Reliability evaluation for smart distribution grids by fault tree analysis

Gonçalo dos Santos Bravo
Instituto Superior Técnico
Universidade de Lisboa
Lisbon, Portugal
goncalo.bravo@ist.utl.pt

***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 to perform a reliability analysis using the fault tree method to determine 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.**

***Index Terms*— Smart grid, reliability, fault tree, failure mode, failure rate, cybersecurity.**

I. Introduction

ELECTRICITY is essential to society and, with its development, the demand has been increasing exponentially. Markets like electric vehicles are already growing and will grow even more in the future. It is expected that by 2050 this market accounts for 9% of the demand [1].

These and other changes like the introduction of more renewables or distributed energy sources pose new challenges that the power system cannot cope with anymore. After acknowledging these fragilities, the smart grid became a necessity to the modern world. Incorporating new computer-based technologies like monitor and control devices, capable of communicating at a distance, will allow to modernize and improve the electrical grid in terms of efficiency and reliability. Given this, it makes sense to continue the research in this area to one day the smart grid instead of being called the future grid, be called the present grid.

Evaluate the reliability of a smart grid, using the fault tree method, is the main objective of this work. This will be done in two phases, the first one consisting of a detailed study of the power system components and, in a second phase, integrate the cyber system components to evaluate their impact on the previously obtained overall system reliability. Firstly, the failure modes of the components of the power system, namely, busbars, circuit breakers (CBs), transformers, and cables, were obtained to build the component fault trees. After this, failure rates and repair times were given to each failure mode. Then, using a model of a distribution system, a reliability analysis was performed, and the most important results acquired. After the reliability study of the conventional part of the grid, cyber components and their failure modes were added and the results for the overall system obtained.

II. Smart grid: An introduction

A. Definition of smart grid

A smart grid is an electricity network that integrates modern technology, like cyber-secure communication, computer-based control and protection systems, that combine to manage and monitor the electricity distribution in a more reliable and efficient way than the conventional systems.

The goal of creating what is called the "future grid" is to improve reliability, efficiency and security of the power grid [2], in generation, transmission and distribution of electricity.

Government policies regarding environmental concerns, urging the implementation of more renewable energy sources, consumers demanding more efficiency and the introduction of computer-based technologies are the three major factors impacting the future electric system [3]. These and other debilities of the power system are the main goal of creating ways to improve it.

B. Characteristics of the smart grid

To improve the conventional grid, the smart grid must have the following characteristics, according to [3]:

- Adaptive – Responds quicker and more efficiently to condition changes with less human intervention;

- Self-healing – In case a component fails, the system can repair itself, removing the failed component and redirecting the power to be able to feed all costumers;
- Flexible – Can rapidly and safely connect the distributed generation and the energy storage at any point of the grid;
- Predictive – Identifies potential faults before they occur using machine learning and weather impact projections;
- Integrated – Allows communications in real time;
- Interactive – Provides real-time information about the status of the grid to both operator and consumer;
- Optimized – Improves reliability, availability, and efficiency by knowing the status of the grid components and autonomously optimizes the flow of energy using alternative routes;
- Secure – All components are physically and cyber secure.

In Table I are summarized the differences between a conventional grid and a smart grid, according to [4].

TABLE I
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

C. Benefits of the smart grid

As said before, the smart grid is a more reliable and efficient way of transmitting and distributing electricity with several benefits [2], such as:

- Efficiency is improved by reducing losses, having peak demand control and implementing smart meters;
- The use of cyber control equipment allows the monitoring in real time of the grid to prevent failures before they even happen, reducing this way the frequency and duration of downtimes;
- Improves the quality of supply;
- Improves the connection and access to the grid, allowing the integration of electric vehicles and the introduction of more renewable energy sources;
- Allows the dynamic adjustment of the price of electricity.

III. RELIABILITY ANALYSIS

A. Basic reliability concepts

The time to failure of a component can be defined as a random variable, T, and modeled by a probability density function (PDF), $f(t)$. Equation 1 represents the probability of a component failing before a time t, given by the cumulative distribution function, $F(t)$.

$$\Pr(\mathrm{T} \leq \mathrm{t}) = F(t) = \int_0^t f(t)\,dt \tag{1}$$

Reliability, $R(t)$, is the probability that a system operates without failure after a length of time t, and can be obtained by,

$$\Pr(T > t) = R(t) = 1 - F(t) \tag{2}$$

The failure rate, $\lambda(t)$, represents the rate that failures occur and can be expressed in terms of the PDF and the reliability function as equation 3 demonstrates.

$$\lambda(t) = \frac{f(t)}{R(t)} \tag{3}$$

The mean time to failure (MTTF) is the expected time a component takes to fail and can be obtained by,

$$MTTF = E(T) = \int_0^\infty t.f(t)\,dt = \int_0^\infty R(t)\,dt \tag{4}$$

The average unavailability, Q_{AV}, is the proportion of time that the system is not operating [5] and can be obtained by the following expression,

$$Q_{AV} = \frac{MTTR}{MTTF + MTTR} \tag{5}$$

where the mean time to repair (MTTR) represents the mean time a component takes to be repaired.

B. Basic fault tree concepts

The fault tree analysis is an analytical-based reliability method used to identify potential causes of failure in a system. Some of the most important concepts related to the fault tree analysis are:

- Basic event – Initiating cause of the failure. These are the events from the lowest level of the fault tree. Can be represented by a circle or a diamond, if the event has more lower level events but the author chose to not represent them;
- Intermediate event – Event that results from a combination of basic events;
- Top event – Event that is going to be analyzed and is the consequence of the lower level events;
- AND gate – Means that the event only occurs if all the predecessor events occur;
- OR gate – Means that the event occurs if at least one of the predecessor events occur;
- Cut set – The combination of basic events to reach the top event;
- Minimal cut set – Is the smallest combination of events to reach the top event.

IV. RELIABILITY ANALYSIS OF THE BIRKA NÄT DISTRIBUTION SYSTEM

A. The grid

The chosen system was the Birka Nät, a real distribution system in Sweden, already analyzed in the reliability context in [6], where the failure rate and repair times of the components is provided. In Figure 1 is represented a simplified model

consisting of busbars, circuit breakers, transformers, and cables with voltages between 220 kV and 0.4 kV. c1 represents the 220 kV substation, c14 the 33 kV substation and c27 the 11 kV substation. c48 and c58 are 33 kV load points and c35 a 0.4 kV load point.

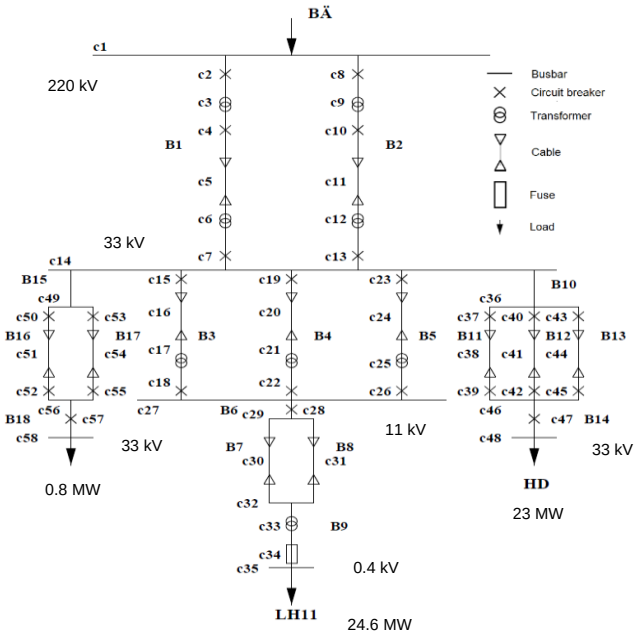

Fig. 1. Birka Nät distribution system, adapted from [6]

B. *Electrical power system fault trees*

In this section, the fault trees of the studied components of the power system will be presented. These fault trees were built using the failure modes of each component and used to build the distribution system fault tree.

1) Busbar

The busbar has the function of receiving the energy from the incoming feeders and distribute it to the outgoing feeders. The failures of this component can be divided into mechanical and electrical. Mechanical failures may happen due to cracking of the connection welds or breakage of the mechanical structure. Regarding electrical failures, the most common is a short circuit, caused by moisture, lightning strikes, a fault in another component of the grid, or by the degradation of the insulators. The fault tree of the busbar and the respective failure distribution (based on [7]**)** is presented in Figure 2.

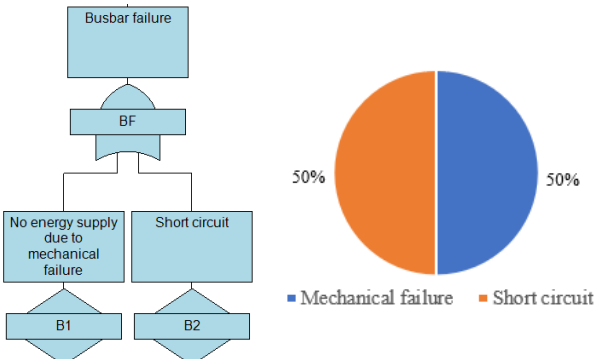

Fig. 2. Busbar fault tree and failure distribution

2) Circuit breaker

The main function of the circuit breakers is to protect the grid from extended damage after a fault by isolating the failed component. The failure modes considered in this work [8] are:

- Dos not close on command - Due to a defective close coil, loss of stored energy, inadequate lubrification, or control circuit failure;
- Does not open on command - This may happen due to an open or 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 – Due to loss of dielectric medium or foreign object damage;
- Opens without command - 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 - Caused by stray current in the close circuit, ground on the close circuit, or vibration on the circuit breaker.

The failure mode “Do not fully close/open” is considered to affect the failure modes “Does not close/open on command”.

In Figure 3 is presented the fault tree for the circuit breaker and the failure distribution (based on [9]**)**.

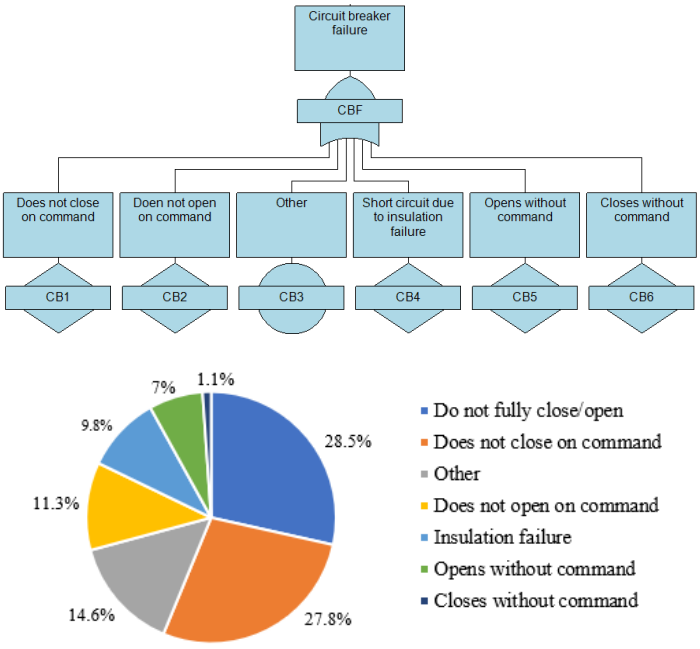

Fig. 3. Circuit breaker fault tree and failure distribution

3) Transformer

The transformers are used to step up or step down the voltage in the power grid.

According to [10], the different parts of a transformer and the respective failures are:

- Windings - Lightning strikes, short circuits in the grid, displacement of the windings, or degradation of the insulation can cause short circuits on the transformer;
- Tap changer – Can fail due to wear or contamination of the oil;

- Bushings – Human sabotage or careless handling can physically damage the bushings, while contamination of the oil or hot spots may lead to short circuits;
- Insulation – The solid insulation provides dielectric and mechanical insulation to the windings, the failure of it can cause short circuits, with aging being the highest contributor to insulation failure. The oil has the purpose of cooling the transformer, and the contamination of the oil can prevent the appropriate function this type of insulation;
- Cooling system – The failure of this part of the transformer may cause an overheat, due the failure of the fans or pumps, or by contamination in the oil;
- Tank - The tank is where the oil is contained, and it 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.

In Figure 4 is presented the fault tree of the transformer and the failure distribution (based on [11]**)**.

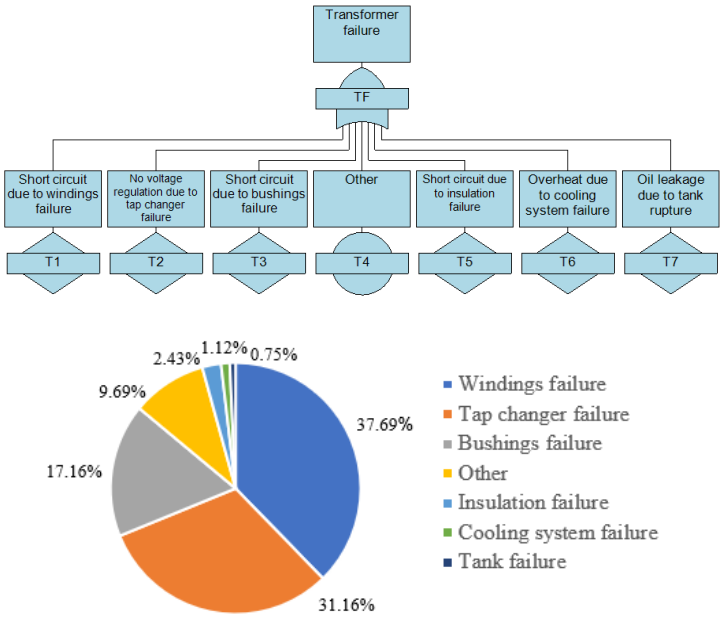

Fig. 4. Transformer fault tree and failure distribution

4) Cable

The cables in this system are underground and have the function of carrying the energy. Sabotage by people, accidentally cut by machine, sharp bending, or vibration causes mechanical damage [12]. Damage in the sheath material will allow moisture to enter the cable, deteriorating the insulation material and causing short circuits. Furthermore, overloads, high ambient temperatures or insufficient ventilation can also lead to insulation degradation. In Figure 5 is represented the fault tree for the cable and the failure distribution (based on [7]**)**.

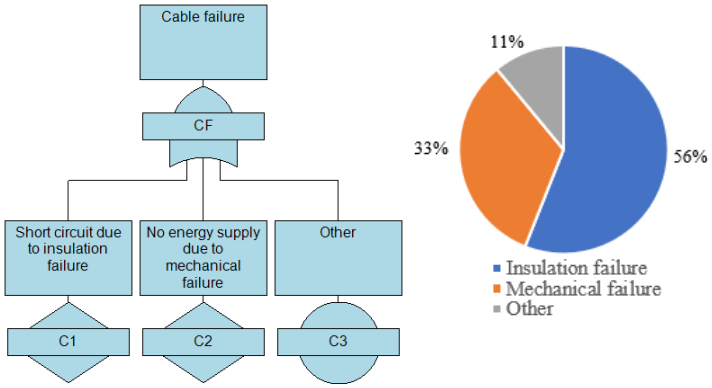

Fig. 5. Cable fault tree and failure distribution

C. Results

1) Reliability of the Birka Nät

This distribution system feeds a total of 37,701 clients, that require an average power of 48.4 MW and a maximum of 81.2 MW [6].

The first computation intends to evaluate the reliability between the 220 kV substation (c1) and the 33 kV substation (c14), being the top event “No power on busbar c14”. These connections affect all three load points, and the fault tree used in this computation, represented in Figure 9 (see appendix), can represent the entire grid if we add the failure modes from the components downstream of busbar c14 that directly affect this busbar. These events are a short circuit on the circuit breakers directly connected to busbar c14 or their malfunction after a fault (not opening on command). Furthermore, the same type of failures in the circuit breakers directly connected to busbar c1 would have the same effect. This type of events would cause an interruption of power in the entire grid and would require the operation of a disconnector, an offload device that disconnects the circuit and is mainly used for maintenance purposes. To simulate this, a similar approach to the one done on the double busbar arrangement was taken. To these events, instead of the normal repair time, one hour was given, to simulate the switching time, i.e. the time that the line with the failed component would take to be isolated and the operation of the grid resumed.

The other events that can stop power from being delivered to busbar c14 are the failure busbar c1, one component from both lines B1 and B2 fails at the same time or the busbar c14 itself fails.

It is also important to note that some failure modes of the circuit breakers, namely “Does not open on command”, “Does not close on command”, “Closes without command”, are dependent on the failure of another component. It is assumed that the circuit breakers start as closed and, in case a circuit breaker fails to isolate a fault, the upstream circuit breaker would open, since the failure of three components at the same time is very unlikely.

The results for the first computation are presented in Table II. All computations presented are for one year.

TABLE II
RESULTS OF THE TOP EVENT "NO POWER ON BUSBAR C14"

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

The results show a favorable situation in terms of reliability, with almost 98%. This can be explained by the redundancy that lines B1 and B2 introduce. In Table II is also possible to see the low value of the unavailability (Q), meaning that the system has an average downtime of 10 minutes per year. The mean time that the system takes to fail is 44 years and the mean downtime for repairs if the system fails is around 7 hours, all acceptable values.

In Table III are presented the importance measures, a useful way of evaluating the critical failure modes and components. These failure modes are sorted by the Fussell-Vesely (FV) value, that is the probability of an event (basic or intermediate) being the cause, or one of the causes, of the top event.

TABLE III
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

The FV value shows that the most critical failure modes are insulation and mechanical failures in the 110 kV cables, the windings and tap changer of the transformers. The Risk reduction worth (RRW) value shows the increase in the overall system reliability if the given event does not happen. In this case, if the top failure mode does not happen, the system would 1.189 times more reliable. The Risk achievement worth (RAW) is the opposite of the RRW, shows the impact on the system if the failure mode happens.

In Table IV are presented the top minimal cut sets (smallest paths to reach the top event) sorted by unavailability and contribution (%). Each minimal cut set is presented by the description of the failure mode, followed by the respective component, or components, if the failure model is common to more than one component with the same unavailability.

The minimal cut sets are of the first order (depend on one event) or second order (depend on two events).

TABLE IV
TOP 5 MINIMAL CUT SETS SORTED BY UNAVAILABILITY OF THE TOP EVENT "NO POWER ON BUSBAR C14"

No.	Q	%	Failure mode 1	Failure mode 2
1	5.663×10^{-7}	2.894	Short circuit due to insulation failure (Cable c5)	Short circuit due to insulation failure (Cable c11)
2	5.502×10^{-7}	2.812	Short circuit (Busbar c1/c14)	
3	5.502×10^{-7}	2.812	No energy supply due to mechanical damage (Busbar c1/c14)	
4	4.257×10^{-7}	2.175	Short circuit due to insulation failure (Cable c5)	Short circuit due to windings failure (Transformer c9)
5	4.257×10^{-7}	2.175	Short circuit due to windings failure (Transformer c3)	Short circuit due to insulation failure (Cable c11)

The minimal cut set analysis confirms the criticality of the failure modes mentioned in the analysis of Table III to the unavailability.

Moreover, the failure modes of busbars c1 and c14 are high contributors to the frequency of the top event (20.99%), therefore need to be considered critical.

2) Reliability of the HD load point

In Figure 1 can be seen that HD and SJ load points have similar topologies, therefore this analysis will cover both.

HD load point supplies 23,400 costumers that require an average power of 23 MW, SJ supplies only one client with an average power of 0.8 MW [6].

In this section's computations, the goal is to evaluate the reliability of the grid to supply the HD load. The top event, in this case, is "No power on busbar 48". This can be caused by having no power on busbar c14, a simultaneous failure in at least one component from lines B11, B12 and B13, a failure in circuit breaker c47 or busbar c48. Similarly to what was done in the computation of the whole grid reliability, a short circuit or malfunction after a fault on circuit breakers c39, c42 or c45, would result in a one-hour outage.

The results for the computation of this load point are presented in Table V.

TABLE V
RESULTS OF THE TOP EVENT "NO POWER ON BUSBAR C48"

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

The reliability in this load point is 97%, 1% less than the one obtained in the computation of the overall grid reliability but still an acceptable value. An average of 12 minutes of downtime

per year is expected, with the failure of the system being expected after 30 years, 13 years less than the overall grid, and the mean downtime for repairs after a failure is approximately 6 hours.

Like it was done in the previous computation, the importance measures were analyzed and are presented in Table VI.

TABLE VI
FAILURE MODE IMPORTANCE VALUE FOR 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

Through the importance values, it is possible to conclude that the most critical failure modes to this load point are the ones that were obtained in the analysis of the overall system. Even though with slightly lower FV value, the insulation and mechanical failures in the 110 kV cables, the windings and the tap changer of the transformers are the most critical to this load point.

In Table VII, it is presented the minimal cut set analysis.

TABLE VII
TOP 5 MINIMAL CUT SETS SORTED BY UNAVAILABILITY OF THE TOP EVENT "NO POWER ON BUSBAR C48"

No.	Q	%	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 damage (Busbar c1/c14/c48)	
5	5.121×10^{-7}	2.227	Opens without command (CB c47)	

The minimal cut set analysis adds the insulation failure and the unintended opening of circuit breaker c47 as important minimal cut sets to this load point, along with the failure modes from busbar c48, due to their high frequency (14.54%), like it was seen in the computation of the whole grid. This was expected since these components have no redundancy and their failure modes are first order minimal cut sets. These failure modes join the ones presented in Table VI as the most critical to the HD load point.

3) Reliability of the LH11 load point

This load point has a total of 14,300 clients who demand an average power of 24.6 MW [6]. The events that would lead to the top event (No power on busbar c35) are not having power on busbar c14, a failure in one of the nonredundant components, c28, c33, c34 or c35, not having power on busbar c27 that results from a simultaneous failure on one of the components of lines B3, B4 and B5, or the failure of the busbar c27 itself. Also, having no power coming from lines B7 and B8 causes an outage on this load point. In lines B7 and B8, it is proposed an alteration to the configuration of the grid. If a fault happens in one of the 11 kV cables c30 and c31, circuit breaker 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 system. 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 circuit breaker on both ends of each 11 kV cable. 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 circuit breakers is beneficial economically in the long term.

The results for this computation are presented in Table VIII.

TABLE VIII
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}

These results are worse than the ones obtained in the HD load point. The unavailability is higher, with an expected downtime of 26 minutes per year, more than double of the expected in the HD load point. The reliability is almost 2.5% less, but still an acceptable value and much better than the original configuration, almost 10% more reliable. The MTTF reduced approximately 13 years and the MTTR is one more hour.

In Table IX are presented the top failure modes sorted by the FV importance measure.

TABLE IX
FAILURE MODE IMPORTANCE VALUES FOR 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	1.992×10^4
	No voltage regulation due to tap changer failure	0.1126	1.127	1.992×10^4
	Short circuit due to bushings failure	0.062	1.066	1.992×10^4
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

The importance values analysis shows the criticality of the 11/0.4 kV transformer, with the events involving the windings, tap changer and bushings being the highest contributors.

In Table X are presented the top minimal cut sets sorted by unavailability.

TABLE X
TOP 5 MINIMAL CUT SETS SORTED BY UNAVAILABILITY OF THE TOP EVENT "NO POWER ON BUSBAR C35"

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

The minimal cut set analysis proves that the failure modes referred in the analysis of Table IX are the most critical to this load point unavailability. To the failure frequency, the failure modes from busbars c27 and c35 are high contributors.

V. RELIABILITY ANALYSIS OF THE BIRKA NÄT SMART GRID CONCEPT

A. The cyber system and its components

Including a cyber network in the power system can improve it in many ways, but as to be taken into account that introducing new components is introducing new potential failures, since every equipment can fail, therefore it is important to study how these failures can impact the power system. These failures can be divided into two groups, direct and indirect failures [13]. Direct failures are the ones that stop the operation of the power system, while the indirect ones refer to the case where a cyber component fails and do not stop the operation of the power system, for example, communication delays can reduce efficiency but do not stop the grid. Other example of indirect failures are the ones related with the equipment responsible for the protection of the grid, this will be discussed ahead with more detail.

Following the most commonly used communication standard in digital substations, IEC 61850, that provides detailed specifications of the communications protocols and allows to improve interoperability, reducing costs and simplifying operations [14], the main components of this type of substations are:

- Merging unit (MU) – Converts into digital the analog signs acquired by the current transformer/potential transformer. [14];
- Intelligent electronic device (IED) - Responsible for protecting and controlling the grid and will eventually replace all the conventional electromagnetic relays [2]. The IEDs receive the data sent by the merging units and take actions on the grid, for example, trip a circuit breaker after a fault;
- Ethernet switch or Router – Every substation has one connected to the one in the control center. This device allows communication in real time between the different devices;
- Servers – Store all the information of the grid. The failure of a server results in permanent data loss, to prevent this from happening, redundant servers must be used;
- Human machine interface (HMI) – Installed in the control center, is where the operator can monitor and control the grid in real time and take actions to improve reliability and efficiency;
- Smart meters – Device that allows real-time communication between client and producer.

In Figure 6 is presented a simple representation of a digital substation.

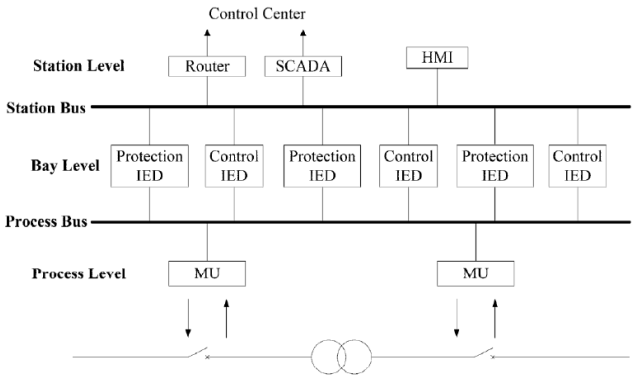

Fig. 6. Architecture of the cyber network, adapted from [15]

B. Impact of indirect failures

As said before, indirect failures are the ones that occur in the cyber system but do not directly affect the operation of the power grid. This concept can be applied to the protection system of the power grid, namely the circuit breakers. If a fault happens in the power system, the merging unit should detect it and communicate with the IED through the ethernet switch, to send a tripping signal to the respective circuit breaker. In case one of these cyber components fails, the circuit breaker would not receive the signal to trip and the fault would not be isolated, possibly causing damage to other components and causing an unnecessary outage on another

part of the grid. Following this analysis, the fault tree presented in Figure 7 was added to the circuit breakers. The merging units and protection IEDs have a failure rate of 0.00667 failures per year, and the ethernet switch 0.02 failures per year, all three with a repair time of 8 hours [15].

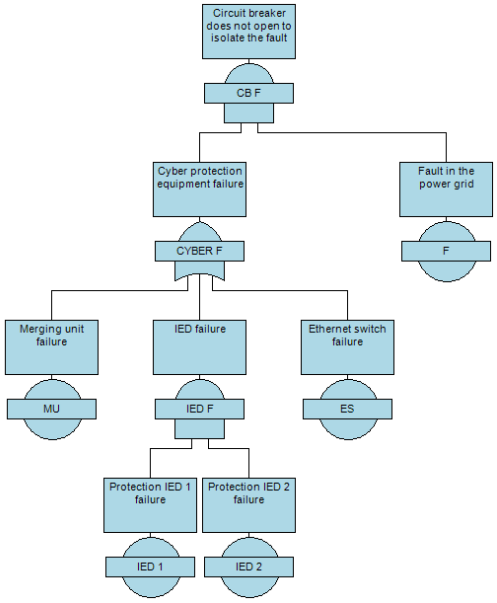

Fig. 7. Fault tree for cyber indirect failures on the circuit breaker

C. Impact of direct failures

Direct failures are the ones that immediately impact the operation of the power grid. In Figure 8 can be seen that these failures can be caused by a cyberattack or 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. Like the analysis of the indirect failures, it is considered that these failures affect the circuit breakers, the component where the hacker can easily cause a power disruption by tripping one, or multiple. The purpose of this computations is to provide an idea of the impact of this type of failures on the overall system. To accomplish this, the fault tree presented in Figure 8 was used, connected to each circuit breaker, since it is considered that the probability of affecting each circuit breaker is the same.

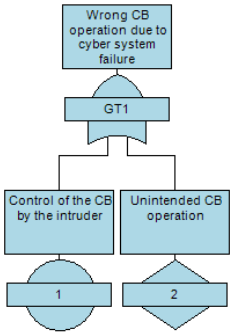

Fig. 8. Fault tree for cyber indirect failures on the circuit breaker

Giving a frequency to these events is not an easy task due to their unpredictability and the smart grid being a relatively new concept, hence there is not enough information available about this type of events. In [16], 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.

Using this data and the data in [17] that classify 64.88% of the cyber incidents as a hacker attack and 18.18% as an unintended service disruption, it is possible to establish a proportion between these two type of events and estimate a frequency of these failure modes.

D. Results

1) Reliability of the Birka Nät

To perform this computation, an identical fault tree to the one presented in Figure 9 (see appendix) was used, adding the fault trees of the cyber failures from Figures 7 and 8. It is assumed that the intruder can operate one of the circuit breakers c2, c4, c7, c8, c10 or c13. The results for this computation are presented in Table XI.

TABLE XI
COMPARISON BETWEEN THE RESULTS OF THE CONVENTIONAL GRID WITH 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}

From these results, it is possible to say that the cyber failures have little impact on the reliability of the system. However, they should not be neglected, since there is some impact on each line, which may represent loss of power, since it is considered that both lines are needed to deliver the required power by the clients, and therefore loss of money. The downtime of each line raised from 36 to 37 hours, one extra hour in a distribution system that feeds almost 38,000 people represents a considerable amount of money lost. Using the FV values 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 grid failures. This event is followed by the unintended operation of the CB, with 0.5%. The indirect failures have a neglectable probability, lower than 0.0004%.

2) Reliability of the HD and LH11 load points

Like was done in section IV, the reliability of each load point was studied individually, and the results presented in Table XII and Table XIII for the HD and LH11 load point, respectively.

TABLE XII
COMPARISON BETWEEN THE RESULTS OF THE COMPUTATION OF THE HD LOAD POINT OF THE CONVENTIONAL GRID WITH THE SMART GRID

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

TABLE XIII
COMPARISON BETWEEN THE RESULTS OF THE COMPUTATION OF THE LH11 LOAD POINT OF THE CONVENTIONAL GRID WITH THE SMART GRID

	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}

It is considered that the cyber failures can affect circuit breakers c37, c39, c40, c42, c43 and c45 on the HD load point, c15, c18, c19, c22, c23 and c26 on the LH11.

Like in the previous computation, the results have almost no changes compared to the conventional grid, this was expected since the goal of the smart grid is to improve reliability.

In the HD load point, the downtime of each line raised from 68 to 87 minutes and the failure of the three lines at the same time is still a very unlikely event, with unavailability of 4.506×10^{-12}. Like it was concluded before, the power grid failures are still the most critical to every load point. In this particular configuration of the grid, this analysis would be different if the hacker had access to the nonredundant circuit breakers, c47 and c28, the unavailability of the HD load point would be 4.089×10^{-5}, the reliability 96.11%, the MTTF 25.17 years and the MTTR 9.022 hours, and the direct failures would be the most critical to this load point.

In sum, although these cyber components add their own failures to the system, their impact is not alarming, but also should not be neglected, especially the cyberattacks, due to their potential catastrophic damage on the grid, it is estimated that a cyberattack on the US smart power grid could cost up to $1 trillion [16].

VI. CONCLUSIONS AND FUTURE WORK

A. Conclusions

The main goal of this work was to evaluate the reliability of a smart grid. In a first stage, only the power system components were considered. The failures of each component were studied and used to build the fault tree for each component and, using this information, to build a fault tree of the distribution system. In a second stage, the components from the cyber system were included in the analysis to evaluate their impact on the overall reliability.

Using Isograph's software was concluded that the events that most contribute to the unavailability of the system are short circuit due to insulation failure on the 110 kV cables and the events that involve the windings and tap changer of both transformers present in each line. To the failure frequency, the failure modes of busbars c1 and c14 proved to be high contributors.

In the detailed analysis of each load point was concluded that busbars c48 and c58 are top contributors to the failure frequency of HD and SJ load points, respectively. Furthermore, in these load points, a short circuit and the unexpected opening of circuit breakers c47 and c57 are also important.

In the LH11 load point the events that involve the windings, tap changer and bushings of the 11/0.4 kV transformer are the most critical to this load point.

In the analysis involving the cyber components was concluded that these failures have a low impact on the overall system reliability. It was also possible to conclude that the cyberattacks are the most critical event in the cyber system and that, although rare, these events should not be neglected due to their potential catastrophic consequences.

B. Future work

The smart grid is still a work in progress and should continue to be studied. One of the obstacles in this work was the lack of information regarding failure rates and repair times of the basic events, since this information is usually given per component, therefore the next step could be performing a reliability analysis using more detailed reliability data.

Furthermore, a Monte Carlo simulation could be performed to simulate a typical lifetime scenario.

Another topic that could be introduced in a future analysis is the economic factor, this combined with a reliability analysis provides an estimate of the money lost in the outages and the possibility of analyzing, for example, if making the system more reliable by introducing another parallel line is viable financially.

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] 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.

[4] 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].

[5] 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.

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

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

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

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

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

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

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

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

APPENDIX

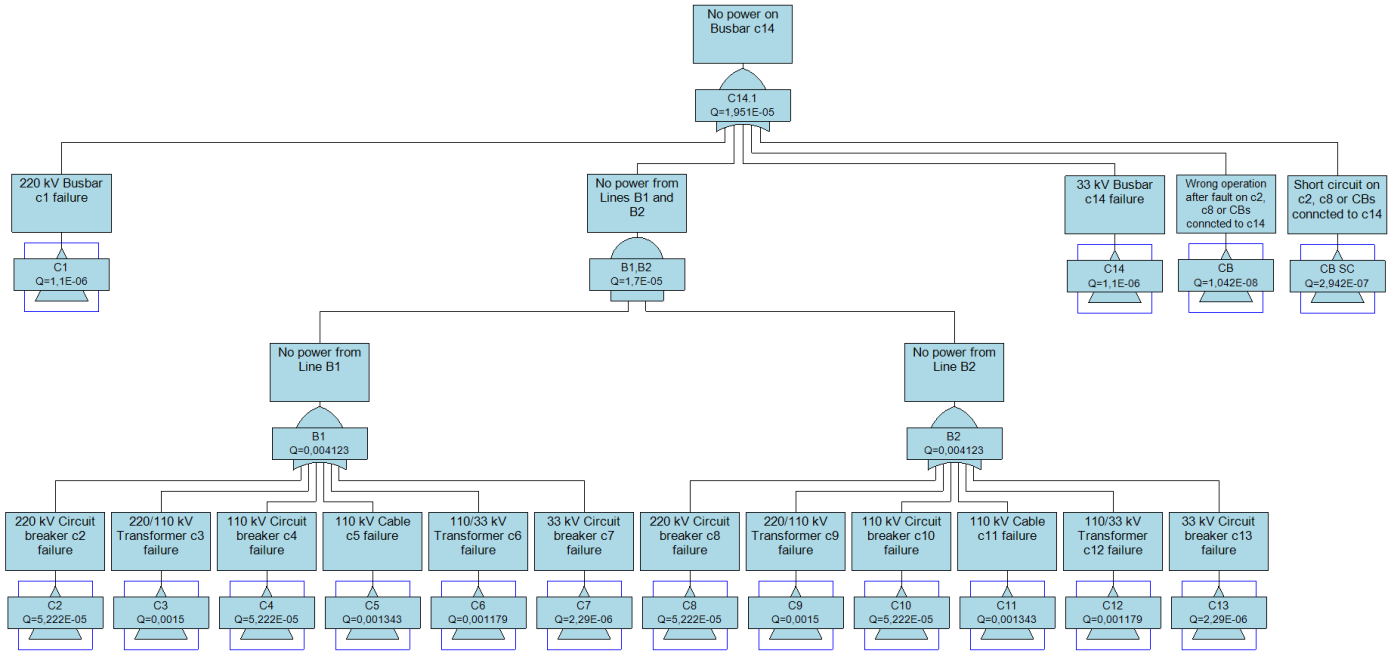

Fig. 9. Fault tree of the top event “No power on busbar c14”