Reliability evaluation for smart distribution grids by fault tree analysis

Gonçalo dos Santos Bravo

Thesis to obtain the Master of Science Degree in

Electrical and Computer Engineering

Supervisors: Prof. João Filipe Pereira Fernandes

Prof. Paulo José da Costa Branco

Examination Committee

Chairperson: Prof. Célia Maria Santos Cardoso de Jesus

Supervisor: Prof. João Filipe Pereira Fernandes

Member of the Committee: Prof. Pedro Manuel Santos de Carvalho

November 2019

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.

“Do what you can with all you have, wherever you are”

- Theodore Roosevelt

Acknowledgments

To Professor João Filipe Pereira Fernandes and Professor Paulo José da Costa Branco, for giving me the opportunity of doing this thesis and for supporting me by clarifying my doubts whenever I needed it.

To Professor Andrés Alejandro Zúñiga Rodríguez, for the many hours spent with me, helping with this thesis.

To my family, especially my parents and sister, who always supported me and were there for me whenever I needed throughout this academic journey.

To my friends, for the good moments that helped me clear my mind when the times were more difficult.

Finally, to my dear grandfather Silvino, that I am sure is proud of me and to whom I dedicate this work.

Resumo

A evolução para uma rede elétrica mais inteligente pretende promover melhorias na fiabilidade e na eficiência da geração, transmissão e distribuição de energia, bem como permitir a integração de mais fontes de energia renovável e de geração distribuída.

Como em qualquer projeto, a rede elétrica inteligente necessita de ser analisada para melhor ser compreendida e planeada. Uma maneira de o fazer consiste em perceber quais são as falhas que afetam a rede elétrica de forma mais frequente e gravosa e, assim, serem definidas estratégias que mitiguem o seu impacto.

Neste contexto, os principais objetivos desta tese são, numa primeira fase, o estudo das principais falhas que afetam os componentes da atual rede elétrica e, usando o estudo anterior, realizar uma análise de fiabilidade usando árvores de falhas para determinar quais os componentes e respetivas falhas mais críticas. Numa segunda fase, a determinação das falhas que afetam o sistema *cyber* e a sua aplicação às árvores de falhas desenvolvidas no ponto anterior, permitem avaliar os impactos destas no sistema global.

Com o decorrer deste trabalho foi possível verificar que a rede estudada é bastante fiável e que os componentes mais críticos são os cabos de 110 kV e os transformadores de 220/110 kV. Foi também verificado que os equipamentos *cyber* não têm grande impacto na fiabilidade da rede.

Palavras-chave: Rede elétrica inteligente, fiabilidade, árvore de falhas, modo de falha, taxa de falha, cibersegurança.

Abstract

The upgrade to a more intelligent electrical grid aims to improve reliability and efficiency on the generation, transmission and distribution of energy, as well as allowing the integration of more renewable energy sources and distributed generation.

Like any project, the smart grid needs to be analyzed to better understand and plan it. One way to do this is to understand which failures affect the electrical grid more often and severely, so strategies can be defined to mitigate their impact.

In this context, the main goals of this thesis are, in a first stage, the study of the main failures that affect the components of the conventional grid and, using this information, perform a reliability analysis using the fault tree method to find which components and failure modes are more critical. In a second phase, identify the cyber system failures and apply them to the fault trees built for the conventional grid, allowing this way to evaluate the impacts on the overall system.

With the development of this work, it was possible to conclude that the studied distribution system is reliable and that the most critical components are the 110 kV cables and the 220/110 kV transformers. It was also verified that the cyber components do not have a major impact on the overall system reliability.

Keywords: Smart grid, reliability, fault tree, failure mode, failure rate, cybersecurity.

Contents

List of Tables

List of Figures

List of Acronyms and symbols

Acronyms

AMI	Advanced Metering Infrastructure
CB	Circuit Breaker
CDF	Cumulative Distribution Function
EV	Electric Vehicle
ES	Ethernet Switch
FT	Fault tree
FV	Fussell-Vesely
HMI	Human Machine Interface
HVDC	High-Voltage Direct Current
IED	Intelligent Electronic Device
IEC	International Electrotechnical Commission
MTTF	Mean Time to Failure
MTTR	Mean Time to Repair
MU	Merging Unit
PDF	Probability Density Function
PT	Proof Time
RBD	Reliability Block Diagram
RISI	Repository of Industrial Security Incidents
RAW	Risk Achievement Worth
RRW	Risk Reduction Worth
SG	Smart Grid
SM	Smart Meter
SCADA	Supervisory Control and Data Acquisition
US	United States

Symbols

A	Availability
E	Expected Value
F	Unreliability
I	Importance Value
Pr	Probability
Q	Unavailability
R	Reliability
r	Repair Time
t	Time
Δ	Variation
λ	Failure Rate
μ	Repair Rate
ω	Frequency

Chapter 1

Introduction

1.1 Motivation

With the development of society, electricity demand has been increasing exponentially. According to [1], global electricity demand will increase 57% by 2050, with China and India being the center of growth. The electric vehicles (EVs) market will grow in the future, and it is expected that by 2050 EVs account for 9% of demand. These and other changes like the introduction of distributed energy sources, the liberalization of the electricity market, the active role of the customers in the grid or environmental factors, with the urge of introducing more renewable energy sources, poses new challenges to the power system [2]. Integrating more renewables is not only beneficial for producers and customers, since there are more ways of producing energy, thereby increasing the reliability of the power system, but also for the planet, from an environmental point of view, since it will reduce the use of fossil fuels. But it also has disadvantages, due to their dependency on the environmental conditions. In some cases, the introduction of more renewables may cause instability in the grid and possibly a blackout. This is an area where the smart grid could improve the power system with the introduction of energy storage.

These weaknesses of the power system are the motivation to create a smarter, more efficient and sustainable grid, therefore the smart grid (SG) concept emerges as an essential step to the modern world. This will be possible due to the emergence of new computer-based technologies like monitoring and control devices. These facts are the key motivation to continue the research in this area and find ways to improve the power system to meet these new requirements.

This work is a contribution to the implementation of the smart grid, focusing on reliability evaluation. The reliability analysis is important in the smart grid context, since new components will be added, increasing the complexity of the grid and, therefore, possibly affecting the reliability of the system. Another factor that may bring new concerns in terms of reliability is the growth in automation and interoperability between the different systems that must be well studied to prevent possible failures.

1.2 Topic overview

Over the last years, fault trees (FTs) proved to be a popular and useful method in the reliability analysis of power systems. Some works have been developed in this area, but to date was not found any work that integrates both power and cyber system with the level of detail that is going to be done in this thesis, identifying not only the critical components of the SG but also the failure modes of each component. In [3], a reliability computer program was developed to study the reliability of a distribution system in Sweden using a reliability-centered maintenance methodology, focusing on the cable component of the system. In [4], the FT methodology was applied to a power system focusing on the disruption of energy delivery from generators to specific load points. An analysis of a small distribution system using the FT method was presented in [5]. Following this work, the same methodology was applied to a HVDC system to identify the minimal cut sets and the most critical components [6]. The authors in [7] performed a reliability analysis on a wind turbine using FTs. The turbine was divided into its components and, through the importance measures, the critical components of the wind turbines were defined.

Some studies have been made on digital substations using the reliability block diagrams (RBDs) methodology [8], [9], [10]. The authors identified the components of the cyber protection system and defined scenarios where the failure of a cyber component would cause extended blackouts. The closest work that was found was an analysis of a SG using the FT method but focusing only on the components and not on the failure modes of each component [11].

1.3 Objectives

The main goal of this thesis is to perform a reliability analysis of a SG. This will be accomplished by, in a first stage, studying the events that contribute to the failure of the main components of a distribution system: the busbars, the circuit breakers (CBs), the transformers and the cables. After the failure modes are defined, failure rates are given to each failure mode instead of just defining a failure rate to the entire component. This allows to see which failure modes are the most critical and, in some cases, which part of each component is the most critical and should be the focus of maintenance.

In a second stage, after the reliability analysis of a conventional distribution system is done, the cyber components failure modes are defined and added to the FT built in the previous stage. This approach allows to evaluate the impact of these new components on the grid.

All of this is performed using the FT method. This method combines events, dependent or not from each other, that lead to the failure of a component and, in some cases, to the failure of the entire system. This is accomplished using Isograph’s software, Reliability workbench 13.0 [12].

1.4 Thesis outline

This thesis is divided into six chapters.

In the first chapter, it is made an introduction to the theme and objectives that are proposed to be achieved.

In the second chapter, it is made a state-of-art and an introduction to the SG concept, presenting its components, characteristics and benefits that make the SG an upgrade to the conventional distribution systems.

In the third chapter, some concepts related to reliability and FTs, that are the base of this work, are presented.

In the fourth chapter, it is done a detailed study of the events that lead to the failure of the different components of a distribution system. Then, a reliability analysis is performed using the FT method. This method allows to conclude which failure modes are the most critical to the system.

In the fifth chapter, the cyber part of the system is added. The same reliability study is done to see the impact of the cyber failures in the physical components of the distribution system.

In the sixth chapter, some final conclusions and ideas of future work are presented.

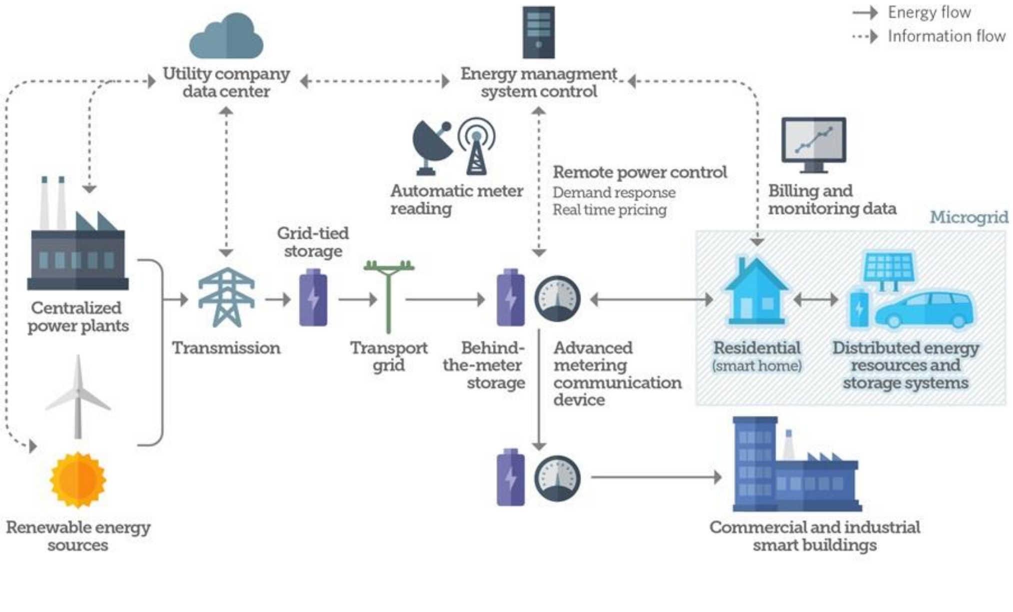
Chapter 2

Smart grid: An introduction

2.1 Definition of smart grid

A SG can be described as an electricity network that integrates modern technology like cyber-secure communication, computer-based control and protection systems, to include more renewable energy sources, EVs and energy storage, to all together manage and monitor the distribution of electricity in a more efficient and reliable way.

The goal of creating the SG is to improve reliability, efficiency and security of the power system. This includes generation, transmission and distribution. In Figure 2.1, it is presented a basic illustration of how the SG works. The generation of energy is no longer centralized, power and information can flow in multiple ways, the transmission and distribution of energy is controlled in real time and the customer has an active role on the grid.



Source: LG CNS

© 2016 The Pew Charitable Trusts

Figure 2.1 Illustration of a smart grid, adapted from [13]

Three major factors are impacting the future of the electric system in the world [14], government policies regarding environmental concerns, urging the implementation of more renewable sources, consumers demanding more efficiency and the introduction of computer-based technologies. Consumers are being encouraged to participate more actively in the energy consumption decisions. Creating consumer awareness aims to raise the use of EVs and distributed generation.

Transportation is one of the areas that most consume energy in the world, and the introduction of EVs has an impact on the grid, for example, charging one EV can double a home's peak load [2]. This is one of the problems that the SG can solve, ensuring that transformers are not overloaded by EVs, using control equipment to protect the grid. The SG will allow utilities to efficiently manage EV charging, by deciding when EV charging should occur and at the same time satisfying the customer's needs through data collected by the smart meters (SMs), the electronic device that allows communication between producer and client in real time, and this way balancing energy usage.

Another important addition that comes with the SG is the ability to store energy. Power sources like solar or wind, require energy storage to be used on cloudy or windless days, and the SG must be able to accommodate this energy. It is expected that energy storage can solve problems like excessive power fluctuation and unstable power supply from renewable energy generation. This energy will serve as load leveling, uninterruptible power supply and emergency power source [2].

2.2 Characteristics of the smart grid

The conventional grid is characterized by having centralized sources of power generation, unidirectional flow of energy, passive participation and knowledge by the consumers, limited to a monthly bill, real-time monitoring and control mainly limited to generation and transmission, and not being flexible to allow injection of electricity from alternative sources at any point of the grid [14]. This urges for improvement that can be achieved by the SG.

To successfully achieve the proposed goal, a SG must have certain characteristics that will be briefly described below.

According to [14], a SG must be:

- **Adaptive:** This means that the system is more autonomous. In a situation of a condition change, the system would respond rapidly and with less human resources;
- **Self-healing:** This means that in case a component fails, the system would be able to repair itself before the entire system fails, removing the failed equipment from the grid and reconfiguring the power flow to sustain power to all customers;
- **Flexible:** The system must be able to rapidly and safely connect the distributed generation and the energy storage, at any point of the grid, at any time;
- **Predictive:** The system can identify potential faults before they occur, using machine learning and weather impact projections, for example;
- **Integrated:** Allows communications in real time;
- **Interactive:** The system must be able to provide information about the status of the grid to the operators and to the customers. This allows the grid to be managed more efficiently;

- **Optimized:** By knowing the status in real time of the components, the system can optimize the flow of energy, maximizing this way the reliability, availability and efficiency;
- **Secure:** All components of the SG must be physically secure as well as cyber secure.

According to [15], the main differences between a SG and a conventional grid can be summarized as in Table 2.1.

Table 2.1 Comparison between conventional and smart grids

Feature	**Conventional grid**	**Smart grid**
Communications	One-way, non-real time	Two-way, real-time
Consumer role	Limited	Extensive
Metering	Mechanical	Digital
Operation and maintenance	Manual	Remote
Generation	Centralized	Centralized and distributed
Power flow control	Limited	Automated
Reliability	Prone to failures	Prevents failures before they happen
Restoration	Manual	Automatic
Topology	One-way power flow	Multiple-way power flow

2.3 Smart grid benefits

Implementing a SG has several benefits [2]:

- Improves efficiency by reducing losses, peak demand control and through the implementation of SMs;
- Improves the reliability of the grid by reducing the frequency and duration of downtimes.
- Improves the quality of supply;
- Improves connection and access to the grid. This is important due to the increased use of renewable energy sources and EVs, for example. The use of renewable energies and EVs will also help the environment by reducing carbon emissions;
- Market benefits. The price of electricity can be adjusted due to the dynamic interaction of the demand with the supply.

Even though the SG has many advantages, one disadvantage comes with it. Cyberattacks are possible in a SG environment. The hacker has the possibility of taking control of the grid and create outages. This topic will be discussed in more detail in chapter 5.

2.4 Smart grid components

To better understand the concept of SG it is important to identify its components. The SG is composed by power components to generate and distribute energy. Some examples are the ones that are going to be focused in this work like the transformers, CBs, cables and busbars. To these components must be added what makes the grid a SG, the communication infrastructure, that allows, for example, to make real-time decisions to more efficiently distribute the energy, and computer-based technologies like digital relays, that are going to replace the old electromagnetic ones, that have the function of monitoring, controlling and protecting the power system.

The MU, a digital equipment that converts the current and voltage analog signals into digital signals, uses the ethernet switch (ES), equipment responsible for allowing communications between all the devices, to send this information to the IEDs, equipment responsible for monitoring and protecting the grid and, in case of a fault, reacting in microseconds, and taking the appropriate measures to isolate the fault [2]. This information is also sent in real time to the control center, where the operator can take actions on the grid to improve efficiency and reliability.

Another important component is the SM, which will replace the conventional analogic meter. These devices are used to meter the energy consumption and monitor statistical consumption data at different time intervals [16].

These components will be discussed in more detail in chapter 5.

2.5 Smart grid current state

To meet these new demands of the modern world, initiatives to implement the SG are already taking place all over the world. In [17], the authors provide an overview of the projects and investments that were already made or are already planned, such as:

- In the European Union, until 2020, is predicted that the investment in the SG will reach €56.5 billion, and by that time 240 million SMs will have been deployed;
- In the United States (US), until 2031, between $338 and $476 billion will be spent. By the end of 2009, 130 SG projects had been implemented. 8 million SMs have already been deployed and, by 2020, 60 million are expected to be in use;
- In China, by 2020, €71 billion are expected to be spent in the implementation of SGs. By 2030, it is expected that 360 million SMs are deployed;
- In South Korea, by 2031, €16.8 billion are going to be used for the implementation of the SG. By 2020, 24 million SMs are expected to be in use.

Chapter 3

Reliability analysis

3.1 Basic reliability concepts

In this section will be described some important reliability concepts, such as:

- Failure, that is the incapacity to perform the required service [6];
- Failure mode, that is the effect caused by a failure on a failed item [6];
- Failure rate, $\lambda(t)$, that is a function of time that represents the rate that failures occur.

The time to failure of a component can be considered as a random variable, T, and modeled using a probability density function (PDF), $f(t)$. As equation 3.1 demonstrates, the probability that a component fails before t is given by the cumulative distribution function (CDF), $F(t)$.

$$\Pr(\mathrm{T} \leq \mathrm{t}) = F(t) = \int_0^t f(t)\, dt \tag{3.1}$$

Reliability, $R(t)$, is defined as the probability that a component operates without failure after a length of time t, and can be obtained using equation 3.2.

$$\Pr(T > t) = R(t) = 1 - F(t) = 1 - \int_0^t f(t)\, dt = \int_t^\infty f(t)\, dt \tag{3.2}$$

The failure rate, $\lambda(t)$, as equation 3.3 proves, is given by the probability that the system fails at some time between t and $t + \Delta t$, given that is not failed at time t, divided by the time interval Δt [6].

$$\lambda(t) = \lim_{\Delta t \to 0} \frac{\Pr\,(\,t < T \leq t + \Delta t |\, T > t)}{\Delta t} = \frac{\dfrac{F(t + \Delta t) - F(t)}{1 - F(t)}}{\Delta t} \tag{3.3}$$

Using equation 3.2,

$$\lambda(t) = \frac{F(t+\Delta t) - F(t)}{\Delta t} \frac{1}{R(t)} \tag{3.4}$$

and knowing that,

$$f(t) = \frac{dF(t)}{dt} = \lim_{\Delta t \to 0} \frac{F(t+\Delta t) - F(t)}{\Delta t} \tag{3.5}$$

the failure rate can be expressed in terms of the PFD and the reliability function, as equation 3.6 shows.

$$\lambda(t) = \frac{f(t)}{R(t)} \tag{3.6}$$

The shape of the behavior of the failure rate function with time is usually called "bathtub curve" (Figure 3.1).

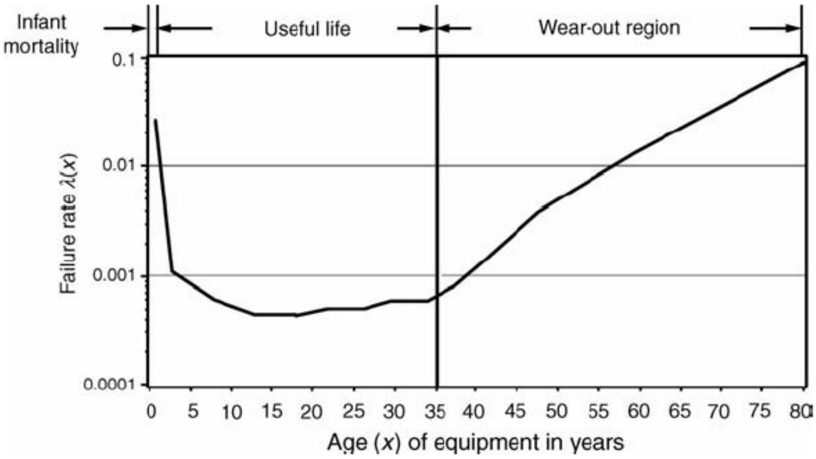


Figure 3.1 Bathtub curve, adapted from [18]

According to the bathtub curve, it is possible to identify three periods related to the life of a component [18]. The first period, at the left side of Figure 3.1, is usually called "infant mortality period", where the failure rate is high at the beginning and decreases along time. Failures in this period are usually related to manufacturing problems, defective materials or installation errors. The second period is called "useful life", where the failure rate is lower and almost constant. In the last period called "wear-out period", the system begins to age and enters its end of life stage, where a lot of the parts start to fail, therefore the failure rate begins to increase.

Since the reliability depends on the failure rate, it is important to relate them. From equations 3.2 and 3.5 it is possible to say that,

$$f(t) = \frac{d}{dt}\big(1 - R(t)\big) \tag{3.7}$$

Using equation 3.6, after some mathematical manipulation, it is possible to conclude that,

$$R(t) = e^{-\int_0^t \lambda(t)\, dt} \tag{3.8}$$

The mean time to failure (MTTF), as the name says, is the expected time, $E(T)$, that a component takes to fail, and can be obtained through equation 3.9, using equations 3.2 and 3.5.

$$MTTF = E(T) = \int_0^\infty t.f(t)\, dt = \int_0^\infty R(t)\, dt \tag{3.9}$$

There are two types of components, repairable and non-repairable. In the second case, after the component fails, it can be repaired, therefore the mean time to repair (MTTR) concept appears. As shown in equation 3.10, MTTR is the expected time that a component takes to be repaired.

$$MTTR = E(T) = \int_0^\infty t.F_R(t)\, dt = \int_0^\infty \left(1 - F_R(t)\right) dt \tag{3.10}$$

Where $F_R(t)$ represents the PDF of the time to repair, T.

For repairable systems, the mean time between failures (MTBF) can also be defined, as equation 3.11 demonstrates, it is the sum of the mean time to fail and the mean time of repair.

$$MTBF = MTTF + MTTR \tag{3.11}$$

Availability, $A(t)$ is the probability that the system is operating at a given time. The average availability, A_{AV}, is the proportion of time that the system is operating [18] and is given by equation 3.12.

$$A_{AV} = \frac{MTTF}{MTTF + MTTR} \tag{3.12}$$

Unavailability, $Q(t)$ is the probability that the system is failed at a given time. The average unavailability, Q_{AV}, can be defined as the proportion of time the system is down, using equation 3.13.

$$Q_{AV} = 1 - A_{AV} = \frac{MTTR}{MTTF + MTTR} \tag{3.13}$$

Reliability work related with electrical and electronics components usually deals with the long useful life (low risk of failure) period of the bathtub curve (Figure 3.1), where the failure rate is almost constant [18]. For this reason, in this thesis is used the constant failure rate model, which is defined by a constant failure rate and repair time.

The constant failure rate model considers that the time to failure is represented by an exponential probability distribution, defined in equation 3.14 and represented in Figure 3.2.

$$f(t) = \begin{cases} \lambda e^{-\lambda t}, & t > 0, \lambda > 0 \\ 0 & otherwise \end{cases} \tag{3.14}$$

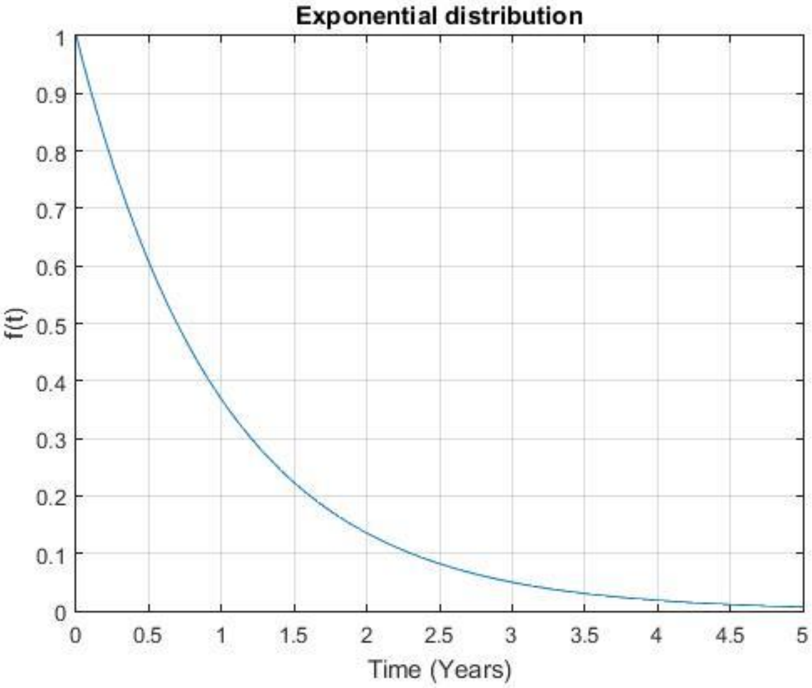


Figure 3.2 Exponential distribution for $\boldsymbol{\lambda} = \mathbf{1}$ failure/year

Using equation 3.8, in this case, the reliability function is expressed as in equation 3.15.

$$R(t) = e^{-\lambda t} \tag{3.15}$$

From equation 3.6, it can be proved that in this model the failure rate is a constant value, as equation 3.16 shows.

$$\lambda(t) = \frac{f(t)}{R(t)} = \frac{\lambda e^{-\lambda t}}{e^{-\lambda t}} = \lambda \tag{3.16}$$

According to equation 3.9, the MTTF in this model is simply,

$$MTTF = \int_0^\infty R(t)\, dt = \int_0^\infty e^{-\lambda t}\, dt = \frac{1}{\lambda} \tag{3.17}$$

The failure rate is easily obtained by,

$$\lambda = \frac{1}{MTTF} \tag{3.18}$$

Similarly, as equation 3.19 shows, the MTTR will be a function of the repair rate, μ, which is analogous to the failure rate but regarding the repair time, r, of the component.

$$\mu = \frac{1}{MTTR} = \frac{1}{r} \tag{3.19}$$

This relation between the MTTR and the repair time is only valid for this model, where it is considered a constant repair rate.

The unavailability, Q, for this model can be expressed in terms of the failure rate and repair time as in equation 3.20, according to equation 3.13.

$$Q = \frac{\lambda}{\lambda + \mu} \tag{3.20}$$

And the failure frequency is given by [6],

$$\omega = \lambda(1 - Q) \tag{3.21}$$

In electrical applications, the unavailability is usually very low, therefore the failure frequency can be approximated as a function of only the failure rate.

Another commonly used failure model is the dormant failure model. This model is frequently used to simulate the behavior of components with dormant or hidden failures. For example, the CB failure mode "does not open on command". This is an example of hidden failure. This means that this failure will only be detected during a proof test, or when another component fails and the CB must operate to protect the rest of the system.

In this case, the average unavailability can be obtained using a test proof time, PT, usually one year, through equation 3.22 [5]:

$$Q_{AV} = \frac{\lambda . PT}{2} + \lambda . MTTR \tag{3.22}$$

3.2 Basic fault tree concepts

The FT analysis is an analytical-based reliability method used to identify possible causes of failure in a system. In electrical systems is useful to define which components are the most critical and what makes them fail.

A FT is composed by basic events that combine through logic gates in different paths that lead to a top event, in this case, the failure of a component of the grid or the entire system.

In Figure 3.3 is presented a basic example of a FT.

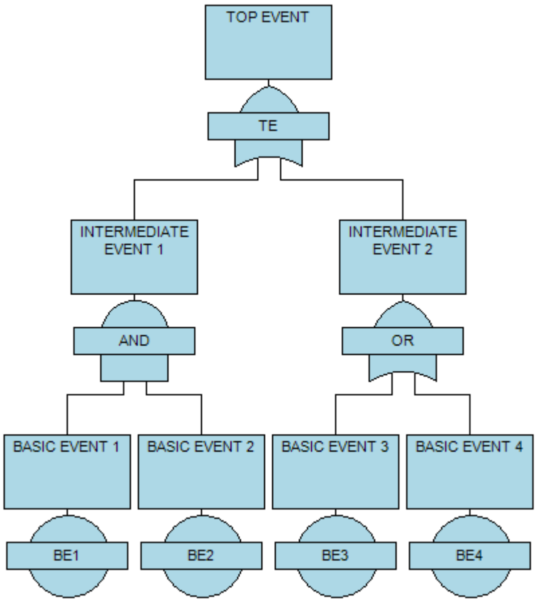


Figure 3.3 Fault tree example

The top event is the event that is going to be analyzed, and results from the combination of lower-level events. In some cases, basic events are not enough to make the top event occur, therefore they combine with other basic events, through an AND gate, resulting in an intermediate event. The basic event is the initial failure that will lead to a top event. Basic events are represented by a circle, but in some cases are represented by a diamond, called undeveloped events. Undeveloped events are used to represent events that have lower-level events but the author chose to not represent them.

The AND gate means that an event only occurs if all the predecessor events occur. The OR gate means that an event occurs if one or more predecessor events occur. When the gate is represented by a triangle, it is a transfer gate, means that the fault tree continues in another tree.

The first step to build a fault tree should be identifying the top event, in this case, the failure of the system. Then, should be identified all the basic and intermediate events that connected through logic gates will lead to the top event.

A FT can have many levels. The more levels it has, the more detailed it is. At the bottom of the FT should be the basic events that are the cause of the intermediate events and that will result in the top event. Every event should be well described, so the risks can be assessed.

To analyze the reliability of the system, using the FT method, two approaches can be taken. The qualitative and the quantitative [6]. In the qualitative method, minimal cut sets are obtained through Boolean reduction and sorted by size (number of events present in a minimal cut set).

A cut set is the combination of basic events to reach the top event. A minimal cut set is the smallest path to reach the top event [19]. This method helps to read the FT because it makes it much simpler by reducing the tree to its most relevant paths.

In the quantitative method, the goal is to determine the unavailability and reliability of the top event. To achieve this, the minimal cut sets must be established and the unavailability of all components of the system must be known.

In a fault tree with an AND gate, the top event (TOP) occurs if all the basic events occur. Therefore, the unavailability of the top event, $Q_{TOP,}$ can be obtained by [6],

$$Q_{TOP}(t) = \prod_{i=1}^{n} q_i(t) \tag{3.23}$$

Where q_i is the unavailability of the i-th basic event.

Similarly, the reliability can be obtained using equations 3.24 and 3.25.

$$F_{TOP}(t) = \prod_{i=1}^{n} F_i\,(t) \tag{3.24}$$

$$R_{TOP}(t) = 1 - F_{TOP}(t) \tag{3.25}$$

For the exponential case, the reliability is given by,

$$R_{TOP}(t) = 1 - \prod_{i=1}^{n} (1 - e^{-\lambda_i t}) \tag{3.26}$$

In a fault tree with an OR gate, the top event occurs if at least one of the basic events occur. Therefore, the unavailability of the top event can be obtained by [6],

$$Q_{TOP}(t) = 1 - \prod_{i=1}^{n} [1 - q_i(t)] \tag{3.27}$$

The reliability for an OR gate is the probability of none of the basic events occur. Therefore, can be obtained by,

$$R_{TOP}(t) = \prod_{i=1}^{n} R_i\,(t) \tag{3.28}$$

And for the exponential case,

$$R_{TOP}(t) = e^{-(\sum_{i=1}^{n} \lambda_i) t} \tag{3.29}$$

A similar way of performing reliability analysis is using RBDs. This methodology is similar to the FTs, instead of representing the system by basic failure events, RBD uses blocks to represent the entire component, where the block means that the component is operating, then for the final block to be working, all the ones connected to it must be working. A FT can be converted in RBD and vice versa.

RBD uses parallel connections to represent dependent events instead of using an AND gate like in a FT, and uses series connections to represent independent events that are represented by an OR gate in the FT analysis.

3.3 Importance measures

One of the results of the reliability analysis is the importance measures. These measures give the relative significance of one component or event regarding the overall reliability of the system, represented by the top event, in terms of the fault tree analysis [19].

This type of analysis is useful because usually there are few events with a high contribution to the top event, making easier to identify which events or components are most critical to the system.

Identify these critical components is important in terms of maintenance and resource allocation, meaning that the operator of the grid will focus more on the components that have more probability of making the system fail. According to [19], the importance indices has helped industries to reduce maintenance resources by 40%, while maintaining or decreasing the probability of the top event, i.e., the system failure.

The importance measures used in this thesis are the following:

- Fussell-Vesely (FV) – This measure represents the contribution of a basic event to the top event, i.e., the probability of a basic event being the cause, or one of the causes, of the system failure, if the system is failed at a given time, t, and it is expressed as in equation 3.30, where Q_{TOP} is the unavailability of the top event and $Q_{TOP}(q_i = 0)$ is the unavailability of the top event if event i is guaranteed to not happen;

$$I^{FV}(i|t) = \frac{Q_{TOP}(t) - Q_{TOP}(t)(q_i = 0)}{Q_{TOP}(t)} \tag{3.30}$$

- Risk reduction worth – This measure indicates the decrease in the probability of the top event if the given basic event does not occur. This measure is defined as the ratio of the top event unavailability, with the top event unavailability, if event i is guaranteed to not happen, as equation 3.31 demonstrates;

$$I^{RRW}(i|t) = \frac{Q_{TOP}(t)}{Q_{TOP}(t)(q_i = 0)} \tag{3.31}$$

- Risk achievement worth – The opposite of the RRW. It is the probability increase of the top event if the given event occurs. Equation 3.32 shows that this measure is defined by the ratio of the top event unavailability, if event i happens, with the top event unavailability.

$$I^{RAW}(i|t) = \frac{Q_{TOP}(t)(q_i = 1)}{Q_{TOP}(t)} \tag{3.32}$$

Chapter 4

Reliability analysis of the Birka Nät distribution system

4.1 The grid

In this chapter, the reliability of the Birka Nät distribution system will be studied using the FT method, with the help of Isograph's software, Reliability workbench 13.0 [12]. This system was chosen because it is a real system, already analyzed in the reliability context in [3], where data regarding the failure rate and repair time of the components are provided. For now, the cyber components will not be considered, this way will be possible to compare the reliability results of a traditional grid with a SG.

The grid is composed by six substations, a 220/110 kV, that includes components c1-c4 and c8-c10, connected to a 110/33 kV one by cables c5 and c11 (7.2 km), that includes components c6, c7, c12-15, c19, c23, c37, c40, c43, c50 and c53. To this substation are connected three load points, two 33 kV ones, SJ, connected by cables c51 and c54 (0.9 km), that includes components c52, c55, c57 and c58, and HD, connected by cables c38, c41 and c44 (2.4 km), that includes components c39, c42, c45, c47 and c48. Also connected to the 110/33 kV substation by cables c16, c20 and c24 (0.03 km) is the 33/11 kV substation, that includes components c17, c18, c21, c22 and c25-c28. Through cables c30 and c31 (8.1 km) is connected the 11/0.4 kV substation that includes components c33-c35 and is connected to the 0.4 kV load point LH11.

The model of the grid presented in [3] proposes a simplification of the real system busbar arrangement. The double busbar arrangement is represented by a single busbar, and instead of the 72 hours of repair time of each busbar, one hour of repair time is given to the single busbar. This one hour intends to simulate the switching of power from one busbar to another after one of the busbars fails.

The system used in the reliability analysis is presented in Figure 4.1.

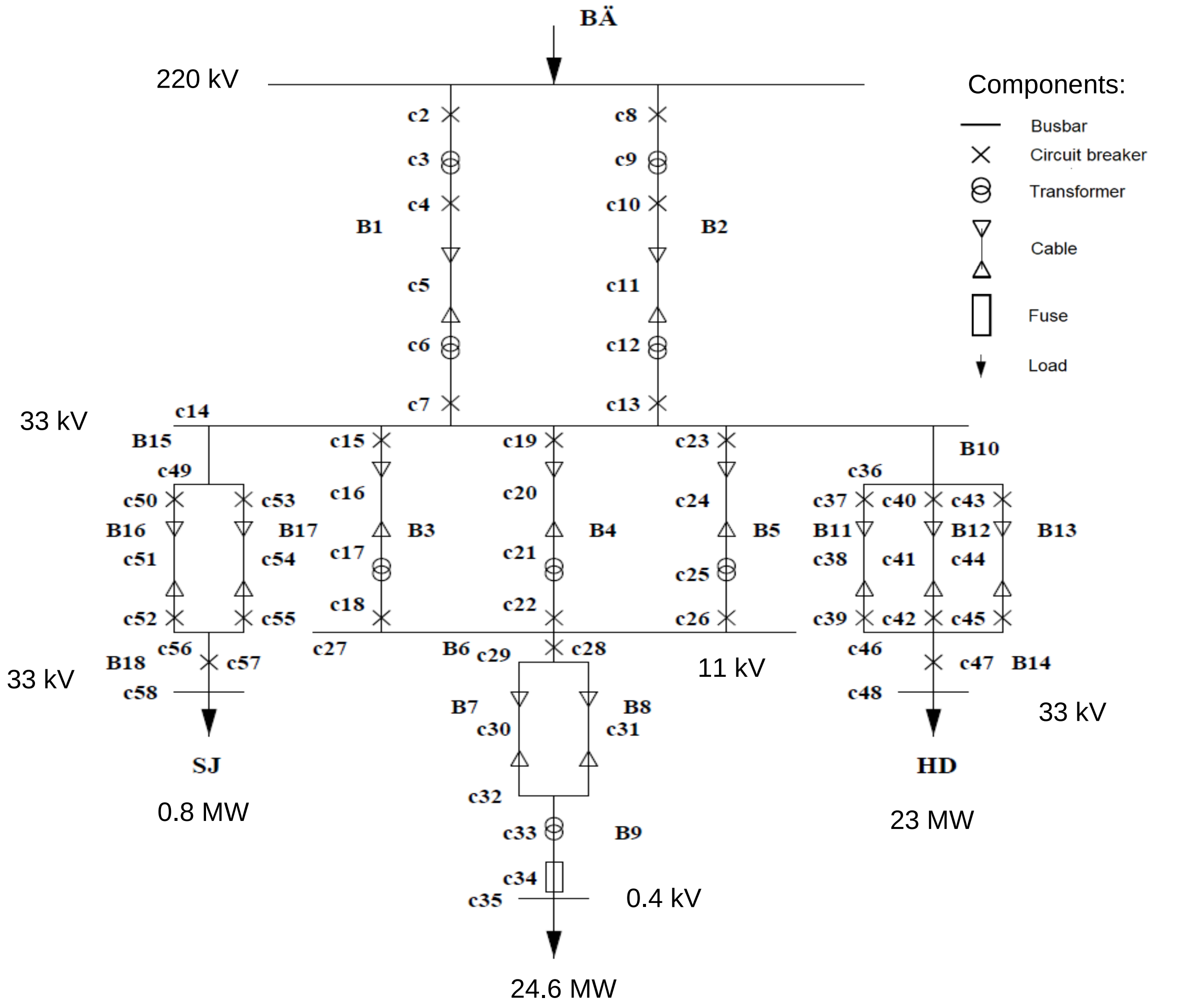


Figure 4.1 Birka Nät distribution system, adapted from [3]

It is important to note that this is a model of the real system and not every component is here represented. The components that are going to be considered are the following:

- 220 kV Busbar (c1);
- 220 kV CBs (c2, c8);
- 220/110 kV Transformers (c3, c9);
- 110 kV CBs (c4, c10);
- 110 kV Cables (c5, c11);
- 110/33 kV Transformers (c6, c12);
- 33 kV CBs (c7, c13, c15, c19, c23, c37, c,39, c40, c42, c43, c45, c47, c50, c52, c53, c55, c57);
- 33 kV Busbars (c14, c48, c58);
- 33 kV HD Cables (c38, c41, c44);
- 33 kV SJ Cables (c51, c54);
- 33 kV LH33 Cables (c16, c20, c24);
- 33/11 kV Transformers (c17, c21, c25);
- 11 kV CBs (c18, c22, c26, c28);
- 11 kV Busbar (c27);

- 11 kV LH11 Cables (c30, c31);
- 11 kV Fuse (c34);
- 11/0.4 kV Transformers (c33);
- 0.4 kV Busbar (c35);

4.2 Electrical power system fault trees

In this section, the failure modes and basic events of each type of equipment of the power system will be presented.

4.2.1 Busbars

The busbar is an important component of a substation. They have the function of receiving the energy from the incoming feeders and distribute them to the outgoing feeders and are required when the number of incoming and outgoing feeders is different. An example of a busbar is presented in Figure 4.2.

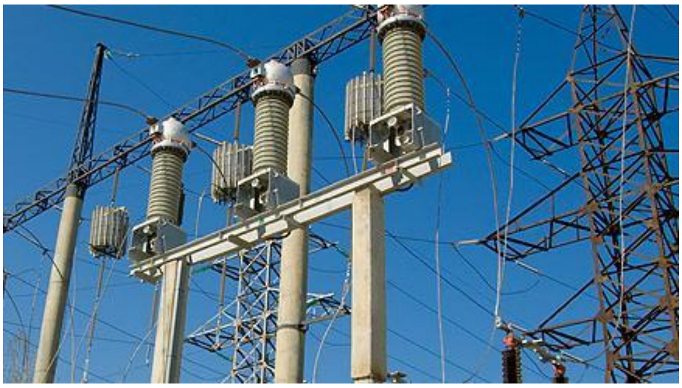


Figure 4.2 Busbar, adapted from [20]

The failure modes of this component are mechanical failures and electrical failures, namely, short circuits [21]. Mechanical failures include the cracking of the connection welds or breakage of the mechanical support structure, caused by natural disasters or a foreign object, for example, human sabotage. Short circuits can be caused by moisture, degradation of the insulators, lightning strikes or a fault in another component of the grid. The FT for the busbar can be seen in Figure 4.3.

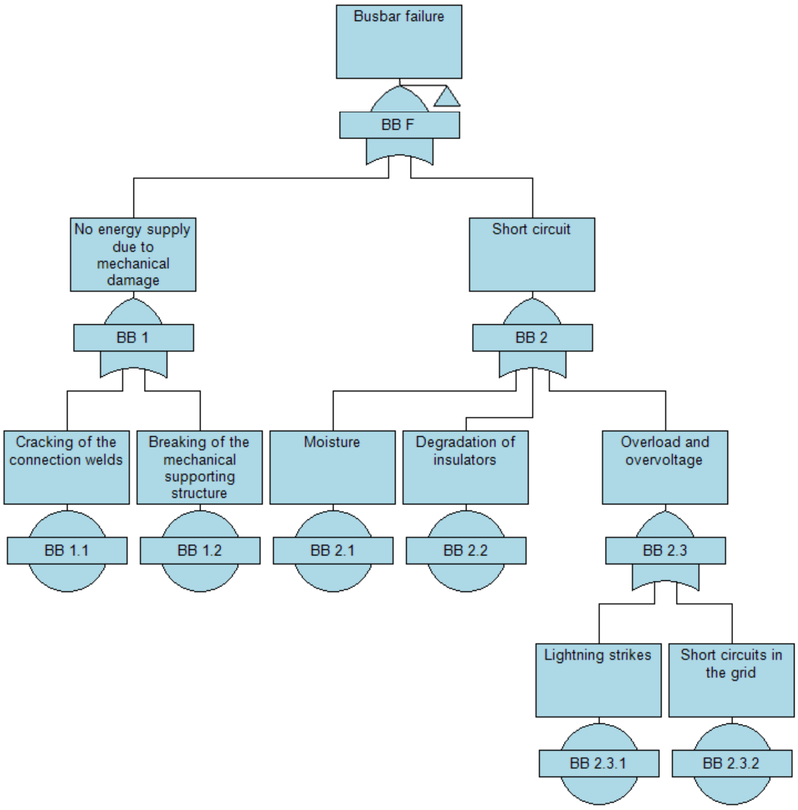

Busbar failure
BB F
No energy supply due to mechanical damage
BB 1
Short circuit
BB 2
Cracking of the connection welds
BB 1.1
Breaking of the mechanical supporting structure
BB 1.2
Moisture
BB 2.1
Degradation of insulators
BB 2.2
Overload and overvoltage
BB 2.3
Lightning strikes
BB 2.3.1
Short circuits in the grid
BB 2.3.2

Figure 4.3 Busbar fault tree

4.2.2 Circuit breakers

According to [22], there are four types of high voltage CBs:

- Oil CBs;
- Air blast CBs;
- Vacuum CBs;
- SF6 CBs.

The high voltage CBs are one of the most important parts of a power system that serve four main purposes [22]:

- Switching-off operating currents;
- Switching-on operating currents;
- Short-circuit current interruption;
- Secure open and closed position.

An example of circuit breaker can be seen in Figure 4.4.

Figure 4.4 Circuit breaker, adapted from [23]

The failure modes that are going to be considered in this analysis are the ones related to operational failures, not opening or closing on command, opening or closing without command and insulation failures that lead to short circuits. These failure modes and their causes [24] can be seen below and the FT in Figure 4.5.

Does not close on command – When the fault is isolated and the component repaired, the operator closes the CB. Sometimes they do not close, this can happen due to a defective close coil, loss of stored energy, inadequate lubrification or a control circuit failure.

Does not open on command – After a fault on another component, the CB responsible for the protection of that component is supposed to open to isolate the fault and not damage other components. Sometimes the CB fails to open, this can happen due to a shorted trip coil, inadequate lubrification, loss of stored interrupting energy, control circuit failure, mechanism linkage failure between operating mechanism and interrupters, trip latch surface wear, deteriorated bearings or mechanism cabinet below required temperature.

Insulation failure – The failures on the CBs are usually only detected after a fault on another component that requires the CB to operate. But they can fail themselves, due to loss of dielectric medium. This dielectric medium depends on the type of CB, can be oil, air, SF_6 gas or vacuum. This type of failure may also happen due to external damage from the environment.

Opens without command – The CBs should only open to isolate faults or for scheduled maintenance. But sometimes they open spontaneously as a result of the trip latch not being secure, stray current in the trip circuit, ground on the trip circuit or loss of voltage on undervoltage trip.

Closes without command – When the CB opens to isolate a fault, it is supposed to stay open until the operator closes it. Sometimes CBs may close without command, this can be caused by stray current in the close circuit, ground on close circuit or vibration in the environment.

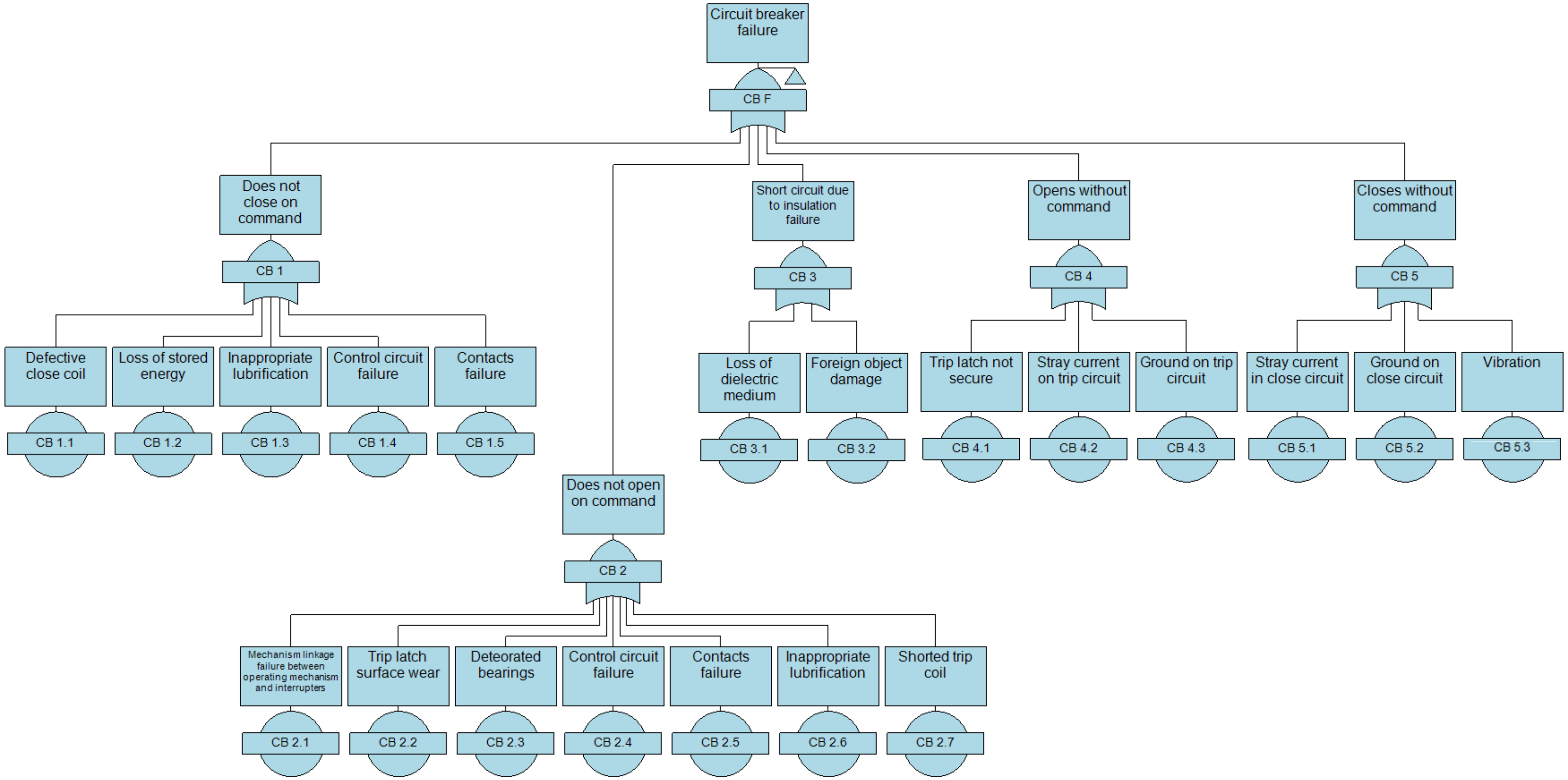


Figure 4.5 Circuit breaker fault tree

4.2.3 Transformers

The transformers have the function of stepping up or down the voltage in the power grid. An example of a transformer can be seen in Figure 4.6.

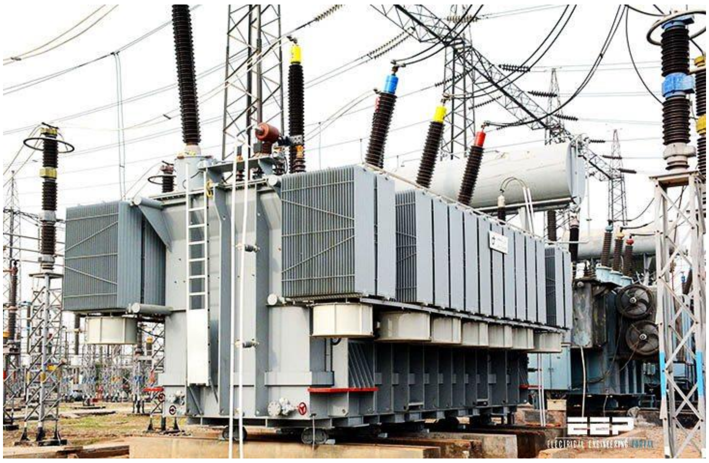


Figure 4.6 Transformer, adapted from [25]

To analyze the failure modes of the transformer it is helpful to divide it into its components. The transformer can be divided into windings, tank, cooling system, tap changer, bushings, and insulation.

The following are the failure modes of the transformer [26], that allowed to build the fault tree presented in Figure 4.7.

Windings – The windings are cylindrical shells wrapped with insulation paper and placed around the core. The most used material in windings is copper, and their function is to carry the current. Lightning strikes, short circuits in the grid, and displacement of the windings can cause short circuits on the transformer. Another cause of failure of the windings is the degradation of the insulation material.

Tap changer – The tap changer is formed by the tap selector and the diverter switch. The function of this component is to regulate the voltage level by changing the turns on the windings. The failures associated with this device are usually due to wear. Furthermore, the oil in the diverter switch must be cleaned to maintain the contacts fully functional.

Bushings – There are many types of bushings. In an oil-filled transformer, the insulation on the bushings is air on one end, and oil on the other end. The main function of the bushings is to connect the windings to the power system outside of the transformer and to provide insulation to the tank and the windings. The physical damage on the bushings can happen due to human sabotage or careless handling. Contamination of the oil or hot spots are other events that lead to short circuits.

Insulation – The function of the solid insulation is to provide dielectric and mechanical insulation to the windings. The major problem is the aging of the cellulose because it is irreversible and expensive to replace.

The oil in the transformer has the purpose of cooling down the transformer but is also responsible for impregnating the cellulose and isolate the different parts of the transformer.

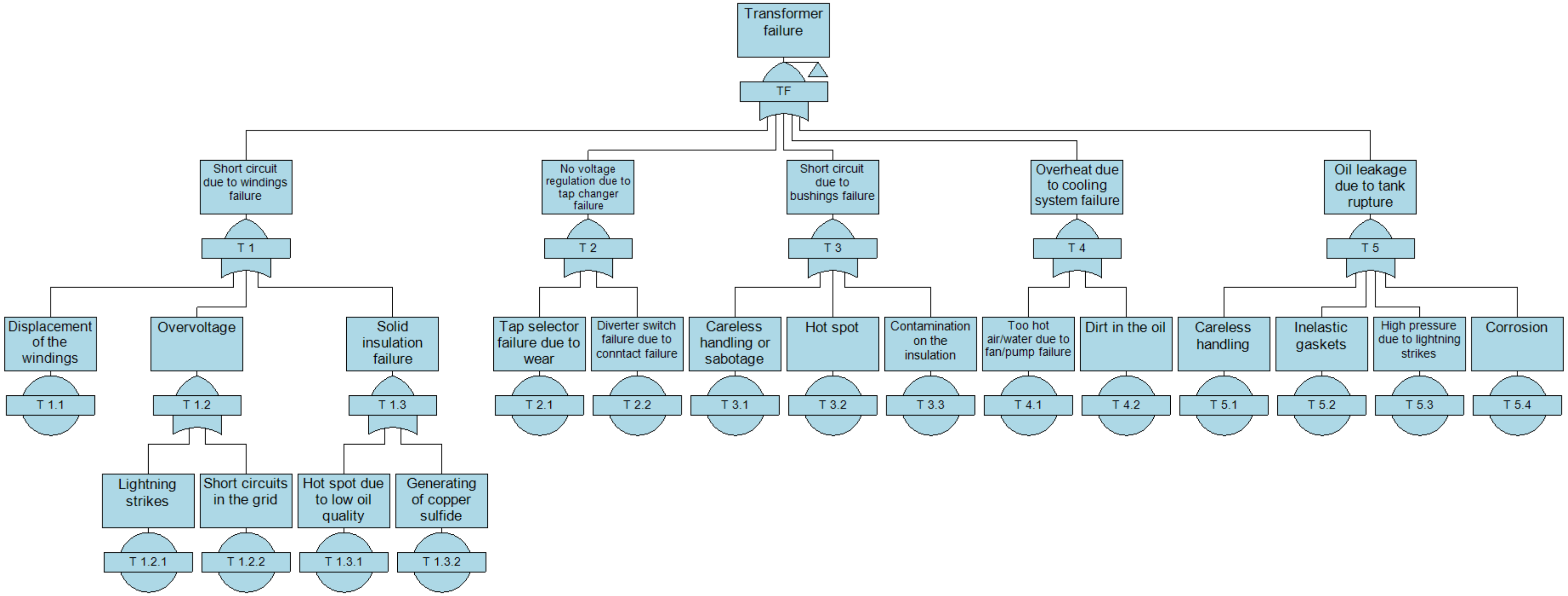

Transformer failure
TF
Short circuit due to windings failure
T 1
No voltage regulation due to tap changer failure
T 2
Short circuit due to bushings failure
T 3
Overheat due to cooling system failure
T 4
Oil leakage due to tank rupture
T 5
Displacement of the windings
T 1.1
Overvoltage
T 1.2
Solid insulation failure
T 1.3
Tap selector failure due to wear
T 2.1
Diverter switch failure due to conntact failure
T 2.2
Careless handling or sabotage
T 3.1
Hot spot
T 3.2
Contamination on the insulation
T 3.3
Too hot air/water due to fan/pump failure
T 4.1
Dirt in the oil
T 4.2
Careless handling
T 5.1
Inelastic gaskets
T 5.2
High pressure due to lightning strikes
T 5.3
Corrosion
T 5.4
Lightning strikes
T 1.2.1
Short circuits in the grid
T 1.2.2
Hot spot due to low oil quality
T 1.3.1
Generating of copper sulfide
T 1.3.2

Figure 4.7 Transformer fault tree

Cooling system - The cooler may be unable to cool down the transformer due to the failure of the fans or a malfunction of the oil circulation, caused by the failure of the oil pump or by dirt in the oil. This will cause an overheat that will lead to the shutdown of the transformer.

Tank – The tank is where the oil is contained and is the physical protection of the active part of the transformer. Lightning strikes can lead to high gas pressures that can rupture the tank and cause oil leakage. Regular maintenance is necessary to prevent corrosion.

4.2.4 Cables

The cables in this system are underground and have the function of carrying the energy. An illustration of a cable system can be seen in Figure 4.8.

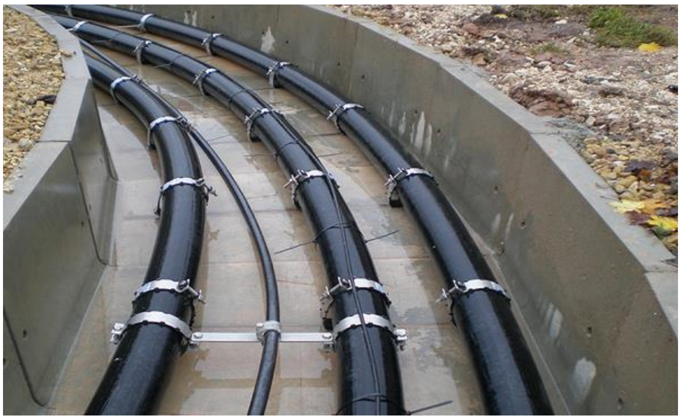


Figure 4.8 Cables, adapted from [27]

Although it is considered that aging is the major threat to cables, it will not be considered as a failure in this analysis, since it is a long-term problem that can be postponed with appropriate maintenance.

The cable failures can be divided into two main categories, mechanical failures and insulation failures. According to [28], mechanical failures may be the result of human sabotage, accidental cut by a machine, sharp bending due to incorrect installation or vibration. When the sheath of the cable is damaged, moisture will enter the cable and slowly deteriorate the insulation material, leading to short circuits and to the failure of the cable. Heat on the cable is another reason for the degradation of the insulation, this may be caused by overloading, high ambient temperatures, or insufficient ventilation.

The fault tree for the cable is presented in Figure 4.9.

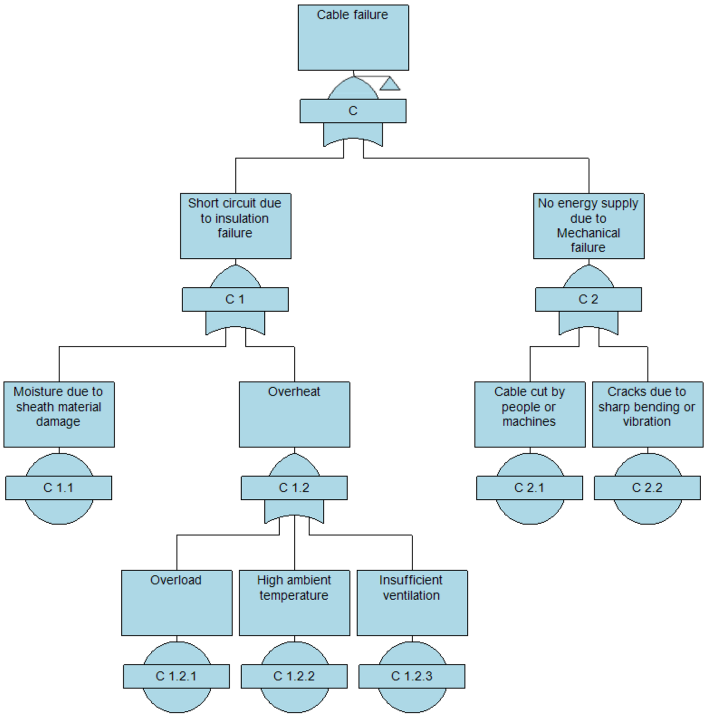

Cable failure
C
Short circuit due to insulation failure
No energy supply due to Mechanical failure
C 1
C 2
Moisture due to sheath material damage
Overheat
Cable cut by people or machines
Cracks due to sharp bending or vibration
C 1.1
C 1.2
C 2.1
C 2.2
Overload
High ambient temperature
Insufficient ventilation
C 1.2.1
C 1.2.2
C 1.2.3

Figure 4.9 Cable fault tree

4.3 Reliability input data

To perform the reliability analysis, the FTs presented in the previous section were simplified, using only the failure modes of each component due to the lack of detailed information related to the failure rate and repair time of each basic event.

The failure rates and repair times per component were obtained from [3]. Since the failure rates usually are given at a component level, the failure rate can be distributed in terms of component's failure modes, considering failure statistics found in the literature, [29], [30], [31]. In these analyses it is possible to find a percentual distribution of the failure modes for each component, allowing this way to study not only the most critical components to the grid but also the critical failure modes.

The detailed reliability input data is presented in Appendix A. In Figures 4.10 to 4.13 are presented the failure modes used in this analysis and the respective failure distribution.

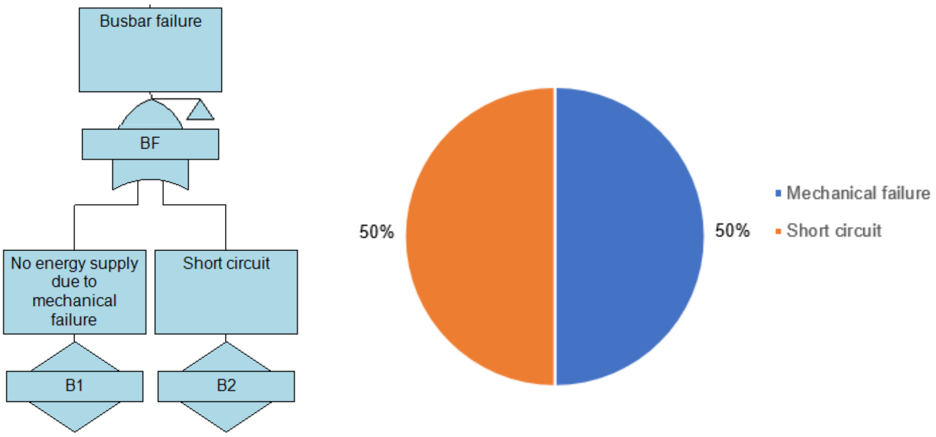


Figure 4.10 Busbar fault tree and failure distribution used in the computations

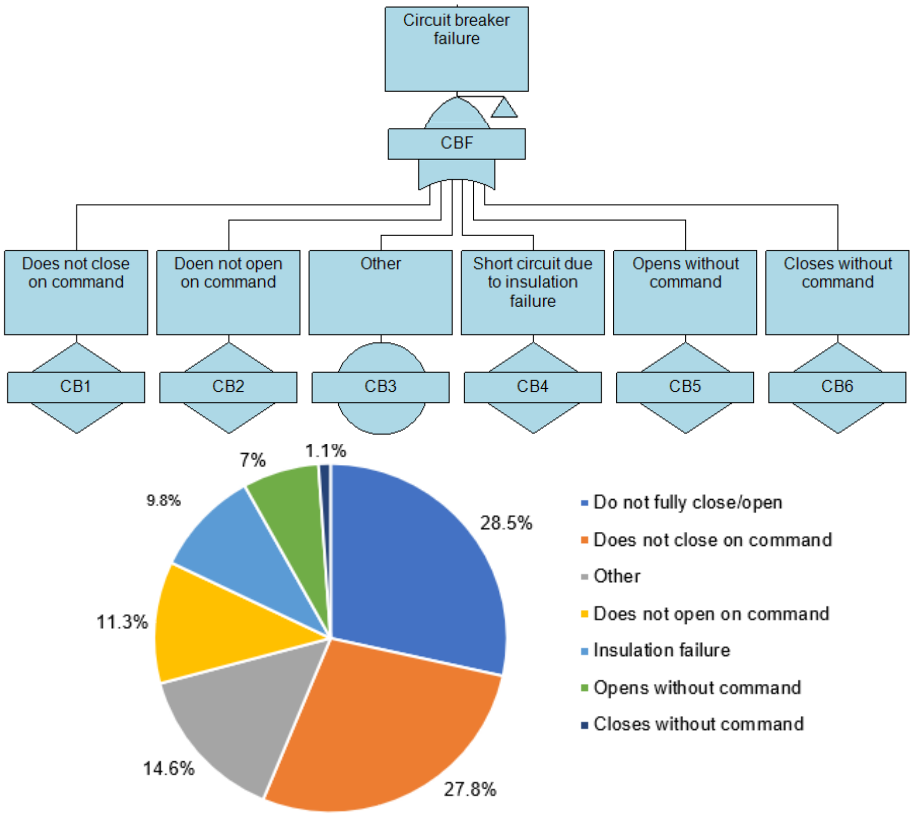


Figure 4.11 Circuit breaker fault tree and failure distribution used in the computations

Note that the failure mode “Do not fully close/open” was assumed to be a part of the failure modes “Does not close on command” and “Does not open on command”.

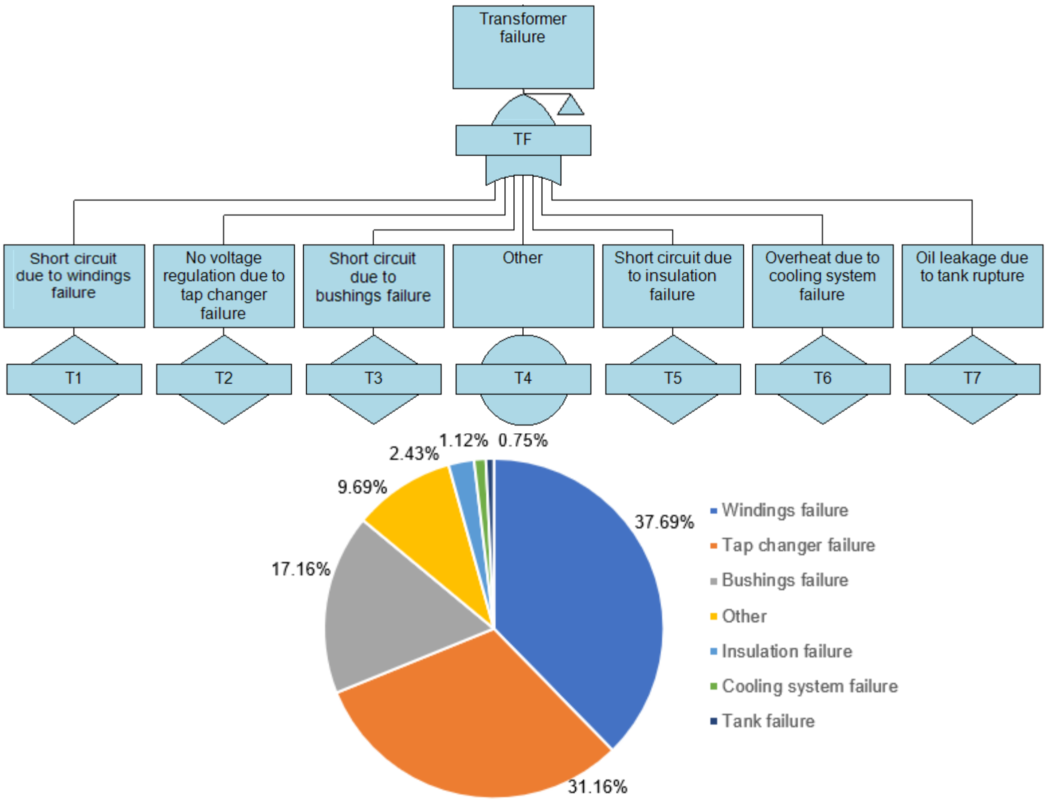

Transformer failure
TF
Short circuit due to windings failure
No voltage regulation due to tap changer failure
Short circuit due to bushings failure
Other
Short circuit due to insulation failure
Overheat due to cooling system failure
Oil leakage due to tank rupture
T1
T2
T3
T4
T5
T6
T7
37.69%
31.16%
17.16%
9.69%
2.43%
1.12%
0.75%
Windings failure
Tap changer failure
Bushings failure
Other
Insulation failure
Cooling system failure
Tank failure

Figure 4.12 Transformer fault tree and failure distribution used in the computations

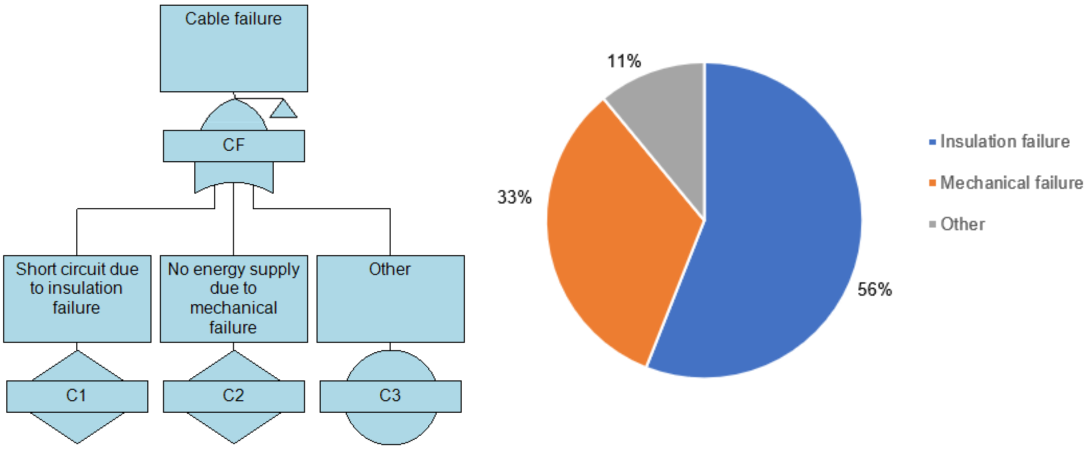

Cable failure
CF
Short circuit due to insulation failure
No energy supply due to mechanical failure
Other
C1
C2
C3
11%
33%
56%
Insulation failure
Mechanical failure
Other

Figure 4.13 Cable fault tree and failure distribution used in the computations

4.4 Results

4.4.1 Reliability of the Birka Nät

This distribution system has 37,701 customers that require an average power of 48.4 MW and a maximum power of 81.2 MW [3].

To study the reliability of the Birka Nät distribution system, the FT presented in Figure 4.15 was used, using the failure modes of each component defined in section 4.3.

This first computation intends to evaluate the reliability of the connections between the 220 kV substation c1 and the 33 kV substation c14. This test was chosen because all three load points are connected to the 33 kV substation c14, therefore this point of the grid can represent the failure of the entire grid, i.e., if there is no power on busbar c14, all three load points will be without power. The top event (No power on busbar c14) happens if busbar c1 fails (gate C1), busbar c14 fails (gate C14) or one of the components from both lines B1 and B2 fails at the same time (gate B1,B2).

Due to memory limitations of the software was not possible to include all the components of the grid in this FT. To overcome this, regarding the components downstream of busbar c14, only the failures from each component that can affect busbar c14 were included. These events are a short circuit on one of the CBs directly connected to busbar c14 (gate CB SC) or their malfunction (gate CB) after a fault (not opening on command), since these events would require an interruption of power from lines B1 and B2, leading to a temporary outage. These kind of failures on the CBs directly connected to busbar c1 would also have this effect. In a real-life scenario, following one of these events, the operation of a disconnector, an offload device that is usually used to disconnect parts of the circuit to perform maintenance work, would be required. Once the operation was stopped, the line that was not isolated due to the short circuit or malfunction of one of the CBs, would be isolated by the disconnector, this way the operation of the grid could be resumed on the healthy parts of the system. These events would cause a temporary outage on the grid, and to these events was taken a similar approach to the one done on the double busbar arrangement. Instead of the normal repair time of each component, one hour was given to these failure modes, to simulate the time to isolate the line with the failed component and resume the operation of the grid.

Even without incorporating all the components of each load point, this is still an accurate evaluation of the entire grid, since to not have power on all three load points at the same time, assuming there is power on busbar c14, at least one non redundant component from each load point would have to fail at the same, a very unlikely event.

Further on this chapter, SJ, HD and LH11 load points will be individually studied in detail, allowing this way to evaluate the reliability of each one and know which are the critical failure modes and components of each load point, since from the point of view of the producer, the objective is to have all load points operating at all times.

The difference from the FTs presented in section 4.3 is that some failure modes of the CBs depend on other components. These failures modes are “Does not open on command”, “Does not close on command” and “Closes without command”.

It is assumed that the CBs start as closed and only open when a fault occurs in another component. If the CB does not open to clear the fault, it is assumed that the next CB will clear the fault, since the failure of three components at the same time is very unlikely. An example of the FT of one CB is presented in Figure 4.14.

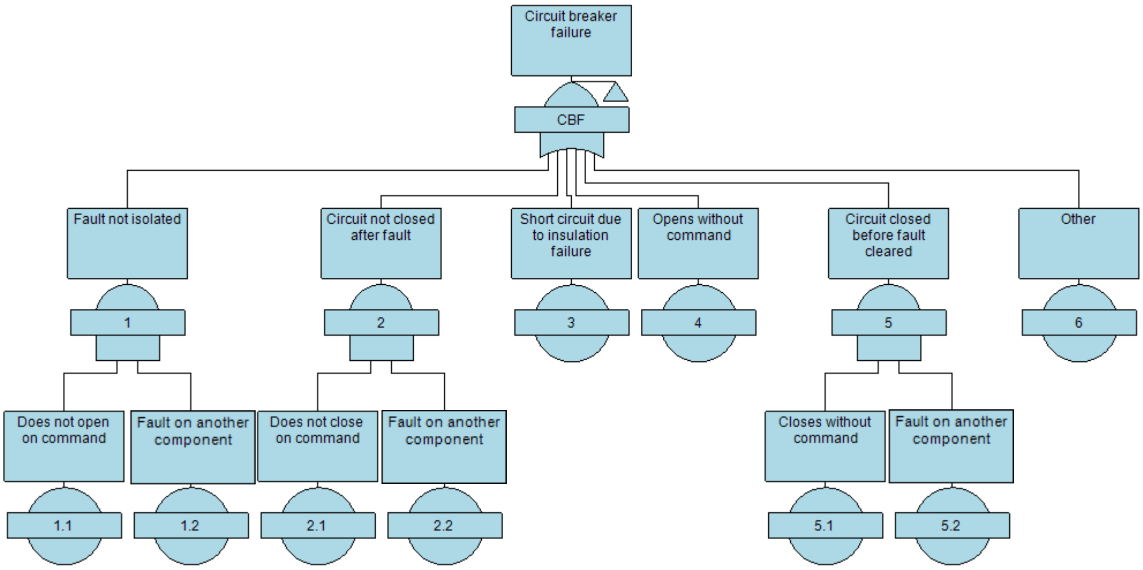

Circuit breaker failure
CBF
Fault not isolated
Circuit not closed after fault
Short circuit due to insulation failure
Opens without command
Circuit closed before fault cleared
Other
1
2
3
4
5
6
Does not open on command
Fault on another component
Does not close on command
Fault on another component
Closes without command
Fault on another component
1.1
1.2
2.1
2.2
5.1
5.2

Figure 4.14 Fault tree from the circuit breaker failure modes adapted to the system

In Figure 4.15 is presented the fault tree used in these computations, as well as the unavailability (Q) of each intermediate event, for a one-year computation.

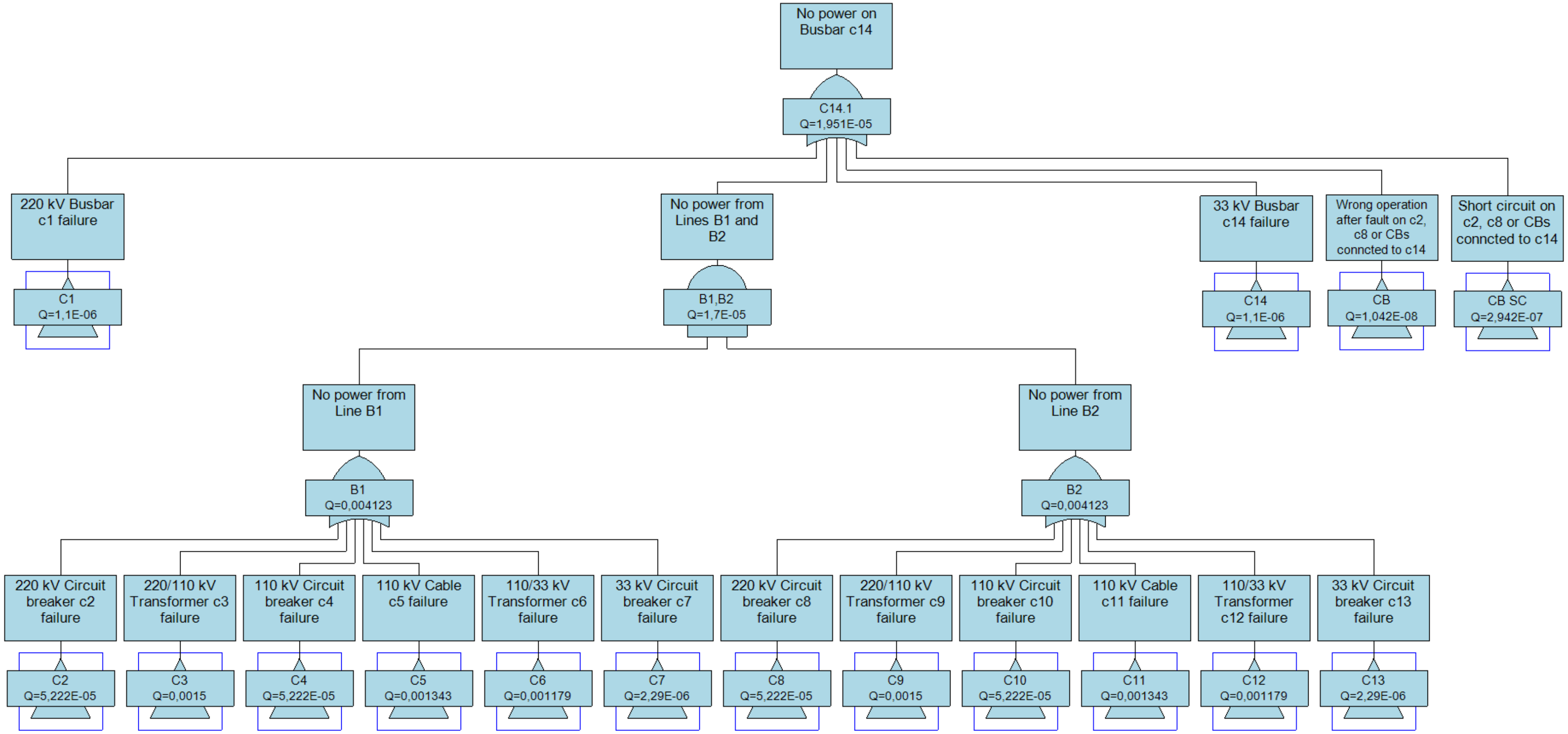

No power on Busbar c14
C14.1
Q=1,951E-05
220 kV Busbar c1 failure
C1
Q=1,1E-06
No power from Lines B1 and B2
B1,B2
Q=1,7E-05
33 kV Busbar c14 failure
C14
Q=1,1E-06
Wrong operation after fault on c2, c8 or CBs conncted to c14
CB
Q=1,042E-08
Short circuit on c2, c8 or CBs conncted to c14
CB SC
Q=2,942E-07
No power from Line B1
B1
Q=0,004123
No power from Line B2
B2
Q=0,004123
220 kV Circuit breaker c2 failure
C2
Q=5,222E-05
220/110 kV Transformer c3 failure
C3
Q=0,0015
110 kV Circuit breaker c4 failure
C4
Q=5,222E-05
110 kV Cable c5 failure
C5
Q=0,001343
110/33 kV Transformer c6 failure
C6
Q=0,001179
33 kV Circuit breaker c7 failure
C7
Q=2,29E-06
220 kV Circuit breaker c8 failure
C8
Q=5,222E-05
220/110 kV Transformer c9 failure
C9
Q=0,0015
110 kV Circuit breaker c10 failure
C10
Q=5,222E-05
110 kV Cable c11 failure
C11
Q=0,001343
110/33 kV Transformer c12 failure
C12
Q=0,001179
33 kV Circuit breaker c13 failure
C13
Q=2,29E-06

Figure 4.15 Fault tree of the connection between busbar c1 and busbar c14

The detailed results of the top event (No power on busbar 14) can be seen in Table 4.1.

Table 4.1 Results of the top event “No power on busbar c14”

Reliability	97.74%
MTTF	43.55 years
MTTR	7.445 hours
Unavailability	1.951 x 10^{-5}

The results show a favorable situation in terms of reliability, almost 98%. This is explained by the redundancy introduced by lines B1 and B2, i.e., both lines would have to fail for busbar c14 to be without power. In Table 4.1, it is also possible to see that the unavailability of the system is very low, this value means that the downtime for this system is approximately 10 minutes per year. The mean time for the system to fail is approximately 44 years and the mean time that the system would be down for repair after a failure is around 7 hours.

To do a more detailed analysis of this system, the importance measures of the most critical failure modes were obtained and presented in Table 4.2, sorted by the FV importance measure, that is the probability of an event (basic or intermediate) being the cause of the top event.

Table 4.2 Failure mode importance values of the top event “No power on busbar c14”

Component	Failure mode	FV	RRW	RAW
Cables (c5/c11)	Short circuit due to insulation failure	0.1588	1.189	211.9
Transformers (c3/c9)	Short circuit due to windings failure	0.1194	1.136	212
	No voltage regulation due to tap changer failure	0.0987	1.11	212
Transformers (c6/c12)	Short circuit due to windings failure	0.0938	1.104	212
Cables (c5/c11)	No energy supply due to mechanical failure	0.0936	1.103	212

It is important to take into account that the FV measure is given per failure mode. In this case, none of these events presented on Table 4.2 would be enough to reach the top event (No power on busbar c14), therefore it is possible that failure modes that contribute directly to the top event, called first order minimal cut sets, have higher unavailability and frequency than the cut sets that involve the failure modes in Table 4.2. This analysis will be made ahead in the minimal cut set analysis.

The analysis of these measures is important in the sense that the idea is to keep every part of the system operational, therefore not only the failure modes that contribute directly to the top event should be focused, but also the ones that contribute to the failure of one of the lines B1 and B2 and, eventually, to the failure of the system.

The most critical failure mode is the insulation failure on cables c5 and c11. This may be caused by moisture or overheat in the cable due to overloads, high ambient temperatures or insufficient ventilation. The second most critical is the short circuit due to windings failure on transformers c3 and c9. This may be caused by the displacement of the windings, an overvoltage due to lightning strikes or short circuits in the grid, or a failure in the insulation system. Furthermore, in these transformers, the tap changer is a critical part, that may fail due to wear on the tap selector or the failure of the contacts of the diverter switch. These events are followed by the short circuit due to windings failure on transformers c6 and c12, and by the failure of cables c5 and c11 by mechanical damage. Therefore, it is possible to conclude that cables c5/c11 and transformers c3/c9 have the most critical failure modes of the system.

The RRW, that is the decrease of the unavailability of the top event if the given event is guaranteed to not happen, i.e., having unavailability equal to zero. For example, if the insulation failure on the 110 kV cables is guaranteed to not happen, the system would be 1.189 times more reliable.

The RAW values are low compared to busbars failure modes (5.114 x 10^4), for example. From equation 3.32, multiplying this value by the top event unavailability, would result in a value close to one, which means that if one of the failure modes from the busbars occurs, the top event would occur.

To better understand the importance of each component and failure mode to the system failure, it is also useful to see the top list of minimal cut sets sorted by unavailability (Table 4.3) and by frequency (Table 4.4), and their contribution (%) to the top event. The minimal cut sets, which is the smallest path to reach the top event, are presented by the description of the failure mode, followed by the respective component, or components, if the failure mode is common to more than one component and both have the same unavailability/frequency. If more than one failure mode is present in the same minimal cut set, means that they are dependent events, called second order minimal cut sets, i.e., both must happen at the same time for the top event to happen.

Table 4.3 Top 10 minimal cut sets sorted by unavailability of the top event "No power on busbar c14"

No.	Unavailability	%	Failure mode 1	Failure mode 2
1	5.663 x 10^{-7}	2.894	Short circuit due to insulation failure (Cable c5)	Short circuit due to insulation failure (Cable c11)
2	5.502 x 10^{-7}	2.812	Short circuit (Busbar c1/c14)	
3	5.502 x 10^{-7}	2.812	No energy supply due to mechanical failure (Busbar c1/c14)	
4	4.257 x 10^{-7}	2.175	Short circuit due to insulation failure (Cable c5)	Short circuit due to windings failure (Transformer C9)
5	4.257 x 10^{-7}	2.175	Short circuit due to windings failure (Transformer c3)	Short circuit due to insulation failure (Cable c11)
6	3.519 x 10^{-7}	1.798	Short circuit due to insulation failure (Cable c5)	No voltage regulation due to tap changer failure (Transformer c9)
7	3.519 x 10^{-7}	1.798	No voltage regulation due to tap changer failure (Transformer c3)	Short circuit due to insulation failure (Cable c11)
8	3.344 x 10^{-7}	1.709	Short circuit due to insulation failure (Cable c5)	Short circuit due to windings failure (Transformer c12)
9	3.344 x 10^{-7}	1.709	Short circuit due to windings failure (Transformer c6)	Short circuit due to insulation failure (Cable c11)
10	3.338 x 10^{-7}	1.706	Short circuit due to insulation failure (Cable c5)	No energy supply due to mechanical failure (Cable c11)

Table 4.4 Top 5 minimal cut sets sorted by frequency of the top event “No power on busbar c14”

No.	Frequency	%	Failure mode 1	Failure mode 2
1	4.82×10^{-3}	20.99	Short circuit (Busbar c1/c14)	
2	4.82×10^{-3}	20.99	No energy supply due to mechanical failure (Busbar c1/c14)	
3	8.526×10^{-4}	3.714	Short circuit due to insulation failure (CB c2/c8)	
4	8.722×10^{-5}	0.3799	Short circuit due to insulation failure (33 kV CBs connected to Busbar c14)	
5	5.905×10^{-5}	0.2572	Short circuit due to insulation failure (Cable c5)	Short circuit due to insulation failure (Cable c11)

The minimal cut set analysis proves that the insulation failures on the 110 kV cables are the highest contributors to the top event (No power on busbar c14) unavailability, confirming the criticality of these cables. To the failure frequency, the highest contributors are the failure modes of busbar c1 and c14, therefore must be considered critical due to their high frequency. This was expected, since these failure modes are first order minimal cut sets.

The busbars do not compare to the transformers in terms of price and importance to the grid, since they are cheaper and easier to replace but, since there is no redundancy, in this case, it is important to pay attention to them too, so the downtime of the grid is minimal.

In a second case scenario, it was assumed that a failure occurred in line B1 and it is out of service, this will allow to see the behavior of the system with only one line.

In this system, it is assumed that both lines are necessary to deliver full power, so the loss of one of the lines would mean the other line would have to carry an additional power, causing more stress on the components and, therefore, an increase on their failure rate. As proposed in [32], it was assumed that the failure rate of all components of line B2 raised 40%.

The results for this case scenario are presented in Table 4.5.

Table 4.5 Comparison of the results for the two case scenarios of the top event “No power on busbar c14”

	With redundancy	Without redundancy
Reliability	97.74%	82.59%
MTTF	43.55 years	5.227 years
MTTR	7.445 hours	266.7 hours
Unavailability	1.951×10^{-5}	5.79×10^{-3}

From these results, it is possible to see that without redundancy the unavailability of the system is much higher than the previous situation, with a downtime of approximately 51 hours per year, an unacceptable value compared to the 10 minutes in the previous case. The reliability is now 82.6%, 15.2% less, a much worse value than the one obtained with redundancy. The mean time for the system to fail is also much worse, being now around 5 years, approximately 38 years less than before. The MTTR is now very high, 267 hours, compared to the 7 hours obtained before, approximately 259 more hours. These results are unacceptable in a real-world situation. Comparing these results with the ones obtained before, it is possible to conclude that having a redundant line is vital to this system.

From the importance values, it is possible to see that the failure mode criticality order is the same than the one obtained with redundancy, with slightly more importance now due to the nonexistent redundancy on any component, therefore the cables and transformers are now even more critical.

In Tables 4.6 and 4.7 are presented the minimal cut sets for this case scenario, sorted by unavailability and frequency, respectively.

Table 4.6 Top 10 minimal cut sets sorted by unavailability without line B1

No.	Unavailability	%	Failure mode
1	1.053×10^{-3}	18.14	Short circuit due to insulation failure (Cable c11)
2	7.917×10^{-4}	13.64	Short circuit due to windings failure (Transformer c9)
3	6.546×10^{-4}	11.28	No voltage regulation due to tap changer failure (Transformer c9)
4	6.22×10^{-4}	10.71	Short circuit due to windings failure (Transformer c12)
5	6.209×10^{-4}	10.7	No energy supply due to mechanical failure (Cable c11)
6	5.143×10^{-4}	8.859	No voltage regulation due to tap changer failure (Transformer c12)
7	3.606×10^{-4}	6.212	Short circuit due to bushings failure (Transformer c9)
8	2.833×10^{-4}	4.88	Short circuit due to bushings failure (Transformer c12)
9	5.108×10^{-5}	0.88	Insulation failure (Transformer c9)
10	4.012×10^{-5}	0.6912	Insulation failure (Transformer c12)

Table 4.7 Top 10 minimal cut sets sorted by frequency without line B1

No.	Frequency	%	Failure mode
1	5.492×10^{-2}	28.73	Short circuit due to insulation failure (Cable c11)
2	3.238×10^{-2}	16.94	No energy supply due to mechanical failure (Cable c11)
3	1.376×10^{-2}	7.199	Short circuit due to windings failure (Transformer c9)
4	1.138×10^{-2}	5.952	No voltage regulation due to tap changer failure (Transformer c9)
5	1.081×10^{-2}	5.655	Short circuit due to windings failure (Transformer c12)
6	8.938×10^{-3}	4.676	No voltage regulation due to tap changer failure (Transformer c12)
7	6.268×10^{-3}	3.279	Short circuit due to bushings failure (Transformer c9)
8	4.924×10^{-3}	2.576	Short circuit due to bushings failure (Transformer c12)
9	4.82×10^{-3}	2.521	Short circuit (Busbar c1/c14)
10	4.82×10^{-3}	2.521	No energy supply due to mechanical failure (Busbar c1/c14)

In this situation, the minimal cut set analysis confirms the criticality of the failure modes from the 110 kV cables, 220/110 kV and 110/33 kV transformers, being the highest contributors to both unavailability and frequency.

It is possible to conclude that the case scenario where only one of the lines B1 and B2 are operating is not acceptable due to the major downtime, therefore it is important to do more maintenance in the crucial components mentioned above in order to prevent this situation from happening, i.e., to always keep both lines B1 and B2 operational, this way preventing possible power losses on the consumers.

Figure 4.16 shows the computed reliability function for the entire system considering both cases, redundancy in lines B1 and B2 (blue line), and without redundancy (red line). It is possible to see that at the five-year mark, the reliability of the system (probability that the system did not failed) with redundancy is approximately 90% and without redundancy 40% (50% less than with redundancy), proving the importance of redundancy in this part of the system. It is important to note that the previous analysis do not consider maintenance interventions in that period of time, assumption that is also made in the next computations.

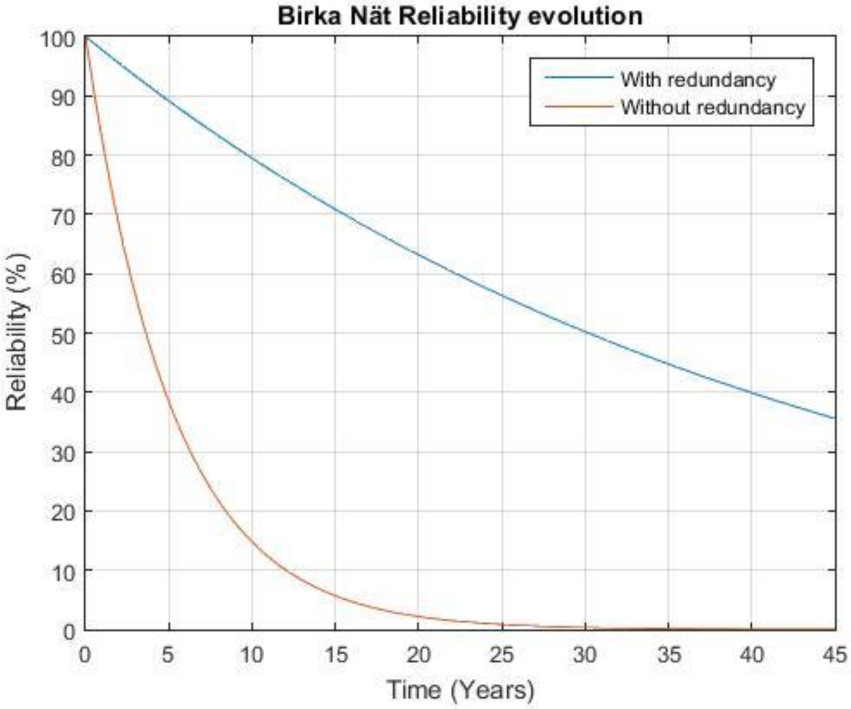


Figure 4.16 Birka Nät reliability evolution

4.4.2 Reliability of the HD load point

This load supplies 23,400 customers that require an average power of 23 MW [3].

This section computations will allow to analyze the reliability of the grid to supply the HD load.

The FT used in these computations is presented in Figure 4.17. Since in this case only one load point is being analyzed, there is no need to represent the other two, since their failure does not influence HD load point, with exception of the events that affect busbar c14, already analyzed in section 4.4.1.

As seen before, no power on busbar c14 (gate C14.2) means no power on busbar c48. If at least one component from all three lines B11, B12 and B13 (gate B11,B12,B13) fails at the same time, a very unlikely event, would also cause an outage. The failure of CB c47 or busbar c48 would also mean no power available on HD load point. In this case, a short circuit or malfunction of CBs c39, c42 or c45 would also cause a one-hour outage on this load point, following the same analysis made in section 4.4.1.

The reliability results of the grid to supply the HD load, for one year are presented in Table 4.8.

Table 4.8 Results of the top event “No power on busbar c48”

Reliability	96.75%
MTTF	30.17 years
MTTR	6.061 hours
Unavailability	2.293 x 10^{-5}

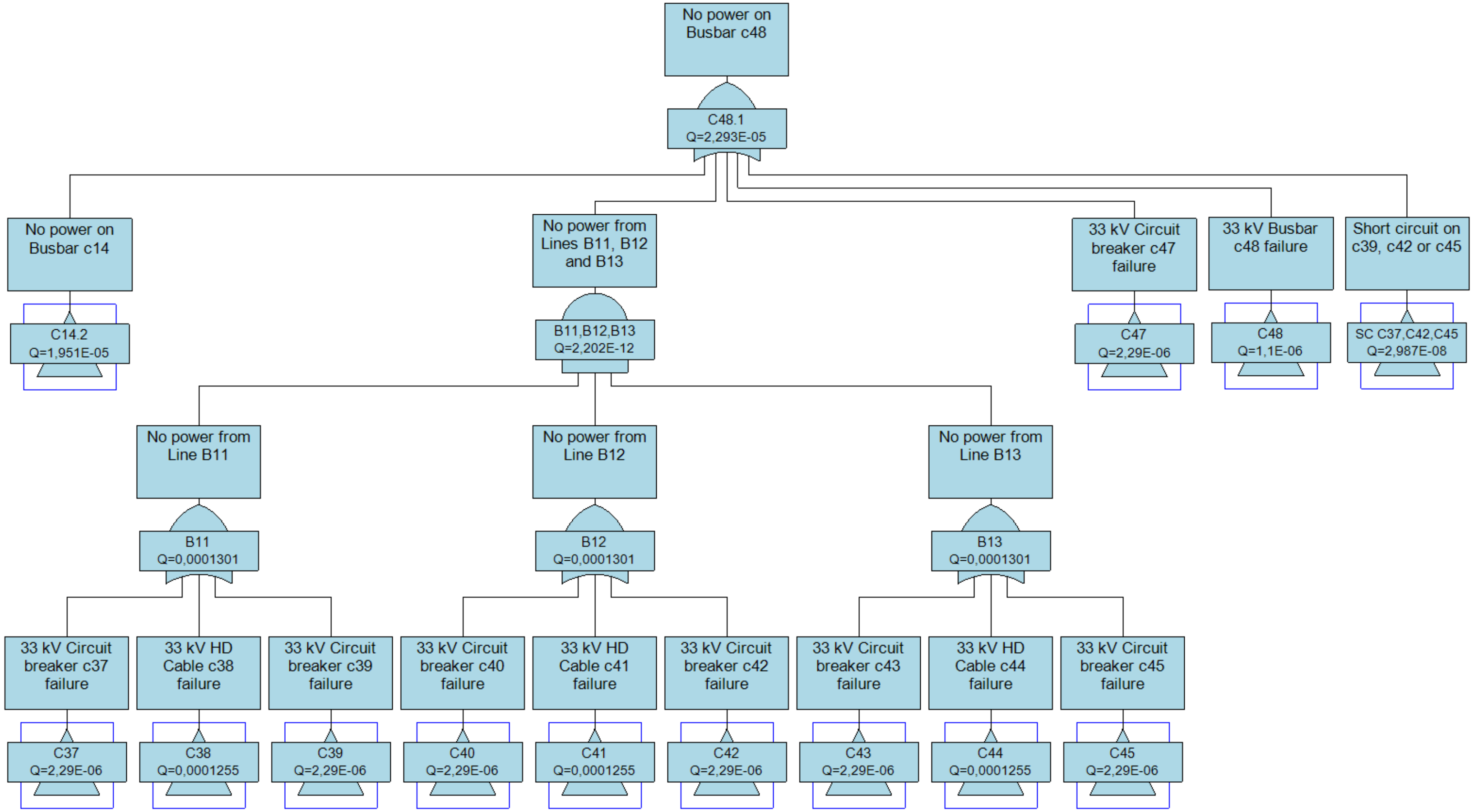

No power on Busbar c48
C48.1 Q=2,293E-05
No power on Busbar c14
C14.2 Q=1,951E-05
No power from Lines B11, B12 and B13
B11,B12,B13 Q=2,202E-12
33 kV Circuit breaker c47 failure
C47 Q=2,29E-06
33 kV Busbar c48 failure
C48 Q=1,1E-06
Short circuit on c39, c42 or c45
SC C37,C42,C45 Q=2,987E-08
No power from Line B11
B11 Q=0,0001301
No power from Line B12
B12 Q=0,0001301
No power from Line B13
B13 Q=0,0001301
33 kV Circuit breaker c37 failure
C37 Q=2,29E-06
33 kV HD Cable c38 failure
C38 Q=0,0001255
33 kV Circuit breaker c39 failure
C39 Q=2,29E-06
33 kV Circuit breaker c40 failure
C40 Q=2,29E-06
33 kV HD Cable c41 failure
C41 Q=0,0001255
33 kV Circuit breaker c42 failure
C42 Q=2,29E-06
33 kV Circuit breaker c43 failure
C43 Q=2,29E-06
33 kV HD Cable c44 failure
C44 Q=0,0001255
33 kV Circuit breaker c45 failure
C45 Q=2,29E-06

Figure 4.17 Fault tree of the HD load point

It was expected that these results were worse than the ones obtained in the computation of the whole grid, since there is less redundancy, i.e., it is only being evaluated the event of not having power on one load point, instead of three at the same time.

The reliability of this load point is almost 97%, 1% less than the overall grid reliability, but still a great value. From the unavailability value it is possible to say that this load point has a downtime of approximately 12 minutes per year. The MTTF is 30 years, 13 years less than the overall grid, and the MTTR is around 6 hours.

To find out which are the critical components and failure modes it is important to check the importance measures. In Table 4.9 is presented a list of the failure modes that most contribute to the top event (No power on busbar c48), sorted by the FV importance value. These results show that the top 5 failure modes from the computation of the whole gird are still the most critical when analyzing load point HD, even though with slightly less importance, since in this computation there are more nonredundant components (CB c47 and busbar c48) contributing directly to the top event.

Table 4.9 Failure mode importance values of the top event “No power on busbar c48”

Component	Failure mode	FV	RRW	RAW
Cables (c5/c11)	Short circuit due to insulation failure	0.1352	1.156	180.5
Transformers (c3/c9)	Short circuit due to windings failure	0.1016	1.113	180.6
	No voltage regulation due to tap changer failure	0.084	1.092	180.6
Transformers (c6/c12)	Short circuit due to windings failure	0.0798	1.087	180.6
Cables (c5/c11)	No energy supply due to mechanical failure	0.0797	1.087	180.6

Next, the top minimal cut set list sorted by unavailability and frequency is presented (Tables 4.10 and 4.11).

Table 4.10 Top 10 minimal cut sets sorted by unavailability of the top event “No power on busbar c48”

No.	Unavailability	%	Failure mode 1	Failure mode 2
1	7.169×10^{-7}	3.118	Short circuit due to insulation failure (CB c47)	
2	5.663×10^{-7}	2.463	Short circuit due to insulation failure (Cable c5)	Short circuit due to insulation failure (Cable c11)
3	5.502×10^{-7}	2.393	Short circuit (Busbar c1/c14/c48)	
4	5.502×10^{-7}	2.393	No energy supply due to mechanical failure (Busbar c1/c14/c48)	
5	5.121×10^{-7}	2.227	Opens without command (CB c47)	
6	4.257×10^{-7}	1.852	Short circuit due to insulation failure (Cable c5)	Short circuit due to windings failure (Transformer c9)
7	4.257×10^{-7}	1.852	Short circuit due to windings failure (Transformer c3)	Short circuit due to insulation failure (Cable c11)
8	3.519×10^{-7}	1.531	Short circuit due to insulation failure (Cable c5)	No voltage regulation due to tap changer failure (Transformer c9)
9	3.519×10^{-7}	1.531	No voltage regulation due to tap changer failure (Transformer c3)	Short circuit due to insulation failure (Cable c11)
10	3.344×10^{-7}	1.454	Short circuit due to insulation failure (Cable c5)	Short circuit due to windings failure (Transformer c12)

Table 4.11 Top 5 minimal cut sets sorted by frequency of the top event “No power on busbar c48”

No.	Frequency	%	Failure mode
1	4.82 x 10^{-3}	14.54	Short circuit (Busbar c1/c14/c48)
2	4.82 x 10^{-3}	14.54	No energy supply due to mechanical failure (Busbar c1/c14/c48)
3	8.526 x 10^{-4}	2.573	Short circuit due to insulation failure (CB c2/c8)
4	8.722 x 10^{-5}	0.2632	Short circuit due to insulation failure (33 kV CBs)
5	6.23 x 10^{-5}	0.188	Opens without command (CB c47)

The minimal cut set analysis confirms that the failure modes from the 110 kV cables, the windings and tap changer of both transformers present in lines B1 and B2 are critical to the unavailability of load point HD. To the unavailability, the highest contributor minimal cut set is the short circuit due to insulation failure on CB c47. Furthermore, the unintended opening of this CB is also a high contributor, making CB c47 an important component to this load point as well. As expected, the failure modes from busbar c48 join busbars c1 and c14 as the top contributors to the failure frequency.

In a second case scenario, it was assumed that line B11 was out of service. The failure rate of the components in lines B12 and B13 was raised by 40% like it was done in section 4.4.1.

In Table 4.12, it is possible to see that the results almost did not changed compared to the previous computation (three lines). The unavailability raised from 2.293 x 10^{-5} to 2.299 x 10^{-5}, the reliability and MTTF almost did not change, as well as the MTTR. These results are explained by the fact that even though one of the three lines is out of service, there is still redundancy. With this computation, it is possible to conclude that having three lines instead of two does not affect the system reliability. Although it is possible to say that from a reliability point of view, the third line has a very small impact, if the three cables in parallel are required to deliver full power to the consumer, then this must be considered.

Since the importance values and minimal cut sets for this case scenario (two lines) are similar to the previous one (three lines), they are not going to be presented.

In a third case scenario, it was assumed that lines B11 and B12 were out of service, therefore the failure rate of the components from line B13 was raised by 70%, again, due to the even higher stress that only one cable would have to support.

The results are presented in Table 4.12.

Table 4.12 Comparison of the results for the three case scenarios of the top event “No power on busbar c48”

	With redundancy (three lines)	With redundancy (two lines)	Without redundancy
Reliability	96.75%	96.75%	93.01%
MTTF	30.17 years	30.19 years	13.78 years
MTTR	6.061 hours	6.083 hours	29.5 hours
Unavailability	2.293 x 10^{-5}	2.299 x 10^{-5}	2.441 x 10^{-4}

In this case, the loss of a second line has an impact on the system’s reliability. The reliability drops to 93%, which is still an acceptable value, the expected downtime of the system is approximately 2 hours, a high value compared to the 12 minutes of the first computation. The MTTF also dropped, it is now about 16 years less, and the MTTR raised approximately 23 hours. It is possible to conclude that, from a reliability point of view, having at least two of the three lines B11, B12 and B13 is vital in this load point. The detailed results of the case scenario without redundancy are presented in Appendix B.

Figure 4.18 shows the reliability function for the HD load point. After five years, the reliability is 85% for the case with two and three cables, and 70% for the case with one cable. It is possible to conclude that losing redundancy on these cables is not as critical as losing redundancy on lines B1 and B2.

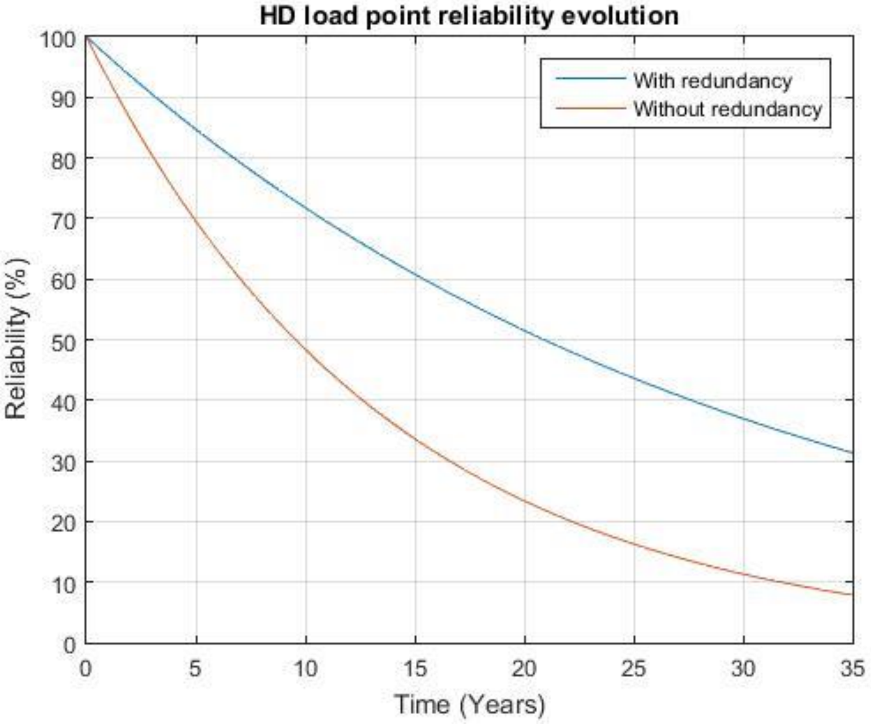


Figure 4.18 HD load point reliability evolution

4.4.3 Reliability of the SJ load point

This load point has only one client that requires 0.8 MW of average power [3].

To study the reliability of the grid to deliver power to this load, the FT presented in Figure 4.19 was used. This load point is similar to the HD, the only difference is that there is one less line, therefore it is expected that the results are also similar.

Like in the HD load point, two different scenarios were considered in this load point. One with both lines B16 and B17 operating and another with line B16 out of service. In the second computation, the failure rate of the components from line B17 was raised by 40%.

The results for the top event (No power on Busbar c58), for one year, are presented in Table 4.13.

Table 4.13 Comparison of the results for the two case scenarios of the top event “No power on busbar c58”

	With redundancy	Without redundancy
Reliability	96.75%	95.56%
MTTF	30.25 years	21.99 years
MTTR	6.075 hours	18.23 hours
Unavailability	2.292 x 10^{-5}	9.459 x 10^{-5}

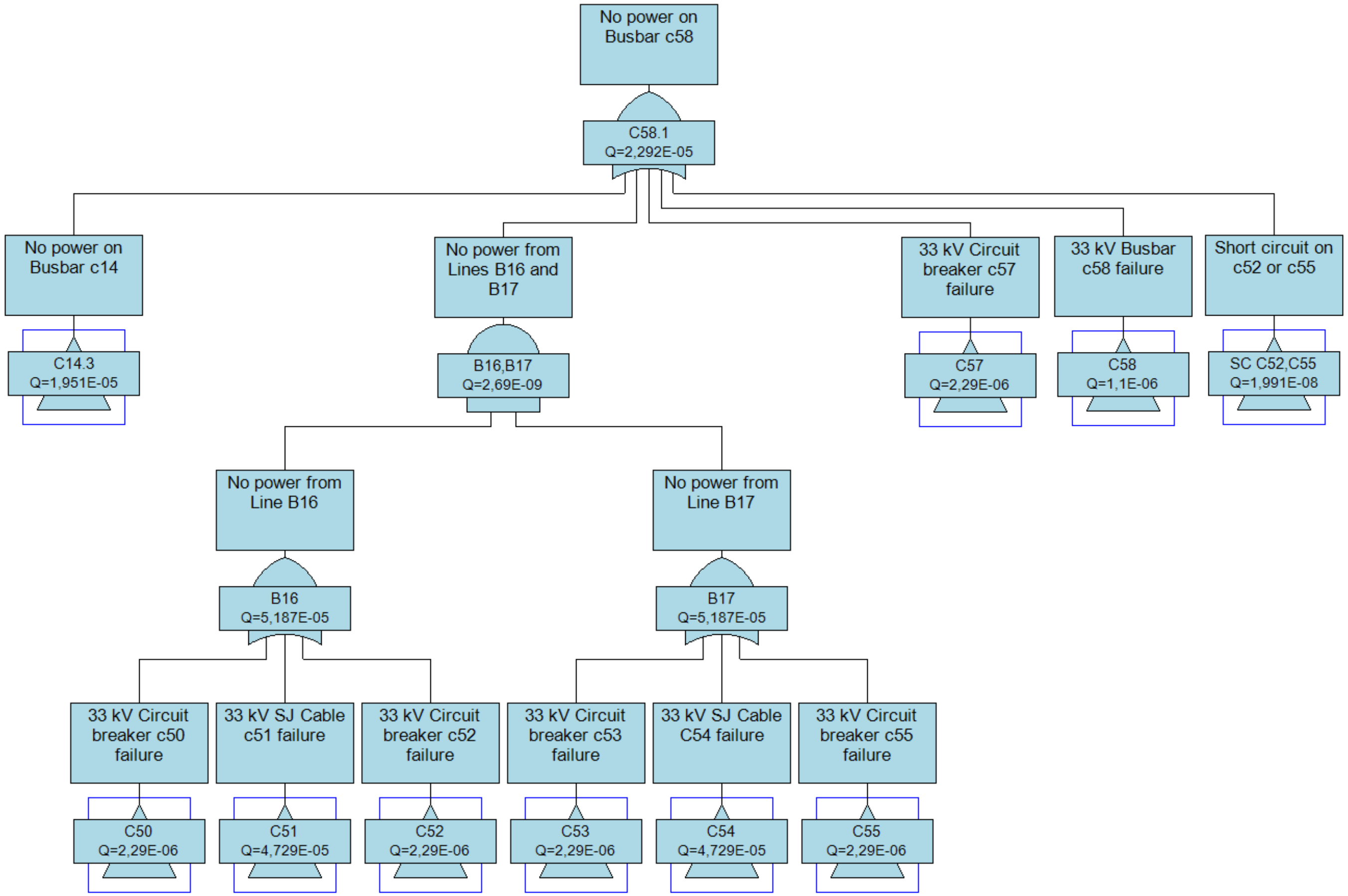


Figure 4.19 Fault tree of the SJ load point

As expected, the results are similar to the ones obtained in the HD load point computation. These are slightly better due to the lower failure rate of the 33 kV cables. For the first computation, the downtime per year is around 12 minutes. The reliability is 97%, the MTTF 30 years and the MTTR 6 hours.

Like it was done before, the importance measures for the top failure modes and minimal cut sets were obtained, and due to their similarity are presented in Appendix C. Like in the HD load point computation, the failure modes of the 110 kV cables and 220/110 kV transformers, from lines B1 and B2, are still the highest contributors to the unavailability of this load point. This is also confirmed by the minimal cut set analysis. Furthermore, from the minimal cut sets analysis, it is possible to conclude that the failure modes from busbar c58, the failure of CB c57 by insulation or unexpected opening, are also important in this part of the grid.

In the second case scenario, the downtime per year is 50 minutes, 38 more minutes than with both lines operating. The reliability dropped 1%, the MTTF 8 years and the MTTR is now 12 more hours. Comparing these results with the HD load point, when only one line is operating, it is possible to see that this situation is more favorable, due to the lower failure rate of the 33 kV cables of this load point. All the detailed results of these computations can be seen in Appendix C.

In Figure 4.20 is presented the reliability function for the SJ load point. With redundancy, the reliability is 85% after 5 years, and 80% in the scenario where there is no redundancy. It is possible to say that in this load point, having no redundancy is less critical than in load point HD.

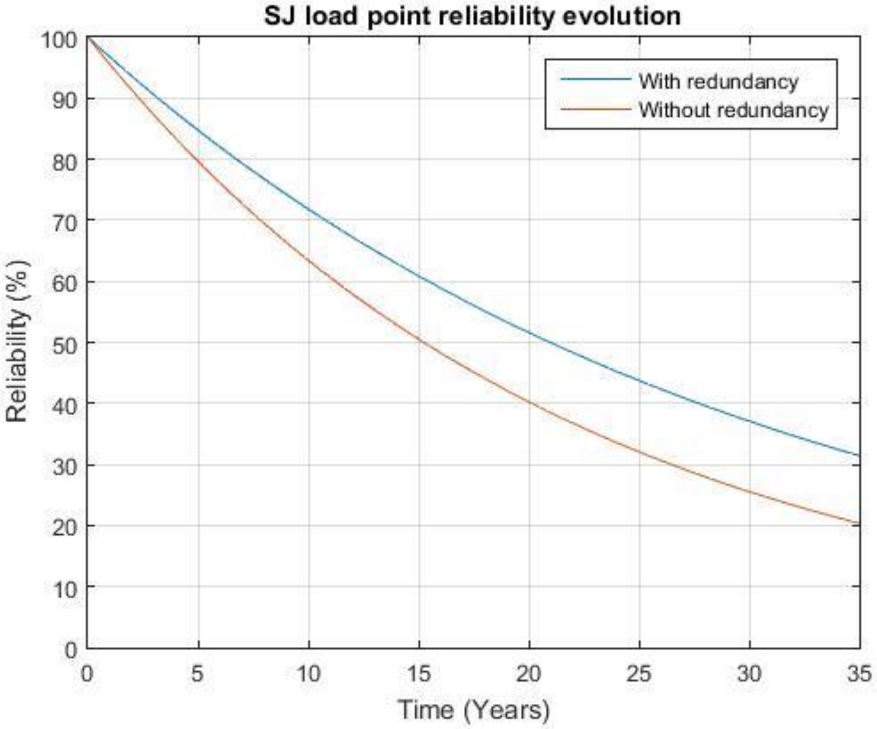


Figure 4.20 SJ load point reliability evolution

4.4.4 Reliability of the LH11 load point

Finally, the reliability of the LH11 load point was tested. This load point has a total of 14,300 clients that require an average power of 24.6 MW [3]. The clients of this load point receive power from 32 identical outgoing feeders connected to the 11 kV substation. In this model, the outgoing feeders are only represented by one feeder with an average length of 8.1 km.

The connections and components on this load point are different from the previous two, therefore it is expected that the results are different.

The FT used for this computations is presented in two different figures. In Figure 4.21, the FT for the top event “No power on Busbar c27” is presented, and in Figure 4.22 the remaining connections until busbar c35. As shown in Figure 4.21, for the system to have no power on busbar c27, one of the following events had to happen: “No power on busbar c14” (gate 14.4), the failure of busbar c27 (gate C27) or the failure of at least one component, at the same time, from lines B3, B4, and B5 (gate B3,B4,B5). The last is very unlikely, though more likely than the redundancy of lines present in the other two load points. Furthermore, in this case, the short circuit or malfunction of CBs c18, c22 or c26 would cause a one-hour outage. Figure 4.22 displays other events that may lead to not having power on busbar c35. These events are the failure of CB c28, both lines B7 and B8 fail at the same time, transformer c33 fails, fuse c34 fails, or busbar c35 fails.

If a fault happens in one of the 11 kV cables c30 or c31, CB c28 would operate to isolate the fault, making power unavailable, since this is a nonredundant component. The purpose of having redundant lines would be lost because a fault on one cable would be enough to stop the operation of load point. A computation was made using the original configuration and the reliability obtained was 84%, a low value compared to the other load points. Given this, it is proposed the introduction of one 11 kV CB on each end of the 11 kV cables. This solution is only proposed from a reliability point of view, which is the focus of this work, then it is recommended a financial study to evaluate if adding these CBs is beneficial economically in the long term.

The results of the top event “No power on busbar c35”, for a period of one year, are presented in Table 4.14.

Table 4.14 Results of the top event “No power on busbar c35”

Reliability	94.23%
MTTF	16.8 years
MTTR	7.383 hours
Unavailability	5.013×10^{-5}

As expected, in this point of the grid the results are much worse than the other two load points. This is explained by the higher number of components compared to the other load points, that introduce more failure probability in the system. The unavailability is higher, 26 minutes, more than double the time compared to the other two load points. The reliability is lower, 94%, almost 2.5% less, but still an acceptable value, and much better than the original configuration of this load point, almost 10% more reliable.

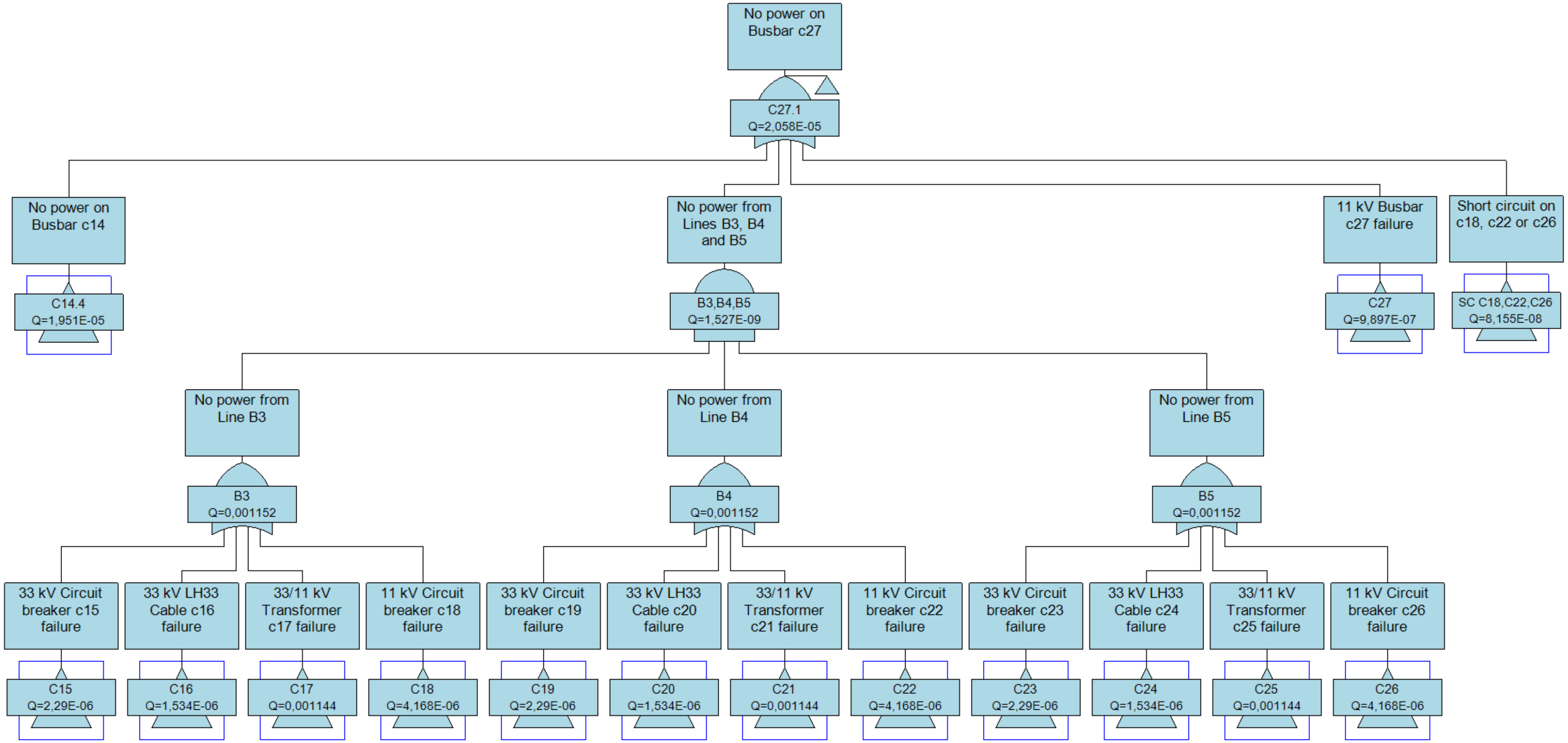

No power on Busbar c27
C27.1
Q=2,058E-05
No power on Busbar c14
C14.4
Q=1,951E-05
No power from Lines B3, B4 and B5
B3,B4,B5
Q=1,527E-09
11 kV Busbar c27 failure
C27
Q=9,897E-07
Short circuit on c18, c22 or c26
SC C18,C22,C26
Q=8,155E-08
No power from Line B3
B3
Q=0,001152
No power from Line B4
B4
Q=0,001152
No power from Line B5
B5
Q=0,001152
33 kV Circuit breaker c15 failure
C15
Q=2,29E-06
33 kV LH33 Cable c16 failure
C16
Q=1,534E-06
33/11 kV Transformer c17 failure
C17
Q=0,001144
11 kV Circuit breaker c18 failure
C18
Q=4,168E-06
33 kV Circuit breaker c19 failure
C19
Q=2,29E-06
33 kV LH33 Cable c20 failure
C20
Q=1,534E-06
33/11 kV Transformer c21 failure
C21
Q=0,001144
11 kV Circuit breaker c22 failure
C22
Q=4,168E-06
33 kV Circuit breaker c23 failure
C23
Q=2,29E-06
33 kV LH33 Cable c24 failure
C24
Q=1,534E-06
33/11 kV Transformer c25 failure
C25
Q=0,001144
11 kV Circuit breaker c26 failure
C26
Q=4,168E-06

Figure 4.21 Fault tree of top event No power on Busbar c27

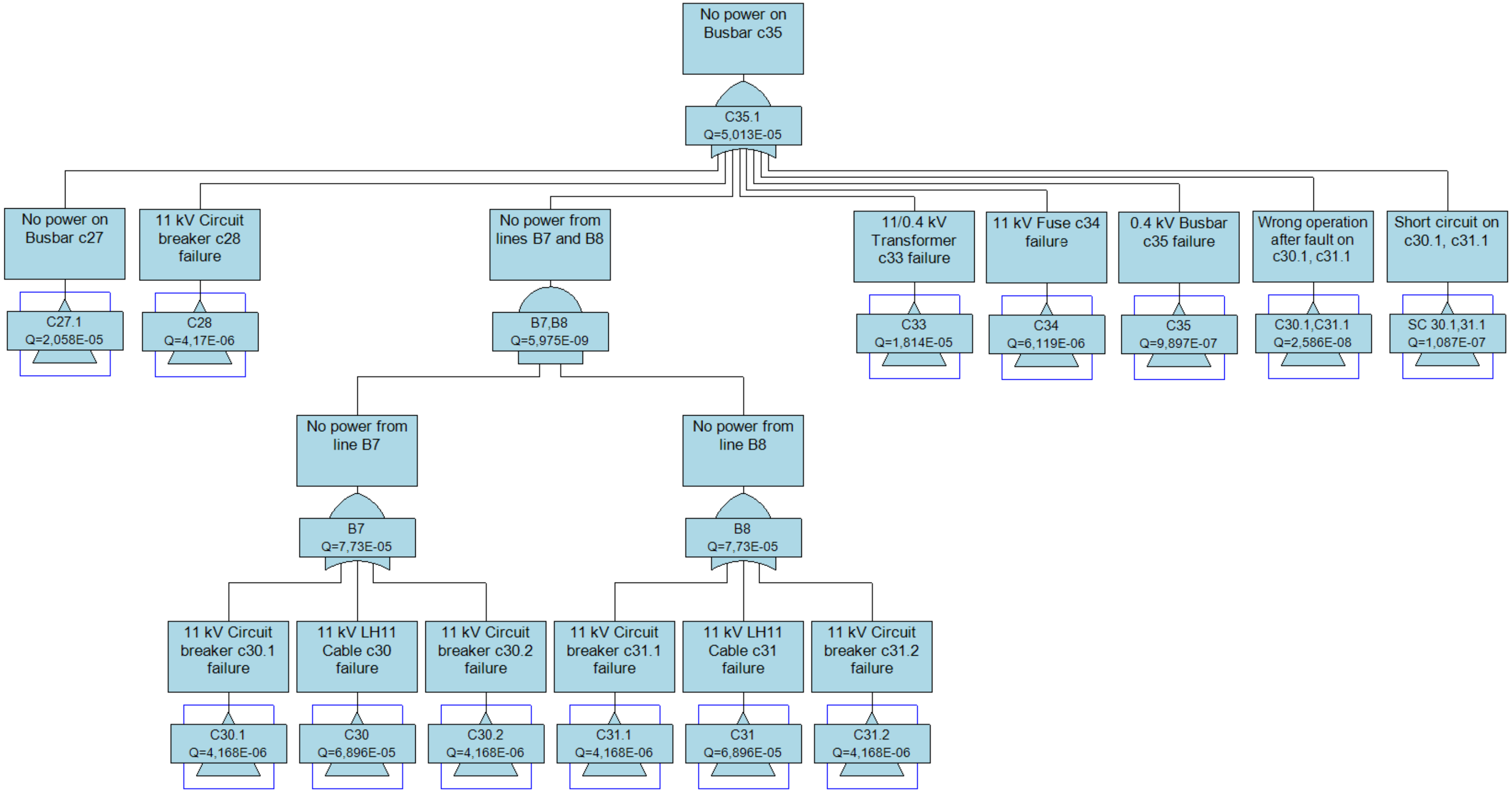

No power on Busbar c35
C35.1
Q=5,013E-05
No power on Busbar c27
C27.1
Q=2,058E-05
11 kV Circuit breaker c28 failure
C28
Q=4,17E-06
No power from lines B7 and B8
B7,B8
Q=5,975E-09
11/0.4 kV Transformer c33 failure
C33
Q=1,814E-05
11 kV Fuse c34 failure
C34
Q=6,119E-06
0.4 kV Busbar c35 failure
C35
Q=9,897E-07
Wrong operation after fault on c30.1, c31.1
C30.1,C31.1
Q=2,586E-08
Short circuit on c30.1, c31.1
SC 30.1,31.1
Q=1,087E-07
No power from line B7
B7
Q=7,73E-05
No power from line B8
B8
Q=7,73E-05
11 kV Circuit breaker c30.1 failure
C30.1
Q=4,168E-06
11 kV LH11 Cable c30 failure
C30
Q=6,896E-05
11 kV Circuit breaker c30.2 failure
C30.2
Q=4,168E-06
11 kV Circuit breaker c31.1 failure
C31.1
Q=4,168E-06
11 kV LH11 Cable c31 failure
C31
Q=6,896E-05
11 kV Circuit breaker c31.2 failure
C31.2
Q=4,168E-06

Figure 4.22 Fault tree of the LH11 load point

The MTTF reduced approximately 13 years, less than half of the value obtained in the previous tests, and the MTTR is one more hour.

To better understand the reliability of this load point, it is important to look at the importance measures of the top failure modes (Table 4.15).

Table 4.15 Failure mode importance values of the top event “No power on busbar c35”

Component	Failure mode	FV	RRW	RAW
Transformer(c33)	Short circuit due to windings failure	0.1362	1.158	1.992 x 10^4
	No voltage regulation due to tap changer failure	0.1126	1.127	1.992 x 10^4
	Short circuit due to bushings failure	0.062	1.066	1.992 x 10^4
Cables (c5/c11)	Short circuit due to insulation failure	0.0619	1.066	83.23
Transformers (c3/c9)	Short circuit due to windings failure	0.0466	1.049	83.24

In this load point, the failure modes of transformer c33 have a higher FV value than the components of lines B1 and B2. The most critical failure modes from transformer c33 are the short circuit due to windings failure and the failure of the tap changer. The insulation failure in cables c5/c11 and short circuits on the transformers c3/c9 due to windings failure are still critical to this load point, although not the most critical like in the other two load points.

In Tables 4.16 and 4.17 are presented the minimal cut sets sorted by unavailability and frequency, respectively.

Table 4.16 Top 5 minimal cut sets sorted by unavailability of the top event “No power on busbar c35”

No.	Unavailability	%	Failure mode
1	6.836 x 10^{-6}	13.62	Short circuit due to windings failure (Transformer c33)
2	5.651 x 10^{-6}	11.26	No voltage regulation due to tap changer failure (Transformer c33)
3	3.112 x 10^{-6}	6.2	Short circuit due to bushings failure (Transformer c33)
4	1.305 x 10^{-6}	2.559	Short circuit due to insulation failure (CB c28)
5	9.321 x 10^{-7}	1.857	Opens without command (CB c28)

Table 4.17 Top 5 minimal cut sets sorted by frequency of the top event “No power on busbar c35”

No.	Frequency	%	Failure mode
1	4.82 x 10^{-3}	8.102	Short circuit (Busbar c1/c14)
2	4.82 x 10^{-3}	8.102	No energy supply due to mechanical failure (Busbar c1/c14)
3	4.335 x 10^{-3}	7.287	Short circuit (Busbar c27/c35)
4	4.335 x 10^{-3}	7.287	No energy supply due to mechanical failure (Busbar c27/c35)
5	1.248 x 10^{-3}	2.097	Short circuit due to windings failure (Transformer c33)

The minimal cut set analysis confirms the failure modes of transformer c33 referred above are the most critical to this load point's unavailability. In terms of frequency, like it was verified in the previous computations, busbars c1, c14, c27 and c35 are the top contributors.

In a second case scenario, it was assumed that line B3 was out of service, therefore the failure rate of the components from lines B4 and B5 was raised by 40% like it was done in the other load points. This will allow to check the importance of having more than two lines after busbar c14.

The results of this computation (Table 4.18) reveal that the unavailability raised from 5.013 x 10^{-5} to 5.27 x 10^{-5}, the reliability and the MTTF did not changed, and the MTTR raises 23 minutes. Comparing with the results obtained in the previous computation (three lines), it is possible to conclude that having a third line does not impact the reliability of the system, like it was concluded in the computation of load points HD and SJ.

In a third case scenario, it was assumed that lines B3 and B4 were out of service, therefore the failure rate of the components from line B5 was raised by 70%. The results for this case scenario are presented in Table 4.18.

Table 4.18 Comparison of the results for the three case scenarios of the top event "No power on busbar c35"

	With redundancy (three lines)	**With redundancy (two lines)**	**Without redundancy**
Reliability	94.23%	94.23%	90.98%
MTTF	16.8 years	16.79 years	10.57 years
MTTR	7.383 hours	7.758 hours	186.3 hours
Unavailability	5.013 x 10^{-5}	5.27 x 10^{-5}	2.007 x 10^{-3}

The unavailability is high compared to the one obtained with redundancy, with the system being down almost 18 hours per year. The reliability dropped to 91%, 3% less, the MTTF is now approximately 6 years less and the MTTR is now 179 more hours, an unacceptable value. Therefore, it is vital in this point of the grid, to keep at least two lines running.

From the list of importance measures and minimal cut sets (see Appendix D), it is possible to see that, with no redundancy, the most critical failure modes correspond to transformer c25, namely the failures related to the windings, tap changer, and bushings, making this the most critical component in order to keep every line healthy. Therefore, to keep this load point from possibly having power losses, regular maintenance should be performed on the 33/11 kV transformers.

In Figure 4.23 is presented the reliability function for the LH11 load point to compare the reliability in all three computations. It is possible to see that, with redundancy, the reliability is 90% after two years. Regarding the third computation, with no redundancy, the reliability is below 85% after two years.

It is possible to conclude that this load point is the most critical of the three, mainly due to having the most complex configuration, with the highest number of components. In order to keep the system working and delivering the expected power to all customers, this load point should be the priority of the maintenance teams.

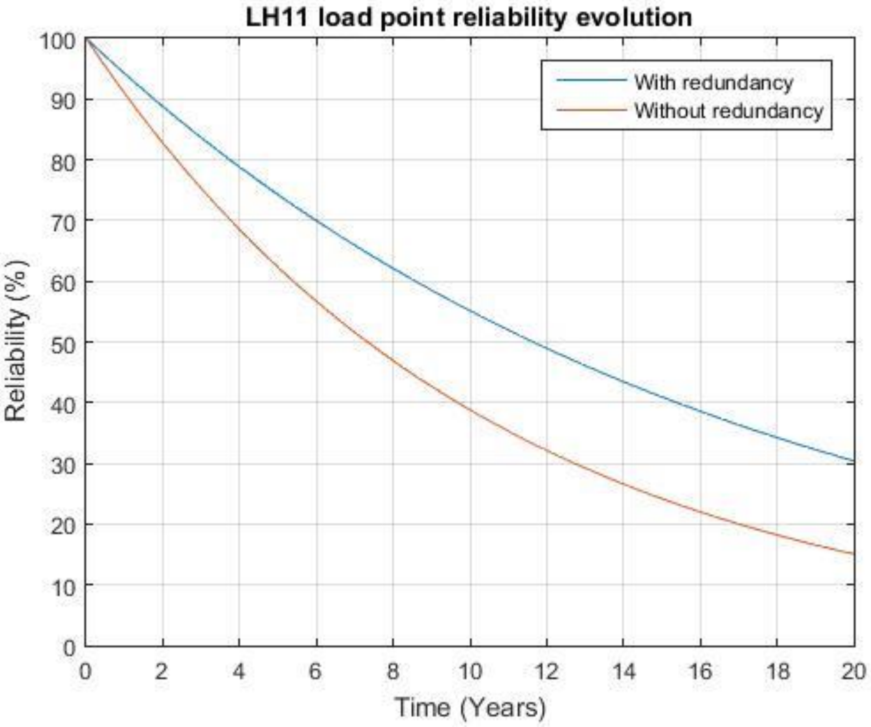


Figure 4.23 LH11 load point reliability evolution

Chapter 5

Reliability analysis of the Birka Nät smart grid concept

5.1 The cyber system and its components

In this section, the cyber part of the system will be considered and a simple architecture of the interconnection of the cyber components will be presented. The impact of the cyber equipment on the distribution system reliability will be studied, with special focus on the circuit breakers.

The inclusion of a cyber network in the power system aims to improve it in different ways [33]. It can improve reliability and fault detection, isolation and restoration. Although, since every equipment can fail, the inclusion of new components in the system will bring more concerns in terms of reliability, therefore, it is important to study how the cyber system can impact the power system. This type of failures can be defined as direct or indirect [34]. Direct failures refer to the case where the failure of a component in the cyber system causes a failure in the power system. Indirect failures are the type of failures that happen in the cyber system and do not affect directly the power system. For example, communication failures may reduce the efficiency of the entire system but do not stop the operation. Another example of indirect failures is the failure of a component responsible for the protection system. This topic will be discussed in more detail in section 5.2.

The most commonly used communication standard in digital substations is IEC 61850. This protocol provides detailed specifications of the communications protocols and allows to improve interoperability, reducing costs and simplifying operations [8].

The most important components of the cyber system are:

- Merging units;
- Intelligent electronic devices;
- Ethernet switches;
- Servers;
- Human machine interface (HMI);
- Smart meters, included in the Advanced metering infrastructure (AMI).

In Figure 5.1 is presented a simple architecture of a digital substation.

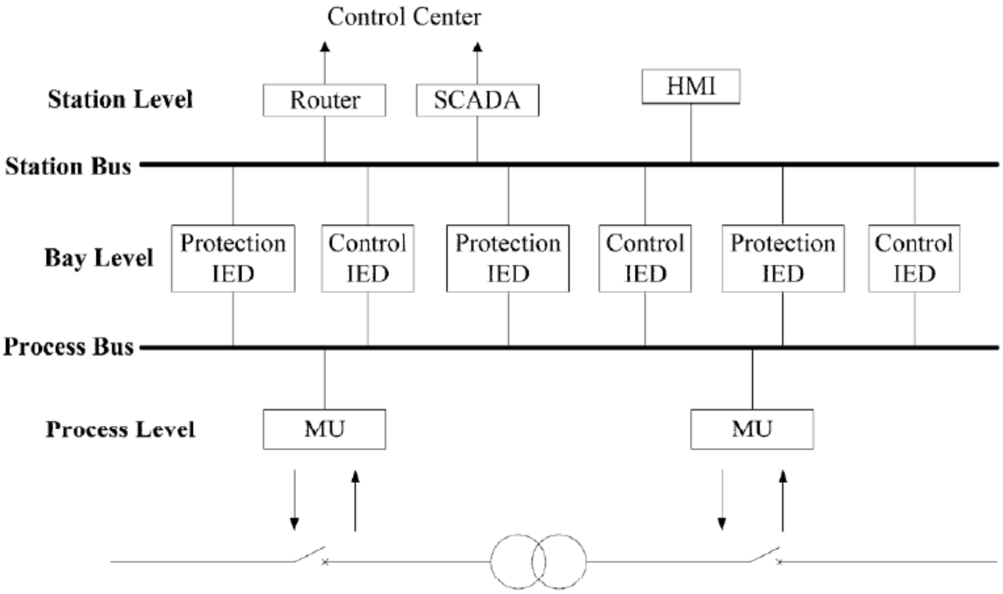


Figure 5.1 Digital substation architecture, adapted from [10]

In the process level, the MUs convert the original analog current and voltage signal acquired by the current transformers/potential transformers into digital signals, and send sample values to the IED and to the control center [8], allowing the operator of the grid to monitor the grid in real time and take actions, if necessary. They are also responsible for detecting faults in the grid and send this information to the IED, which will operate the correspondent CB to isolate the fault, preventing extended damage on the grid. In Figure 5.2 can be seen an example of a merging unit.

Figure 5.2 Merging unit, adapted from [35]

In the bay level, the IEDs (Figure 5.3) are the devices responsible for protecting and controlling the grid. These devices will eventually replace the conventional electromagnetic relays, also responsible for protecting the system [2]. The IEDs receive the data collected by the MUs, and take actions on the grid, namely tripping the necessary CBs to isolate faults.

In the IEC 61850 protocol, three types of IEDs can be applied [8].

- Protection IEDs, responsible for the protection of the busbars, cables and transformers.
- Control IEDs, responsible for the tap changer of the transformer.
- Breaker IEDs, to monitor and operate the CBs.

Figure 5.3 Control and protection IED, adapted from [36]

For these cyber components to function properly, they need to send information between each other. To accomplish this, all the devices are connected to a central ES. Every substation has one ES connected to the main ES in the control center. In Figure 5.4 is presented a model of an ethernet switch.

Figure 5.4 Ethernet switch, adapted from [37]

To store all the information from the grid, servers (see Figure 5.5) are used. The failure of a server means permanent loss of data. To maintain the information of the grid always available, redundant servers can be used to immediately replace the failed ones, this way keeping the reliability of the cyber network high [38].

Figure 5.5 Server, adapted from [39]

In the station level is located the central component of the SG, the HMI, and the supervisory control and data acquisition (SCADA) system, where the operator can see the status of the grid in real time and take actions to improve efficiency and reliability. The functions at this level include schedule of power generation to deliver the required energy by the client, monitor the grid in real time or manage the price of electricity [14]. In Figure 5.6 is a representation of a control center of a smart grid.

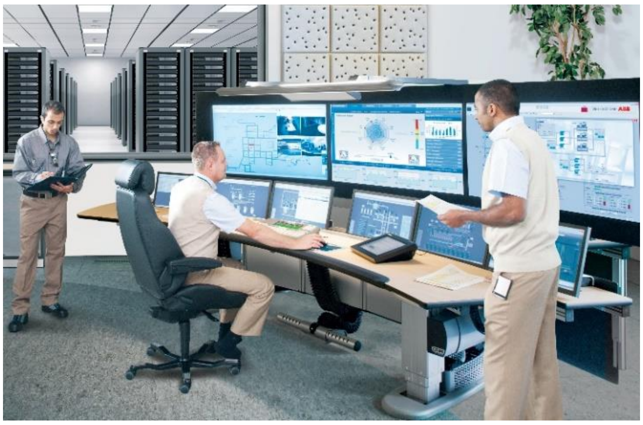


Figure 5.6 HMI in the control center, adapted from [40]

The communication between customer and producer is made through a SM (Figure 5.7), part of the AMI. Using SMs will help the electricity provider to monitor the energy consumption of each client in real time [2], and this way, provide better knowledge of what is the better time to, for example, charge an EV, by analyzing the customer needs and the price of energy in real time.

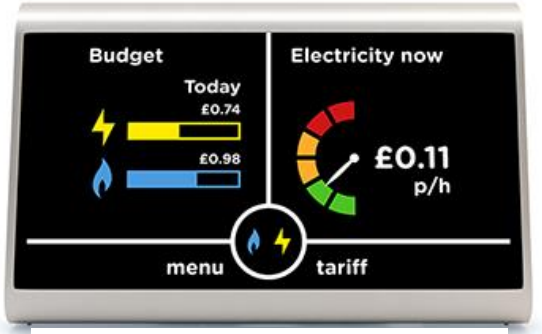


Figure 5.7 Smart meter, adapted from [41]

5.2 Impact of indirect failures

In this section, the impact of indirect failures will be studied.

As said before, one of the advantages of the SG is the possibility of monitor the power system in real time, allowing the early detection of a failure, with the appropriate measures taken faster than in a conventional grid, this way making the impact on the rest of the components minimal, and ultimately reducing their failure rate.

Like any other component, the components responsible for monitoring and protecting the grid can fail and, in this case, are called indirect failures. According to [33], the concept of indirect failures applied to the SG, means that when a component in the cyber network fails, it does not stop the operation of the power grid but will impact the performance of some components when a failure in the power grid occurs. In this case, it is interesting to apply this to the CBs, since in case of a fault in the grid and the failure of a cyber component responsible for the protection system, the CB required to isolate the fault would not receive the tripping signal.

The selected approach to model the indirect failures in a digital substation is based on the methodology presented in [10]. In the process level, the MUs are connected to redundant protection IEDs present in the bay level. The introduction of two IEDs connected in parallel offers more reliability because it would be necessary that both IEDs fail at the same time, which is highly unlikely, for this part of the system to fail. The communication of the IEDs with the MU is done through the substation ES. The failure of one of these components at the same time a fault occurs in the power system would cause the CB to not receive the appropriate tripping signal, and would require the operation of the CB located upstream, causing an extended outage and possible damage on the components of the power system. This situation is represented by the FT in Figure 5.8.

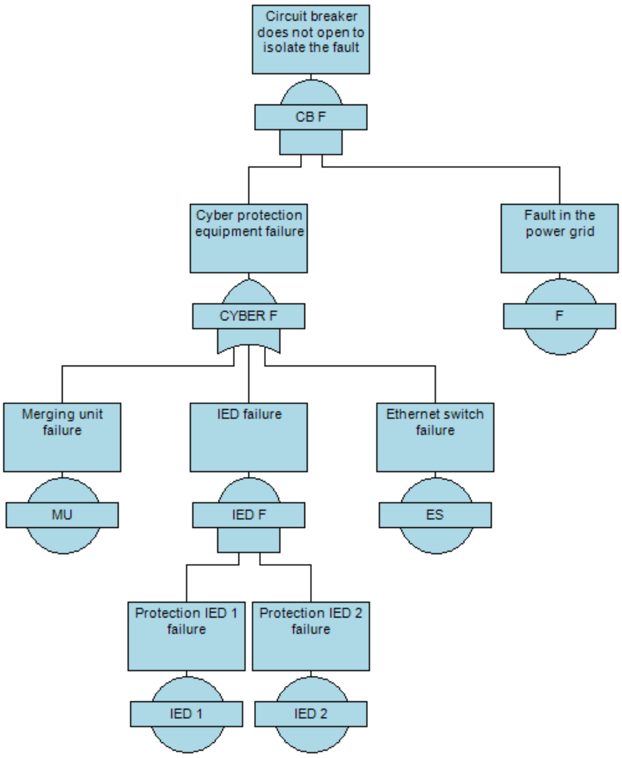


Figure 5.8 Fault tree for cyber indirect failures on the circuit breaker

This fault tree represents a new failure mode of the CBs. The AND gate at the top event means that a failure in both the power and the cyber system would be needed for this failure mode to occur. A fault in one or more equipment in the cyber system, at a given time, would not make the power grid to fail, hence the concept of indirect or hidden failure.

An isolated fault in the cyber components would impact the system in terms of efficiency, for example, a delay in the communications would prevent the operator of controlling the system in real time, but the operation of the power system would not be stopped, which is the purpose of this analysis.

In Table 5.1 is possible to see the input data proposed to these events, according to [10].

Table 5.1 Indirect failures input data

Failure mode	**λ (/year)**	**r (h)**
Merging unit failure	0,00667	8
Protection IED failure	0,00667	8
Ethernet switch failure	0.02	8

5.3 Impact of direct failures

In this section, the impact on the power grid caused by failures that directly affect the operation of the system will be studied. These failures are mainly divided into two, cyberattacks and unintended operations in the power grid, caused by a human error or by an incorrect measurement by a control device, due to an internal malfunction. Particularly, will be simulated the impact of these failures on the CBs, the devices where the hacker can easily cause an outage on the grid.

According to [42], the power system has faced many cyberattacks, raising the question of cybersecurity and its impacts. Although this type of attack is becoming more frequent, it does not mean they are successful. Probably the most popular cyberattack happen in Ukraine on December 23, 2015. The intruders were able to hack into the control center, opening multiple CBs, and taking about 30 substations offline, causing a blackout that affected 230,000 people [43].

Also in [42], some examples of outages caused by non-cyberattacks are presented, like on August 14, 2003, in the Midwest and Northeast US and Ontario, Canada, a blackout that lasted for 4 days in some areas, affected nearly 50 million people and 61,800 MW of energy. This blackout was caused by a failure in the software of the cyber system. On September 28, 2003, caused by a human error, Italy and Switzerland, faced a blackout that affected 56 million people. Even though the operation was restored after 18 hours, still had a huge financial impact.

These numbers demonstrate that, even though these types of failures are rare, when they happen, the impact on people’s lives and on the producer, that is not selling energy, can be significant.

Figure 5.9 is a simple representation of the path of a cyberattack.

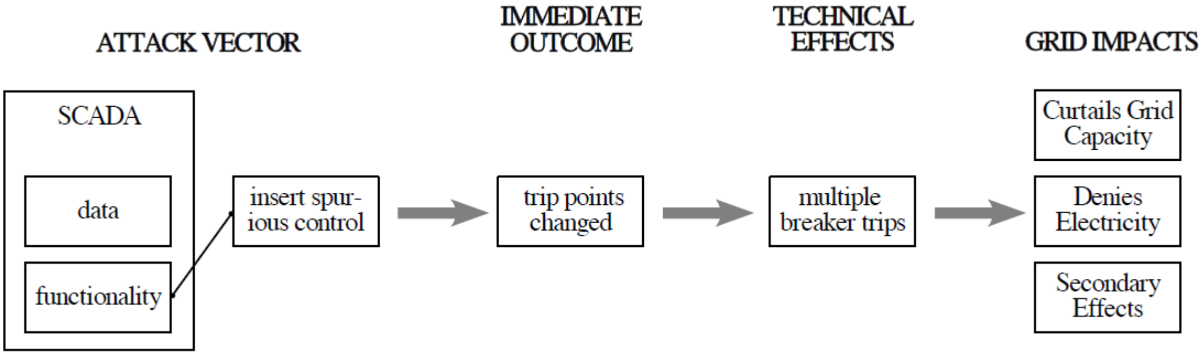


Figure 5.9 Effects of a cyberattack, adapted from [44]

In [45], the author analyses the type of cyberattacks and ways to prevent them. The attackers can be divided into five groups:

- Non-malicious, driven by intellectual challenge and curiosity;
- Consumers driven by vengeance;
- Terrorists;
- Disgruntled employees;
- Competitors, for the sake of financial gain.

These attacks can be divided into three categories [46]:

- Component-wise attacks. In the context of a SG, it may target the MU or the IED. The hacker takes control of these device and sends orders to other components, for example, open a CB;
- Protocol-wise attacks target the communication protocol and inject false data into the network;
- Topology wise attacks launch a Denial-of-service attack, preventing the operator from seeing the power grid in real time, causing wrong decisions.

Some solutions to prevent cyberattacks were also presented in [45], such as:

- Having a strong authentication mechanism with more than one step;
- Malware protection and updated antivirus software;
- Network intrusion prevention system and network intrusion detection system;
- Annual vulnerability assessments;
- Educate the operators about security best practices;
- Devices should know the source and destiny of their communication. This can be done with transport layer security or internet protocol security;
- Devices should be able to communicate through virtual private networks;
- Devices should only collect relevant data, to prevent overloads in the communication system;
- SG design must include a security plan, this way not being dependent on vendor specifics, avoiding this way incompatibility issues.

The purpose of this computation is to provide an idea of the impact of a direct failure on the SG reliability. To achieve this, a failure rate was given to both events represented in Figure 5.10. Giving a failure rate to these events was not an easy task due to their unpredictability and to the SG being a relatively new concept, therefore, the available data is not enough to give an accurate frequency to this type of events.

Given this, statistical data for SCADA systems integrated in the industry [47] was used. According to RISI online incident database [48], until 2014, 45 cyber incidents were registered in the power and utilities industry, 33 of them in the US. Considering all the industries, 212 incidents were registered, with the year 2009 being the highest contributor, with 45.

These incidents were divided by the intentions of the attack. 53.31% had the intention of disrupting the service, in the context of the SG, would be stopping the energy supply, 7.85% were considered sabotage, which means the attacker had the intention of causing damage in the equipment and 3.72% were classified as accident, in this case, the attacker means to harm, not only the system but also the people operating it. 18.18% were classified as an unintended service disruption, in this case, the responsible for the incident was not an external attacker, was caused by an error of the operator or an error of the network itself, probably caused by aged software and hardware, that may cause incorrect acquiring of measures by the MU. This wrong data would be sent to the IED, that could wrongly open a CB.

These reports provide an idea of the proportion between these two failure modes. In [49], a study of the impacts of a cyberattack on the US power grid was conducted, and a probability of 1 in 200 years was given to a successful event of this kind, with an average time to restore the operation of 24 hours.

Given this, the data used in these computations (see Table 5.2) was defined.

Table 5.2 Direct failures input data

Failure mode	**λ (/year)**	**r (h)**
Control of the CB by the intruder	0.005	24
Unintended CB operation	0.0014	24

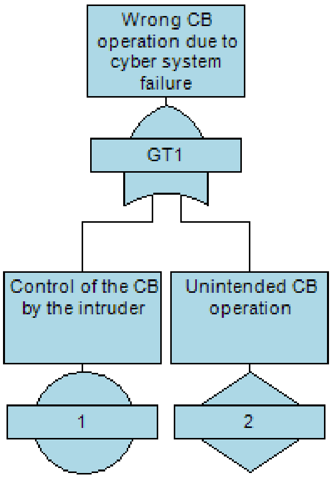

Wrong CB operation due to cyber system failure
GT1
Control of the CB by the intruder
Unintended CB operation
1
2

Figure 5.10 Fault tree for cyber direct failures on the circuit breaker

5.4 Results

5.4.1 Reliability of the Birka Nät smart grid concept

To evaluate the reliability of the Birka Nät distribution system considering the cyber failure modes, an identical FT to the one presented in section 4.4.1 (see Figure 4.15) was used. To this FT, was added to each CB the FT presented in Figure 5.8 that represents the indirect failures that affect the operation of the CBs and consequently the operation of the grid. Was also added to each CB FT, the direct failures represented in Figure 5.10, that include cyberattacks that can take control of CB and cause major outages, and unintended interruptions that can be caused by incorrect network configuration, poor maintenance and aged software/hardware, human error, incorrect programming or, incomplete or invalid measurements due to a MU or IED malfunction.

In this case, it is assumed that the intruder can control one of the CBs c2, c4, c7, c8, c10 or c13 before the operator of the grid can act.

All the computations in this section are also for one year like it was done in section 4.4. The results for the top event (No power on busbar c14) are presented in Table 5.3.

Table 5.3 Comparison of the results for the conventional and the smart grid

	Conventional grid	**Smart grid**
Reliability	97.74%	97.72%
MTTF	43.55 years	43.22 years
MTTR	7.445 hours	7.553 hours
Unavailability	1.951×10^{-5}	1.994×10^{-5}

As Table 5.3 shows, the impact of cyber failures is not alarming. The unavailability of the system is practically the same, with the reliability dropping only 0.02%. The MTTF is now 4 months less and the MTTR raised 7 minutes. These results reveal that even when adding more components from the cyber control system, the global system is still very reliable. As said before, this computation was done assuming that the hacker or the unintentional error only affects one CB at a time. Naturally, the results would be different depending on the type of attack, for example, if the hacker could operate multiple CBs, and possibly interrupt the power on both lines B1 and B2 at the same time.

The analysis of the importance values and minimal cut sets are similar to the one presented in section 4.4.1, therefore the most critical failure modes and components are still the same.

Even though these cyber failures do not heavily impact the system's reliability, they still have some impact on each line, which may represent power loss and, therefore, money lost by the producer. The downtime of each line raised from 36 hours to 37 hours, and the downtime of both lines, that make the entire system to fail, is about the same. One extra hour of downtime in each line is a significant value, and represents one extra hour of, potentially, not delivering and selling the required energy, since it is assumed that both lines are necessary to deliver the required power, therefore it is important to acknowledge these failures and find ways to prevent them.

In this case, using the FV measure, it is possible to say that the cyberattack is the most critical between the cyber failures, with 1.7% probability, a low value compared to the power system failure modes. This event is followed by the unintended operation of the CB with almost 0.5%. The indirect failures, that involve the cyber protection equipment, have a neglectable probability, lower than 0.0004%, which is expected since these failures depend on the failure of at least two components at the same time, an unlikely event.

It is possible to conclude that even though the failure modes from the cyber control part of the system are not the most critical to the top event, they still have some impact in the downtime of each transmission line and, as it was seen before, although the system does not fail when one line fails, it may lose power, therefore it is important to prevent this type of failures, especially cyberattacks, the ones with the highest probability and the ones that can have the most catastrophic consequences.

5.4.2 Reliability of the HD load point

Like it was done in chapter 4, each load point was evaluated individually. Due to the similarities between SJ and HD load points, this analysis will cover both. In this case, the cyber failures can now also affect CBs c37, c39, c40, c42, c43 and c45. The FT used in this computation is similar to the one presented in Figure 4.17. The results for the top event "No power on busbar c48" are presented in Table 5.4.

Table 5.4 Comparison of the results for the conventional and the smart grid of the HD load point

	Conventional grid	Smart grid
Reliability	96.75%	96.73%
MTTF	30.17 years	30.02 years
MTTR	6.061 hours	6.144 hours
Unavailability	2.293 x 10^{-5}	2.336 x 10^{-5}

In this case, the downtime would be almost the same compared to the conventional grid. The reliability dropped only 0.02%, the MTTF is almost 2 months less and the MTTR raised 5 minutes.

Since the SG results are similar to the ones obtained for the conventional grid, the critical failure modes and components are the same.

In each of the lines B11, B12 and B13, the unavailability raised from 1.301 x 10^{-4} to 1.652 x 10^{-4}, corresponding to a downtime raise from 68 to 87 minutes. The failure of the three lines is still a very unlikely event with an unavailability of 4.506 x 10^{-12}. Like in the previous case, it is possible to say that even though the introduction of cyber failures does not heavily impact the reliability of the entire system, it still has an impact on each line of this load point, with the cyberattack still being the highest contributor between the cyber failures.

These results would be different if the hacker had access to the nonredundant CBs, in this case, c47. The unavailability would be 4.089 x 10^{-5}, the reliability 96.11%, the MTTF 25.17 years and the MTTR 9.022 hours. In this case, the direct failures that affect this CB would be the most critical failure modes to the top event.

5.4.3 Reliability of the LH11 load point

Finally, the reliability of the LH11 load point was evaluated. In this case, it is considered that CBs c15, c18, c19, c22, c23 and c26 can also be affected by the cyber failures.

The FTs used are similar to the ones presented in Figures 4.21 and 4.22. The results for the top event “No power on busbar c35” are presented in Table 5.5.

Table 5.5 Comparison of the results for the conventional and the smart grid of the LH11 load point

	Conventional grid	**Smart grid**
Reliability	94.23%	94.21%
MTTF	16.8 years	16.75 years
MTTR	7.383 hours	7.425 hours
Unavailability	5.013×10^{-5}	5.058×10^{-5}

Like it was verified on the other two load points, the results have almost no changes. The unavailability raised approximately half a minute and the reliability dropped 0.02%.

In sum, it was verified that the critical failures from the components of the power grid are more critical to the overall system than the failures introduced by the cyber system. It is also possible to say that indirect failures are less critical than direct failures. This was expected since the indirect failures depend on another component failure. In a real-world situation, since the components from the protection system also have the function of giving the operator data in real time, so he can optimize and control the grid, a failure in one of these probably would be detected before a failure in the power system occurred and require the action from the protection system, lowering even more the impact on the system’s reliability.

It was also concluded that a cyberattack is the most critical event between the failures of the cyber system that can affect the power grid. The frequency of these events is hard to predict because it depends on the will of the attacker to choose a target and a time, but nowadays it is still considered a rare event. Although rare, this type of event should not be neglected due to the huge financial impact they can have, for example, it is estimated that a cyberattack on the US smart power grid could cost up to $1 trillion [49]. To keep the SG reliable, a strong cybersecurity system should be implemented. Since technology is constantly evolving, regular training programs to employees should also be a part of the SG planning, this way also preventing possible human errors.

Chapter 6

Conclusions and Future Work

6.1 Conclusions

The purpose of this thesis was to study the reliability of a SG. In a first stage, using just the power system components and, in a second stage, adding the cyber system. This was achieved by building FTs for each component and using them to build the FT that represents the distribution system.

The system used was the Birka Nät, composed by three load points that were studied individually. This was done to analyze the reliability of the connections to each load, this way obtaining more detailed results.

Using Isograph's software was possible to conclude which are the critical failure modes for this distribution system. Regarding the three load points, in the 110 kV cables, the short circuit of the cable due to insulation failure is the most critical to the system's unavailability, followed by the failures on the windings and tap changer of the 220/110 kV transformers. Furthermore, the failure modes of busbars c1 and c14 proved to be high contributors to failure frequency, and for that reason are also critical.

In a more detailed analysis, the failure modes of busbars c48 and c58 proved to be critical to load points HD and SJ, respectively. Moreover, in these load points, short circuit and the unexpected opening of CBs c47 and c57 are also important.

In the LH11 load point, the 11/0.4 kV transformer is the most critical component, with the top failure modes being the failures on the windings and bushings, as well as the failure of the tap changer.

The next step was to add the cyber components and their failure modes to the FTs already created. This was a more challenging task because the SG is still a work in progress and it is not well established which are the events that cause failures in the cyber system and, by consequence, on the conventional grid. In the literature was found that one of the major concerns when planning a SG is cybersecurity. This was verified in the computations that were performed in this work. The cyberattacks are the most critical event between the cyber system failures. It was also concluded that the cyber failures have almost no effect on the overall system reliability, except for the case where the hacker controls a nonredundant CB.

In the context of the indirect failures, a failure in the communication system, even though it does not stop the operation of the grid, it can have an impact on the efficiency of the system, since the operator loses control and is unable to take actions to raise the efficiency, one of the goals of the SG.

Regarding the direct failures, the importance of preventing them is even higher, since it causes an immediate outage, especially the cyberattacks, that not only can cause outages, but also cause damage on the equipment, resulting in a possible large financial loss.

In sum, the main goal of this work, evaluate the reliability of a distribution system and identify the most critical failure modes/components, was achieved. The FTs proved to be a useful method of performing reliability evaluation and an intuitive way of representing the events that can lead to the failure of a system.

6.2 Future work

Since the SG is still a work in progress, it is important to keep the research active in this area, and reliability studies are a valuable way to do it because through the analysis of failures, the system is also being analyzed, and at the same time, new ways to improve it are being found.

One of the struggles of this analysis was finding detailed information about the failure rates and repair times of the basic events of each component, since usually this type of analysis is performed per component instead of per basic event. Therefore, the next step could be to do a reliability analysis using more detailed information.

Since this is a basic reliability analysis, using the information obtained in this work, a Monte Carlo simulation could be performed to simulate a typical lifetime scenario, allowing this way to obtain more realist results.

Another topic that can be introduced in future projects is the economic factor. This factor combined with a reliability analysis gives the owner of the grid an idea on whether the project is well planned, not only in terms of reliability, but also financially, by analyzing the money lost in each outage and if it pays off to improve reliability, for example, by adding more redundancy to the system with more parallel lines.

References

[1] BloombergNEF, "Global Electricity Demand to Increase 57% by 2050," September 4, 2018. [Online]. Available: https://about.bnef.com/blog/global-electricity-demand-increase-57-2050/. [Accessed March 11, 2019].

[2] S. K. Salman, *Introduction to the Smart Grid: Concepts,Technology and Evolution*, The Institution of Engineering and Technology, London, 2017.

[3] L. Bertling, "Reliability Centred Maintenance for Electric Power Distribution Systems," PhD Thesis, Royal Institute of Technology (KTH), Stockholm, 2002.

[4] A. Volkanovski, M. Cepin and B. Mavko "Application of the fault tree analysis for assessment of power system reliability," *Reliability Engineering and System Safety,* vol. 94, no. 6, pp. 1116–1127, January 2009.

[5] R. Bono, R. Alexander, A. Dorman, Y. Kim and R. Jack, "Analyzing reliability, a simple yet rigourous approach," *in IEEE Industry Applications Society 50th Annual Petroleum and Chemical Industry Conference,* pp. 229-237, 2003.

[6] L. Yu, "Fault Tree Analysis and Reliability Assessment of Auxiliary Power Supply system for an HVDC Plant," Master Thesis, Royal Institute of Technology (KTH), Stockholm, 2007.

[7] S. Katsavounis, N. Patsianis, E. I. Konstantinidis and P. N. Botsaris, "Reliability Analysis on Crucial Subsystems of a Wind Turbine through FTA Approach," *in Maintenance Performance Measurement and Management,* 2014.

[8] Y. Zhang, A. Sprintson and C. Singh, "An Integrative Approach to Reliability Analysis of an IEC 61850 Digital Substation," *in 2012 IEEE Power and Energy Society General Meeting,* pp. 1-8, 2012.

[9] M. G. Kanabar and T. S. Sidhu, "Reliability and Availability Analysis of IEC 61850 Based Substation Communication Architectures," *in 2009 IEEE Power Energy Society General Meeting,* pp. 1-8, July 2009.

[10] H. Lei, C. Singh and A. Sprintson, "Reliability Modeling and Analysis of IEC 61850 Based Substation Protection Systems," *IEEE Transactions on Smart Grid,* vol. 5, no. 5, pp. 2194-2202, September 2014.

[11] H. Chen, B. Guo and G. Song, "A Layered Fault Tree Model for Reliability Evaluation of Smart Grids," *Energies,* vol. 7, no. 8, pp. 4835-4857, 2014.

[12] Isograph, [Online]. Available: https://www.isograph.com/. [Accessed February, 19 2019].

[13] PEW, "The Smart Grid: How Energy Technology Is Evolving," February 26, 2016. [Online]. Available: https://www.pewtrusts.org/en/research-and-analysis/issue-briefs/2016/02/the-smart-grid-how-energy-technology-is-evolving. [Accessed February 14, 2019].

[14] R. Ghafurian and H. Gharavi, "Smart Grid: The Electric Energy System of the Future," *Proceedings of the IEEE,* vol. 99, no.6, pp.917-921, May 2011.

[15] ABB, "Toward a smarter grid ABB’s Vision for the Power System of the Future," [Online]. Available: https://pdfs.semanticscholar.org/8d1e/26bd3a8b814985d930a6a72992db24f91925.pdf. [Accessed October 14, 2019].

[16] K. Sgouras, A. Birda and D. Labridis, "Cyber Attack Impact on Critical Smart Grid Infrastructures," *in 2014 IEEE PES Innovative Smart Grid Technologies Conference,* pp. 1-5, 2014.

[17] V. Giordano, F. Gangale, G. Fulli and M. Jiménez, "Smart Grid projects in Europe: lessons learned and current developments," Joint Research Centre of the European Commission, The Netherlands, 2011.

[18] A. A. Chowdhury and D. O. Koval, *Power Distribution System Reliability*, IEEE Press, New Jersey, 2009.

[19] M. Stamatelatos and W. Vesely, *Fault Tree Handbook with Aerospace Applications*, NASA, Washington, DC, 2002.

[20] V. Lackovic, "High Voltage Busbar Protection," [Online]. Available: https://www.pdh-pro.com/course/high-voltage-busbar-protection/. [Accessed May 9, 2019].

[21] Y. J. Bao, K. Ding, K. W. E. Cheng and D. H. Wang, "The Study on the Busbar System and its Fault Analysis," *in 2013 5th International Conference on Power Electronics Systems and Applications,* pp. 1-7, December 2013.

[22] P. Choonhapran, "Applications of High Voltage Circuit-Breakers and Development of Aging Models," PhD Thesis, Darmstadt University of Technology, Darmstadt, 2007.

[23] Electrical Engineering Portal, "Fundamentals of High Voltage Circuit Breakers, Switching Stresses and Failure Modes," [Online]. Available: https://electrical-engineering-portal.com/download-center/books-and-guides/electricity-generation-t-d/fundamentals-hv-cbs. [Accessed May 9, 2019].

[24] IEEE, "IEEE Guide for the Selection of Monitoring for Circuit Breakers," *IEEE Std C37.10.1-2000,* pp. 1-58, 2001.

[25] E. Csanyi, "When does exciting current inrush occur in power transformer?," September 7, 2016. [Online]. Available: https://electrical-engineering-portal.com/exciting-current-inrush-power-transformer. [Accessed May 9, 2019].

[26] A. Franzén and S. Karlsson, "Failure Modes and Effects Analysis of Transformers," Master Thesis, Royal Institute of Technology (KTH), Stockholm, 2007.

[27] Excalon, "EHV Power Cables Division," [Online]. Available: https://www.excalon.com/-services/ehv-division. [Accessed November 25, 2019].

[28] M. Bolotinha, "Cable Faults," September 24, 2015. [Online]. Available: https://www.linkedin.com/-pulse/cable-faults-manuel-bolotinha/. [Accessed April 17, 2019].

[29] IEEE, "IEEE Recommended Pratice for the Design of Reliable Industrial and Commercial Power Systems," *IEEE Std 493-1997,* pp. 1-464, 1998.

[30] CIGRÉ, "Final Report of the Second International Enquiry on High Voltage Circuit-Breaker Failures and Defects in Service," 1994.

[31] CIGRE WG A2.37, "Power Transformers Failure Modes, Investigation & Prevention Techniques," *in CIGRE SC A2 Colloquium*, Shanghai, 2015.

[32] N. Lázaro, "Diagrama de Blocos de Fiabilidade (RBD) aplicado ao conceito de Smart Grid: Uma introdução," Master Thesis, Instituto Superior Técnico, Lisbon, 2018.

[33] B. Falahati and Y. Fu, "Reliability Assessment of Smart Grids Considering Indirect Cyber-Power Interdependencies," *IEEE Transactions on Smart Grid,* vol. 5, no. 4, pp. 1677-1685, 2014.

[34] H. Lei, B. Chen, K. Butler-Purry and C. Singh, "Security and Reliability Perspectives in Cyber-Physical Smart Grids," *in 2018 IEEE Innovative Smart Grid Technologies*, pp. 42-47, May 2018.

[35] G. Solutions, "Networked Merging Units," [Online]. Available: https://www.gegridsolutions.com/-multilin/catalog/amu.htm. [Accessed August 8, 2019].

[36] ICE, "NPT916 - Differential Protection IED," [Online]. Available: https://www.icelec.com/en/-produit/npt916_transformer-protection-ied#prettyPhoto. [Accessed August 8, 2019].

[37] B. Electric, "IEC 61850-3 Ethernet Switch," [Online]. Available: http://www.bueno-electric.com/products/industrial-ethernet-switch/iec-61850-3-ethernet-switch/iec-61850-3-ethernet-switch-rack-chassis.html. [Accessed August 8, 2019].

[38] B. Falahati and E. Chua, "Failure Modes in IEC 61850-Enabled Substation," *in 2016 IEEE/PES Transmission and Distribution Conference and Exposition (T&D,)* pp. 1-5, 2016.

[39] Dell, "PowerEdge R830 Rack Server," [Online]. Available: https://www.dell.com/ae/business/-p/poweredge-r830/pd. [Accessed August 8, 2019].

[40] ABB, "ABB Smart Grid Center of Excellence," [Online]. Available: https://new.abb.com/-us/customer-experience-centers/abb-smart-grid-center-of-excellence. [Accessed August 8, 2019].

[41] S. E. GB, "Smart Meters Explained," [Online]. Available: https://www.smartenergygb.org/en/about-smart-meters. [Accessed August 8, 2019].

[42] A. Anwar and A. Mahmood, "Cyber Security of Smart Grid Infrastructure," *The State of the Art in Intrusion Prevention and Detection*, CRC Press, Taylor & Francis Group, pp. 449-472, USA, January 2014.

[43] K. Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," Wired, March 3, 2016. [Online]. Available: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/. [Accessed September 2, 2019].

[44] J. Stamp, A. McIntyre and B. Ricardson, "Reliability Impacts from Cyber Attack on Electric Power Systems," *in 2009 IEEE/PES Power Systems Conference and Exposition,* pp. 1-8, March 2009.

[45] F. Aloul, A. R. Al-Ali, R. Al-Dalky, M. Al-Mardini and W. El-Hajj, "Smart Grid Security: Threats, Vulnerabilities and Solutions," *International Journal of Smart Grid and Clean Energy,* vol. 1, pp. 1-6, September 2012.

[46] D. Wei, Y. Lu, M. Jafari and P. Skare, "Protecting Smart Grid Automation Systems Against Cyberattacks," *IEEE Transactions on Smart Grid,* vol. 2, no. 4, pp. 782-795, December 2011.

[47] R. I. Ogie, "Cyber Security Incidents on Critical Infrastructure and Industrial Networks," *in Proceedings of the 9th International Conference on Computer and Automation Engineering,* pp. 254-258, February 2017.

[48] RISI, "Online Incident Database," [Online]. Available: https://www.risidata.com/Database /country/desc. [Accessed July 3, 2019].

[49] University of Cambridge and Lloyd's, "Business Blackout - The insurance implication of a cyber attack in the US power grid," Emerging Risk Report, United Kingdom, 2015.

Appendix A

Detailed reliability input data

Table A.1 Busbars reliability input data, based on [3], [29]

Failure modes	220 kV		33 kV		11 kV		0.4 kV	
	λ (/year)	r (h)	λ (/year)	r (h)	λ (/year)	r (h)	λ (/year)	r (h)
B1	0.0048	1	0.0048	1	0.0043	1	0.0043	1
B2	0.0048	1	0.0048	1	0.0043	1	0.0043	1
Total	0.0096	-	0.0096	-	0.0087	-	0.0087	-

Table A.2 Circuit breakers reliability input data, based on [3], [30]

Failure modes	220 kV		110 kV		33 kV		11 kV	
	λ (/year)	r (h)	λ (/year)	r (h)	λ (/year)	r (h)	λ (/year)	r (h)
CB1	0.0037	168	0.0037	168	0.0004	72	0.0010	48
CB2	0.0022	168	0.0022	168	0.0002	72	0.0006	48
CB3	0.0013	168	0.0013	168	0.0001	72	0.0004	48
CB4	0.0009	168	0.0009	168	8.722×10^{-5}	72	0.0002	48
CB5	0.0006	168	0.0006	168	6.23×10^{-5}	72	0.0002	48
CB6	9.57×10^{-5}	168	9.57×10^{-5}	168	9.79×10^{-6}	72	2.673×10^{-5}	48
Total	0.0087	-	0.0087	-	0.0009	-	0.0024	-

Table A.3 Transformers reliability input data, based on [3], [31]

Failure modes	**220/110 kV**		**110/33 kV**		**33/11 kV**		**11/0.4 kV**	
	λ (/year)	**r (h)**	**λ (/year)**	**r (h)**	**λ (/year)**	**r (h)**	**λ (/year)**	**r (h)**
T1	0.0098	504	0.0077	504	0.0075	504	0.0012	48
T2	0.0081	504	0.0064	504	0.0062	504	0.0010	48
T3	0.00445	504	0.0035	504	0.0034	504	0.0006	48
T4	0.0025	504	0.0020	504	0.0019	504	0.0003	48
T5	0.0006	504	0.0005	504	0.0005	504	8.043×10^{-5}	48
T6	0.0003	504	0.0002	504	0.0002	504	3.707×10^{-5}	48
T7	0.0002	504	0.0002	504	0.0001	504	2.483×10^{-5}	48
Total	0.0261	-	0.0205	-	0.0199	-	0.0033	-

Table A.4 Cables reliability input data, based on [3], [29]

Failure modes	**110 kV**		**33 kV SJ**		**33 kV HD**		**33 kV LH33**		**11 kV LH11**	
	λ (/year)	**r (h)**	**λ (/year)**	**r (h)**	**λ (/year)**	**r (h)**	**λ (/year)**	**r (h)**	**λ (/year)**	**r (h)**
C1	0.0393	168	0.0048	48	0.0128	48	0.0002	48	0.0564	6
C2	0.0231	168	0.0028	48	0.0076	48	9.24×10^{-5}	48	0.0332	6
C3	0.0077	168	0.0009	48	0.0025	48	3.08×10^{-5}	48	0.0111	6
Total	0.0701	-	0.0086	-	0.0229	-	0.0003	-	0.1007	-

Appendix B

Results for the HD load point computation

Table B.1 Failure mode importance values without lines B11 and B12

Component	Failure mode	FV	RRW	RAW
33 kV HD Cable(c44)	Short circuit due to insulation failure	0.4894	1.959	4097
	No energy supply due to mechanical failure	0.2884	1.405	4095
Cables (c5/c11)	Short circuit due to insulation failure	0.0127	1.013	17.91
Transformers (c3/c9)	Short circuit due to windings failure	0.0096	1.01	17.91
	No voltage regulation due to tap changer failure	0.0079	1.008	17.91

Table B.2 Top 5 minimal cut sets sorted by unavailability without lines B11 and B12

No.	Unavailability	%	Failure mode
1	1.195×10^{-4}	48.94	Short circuit due to insulation failure (Cable c44)
2	7.042×10^{-5}	28.84	No energy supply due to mechanical failure (Cable c44)
3	1.219×10^{-6}	0.4992	Short circuit due to insulation failure (CB c43/c45)
4	8.705×10^{-7}	0.3566	Opens without command (CB c43/c45)
5	7.169×10^{-7}	0.2936	Short circuit due to insulation failure (CB c47)

Table B.3 Top 5 minimal cut sets sorted by frequency without lines B11 and B12

No.	Frequency	%	Failure mode
1	2.181×10^{-2}	30.08	Short circuit due to insulation failure (Cable c44)
2	1.285×10^{-2}	17.73	No energy supply due to mechanical failure (Cable c44)
3	4.82×10^{-3}	6.648	Short circuit (Busbar c1/c14/c48)
4	4.82×10^{-3}	6.648	No energy supply due to mechanical failure (Busbar c1/c14/c48)
5	8.526×10^{-4}	1.176	Short circuit due to insulation failure (CB c2/c8)

Appendix C

Results for the SJ load point computation

Table C.1 Failure mode importance values for of top event “No power on busbar c58”

Component	Failure mode	FV	RRW	RAW
Cables (c5/c11)	Short circuit due to insulation failure	0.1353	1.156	180.6
Transformers (c3/c9)	Short circuit due to windings failure	0.1017	1.113	180.6
	No voltage regulation due to tap changer failure	0.0841	1.092	180.7
Transformers (c6/c12)	Short circuit due to windings failure	0.0799	1.087	180.7
Cables (c5/c11)	No energy supply due to mechanical failure	0.0797	1.087	180.7

Table C.2 Top 10 minimal cut sets sorted by unavailability of the top event “No power on busbar c58”

No.	Unavailability	%	Failure mode 1	Failure mode 2
1	7.169 x 10^{-7}	3.119	Short circuit due to insulation failure (CB c57)	
2	5.663 x 10^{-7}	2.464	Short circuit due to insulation failure (Cable c5)	Short circuit due to insulation failure (Cable c11)
3	5.502 x 10^{-7}	2.394	Short circuit (Busbar c1/c14/c58)	
4	5.502 x 10^{-7}	2.394	No energy supply due to mechanical failure (Busbar c1/c14/c58)	
5	5.121 x 10^{-7}	2.228	Opens without command (CB c57)	
6	4.257 x 10^{-7}	1.852	Short circuit due to insulation failure (Cable c5)	Short circuit due to windings failure (Transformer c9)
7	4.257 x 10^{-7}	1.852	Short circuit due to windings failure (Transformer c3)	Short circuit due to insulation failure (Cable c11)
8	3.519 x 10^{-7}	1.531	Short circuit due to insulation failure (Cable c5)	No voltage regulation due to tap changer failure (Transformer c9)
9	3.519 x 10^{-7}	1.531	No voltage regulation due to tap changer failure (Transformer c3)	Short circuit due to insulation failure (Cable c11)
10	3.344 x 10^{-7}	1.455	Short circuit due to insulation failure (Cable c5)	Short circuit due to windings failure (Transformer c12)

Table C.3 Top 5 minimal cut sets sorted by frequency of the top event “No power on busbar c58”

No.	Frequency	%	Failure mode
1	4.82×10^{-3}	14.58	Short circuit (Busbar c1/c14/c58)
2	4.82×10^{-3}	14.58	No energy supply due to mechanical failure (Busbar c1/c14/c58)
3	8.526×10^{-4}	2.58	Short circuit due to insulation failure (CB c2/c8)
4	8.722×10^{-5}	0.2639	Short circuit due to insulation failure (33 kV CBs)
5	6.23×10^{-5}	0.1885	Opens without command (CB c57)

Table C.4 Failure mode importance values without line B16

Component	Failure mode	FV	RRW	RAW
SJ Cable(c54)	Short circuit due to insulation failure	0.3917	1.644	1.057×10^{4}
	No energy supply due to mechanical failure	0.2308	1.3	1.057×10^{4}
Cables (c5/c11)	Short circuit due to insulation failure	0.0328	1.034	44.61
Transformers (c3/c9)	Short circuit due to windings failure	0.0247	1.025	44.62
	No voltage regulation due to tap changer failure	0.0204	1.021	44.62

Table C.5 Top 5 minimal cut sets sorted by unavailability without line B16

No.	Unavailability	%	Failure mode
1	3.707×10^{-5}	39.17	Short circuit due to insulation failure (Cable c54)
2	2.185×10^{-5}	23.08	No energy supply due to mechanical failure (Cable c54)
3	1.004×10^{-6}	1.06	Short circuit due to insulation failure (CB c53/c55)
4	7.169×10^{-7}	0.7569	Opens without command (CB c53/c55)
5	7.169×10^{-7}	0.7569	Short circuit due to insulation failure (CB c57)

Table C.6 Top 5 minimal cut sets sorted by frequency without line B16

No.	Frequency	%	Failure mode
1	6.766×10^{-3}	14.88	Short circuit due to insulation failure (Cable c54)
2	4.82×10^{-3}	10.6	Short circuit (Busbar c1/c14/c58)
3	4.82×10^{-3}	10.6	No energy supply due to mechanical failure (Busbar c1/c14/c58)
4	3.987×10^{-3}	8.771	No energy supply due to mechanical failure (Cable c54)
5	8.526×10^{-4}	1.876	Short circuit due to insulation failure (CB c2/c8)

Appendix D

Results for the LH11 load point computation

Table D.1 Failure mode importance values without lines B3 and B4

Component	Failure mode	FV	RRW	RAW
33/11 kV Transformer (c25)	Short circuit due to windings failure	0.3647	1.574	498.4
	No voltage regulation level due to tap changer failure	0.3015	1.432	498.4
	Short circuit due to bushing failure	0.1661	1.199	498.6
	Insulation failure	0.0235	1.024	498.7
	Overheat due to cooling system failure	0.0108	1.011	498.7

Table D.2 Top 5 minimal cut sets sorted by unavailability without lines B3 and B4

No.	Unavailability	%	Failure mode
1	7.327×10^{-4}	36.47	Short circuit due to windings failure (Transformer c25)
2	6.058×10^{-4}	30.15	No voltage regulation due to tap changer failure (Transformer c25)
3	3.337×10^{-4}	16.61	Short circuit due to bushings failure (Transformer c25)
4	4.727×10^{-5}	2.353	Insulation failure (Transformer c25)
5	2.179×10^{-5}	1.084	Overheat due to cooling system failure (Transformer c25)

Table D.3 Top 10 minimal cut sets sorted by frequency without lines B3 and B4

No.	Frequency	%	Failure mode
1	1.273×10^{-2}	13.47	Short circuit due to windings failure (Transformer c25)
2	1.053×10^{-2}	11.14	No voltage regulation due to tap changer failure (Transformer c25)
3	5.8×10^{-3}	6.134	Short circuit due to bushings failure (Transformer c25)
4	4.82×10^{-3}	5.097	Short circuit (Busbar c1/c14)
5	4.82×10^{-3}	5.097	No energy supply due to mechanical failure (Busbar c1/c14)
6	4.335×10^{-3}	4.584	Short circuit (Busbar c27/c35)
7	4.335×10^{-3}	4.584	No energy supply due to mechanical failure (Busbar c27/c35)
8	1.248×10^{-3}	1.319	Short circuit due to windings failure (Transformer c33)
9	1.031×10^{-3}	1.091	No voltage regulation due to tap changer failure (Transformer c33)
10	8.526×10^{-4}	0.9016	No energy supply due to insulation failure (CB c2/c8)