopt possible adjustments in FMEA methodology: for instance, by considering new risk factors such as economic impacts or considering relative importance between OCC, SEV and DET;
- Develop a new strategy to determine FMEA risk factors, for instance through fuzzy logic, and evaluate its impact in reliability analysis in small smart electrical distribution systems comparing with traditional FMEA
- Perform a prioritization of failure modes taking into account economic constraints in order to achieve cost-effective maintenance strategies;
- Evaluate smart grid reliability analysis through different approaches by developing new strategies to detect failure modes and their causes and mitigate their effects on the system;
- Perform a study on each equipment failure mode and their causes and obtain failure rates estimates. This would make the assumptions in section 4.4 dispensable and realistic failure rates estimates for each failure mode would be taken into account;

References

[1] S. Bilgen. Structure and Environmental Impact of Global Energy Consumption. *Renewable and Sustainable Energy Reviews*, 38:890–902, Oct. 2014.

[2] Y. Yan, Y. Qian, H. Sharif, and D. Tipper. A Survey on Smart Grid Communication Infrastructures: Motivations, Requirements and Challenges. *IEEE Communications Surveys & Tutorials*, 15(1): 5–20, 2013.

[3] J. A. P. Lopes, N. Hatziargyriou, J. Mutale, P. Djapic, and N. Jenkins. Integrating Distributed Generation into Electric Power Systems: A Review of Drivers, Challenges and Opportunities. *Electric Power Systems Research*, 77(9):1189–1203, July 2007.

[4] K. Moslehi and R. Kumar. A Reliability Perspective of the Smart Grid. *IEEE Transactions on Smart Grid*, 1(1):57–64, June 2010.

[5] E. Santacana, G. Rackliffe, L. Tang, and X. Feng. Getting Smart. *IEEE Power & Energy Magazine*, 8(2):41–48, Mar. 2010.

[6] H. Farhangi. The Path of the Smart Grid. *IEEE Power and Energy Magazine*, 8(1):18–28, Jan. 2010.

[7] R. S. de Carvalho and S. Mohagheghi. Impact of Communication System on Smart Grid Reliability, Security and Operation. *Proc. IEEE North Amer. Power Symp.*, pages 1–6, 2016.

[8] Y. Wang and X. Han. Probability Model of Power Equipment Maintenance Based on Full State Process. *The Open Electrical & Electronic Engineering*, 9:99–106, 2015.

[9] A. Ozdemir and E. D. Kuldasli. RCM Application for Turkish National Power Transmission System. In *2010 IEEE 11th International Conference on Probabilistic Methods Applied to Power Systems*, Singapure, Singapure, July 2010. IEEE.

[10] I. P. de Siqueira. Measuring the Impacts of an RCM Program on Power System Performance. In *IEEE Power Engineering Society General Meeting*, San Francisco, CA, USA, June 2005. IEEE.

[11] L. Pottonen and F. Oyj. A Method for Analysing the Effect of Substation Failures on Power System Reliability. In *Proc. 15th Power Syst. Comput. Conf*, Liege, Belgium, Aug. 2005. IEEE.

[12] D. Zhang, W. Li, and X. Xiong. Overhead Line Preventive Maintenance Strategy Based on Condition Monitoring and System Reliability Assessment. *IEEE Transactions on Power Systems*, 29(4):1839–1846, July 2014.

[13] L. Andersson, K. P. Brand, C. Brummer, and W. Wimmer. Reliability Investigations for SA Communication Architectures based on IEC 61850. In *2005 IEEE Russia Power Tech*, St. Petersburg, Russia, June 2005. IEEE.

[14] A. Volkanovski, M. Cepin, and B. Mavko. Application of the fault tree analysis for assessment of power system reliability. *Reliability Engineering & System Safety*, 94(6):1116–1127, June 2009.

[15] M. K. Rahmat and S. Jovanovic. Power Systems Reliability Estimation Method. In *2015 IEEE 13th International Conference on Industrial Informatics (INDIN)*, Cambridge, UK, Oct. 2015. IEEE.

[16] T. N. Aeronautics and S. Administration. Reliability-Centered Maintenance Guide for Facilities and Collateral Equipment. Technical report, NASA, Feb. 2008.

[17] H.-C. Liu. *FMEA Using Uncertainty Theories and MCDM Methods*. Springer, 1st edition, 2016. ISBN 978-981-10-1466-6.

[18] M. I. M. Ridzuan, I. Hernando-Gil, S. Djokic, R. Langella, and A. Telsa. Incorporating regulator requirements in reliability analysis of smart grids. part 1: Input data and models and part 2: Scenarios and results. *IEEE PES Innovative Smart Grid Technologies, Europe*, Feb. 2015.

[19] I. Hernando-Gil, I.-S. Ilie, and S. Z. Djokic. Reliability performance of smart grids with demand-side management and distributed generation/storage technologies. In *2012 3rd IEEE PES Innovative Smart Grid Technologies Europe*, Berlin, Germany, Feb. 2012. IEEE.

[20] J. A. P. Lopes, A. G. Madureira, and C. C. L. M. Moreira. A view of microgrids. *WIREs Energy Environ.*, 2(1):86–103, Jan. 2013.

[21] CSE. What is a microgrid? Available at url: https://https://energycenter.org/self-generation-incentive-program/business/technologies/microgrid, Accessed in 30/09/2018.

[22] K. C. Budka, J. G. Deshpande, and M. Thottan. *Communication Networks for Smart Grids*. Springer, 1st edition, 2014. ISBN 978-1-4471-6301-5.

[23] M. M. Farag, M. Azab, and B. Mokhtar. Cross-layer security framework for smart grid: Physical security layer. In *5th IEEE PES Innovative Smart Grid Technologies Europe*, Istanbul, Turkey, Oct. 2016. IEEE.

[24] H. He and J. Yan. Cyber-physical attacks and defences in the smart grid: a survey. *IET Cyber-Physical Systems: Theory & Applications*, 1(1):13–27, 2016.

[25] B. Falahati. *Reliability Assessment of Smart Grid Considering Cyber-Power Interdependencies*. PhD thesis, Faculty of Mississippi State University, Aug. 2013.

[26] D. B. Rawat and C. Bajracharya. Cyber Security for Smart Grid Systems: Status, Challenges and Perspectives. In *Proceedings of the IEEE SoutheastCon 2015*, Fort Lauderdale, FL, USA, Apr. 2015. IEEE.

[27] B. Falahati and E. Chua. Failure Modes in IEC 61850-Enabled Substation Automation Systems. In *2016 IEEE/PES Transmission and Distribution Conference and Exposition (T&D)*, Dallas, TX, USA, May 2016. IEEE.

[28] S. Jaloudi, E. Ortjohann, A. Schmelter, P. Wirasanti, and D. Morton. General Communication Strategy for Control of Distributed Energy Resources in Smart Grids via International Standards. In *2011 16th International Conference on Intelligent System Applications to Power Systems*, Hersonissos, Greece, Sept. 2011. IEEE.

[29] R. E. Mackiewicz. Overview of IEC 61850 and Benefits. In *2006 IEEE PES Power Systems Conference and Exposition*, Atlanta, GA, USA, Oct. 2006. IEEE.

[30] D. Markovic, I. Branovic, and R. Popovic. Smart Grid and Nanotechnologies: a Solution for Clean and Sustainable Energy. *Energy and Emission Control Technologies*, 3:1–13, Jan. 2015.

[31] B. Falahati, Y. Fu, and L. Wu. Reliability Assessment of Smart Grid Considering Direct Cyber-Power Interdependencies. *IEEE Transactions on Smart Grid*, 3(3):1515–1524, Sept. 2012.

[32] M. Azarm, R. Bari, Y. Meng, and Z. Musicki. Electrical Substation Reliability Evaluation with Emphasis on Evolving Interdependence on Communication Infrastructure. In *2004 International Conference on Probabilistic Methods Applied to Power Systems*, Ames, IA, USA, Sept. 2004. IEEE.

[33] A. H. Ahangar and H. A. Abyaneh. Improvement of Smart Grid Reliability Considering Various Cyber Network Topologies and Direct Interdependency. In *2016 IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC)*, Xi'an, China, Oct. 2016. IEEE.

[34] Inovonics. Physical Security of the U.S. Electric Grid. Available at url: https://www.inovonics.com/wp-content/uploads/2017/12/Physical-Security-of-the-US-Electric-Grid.pdf, Accessed in 30/09/2018.

[35] ICS-CERT. Cyber-Attack Against Ukrainian Critical infrastructure. Available at url: https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01, Accessed in 30/09/2018.

[36] T. Flick and J. Morehouse. *Securing the Smart Grid: Next Generation Power Grid Security*. Syngress, 1st edition, 2011. ISBN 978-1-59749-570-7.

[37] C. W. Ten, A. Ginter, and R. Bulbul. Cyber-Based Contingency Analysis. *IEEE Transactions on Power Systems*, 31(4):3040–3050, Sept. 2016.

[38] D. Wei, Y. Lu, M. Jafari, P. M. Skare, and K. Rhode. Protecting Smart Grid Automation Systems Against Cyberattacks. *IEEE Transactions on Smart Grid*, 2(4):782–795, Dec. 2011.

[39] A. L. Buczak and E. Guven. A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. *IEEE Communications Surveys & Tutorials*, 18(2):1153–1176, Oct. 2016.

[40] F. Aloula, A. R. Al-Alia, R. Al-Dalkya, M. Al-Mardinia, and W. El-Hajjb. Smart Grid Security: Threats, Vulnerabilities and Solutions. *International Journal of Smart Grid and Clean Energy*, 1(1), Sept. 2012.

[41] I. H. Afefy. Reliability-centered maintenance methodology and application: A case study. *Scientific Research Engineering*, pages 863–873, Nov. 2010.

[42] A. Pourramazan, S. Saffari, and A. Barghandan. Study of Failure Mode and Effect Analysis (FMEA) on Capacitor Bank Used in Distribution Power Systems. *International Journal of Innovative R]esearch in Electrical, Electronics, Instrumentation and Control Engineering*, 5, Feb. 2017.

[43] M. Akbari, P. Khazaee, I. Sabetghadam, and P. Karimifard. Failure Modes and Effects Analysis (FMEA) for Power Transformers. In *28th Power System Conference*, 2013.

[44] Pumps and Systems. The bathtub curve as applied to pumping systems. Available at url: https://www.pumpsandsystems.com/bathtub-curve-applied-pumping-systems, Accessed in 11/08/2018.

[45] M. Krasich. How to estimate and use MTTF/MTBF would the real MTBF please stand up? In *2009 Annual Reliability and Maintainability Symposium*, Fort Worth, TX, USA, Jan. 2009. IEEE.

[46] S. AB. *T-book Reliability Data of Components in Nordic Nuclear Power Plants*. Stockholm: TUD Office, 6th edition, 2005. ISBN 91-631-7232-1.

[47] F. Berghmans, S. Eve, and M. Held. An introduction to reliability of optical components and fiber optic sensors. *Optical Waveguide Sensing and Imaging*, pages 73–100, Dec. 2007.

[48] EKE-Electronics. Human machine interface technical specifications. Available at url: https://www.eke-electronics.com/human-machine-interface, Accessed in 30/09/2018.

[49] Cisco. Cisco industrial ethernet 5000 series switches data sheet. Available at url: https://www.cisco.com/c/en/us/products/collateral/switches/industrial-ethernet-5000-series-switches/datasheet-c78-734967.html, Accessed in 30/09/2018.

[50] Backblaze. Hard drive stats. Available at url: https://www.backblaze.com/blog/hard-drive-failure-rates-q1-2017/, Accessed in 30/09/2018.

[51] S. E. Laboratories. Comparing the reliability of ethernet network topologies in substation control and monitoring networks. Available at url: https://cdn.selinc.com/assets/Literature/Publications/Technical%20Papers/6103_ComparingReliability_20020612_Web.pdf, Accessed in 30/09/2018.

[52] F. Economics. Research into the costs of smart meters for electricity and gas DSOs. Available at url: https://www.acm.nl/sites/default/files/old_download/documenten/nma/Kostenonderzoek_FE%26L_webversie.pdf, Accessed in 30/09/2018.

Appendix A

Format of a FMEA table

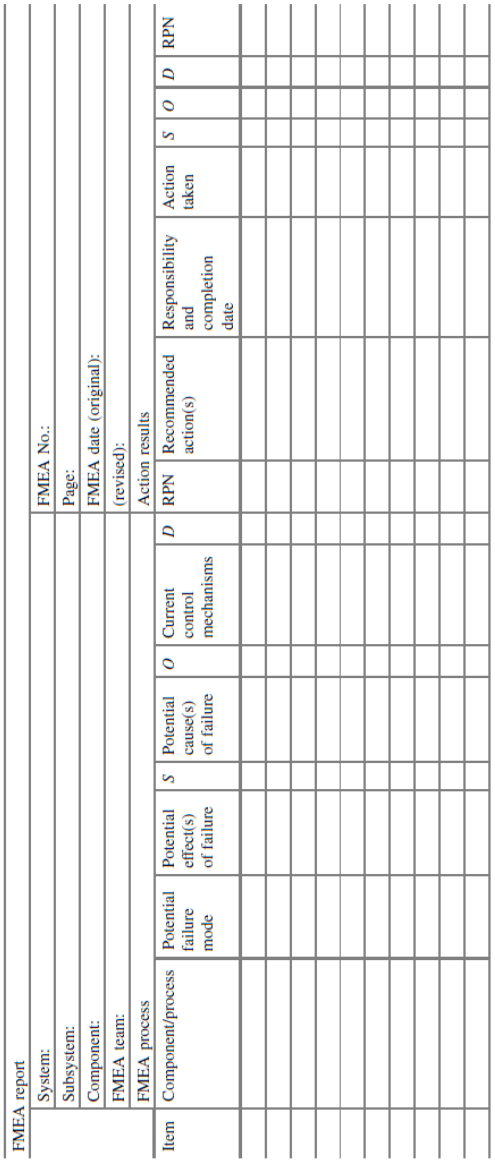

Figure A.1: Example of a FMEA worksheet (from [17])

Appendix B

RPN of each failure cause

Table B.1: RPN obtained for each failure cause

Equipment	Failure Mode(s)	Failure Cause(s)	OCC	DET	SEV	RPN
Bus bar	Loss of electrical efficiency	Moisture, Humidity	4	2	7	56
	Loss of structural integrity	Fracture of the copper bar	5	9	7	315
		Break of the support insulators	6	9	7	378
		Human sabotage	2	10	7	140
		Cracking of connection welds	5	9	7	315
	Loss of electrical continuity	Arc flash	4	10	8	320
	Electrical disturbances	Short circuits between bus bars	4	10	8	320
		Harmonics	4	8	8	256
		Ohmic heating (overload)	4	3	8	96
Cable	Insulation failure	Insulation aging	5	3	6	90
	Cable integrity defect	Manufacturing imperfection	1	1	8	8
		Incorrect installation	2	2	8	32
		Lightnings	7	5	8	280
		Cable breakdown (human sabotage)	4	5	8	160
	Electrical operation failure	Overload	8	2	6	96
		Short circuits transients	6	10	6	360
		Shield damage	6	6	6	216
		Moisture	6	2	6	72

Equipment	Failure Mode(s)	Failure Cause(s)	OCC	DET	SEV	RPN
CB	Insulation failure	Loss of dielectric properties	5	7	6	210
	Wrong operation (Spurious opening and closure)	Improper manual installation	5	4	7	140
		Improper sizing	5	4	7	140
		Overload	6	4	7	168
	Bushing breakdown	Lightning	4	5	6	120
		External short circuit	5	10	6	300
	Bushing terminal hot spot	Heat, oxidation, acidity and moisture	4	3	6	72
		Mechanical stress due to external short circuit conditions	4	8	6	192
	Loss of dielectric strength in bushings	Heat, oxidation, acidity and moisture	4	3	6	72
	CB mechanical failure in operating mechanism	Corrosion	4	3	6	72
		Dirt/contamination	4	3	6	72
		Lack of lubrication	5	3	6	90
	CB contacts degradation	Contact wear	5	3	6	90
		Electrical treeing (partial discharges)	5	9	6	270
Transformer	Bushing breakdown	Lightning	4	5	6	120
		External short circuit	4	10	6	240
	Bushing terminal hot spot	Heat, oxidation, acidity and moisture	4	4	6	96
		Mechanical stress due to external short circuit conditions	4	7	6	168
	Loss of dielectric strength in bushings	Heat, oxidation, acidity and moisture	4	4	6	96
	Magnetic-Core delamination	Harmonics	4	7	6	168
		Corrosion	4	3	6	72
	Winding overheating	Overload	6	7	7	294
	Tap changer mechanical failure in drive mechanism	Corrosion	3	3	6	54
		Dirt/contamination	3	3	6	54
		Friction	3	4	6	72
	Tap changer contacts degradation	Contact wear	3	3	6	54
		Electrical treeing (partial discharges)	3	9	6	162

Equipment	Failure Mode(s)	Failure Cause(s)	OCC	DET	SEV	RPN
	Tank rupture	Vibration-induced damage	3	6	8	144
		Corrosion	3	3	8	72
		Cracking of welds	3	9	8	216
	Windings isolation degradation or breakdown	Short circuits and overloads	4	10	6	240
		Oil contamination	5	3	6	90
		Oil moisture	4	3	6	72
	Distortion, loosening or displacement of the windings	Short circuits	5	9	7	315
	Transformer explosion	Human sabotage	1	3	9	27
		Internal short circuit	5	10	9	450
	Cooling system failure	Cooling pipes obstruction	3	7	8	168
		Damaged fans	3	6	8	144
HMI	Operational failure	Poor communication between HMI and other cyber components	8	3	5	120
		Human error	8	10	5	400
		Poor software design	8	5	5	200
	Power outage	Remote disconnection of power	3	10	5	150
	Security failure	Direct human intrusion: faulty commands (cyber-attacks)	2	6	9	108
		Human Vengeance	2	10	9	180
SW	Performance decrease	Multicast traffic	7	6	6	252
		Blocking (High traffic loads)	5	6	6	180
	Operational failure (SW blackout)	Bad SW configuration	5	2	6	60
		SW is locked up	6	10	6	360
		Module failure	5	10	6	300
	Network/Cyber storm	Broadcast of excessive amount of messages in uncontrollable way (misleading information)	4	7	6	168
	Power outage	Remote disconnection of power	3	10	6	180
	Security failure	Faulty signal injections (cyber-attacks)	2	5	8	80

Equipment	Failure Mode(s)	Failure Cause(s)	OCC	DET	SEV	RPN
SV	Data overload	Lower storage capacity or unexpected large amount of data to storage	3	4	6	72
	Hardware crash	Overheating and high humidity	6	2	8	96
		Hard drive crash	6	10	8	480
		Hardware sabotage	6	2	8	96
		Physical disaster (such as fire, earthquake, lightning or flooding)	1	5	9	45
	Data errors	Software malfunction	5	10	6	300
	Power outage	Remote disconnection of power	3	10	7	210
	Security failure	Denial of service attack (DoS)	2	10	10	200
		Hacking for sensitive information	2	10	9	180
EB	Communication Error	Malicious software infection	2	10	9	180
		Poor signal with SV	4	2	4	32
	Power consumption misreading	Manual manipulation	4	8	4	128
		Significant measurement error, or even inability to measure power consumption	5	8	4	160
	Operation failure	Improper EB programming and parameterization	4	8	4	128
		Erroneous installation	4	3	4	48
		Power supply failure	4	5	4	80
	'Catastrophic' failure (burning, melting or explosion)	Temperature stress	3	4	8	96
	Security failure	Hacking for personnel sensitive information or faulty information injection (cyber-attack)	1	5	7	35
IED	Communication failure	Damaged transducers	3	8	6	144
		Poor communication between IED and remaining cyber-network	5	8	6	240
		Signal processing error (corrupted data)	4	8	6	192
		Network/Cyber storm	5	7	6	210

Equipment	Failure Mode(s)	Failure Cause(s)	OCC	DET	SEV	RPN
	Monitoring failure	I/O port damage	5	4	6	120
		Significant measurement error	5	6	6	180
	Control failure	Inability to apply control commands	7	3	8	168
		Software error (Defective data processing)	7	7	8	392
	Power outage	Remote disconnection of power	3	10	7	210
	Security failure	Hacking for personnel sensitive information	3	7	9	189
		Faulty information injection (cyber-attack)	3	7	9	189
Network link - Ethernet link	Cross talk (overload)	Excessive traffic/ congestion of packets	1	8	4	32
	Network link integrity defect	Manufacturing imperfection	1	2	4	8
		RJ45 degradation	2	2	4	16
		Incorrect installation	1	2	4	8
	Network link breakdown	External damage (accidents)	1	10	4	40
Network link - optical fiber	Fracture	Stress, corrosion or fatigue due to micro cracks	3	10	4	120
	Lead-bonds degradation in plated contacts	Temperature stress	3	3	4	36
	Humidity induced	Electro-chemical oxidation of transmitters and receivers	3	10	4	120