

Article

A Methodology for Dependability Evaluation of Smart Grids

Gisliany Alves ^{1,*} , Danielle Marques ², Ivanovitch Silva ² , Luiz Affonso Guedes ¹ and Maria da Guia da Silva ³

¹ Department of Computer Engineering and Automation, Federal University of Rio Grande do Norte, Campus Universitário, Lagoa Nova, Natal 59078-900, RN, Brazil; affonso@dca.ufrn.br

² Digital Metropolis Institute, Federal University of Rio Grande do Norte, Campus Universitário, Lagoa Nova, Natal 59078-900, RN, Brazil; marques.danielleb@gmail.com (D.M.); ivan@imd.ufrn.br (I.S.)

³ Department of Electrical Engineering, Federal University of Maranhão, Av. dos Portugueses 1966, Vila Bacanga, São Luís 65080-805, MA, Brazil; guia@dee.ufma.br

* Correspondence: gisliany.alves@gmail.com

Received: 13 March 2019; Accepted: 13 April 2019; Published: 13 May 2019



Abstract: Smart grids are a new trend in electric power distribution, which has been guiding the digitization of electric ecosystems. These smart networks are continually being introduced in order to improve the dependability (reliability, availability) and efficiency of power grid systems. However, smart grids are often complex, composed of heterogeneous components (intelligent automation systems, Information and Communication Technologies (ICT) control systems, power systems, smart metering systems, and others). Additionally, they are organized under a hierarchical topology infrastructure demanded by priority-based services, resulting in a costly modeling and evaluation of their dependability requirements. This work explores smart grid modeling as a graph in order to propose a methodology for dependability evaluation. The methodology is based on Fault Tree formalism, where the TOP event is generated automatically and encompasses the hierarchical infrastructure, redundant features, load priorities, and failure and repair distribution rates of all components of a smart grid. The methodology is suitable to be applied in early design stages, making possible to evaluate instantaneous and average measurements of reliability and availability, as well as to identify eventual critical regions and components of smart grid. The study of a specific use-case of low-voltage distribution network is used for validation purposes.

Keywords: smart grid; fault tree; reliability; availability; dependability

1. Introduction

Nowadays, power grid infrastructures are not designed to support the upcoming transition towards decentralized and distributed energy system. Traditional grids are essentially radial and designed for centralized power generation [1,2]. In the last decades, these electric networks became widely interconnected with large-scale generating stations built to provide massive amounts of energy. However, this model proved to be unreliable and inadequate [3,4], having operated the same way for decades with characteristics that contributed to the frequent occurrence of blackouts in the last 40 years [5].

Despite the introduction of Information and Communication Technologies (ICT) in the power generation industry, this innovation is concentrated in central nodes and partially incorporated to remote substations, whereas remote terminals are almost entirely archaic [6]. Additionally, factors such as population growth, climate change, equipment failures, restrictions in power generation capacity, demand for resilience and the reduction of fossil fuels are identified as reason for the creation of a new infrastructure for power distribution [7].

In this context, the concept of Smart Grid arises as an intelligent power grid. This infrastructure is an enhancement of existing power grids enabling benefits such as: efficient transmission of electricity, better restoration of services under power disturbances, integration of power generation systems and security issues [8,9]. The integration of renewable energy with the existing power grid is one of the most important benefits when considering the application of a smart grid. The current renewable energy generators work from small-scale residential applications to large-scale installations bringing several challenges for the whole electrical power system. The effects of renewable energy introduction with its inherent variability induce vulnerabilities to the system, requiring sophisticated security mechanisms. Thus, in order to make all these aspects beneficial to customers, it is necessary to ensure that a distribution system is capable of satisfying distributed scenarios (a large number of geographically spread generators with intermittent and stochastic generation), while meeting high reliability, resilience, efficiency and sustainability requirements [10,11].

Therefore, due to the stringent fault tolerance requirements imposed on power grids, quantitative evaluations are recommendable to be carried out even in the initial steps of power grid project. An early assessment of potential problems in a power grid, considering their probabilities, makes them easier to prevent and ensures continuity of power supply. The dependability analysis of smart grid infrastructure represents a valid approach to face this. Dependability can be understood as the ability of a system to avoid failure in the most critical services by combining and integrating attributes such as reliability, availability, maintainability, integrity and security properties [12]. Dependability analysis evaluates the ability of a target system to avoid service failures that can cause large losses, much higher than acceptable. Analyzing dependability of a system aims to determine its potential weaknesses and to improve its correct operation [13]. Currently, dependability analysis has been applied to many critical systems, such as national defense, aircraft, communications networks and many others [14–16].

Historically, dependability evaluation solutions in a smart grid context have been implemented focusing on Monte Carlo simulation [17,18]. Using this technique, there are contributions focused on distributed generation [19,20] and some simple models are proposed to energy storage [21]. On the other hand, alternative solutions based on probabilistic techniques emerged as a counterpoint to the Monte Carlo approach, aiming to reduce computational costs when compared to that simulation [22]. Considering smart grid scenarios, new analytic solutions for dependability evaluation should be developed emphasizing their feasibility for systematization, since smart grid analysis are in general difficult to execute due to the complexity of the grid infrastructure.

This work proposes, therefore, a methodology for dependability analysis of smart grids considering that components of distribution grid (transformer, distributed generators, feeders, ICT devices) are meant to fail and must be preventively repaired or replaced. The smart grid is represented as a graph where the hierarchical infrastructure is naturally modeled from an adjacency matrix. Regarding the analytic technique adopted in the methodology, Fault Tree (FT) formalism was chosen because of its flexibility and good suitability to modeling complex systems. The FT evaluation will be performed by SHARPE, a tool widely used in literature [23], and a software that provides a graphical interface and a textual procedure (programming language) to describe and evaluate modeling paradigms as FTs. A case study encompassing a model adaptation of an European low voltage distribution network is then used to validate the proposed methodology [24].

The main contribution of this work is a flexible methodology that can be entirely automatized to evaluate smart grids dependability. The proposed methodology can handle any infrastructure topology (islanded and grid-connected operation), different fault conditions and load prioritization, besides being able to support distributed generation and energy storage. The strategy adopted in the proposed methodology can deal with any component (power grid and ICT components) by modeling it as generic vertex of a graph. Furthermore, the proposed methodology supports any quantitative analysis admitted in the fault tree formalism and any evaluation metric available in SHARPE tool.

The remainder of this paper is organized as follows: Section 2 presents a recent literature review regarding the subject; Section 3 provides a brief description of dependability and state of the art.

The methodology is presented in Section 4, while results are discussed in Section 5. Finally, Section 6 concludes the paper and presents directions for future studies.

2. Related Works

Interesting works related to assessment of dependability in smart grids have been developed in recent years and they are mainly focused on security [25–27] and network integrity [28–31]. Since smart grids have the ability to establish bidirectional digital communication, and for that use information technologies, they are susceptible to cyber attacks. Because of this, many studies review cybersecurity issues, focusing on preventing attacks and network breaches that may be favored to potential vulnerabilities of control and communication systems [32–34]. However, few studies on assessing the dependability of smart grids considering their physical infrastructure and different supplies of power generation can be found in the literature. In [18], the authors developed a simulation model able to perform such assessment, nevertheless, conditions and evaluation scenarios are explored in a restrictive approach, not supporting common mode failures or network fault conditions. Furthermore, the authors used the fault tree formalism to evaluate dependability and proposed an interesting strategy to construct a simpler fault tree for a smart grid, but they did not present an automated way to accomplish it.

There are studies also performing reliability evaluations on modern distribution systems using renewable generation or hybrid energy storage [17,19–21]. These studies applied the Monte Carlo simulation method to compute quantitatively the system reliability indices including the influence of islanded operation mode. However, the Monte Carlo approach is a more time-consuming method, being difficult to scale the analysis to bigger scenarios. The same problem can be also found in [18] as discussed before.

An approach concerning the best strategy to face failure scenarios in transmission lines of a smart grid was conducted in [35]. The authors used a generic model based on Markov chains to evaluate cascade failures. When considering failures in transmission lines, this work provides an important contribution. However, the technique created by the authors is restricted to reliability and resilience analysis and there is no modeling for other metrics such as availability or importance measures.

Another strategy for examining the dependability of a smart grid is to model the grid as a graph. Vertices of the graph would act as physical infrastructure components of the smart grid while the edges would be the transmission lines. Dependability analysis in a graph has been addressed by transforming a graph into a fault tree [14]. Moreover, that strategy considers the use of a generic fault condition based on the two-terminal problem whereas smart grids context turned the analysis into a modified k -terminal problem. This problem is defined considering a grid with N devices and a set of K devices ($K \subset N$ and $|K| < |N|$), where K is a combination of a centralized device and $K-1$ field devices. Setting a centralized device $s \in K$, k -terminal problem is expressed as a probability of existing at least one way in s for each field device K included. *two-terminals* problem is the case where $K = 2$. Thus, a smart grid has multiple generating sources (k) and one or more loads (centralizers in the case of the problem graph). This way it has been labeled as a new assessment class, the modified k -terminal problem.

From the above discussion, it becomes clear that the works already developed in the literature have provided only a partial solution to the problem, since they are not focused on the physical infrastructure of the smart grid. In addition, these works are very restrictive regarding the definition of fault conditions, evaluation metrics, loads priorities and topologies. Revisiting all these aspects, this work proposes a methodology to analyse dependability of smart grids that can be entirely automatized and is based on a validated approach in literature [14] limited only to industrial wireless sensor network context. To refine this methodology [14], it was necessary to incorporate the specific nature of smart grids by addressing the modified k -terminal problem (many sources and many loads), dealing with load prioritization and being concerned about resilient topologies. Section 4 will explore

this methodology in more detail. Additionally, to highlight the contributions of this work, Table 1 compares the mentioned studies of literature review with the proposed methodology.

Table 1. Summary of literature reviews closely related with the proposed methodology.

Reference	Findings	Limitations	Comparing with Proposed Methodology
[14]	A methodology to analyze dependability of wireless sensor networks using a fault tree-based formalism and graph modeling.	The fault condition is based on two-terminal problem, because of its application scenario. Smart grids are modeled by K-terminal problem.	It maps the K-terminal problem to the fault tree formalism applied to smart grids scenario.
[17,19–21]	Perform reliability evaluations on modern distribution systems including islanded operation analysis	Use a Monte Carlo simulation method that is more time-consuming	Use analytical techniques and can be entirely automatized
[18]	A simulation model to assess dependability of smart grids physical infrastructure.	No support to common mode failures or network fault conditions. An automatized way to generate the TOP event was not presented.	It handles network fault conditions and can be entirely automatized to generate the fault tree TOP event for a smart grid.
[35]	A Markovian model that calculates reliability of smart grids.	It does not handle availability or component importance analysis	Any evaluation metric supported by the fault tree formalism can be calculated, including availability and importance measures.

3. Dependability and Fault Tree Analysis

In this section, we provide a brief introduction to dependability and fault tree analysis concepts. As was mentioned, these definitions are closely related to the proposed methodology.

3.1. Dependability

Dependability is a widely discussed concept in literature [12,36,37] with several definitions. The original proposition [36] defines dependability as the capacity to deliver service that can justifiably be reliable. According to [37], the term is used to describe that a system can be reliable under certain operating conditions for a specific period of time. In this paper, the assumed definition of dependability is given by the system's capacity of avoiding failures in critical services [12]. This interpretation can be applied to smart grids context, where failures in critical services can cause power supply outage and result in severe consequences.

According to [12], the dependability concept comprises the following combined attributes:

- Availability: ability to provide correct service when required. In other words, it is the probability of a system being operational when required.
- Reliability: continuity of correct service, which may be read as the probability of a defect does not occur in a given period of time.
- Safety: absence of catastrophic consequences to users and environment.
- Integrity: absence of improper system alterations or without authorization.
- Maintainability: ability to undergo modifications and repairs.

These attributes must be quantified, making it possible to assess how reliable is a particular system. The importance of each of them is subjective and depends on the context of the evaluated application [38].

3.2. Fundamental Measures

System dependability can be essentially described by two fundamental measures: reliability and availability [39]. These attributes are well described in the following subsections.

3.2.1. Reliability

The reliability $R(t)$ of a system is the probability of a failure not occurring in the interval $[0,t)$ [39]. Suppose without losing generality that a system has two states [12], as shown in Figure 1. The transition from operating state to faulty state is triggered by the *failure rate function* $\lambda(t)$.

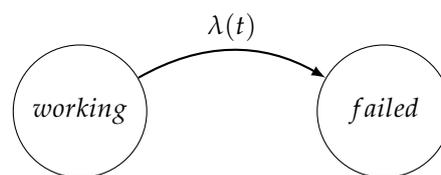


Figure 1. Two state model from the reliability point of view.

Now, consider T as the *time to failure* of a system component. If T is a random variable defined by a Cumulative Distribution Function (CDF) $F(t)$, it follows that reliability is given by:

$$R(t) = P(T > t) = 1 - F(t) \quad (1)$$

It can be proved that $R(t)$ and $\lambda(t)$, which describes the instantaneous failure rate of a system component, are associated as given by the Equation (2) [40]:

$$R(t) = \exp\left(-\int_0^t \lambda(u)du\right) \quad (2)$$

Another metric related to $R(t)$ is the *Mean Time To Failure* (MTTF). This measure is defined as the expected time $E(t)$ elapsed until the occurrence of the (first) system failure [39]. Formally, MTTF is given by [40]:

$$MTTF = E(t) = \int_0^{\infty} tf(t)dt \quad (3)$$

3.2.2. Availability

The availability $A(t)$ of a system is defined as the probability of the system being operational at a instant t [39]. As well as the reliability, availability also can be described as a model having two states, as shown in Figure 2. However, after the occurrence of a system fault, this new model may be repaired (maintenance). The transition from a faulty state to an operating state is induced by the *repair rate function* $\mu(t)$.

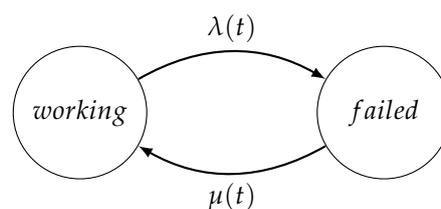


Figure 2. Two state model from the availability point of view.

Availability can be obtained in the same way as reliability, by replacing each event for the failure and repair rate functions ($\lambda(t)$ and $\mu(t)$, respectively). Supposing that $\lambda(t)$ and $\mu(t)$ have constant values, then it can be proved that $A(t)$ is expressed by [40]:

$$A(t) = \frac{\mu}{\mu + \lambda} + \frac{\lambda}{\mu + \lambda} e^{-(\lambda + \mu)t} \quad (4)$$

Assuming that n periods occurred (with *working* and *failed* states), the steady-state availability A_∞ can be outlined by Equation (5) [40]. In this case, $MTTF = 1/\lambda$ and $MTTR$ (*Mean Time to Repair*) = $1/\mu$.

$$A_\infty = \frac{MTTF}{MTTF + MTTR} \quad (5)$$

3.3. Importance Measure

In dependability evaluations, importance analysis is usually adopted to determine the sensibility of a system measure on the variation of the component features [13]. Generally, some components are more important for the system reliability than others and importance analysis aims to classify and quantify how the reliability of a component influences the whole system reliability [40].

Still according to [40], the component importance measure can be applied since the design phase to the operational period of a system's life cycle. During the system planning, the importance measures must help the designer to identify weak points (bottlenecks) and components that should be improved. During the operational phase, importance measures may be used to guide the inspection and the maintenance actions to the most important components.

Several importance metrics have been developed to measure the relative importance of a component, in comparison with others and with respect to the system [41]. This section focus on one of these importance metrics: the Birnbaum measure [42].

For better understanding, suppose a system with n independent components, wherein each component i has a reliability function $R_i(t)$. Birnbaum measure $I^B(i/t)$ describes the reliability importance of the i th component. This metric is defined as a partial derivative of the system reliability with respect to the component reliability i , as shown in Equation (6).

$$I^B(i/t) = \frac{\partial R(t)}{\partial R_i(t)}; i=1,2,\dots,n \quad (6)$$

If $I^B(i/t)$ is a high value, a small variation of component i reliability will result in a considerable deviation of system reliability. A component i is critical to the system if its fault implies a system fault. Thus, Birnbaum measure can also be interpreted as the probability of a component being critical to the system at time t [40]. Namely, Birnbaum importance evaluates the probability of a system being in a critical condition with respect to a certain event (component fault) [43].

3.4. Fault Tree Analysis

The fault tree model is a resource applied to dependability analysis. It is a tree structure model representing a sequence of components' individual failures that can cause a system breakdown. The first step to implement a fault tree is to determine a unique and well defined undesirable event, which is the TOP event and also is the single FT output [44]. In other words, the TOP event represents a system failure.

In general, FTs are graphical models representing a combination of events that are responsible for causing a system failure. The model uses a tree structure consisting of events and logic gates. The events represent the normal conditions as well as system failures (components failures, environmental conditions, human errors, and many others) and implement the boolean logic, i.e., they occur or do not occur. On other hand, the cause-effect relationships between events are represented by logic gates. A gate input can be a single event or a combination of events originated from the output of another

logic gate [44]. In addition, there are several types of gates available on the formalism, like *and*, *or* and *k-out-of-n* gates.

Regarding assessment issues, Fault Tree Analysis (FTA) is an effective technique to evaluate qualitatively and quantitatively systems' reliability and availability [45]. To perform qualitative analysis, FTA depends on the system stage. The development stage aims to identify potential problems that can lead to failures. In commissioning stage, the FTA technique can be used to identify the failure causes. Conversely, during the quantitative analysis process, it is possible to measure the reliability and availability of a system under assessment.

The main advantages of FTA are the execution of an intuitive procedure to describe the events that lead to system faults, and the minimization of the state space explosion problem, very common when modeling large systems [44].

The evaluation of a fault tree is performed by calculating the TOP event (system failure condition) probability based on basic events probabilities. This calculation is conducted differently for each type of logic gate. Assuming n independent inputs/events, the occurrence of event i is described by its cumulative distribution function $F_i(t)$. The logic gates outputs are indicated in Figure 3. When an *and* gate is used, the failure condition is only enabled when all inputs/events occur. On the other hand, the output of an *or* gate is enabled when at least one of its inputs/events is active. Finally, if a *k-out-of-n* gate is used, the output is enabled if at least k inputs/events occurred.

$$\begin{array}{ccc}
 F(t) = 1 - \prod_{i=1}^n (1 - F_i(t)) & F(t) = \prod_{i=1}^n F_i(t) & F(t) = \sum_{|I| \geq k} \left(\prod_{i \in I} F_i(t) \right) \left(\prod_{i \notin I} (1 - F_i(t)) \right) \\
 \begin{array}{c} \text{or} \\ \text{---} \\ F_i(t) \cdots F_n(t) \end{array} & \begin{array}{c} \text{and} \\ \text{---} \\ F_i(t) \cdots F_n(t) \end{array} & \begin{array}{c} \text{k-out} \\ \text{of-n} \\ \text{---} \\ F_i(t) \cdots F_n(t) \end{array}
 \end{array}$$

Figure 3. Cumulative distribution function $F(t)$ for the gate output (*and*, *or*, *k-out-of-n*).

The equations presented in Figure 3 refers to a fault tree without repeated events. When repeated events occur, the equations are invalidated, hence, a different technique such as *Sum of Disjoint Products* (SDP) can be applied [46].

The SDP method can be efficiently applied to fault trees with repeating events and it is easily automated. The basic idea is to find a boolean function $\phi(x)$ describing the system fault condition (TOP event) and transform it to a different function whose individual terms are mutually exclusive. According to [47], this structural boolean function $\phi(x)$ is given by:

$$\phi(x) = \begin{cases} 1 & \text{system failed} \\ 0 & \text{system is working} \end{cases} \quad (7)$$

where x is defined as the *state vector*, $x = (x_1, x_2, \dots, x_n)$. Each element x_i is a boolean variable, that represents the component state i .

4. Methodology for Dependability Evaluation

The proposed methodology aims to evaluate the dependability of a smart grid based on a fault tree model. In other words, by applying this methodology it will be possible to calculate a particular load's reliability and availability. Still at grid design stage, the methodology may be used as an information provider (it needs grid topology, devices priority, redundancy level, and others as data input) to create a more robust and reliable infrastructure. The same information can also be used during the operating stage and grid expansion phase.

Figure 4 shows a methodology overview. The process begins by providing information about the grid topology, components failure and repair rates, evaluation metrics, loads prioritization and grid failure condition. It is worth mentioning that the grid failure condition is a logic expression that corresponds to the fault states of smart grid loads for a given scenario. Additionally, loads prioritization is a crucial information mainly in case of power supplies failure, when some loads may have higher priority than others. Turning back to the methodology's big picture, the next step is to simplify the boolean expressions representing the different combinations of energy sources faults by applying the Quine–McCluskey classical algorithm [48]. The simplified expressions are the loads TOP events that comprise the energy sources situation. At this point, it is desirable that the methodology also handles more flexible failure conditions by incorporating the potential faults in the path between power supplies and loads. In this regard, an approach based on the modified *k-terminal* problem is performed to integrate the grid topology situation to the loads TOP events expressions. The resulting logical expressions are combined by the failure condition and transformed into a fault tree that can be processed by any FTA resolver (software). In this work, we adopted the SHARPE tool as solver, because it is widely used in academia and provides analytic or symbolic approaches to compute the required metrics [23]. We also decide to use the SHARPE's textual procedure instead of the graphical mode because the first one is easier to automatize and as intuitive as the graphical interface. After considering that, the generated fault tree can be inputted into SHARPE using the textual syntax without having any adaptation in the FT logical expression.

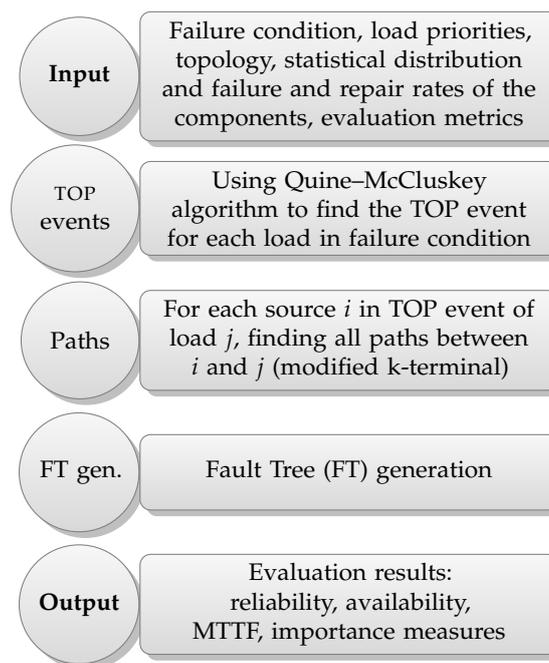


Figure 4. Overview of the methodology for dependability evaluation of smart grids.

4.1. Data Input

This section describes each methodology data input required for dependability evaluation.

4.1.1. Topology

The initial stage of the process consists in the definition of the optimal data structure which will model the smart grid topology. In this work, the grid is represented as a graph $G(V, E)$ with n vertices (V) and k edges (E). The vertices represent the physical components of the smart grid infrastructure while the edges represent communication links. The grid topology is stored in a adjacency matrix ($M_{n \times n}$) of the graph G . If a component N_i has a neighbor N_j , then the m_{ij} and m_{ji} entries of M will be

one, otherwise they will be substituted by zero. Within this approach, any smart grid topology can be represented as a graph (adjacency matrix).

For the sake of understanding, the Figure 5 describes the procedure to transform an one-line smart grid diagram into a graph representation. Note that the on-line diagram’s components are typical of smart grid scenarios [49]. Although no ICT component is shown in Figure 5, we highlight that any type of component can be modeled since an element of the graph has a generic representation.

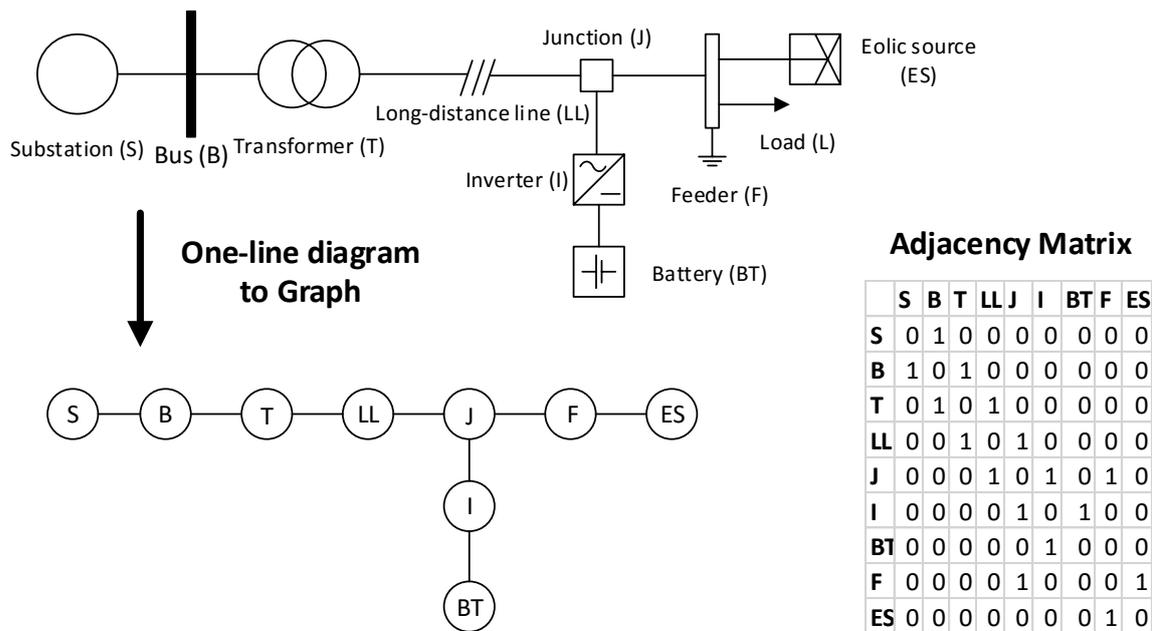


Figure 5. Topology configuration from one-line diagram to graph and its respective adjacency matrix.

4.1.2. Fault Settings

The proposed methodology is able to handle the permanent fault of physical infrastructure components of a smart grid and of its transmission lines. After a permanent fault, a grid device is considered permanently inoperative. To be operational again, a repair process must be performed. This work assumes that repairs are independent and they are limitless. Also, a load is inoperative if for any reason its energy demands can not be met.

At first any probability distribution can be used for modeling fault and repair processes. However, SHARPE tool was adopted to perform quantitative analysis and it requires that CDF of components should be expressed using exponential polynomials as described by Equation (8).

$$F(t) = \sum_{j=1}^n a_j t^{k_j} e^{b_j t} \tag{8}$$

a_j , k_j and b_j terms are parameters of the exponential polynomial while e is the Euler number. k_j is a non-negative integer and a_j and b_j are real or complex numbers. Many distributions can be expressed by Equation (8) (e.g., exponential, erlang, hypoexponential, hyper-exponential). Others non-exponential distributions (e.g., weibull, lognormal, deterministic) can be approximated using hybrid techniques involving a combination of moments and nonlinear least squares method [23].

4.1.3. Grid Failure Condition

Depending on the applications requirements, faults in specific devices can lead to failures in the entire grid. To perform more reliable analysis when applying the proposed methodology, it is fundamental to point out the loads combination which, in case of fault, leads to a grid failure.

This methodology supports failure conditions whose combination of devices can be set using logic gates *and*, *or* or *k-out-n*. In practice, any configuration could be used.

4.1.4. Priorities

Load priorities are also represented in the methodology. Priorities are essential parameters because in case of a fault, loads with higher priority are met first. The prioritization should be determined to provide a systematic sequence of service that satisfies the system conditions. Electrical system loads can have different priorities depending on its importance in the system. Priorities determination is guided by the requirements that the grid designer and the system operator decide to adopt.

4.1.5. Evaluation Metrics

The evaluation metrics that can be calculated using the proposed methodology are: reliability, availability, MTTF, and component importance measures. Some of these metrics need supplementary information to be evaluated. For instance, to estimate reliability, MTTF, and components importance measures, it is necessary to inform the elements failure rates and their probabilistic distributions such as those mentioned before.

4.2. TOP Event to the Loads

After defining the grid failure condition, it is necessary to find the TOP event for each load belonging to that condition. At this point, it is crucial that priority requirements are met. Thus, it is necessary to calculate all combinations of faults in the supplies that lead to a failure in a load.

Every load has a L demand while each supply has a S capacity. Without loss of generality, assuming two loads whose demands are L_1 and L_2 (the first load priority is higher than the second one), two supplies with S_1 and S_2 capacities, the following failure scenarios can be identified:

- Load 1
 - $L_1 > \sum \text{active sources}$
- Load 2
 - $L_2 > (\sum \text{active sources}) - L_1$

Based on this logic, a truth table can be created where input events are the supplies and output events are the loads. The classic Quine–McCluskey (Karnaugh mapping) algorithm can be used to simplify the boolean functions for each load [50]. This simplification is advised to make logical expressions simpler and consequently to reduce the evaluation time. As result, we find the TOP event for each load.

4.3. Modified k -Terminal Problem

The TOP event described in the previous section is a function of the smart grid supplies. However it is still necessary to consider the grid topology and therefore faults in connection elements and transmission lines. Assuming that the grid failure condition refers to k devices, then the dependability quantitative analysis falls into the classic k -terminal reliability problem.

The first step is to find all the paths between a energy source and a load i . This procedure can be performed using a Depth-First Search (DFS) to traverse the whole adjacency matrix representing the topology from a target load to a power supply, as described in Algorithm 1. Thus, all the paths

between a given supply and a load must be found. If at least one path is operational, the supply is considered operational. A path fails if at least one of its elements fail.

Algorithm 1: Finding all paths between a load and a energy source.

```

// load: load identifier ; supply: supply identifier
// topology: adjacency matrix of the grid topology

algorithm: DFS(load, supply, topology)
output : All paths between a load and a supply

// Any dimension of topology represents the number of grid devices
1 for  $i \leftarrow 0$ ;  $i < topology.shape[0]$ ;  $i++$  do
    // if currentPath has the device i, this for loop iteration is skipped
2 if currentPath.has(i) then
3     | continue;
    // if supply is achieved, thus a path between load and supply was found
4 else if  $i == supply$  then
5     | paths.add(currentPath);
    // traversing the neighboring components of load
6 else if topology[load][i] == 1 and not currentPath.has(i) then
7     | currentPath.add(i);
8     | DFS(i, supply, topology);
9     | currentPath.remove(i);
10 end

11 return paths

```

4.4. Construction of Fault Tree and Evaluation

The final step of the proposed methodology is the construction of the fault tree and its respective evaluation.

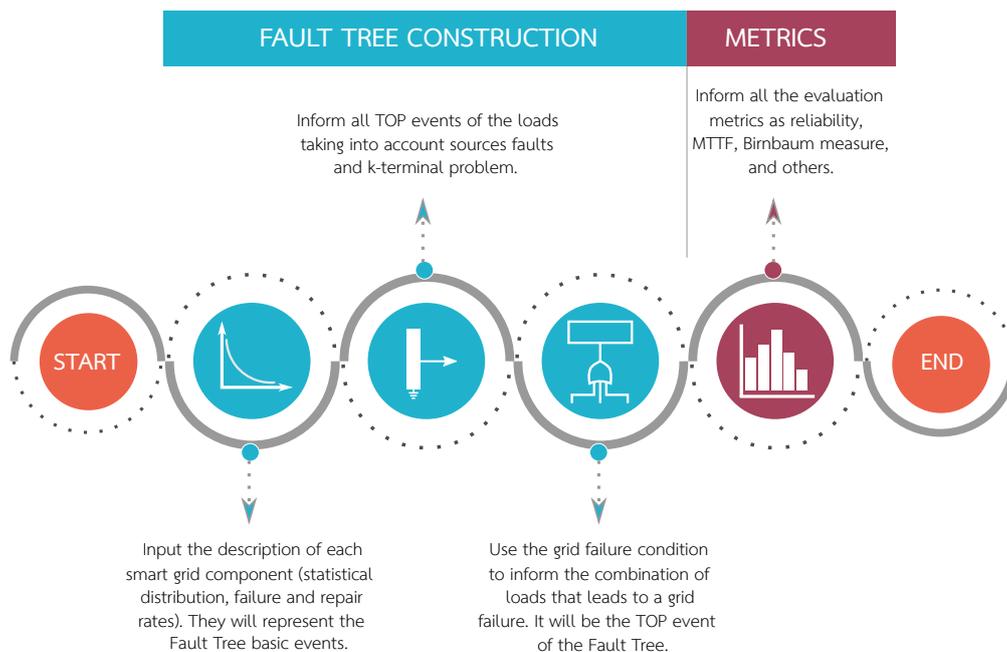


Figure 6. Fault Tree construction and evaluation metrics.

The construction strategy of the fault tree basically includes three steps as shown in Figure 6. Firstly, each component of the smart grid must be defined in terms of its statistical distribution and its failure and repair rates. These components then represent basic events of the fault tree. After this, the next step is to list all the TOP events of the loads obtained previously. They are simplified expressions of the loads that comprise the energy sources and the topology situations. Finally, the TOP event of the fault tree will be the grid failure condition representing the combination of loads that leads to a grid failure.

Once the fault tree is constructed, we can provide the chosen metrics to perform the analysis. The metrics used in the evaluation are the reliability and the availability of the smart grid as well as the criticality for a particular grid component.

5. Results

To validate the proposed methodology, we will describe a case study involving a microgrid. A microgrid is a plug-and-play small-scale system operating under low or medium voltage, having distributed generation and loads. Microgrids allow smart grid concepts to be applied in the current power supply system and can operate concomitant with main grid (connected to the grid) or independently (isolated mode of operation). The operation in isolated mode is performed when the main grid is disturbed by main power supply faults. In this case, the microgrid can disconnect itself from the main grid and operates in isolated mode, continuing to supply the loads through distributed generators, regardless of problem occurred at the power distribution utility.

5.1. Assumptions

A single-line diagram describing the case study is presented in Figure 7. The system is composed by five loads ($L1, L2, L3, L4, L5$) with priority defined as $L1 > L2 > L3 > L4 > L5$. It also has five power supplies ($S1, S2, S3, S4, S5$). For the sake of simplicity, the inverter component was not considered in the evaluation.

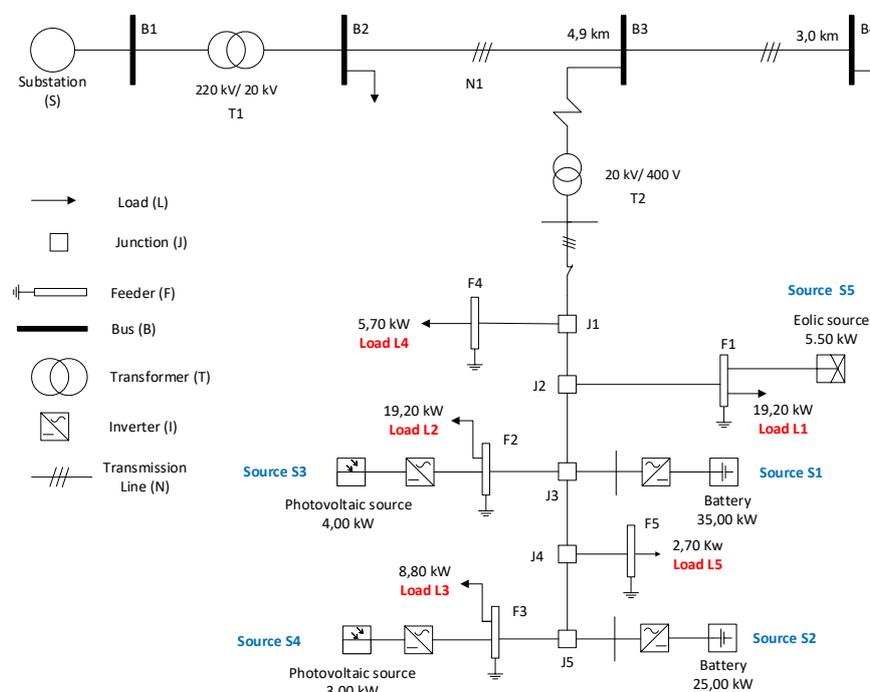


Figure 7. Evaluation scenario of a typical single-line diagram.

The objective of the study is to analyze the microgrid dependability (probability of load loss and expected load cuts) for the third bus (*B3*) using the proposed methodology. This evaluation is performed considering that the microgrid connected to *B3* disconnects from the medium voltage distribution grid when faults occur in the following components: 220 kV/20 kV transformer, medium voltage grid sections (4.9 km line), 20 kV/400 V transformer, distributed generation (solar, wind and batteries) and junctions *J1, J2, J3, J4, J5*. In the isolated mode of operation, a fault occurs in the microgrid when there is insufficient generating capacity to meet the original load demand.

Regarding the study scenario, some issues concerning the faults and metrics rates also need to be considered: (1) the evaluation metrics to be considered were the reliability and MTTF of microgrid, and the components importance measure; (2) the fault rates of system components are distributed exponentially (other distributions can be used, as long as exponential polynomials are used to describe them, as required in SHARPE tool) and the time unit is hours. Fault rates adopted in this study comply with typical values found in literature [44] and are described in Table 2.

Table 2. Typical failure rates of smart grid components.

Component	Failure Rate	MTTF
4.9 km Line	1.04×10^{-4}	1.09 years
220 kV Transformer	1.14×10^{-6}	100 years
20 kV Transformer	1.71×10^{-6}	67 years
Photovoltaic Source	7.61×10^{-6}	15 years
Battery	1.14×10^{-5}	10 years
Eolic Source	1.43×10^{-5}	8 years
Junctions	1.14×10^{-5}	10 years

These fault rates were informed to SHARPE by using its intuitive textual procedure as shown in Figure 8. In this code, each component's fault rate was associated to a variable. For instance, the `flr_rate_transformer1` has the value 1.14e-6 and refers to the failure rate of the 220 kV transformer.

```

variables definition (1-9) | bind
flr_rate_transformer1 0.00000114
flr_rate_transformer2 0.00000171
flr_rate_line 0.000104
flr_rate_photovoltaic 0.00000761
flr_rate_battery 0.0000114
flr_rate_eolic 0.0000143
flr_rate_junction 0.0000114
end

```

Figure 8. Variables representing the components' fault rates (SHARPE code).

5.2. TOP Event of Loads

A main step in the methodology is the TOP event building for the loads in the evaluated scenario. This step involves load prioritization and consequently total generation of distributed sources, which are designed to supply all demand. Total generation of distributed sources for the case study scenario is: $\sum_{i=1}^5 S_i = 35.00 + 25.00 + 4.00 + 3.00 + 5.50 = 72.5$ kW.

At this point, a truth table is created with the five supplies as inputs and the five loads as outputs. Therefore, each load will have one TOP event. Bear in mind that, in this work, the zero value represents that a element has not faults, i.e., it is operational, and the one value denotes the occurrence of a failure (a component is defective). Furthermore, it is well known that each row of the truth table has one possible combination of the input variables and the result of the evaluation for those values. Hence, with five sources, there is a total of 2^5 configurations for the sources states, which may or may

not lead to a load fault state. All of this configurations are needed to be considered in the TOP event building and they are described in Table 3.

Table 3. Failure combinations.

Total (kW)	Sources (kW)					Loads (kW)				
	S1 35	S2 25	S3 4.0	S4 3.0	S5 5.5	L1 19.2	L2 19.2	L3 8.8	L4 5.7	L5 2.7
72.5	0	0	0	0	0	0	0	0	0	0
67.0	0	0	0	0	1	0	0	0	0	0
69.5	0	0	0	1	0	0	0	0	0	0
64.0	0	0	0	1	1	0	0	0	0	0
68.5	0	0	1	0	0	0	0	0	0	0
63.0	0	0	1	0	1	0	0	0	0	0
65.5	0	0	1	1	0	0	0	0	0	0
60.0	0	0	1	1	1	0	0	0	0	0
47.5	0	1	0	0	0	0	0	0	1	1
42.0	0	1	0	0	1	0	0	1	1	1
44.5	0	1	0	1	0	0	0	1	1	1
39.0	0	1	0	1	1	0	0	1	1	1
43.5	0	1	1	0	0	0	0	1	1	1
38.0	0	1	1	0	1	0	1	1	1	1
40.5	0	1	1	1	0	0	0	1	1	1
35.0	0	1	1	1	1	0	1	1	1	1
37.5	1	0	0	0	0	0	1	1	1	1
32.0	1	0	0	0	1	0	1	1	1	1
34.5	1	0	0	1	0	0	1	1	1	1
29.0	1	0	0	1	1	0	1	1	1	1
33.5	1	0	1	0	0	0	1	1	1	1
28.0	1	0	1	0	1	0	1	1	1	1
30.5	1	0	1	1	0	0	1	1	1	1
25.0	1	0	1	1	1	0	1	1	1	1
12.5	1	1	0	0	0	1	1	1	1	1
7.0	1	1	0	0	1	1	1	1	1	1
9.5	1	1	0	1	0	1	1	1	1	1
4.0	1	1	0	1	1	1	1	1	1	1
8.5	1	1	1	0	0	1	1	1	1	1
3.0	1	1	1	0	1	1	1	1	1	1
5.5	1	1	1	1	0	1	1	1	1	1
0.0	1	1	1	1	1	1	1	1	1	1

The first row of Table 3 refers to a combination in which there is no source faults (all columns have zero values). In this scenario it is possible to get the total generation capacity of the distributed sources (72.5 kW). On the other hand, the row with a total power of 47.5 kW presents a configuration where the source S2 has failed (the logical value for S2 column is 1). Therefore, total generation is now $72.5 \text{ kW} - S2 (25.00 \text{ kW}) = 47.5 \text{ kW}$. It is necessary to evaluate the load faults according to their priorities. Load L1 is supplied by 47.5 kW. Then, the remaining generation relative to other loads will be 28.3 kW ($47.5 \text{ kW} - L1$, where $L1 = 19.2 \text{ kW}$). The remaining generation is enough to supply L2 and L3, but not to supply L4 and L5. Note that L4 and L5 in Table 3 are marked with 1. Finally, configuration of row where total power is 37.5 kW allows just L1 load to be supplied.

Finally, it is necessary to apply the Quine–McCluskey algorithm to perform the boolean simplification and get the correspondent expression for each load according to the distributed sources. For all 32 combinations of Table 3, it is possible to get the following TOP events:

$$L1 = S1.S2 \quad (9)$$

$$L2 = S1 + S2.S3.S5 \quad (10)$$

$$L3 = S1 + S2.(S3 + S4 + S5) \quad (11)$$

$$L4 = L5 = S1 + S2 \quad (12)$$

5.3. K-Terminal Problem

Equations (9)–(12) still do not represent the entire TOP event for the loads. They consider only faults in isolated mode of the microgrid. A downtime for a service occur if the main power supply and the isolated mode of a microgrid fail. Thus, it is necessary also to consider faults in transformers and junctions as well as topology aspects of a microgrid (k-terminal problem). The latter is only figured out from the graph model of the scenario under study (Figure 7) whose representation is described in Figure 9. Note that a path between a supply and a load fails if at least one element fails along the path.

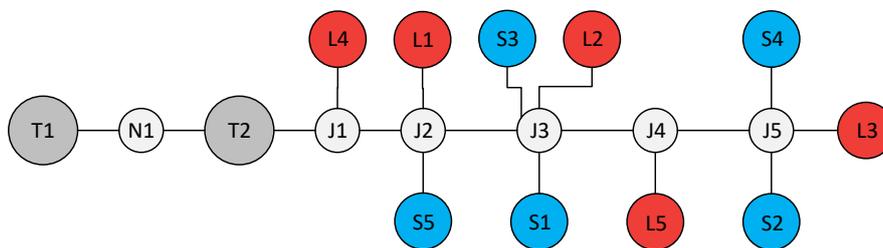


Figure 9. Graph model of single-line diagram under study.

To simplify things, it is assumed that only junctions from $J1$ to $J5$ can fail. Additionally, assuming that faults in 220 kV/20 kV and 20 kV/400 V transformers are $T1$ and $T2$ respectively, and in the 4.9 km long transmission line is $N1$, the TOP event to load $L1$ can be found as described in Figure 10. Note that, as previously mentioned in Section 4.3, it was necessary to find all paths between the load $L1$ and the sources $S1$ and $S2$, which are contained in $L1$'s TOP event (isolated mode failure without k-terminal) showed in Equation (9).

It is also considered that due to the peculiarity of the system topology, only one path between a supply and a load exists. The TOP event for all loads can be deducted in following equations:

$$L1 = (T1 + N1 + T2 + J1 + J2) \quad (13)$$

$$.(S1 + J3 + J2).(S2 + J5 + J4 + J3 + J2)$$

$$L2 = (T1 + N1 + T2 + J1 + J2 + J3) \quad (14)$$

$$.((S1 + J3) + (S2 + J3 + J4 + J5))$$

$$.(S3 + J3).(S5 + J2 + J3)$$

$$L3 = (T1 + N1 + T2 + J1 + J2 + J3 + J4 + J5) \quad (15)$$

$$.((S1 + J3 + J4 + J5) + (S2 + J5))$$

$$.((S3 + J3 + J4 + J5) + (S4 + J5))$$

$$+(S5 + J2 + J3 + J4 + J5))$$

$$L4 = T1 + N1 + T2 + J1).((S1 + J3 + J2 + J1) \quad (16)$$

$$+(S2 + J5 + J4 + J3 + J2 + J1))$$

$$L5 = (T1 + N1 + T2 + J1 + J2 + J3 + J4) \quad (17)$$

$$.((S1 + J3 + J4) + (S2 + J5 + J4))$$

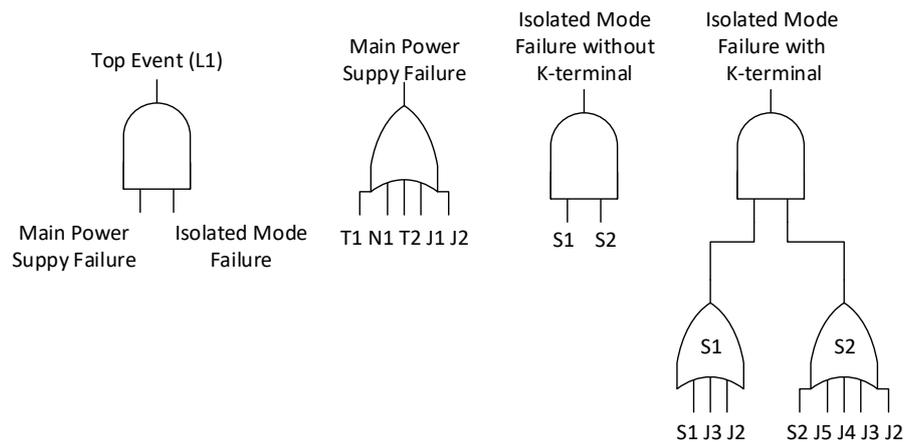


Figure 10. TOP event for the load L1.

```

fault tree model  ftree ft_smart_grid

events initialization (3-15)
    repeat t1      exp(fl_rate_transformer1)
    repeat t2      exp(fl_rate_transformer2)
    repeat n1      exp(fl_rate_line)
    repeat j1      exp(fl_rate_junction)
    repeat j2      exp(fl_rate_junction)
    repeat j3      exp(fl_rate_junction)
    repeat j4      exp(fl_rate_junction)
    repeat j5      exp(fl_rate_junction)
    repeat s1      exp(fl_rate_battery)
    repeat s2      exp(fl_rate_battery)
    repeat s3      exp(fl_rate_photovoltaic)
    repeat s4      exp(fl_rate_photovoltaic)
    repeat s5      exp(fl_rate_eolic)

L1 TOP event (17-21)
    * L1 subtree
    or      or_l1_01      t1 t2 l1 j1 j2
    or      or_l1_02      j2 j3 s1
    or      or_l1_03      j2 j3 j4 j5 s2
    and     l1            or_l1_01 or_l1_02 or_l1_03

L2 TOP event
    * L2 subtree
    * ...

L3 TOP event
    * L3 subtree
    * ...

L4 TOP event
    * L4 subtree
    * ...

L5 TOP event
    * L5 subtree
    * ...

end

```

Figure 11. Representation of each load TOP events in SHARPE tool.

These TOP events of the loads were then input into SHARPE tool as part of a fault tree. For the sake of better understanding, the code shown in Figure 11 implements the events representing components

faults and the L1 TOP event. The first line initializes a fault tree structure. In sequence, the events are created with their types, names and fault rate distributions respectively. For instance, line 3 represents the T1 event mentioned before and describes it as a repeated event t_1 (events are considered repeated when they occur more than once in a fault tree) exponentially distributed (exp function) with `f1r_rate_transformer1` as fault rate. Similarly, lines 4 to 15 correspond to the other events. Lines 17 to 21 presents the L1 TOP event indicated by Equation (13). In each line the gate type, name and inputs are informed respectively until composing the final TOP event expression. TOP events from other loads will be analogously implemented in the following lines before the end command.

5.4. Evaluation Metrics

This section describes two evaluation scenarios for the microgrid under study, in which concepts presented in this work are applied to. The objective is to evaluate different scenarios where all the features supported in the methodology can be validated, proving its wide application flexibility. As previously mentioned, the quantitative evaluation of fault tree generated by the methodology is solved by the SHARPE tool. Scripts used in the experiments are available online for reproducibility purposes (<https://github.com/gisliany/lii-system-ft>).

5.4.1. Scenario I

In this first scenario, two fault conditions in the microgrid are confronted. Reliability and MTTF of the smart grid are calculated based on expressions describing TOP events for loads L1 and L2. The following fault conditions were considered:

1. $L1 + L2$: the grid fail when at least one load is not fed;
2. $L1 \cdot L2$: the grid failure occurs only when those two loads are not fed simultaneously.

```

fault tree model  ftree ft_smart_grid
* ...

L5 TOP event    * L5 subtree
* ...

Failure condition * Scenario I
or               or_l1_l2           11 12
* and           and_l1_l2          11 12

end

MTTF           * Mean Time To Failure
expr mean(ft_smart_grid)

Reliability (from 0 to 100000) * Reliability
loop t,0,100000,10000
expr 1-tvalue(t;ft_smart_grid)
end

end

```

Figure 12. Failure conditions and evaluation metrics for scenario I (SHARPE code).

At this point, the fault conditions and the requested metrics (reliability and MTTF) are provided to SHARPE. The script that specifies all these parameters is shown in Figure 12. Only one fault condition is evaluated at a time and it must be still specified inside the fault tree structure. In Figure 12, the fault condition $L1 + L2$ is enabled and the condition $L1.L2$ is commented in a line below to be computed in

the next execution. The evaluation metrics are described right after the fault tree. The mean built-in function estimates the MTTF and the $1-t$ value function is repeated inside a loop from 0 to 100,000 (hours) to evaluate the reliability in this period of time.

Reliability results for the two situations can be seen in Figure 13. Through the analysis of the generated curves, notice that $L1 + L2$ condition is more pessimistic than the $L1 \cdot L2$ condition, since the first mentioned condition is more likely to occur. For instance, when $t = 20,000$ h, reliability for $L1 + L2$ is 0.509, whereas for $L1 \cdot L2$ condition, reliability reaches a higher value (0.711). The same happens to the MTTF. The former has a 3.16 years MTTF, while the latter provides a 4.85 years MTTF (a relative difference of 35%). This kind of evaluation can be useful to determine if a given failure condition reaches a specific dependability requirement in a microgrid project.

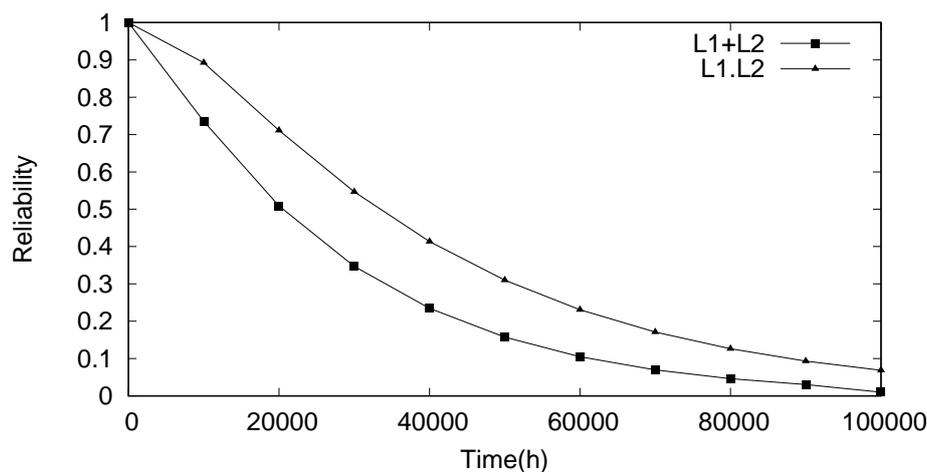


Figure 13. Reliability evaluation for scenario I.

5.4.2. Scenario II

The second evaluation scenario leads with five different situations of fault condition considering all loads of the microgrid. For this evaluation, the logic gate k -out-of- n is used to represent the possible states for grid faults where k is the amount of loads that are not electrically powered by sources, or in other words, in fault conditions.

The use of the logic gate k -out-of- n allows to test a wider range of fault settings. In the case, as there are five loads, the use of this gate makes five defects conditions possible:

- Case I (1oo5), at least one load is not fed;
- Case II (2oo5), at least two loads are not fed;
- Case III (3oo5), at least three loads are not fed;
- Case IV (4oo5), at least four loads are not fed;
- Case V (5oo5), all loads are not fed.

For the sake of understanding, the SHARPE code for the Case I is illustrated in Figure 14. This code is similar to that of Figure 12 and the only difference is the fault condition and appending the Birnbaum measure for S1 source as an example. In the case, the failure condition is specified by the gate type (kofn), name, k value, n value, and inputs.

Reliability results for each case is shown in Figure 15. As expected, analyzing the generated curves it is possible to conclude that the case wherein all devices failed (working as logic *and* gate) has a greater reliability since it is less likely to occur. It is clear that cases I and V are extreme, however, other cases can be used to delineate dependability limits for a specific microgrid project.

```

fault tree model  ftree ft_smart_grid
                  * ...

Failure condition * Scenario II
                  kofn k1_of_n5 1, 5, 11 12 13 14 15
                  end

MTTF and Reliability (from 0 to 100000) * MTTF and Reliability ...

Birnbbaum (from 0 to 100000) * Birnbbaum measure for S1
                              loop t,0,100000,10000
                              expr bimpt(t;ft_smart_grid,s1)
                              end

                              end
    
```

Figure 14. Failure condition and Birnbbaum measure example for scenario II—case I (SHARPE code).

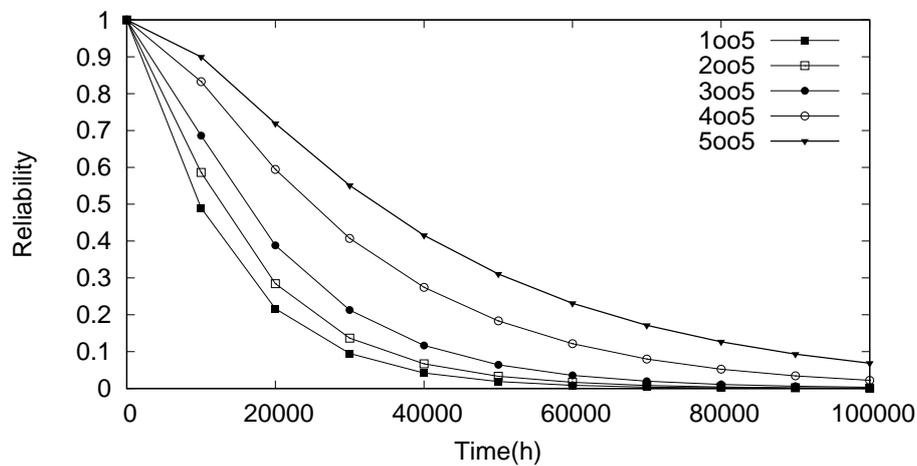


Figure 15. Reliability evaluation for scenario II.

Similar to that observed in evaluation of scenario I, MTTF values for each case can be extracted. This analysis is described in Table 4. The relationship between the MTTF and the number of devices in fault condition (*k* value in *k-out-of-n* gate) is directly proportional. The greater the number of devices failing at the same time, the greater is the time to fail. Table 4 also presents a comparison of each case with the highest probability of occurrence (case I). In the most optimistic scenario (case V), the increase rate means that the time to failure more than doubles as compared to the most pessimistic scenario (case I). This result confirms the previous reliability evaluation described in Figure 15.

Table 4. MTTF evaluation for *k-out-of-n* fault condition.

Case	MTTF (h)	Increase over 10o5
10o5	1.327×10^4	-
20o5	1.617×10^4	21.79%
30o5	2.036×10^4	53.37%
40o5	3.141×10^4	136.62%
50o5	4.277×10^4	222.17%

Another evaluation metric is the Birnbbaum measure. This metric describes the importance of a component for the microgrid reliability. A component is considered critical when its failure implies in a microgrid failure. The higher the value of this metric, the larger the variation in the reliability

of the microgrid. The results of this evaluation are described in Table 5. To make things simpler, the components considered were only the sources and the transformers.

Table 5. Evaluation results using Birnbaum metric.

Case	S1	S2	S3	S4	S5	T1	T2
1oo5	3.312×10^{-1}	3.312×10^{-1}	0.000×10^0	0.000×10^0	0.000×10^0	4.006×10^{-2}	4.029×10^{-2}
2oo5	4.131×10^{-1}	4.131×10^{-1}	0.000×10^0	0.000×10^0	0.000×10^0	8.267×10^{-2}	8.315×10^{-2}
3oo5	4.957×10^{-1}	1.685×10^{-1}	3.394×10^{-2}	3.394×10^{-2}	3.628×10^{-2}	7.632×10^{-2}	7.675×10^{-2}
4oo5	6.267×10^{-1}	5.272×10^{-2}	2.662×10^{-2}	0.000×10^0	1.045×10^{-2}	6.415×10^{-2}	6.452×10^{-2}
5oo5	2.251×10^{-1}	5.082×10^{-2}	1.722×10^{-2}	0.000×10^0	0.000×10^0	4.488×10^{-2}	4.513×10^{-2}

Looking at the case I, it is observed by the values shown in the Table 5 that the Birnbaum values for S3, S4 and S5 sources were zero. This means that they are not important to supply the demand of the example microgrid. It is also interesting to note that T1 and T2 had higher Birnbaum values when compared to that sources. On the other hand, the Birnbaum value for S1 and S2 sources are the highest of all. This result indicates that those components have great importance for the normal functioning of the microgrid in case I. The same procedure can be carried out to analyze the other cases.

6. Conclusions

Smart grids are currently a very relevant topic in the field of power systems, mainly because they represent a trend in generation and distribution systems. Economic, technological and environmental changes are paving the way new electrical systems are structured to increase the availability of energy supply. The study of a smart grid from the dependability analysis point of view is a critical task to the design and efficient execution of different scenarios.

This paper described a methodology for dependability evaluation of a smart grid. The proposal is flexible as it supports any topology, different fault conditions and evaluation metrics. During the design stage, the methodology can be used to identify critical areas needing improvements in the grid, as well as to evaluate the cost and safety issues.

The methodology is based on fault tree formalism and is tool-agnostic. Thus, any quantitative analysis supported by the formalism of fault trees will also be supported by the developed methodology. The following evaluation metrics were implemented: grid reliability and MTTF, and measure the importance of the components (Birnbaum). The results showed the feasibility of proposed methodology in evaluating the dependability of a smart grid.

As future work, it is intended to adopt more complex fault models (using Stochastic Petri Net and Dynamic fault tree formalism), considering the variability of the power generation due to distributed sources and failures in sequence. The systematization of the methodology will be also addressed in a future work by implementing a tool capable of generating the code to be submitted to SHARPE.

Author Contributions: Conceptualization, D.M., I.S. and M.d.G.d.S.; methodology, D.M. and I.S.; validation, D.M., I.S., M.d.G.d.S. and G.A.; formal analysis, D.M., I.S. and L.A.G.; writing—original draft preparation, D.M., I.S. and G.A.; writing—review and editing, G.A. and I.S.; supervision, I.S., L.A.G. and M.d.G.d.S.

Acknowledgments: The authors would like to thank Federal University of Rio Grande do Norte and the Graduate Program in Electrical and Computer Engineering (PPgEEC) for funding this work.

Conflicts of Interest: The authors declare no conflict of interest.

References

- Gungor, V.; Sahin, D.; Kocak, T.; Ergut, S.; Buccella, C.; Cecati, C.; Hancke, G. A Survey on Smart Grid Potential Applications and Communication Requirements. *IEEE Trans. Ind. Inform.* **2013**, *9*, 28–42. [[CrossRef](#)]
- González-Romera, E.; Ruiz-Cortés, M.; Milanés-Montero, M.I.; Barrero-González, F.; Romero-Cadaval, E.; Lopes, R.A.; Martins, J. Advantages of Minimizing Energy Exchange Instead of Energy Cost in Prosumer Microgrids. *Energies* **2019**, *12*, 719. [[CrossRef](#)]

3. Ardito, L.; Procaccianti, G.; Menga, G.; Morisio, M. Smart grid technologies in Europe: An overview. *Energies* **2013**, *6*, 251–281. [[CrossRef](#)]
4. Bukhsh, R.; Javaid, N.; Ali Khan, Z.; Ishmanov, F.; Afzal, M.K.; Wadud, Z. Towards Fast Response, Reduced Processing and Balanced Load in Fog-Based Data-Driven Smart Grid. *Energies* **2018**, *11*, 3345. [[CrossRef](#)]
5. Siano, P. Demand response and smart grid: A survey. *Renew. Sustain. Energy Rev.* **2014**, *30*, 461–478. [[CrossRef](#)]
6. Uslar, M.; Rohjans, S.; Neureiter, C.; Prössl Andrén, F.; Velasquez, J.; Steinbrink, C.; Efthymiou, V.; Migliavacca, G.; Horsmanheimo, S.; Brunner, H.; et al. Applying the Smart Grid Architecture Model for Designing and Validating System-of-Systems in the Power and Energy Domain: A European Perspective. *Energies* **2019**, *12*, 258. [[CrossRef](#)]
7. Vardakas, J.S.; Zorba, N.; Verikoukis, C.V. Performance evaluation of power demand scheduling scenarios in a smart grid environment. *Appl. Energy* **2015**, *142*, 164–178. [[CrossRef](#)]
8. Xenias, D.; Axon, C.J.; Whitmarsh, L.; Connor, P.M.; Balta-Ozkan, N.; Spence, A. UK smart grid development: An expert assessment of the benefits, pitfalls and functions. *Renew. Energy* **2015**, *81*, 89–102. [[CrossRef](#)]
9. Rezkallah, M.; Chandra, A.; Singh, B.; Singh, S. Microgrid: Configurations, Control and Applications. *IEEE Trans. Smart Grid* **2017**, *10*, 1920–1302. [[CrossRef](#)]
10. Wang, K.; Qiu, X.; Guo, S.; Qi, F. Fault Tolerance Oriented Sensors Relay Monitoring Mechanism for Overhead Transmission Line in Smart Grid. *IEEE Sens. J.* **2015**, *15*, 1982–1991. [[CrossRef](#)]
11. Wang, C.; Zhang, T.; Luo, F.; Li, F.; Liu, Y. Impacts of Cyber System on Microgrid Operational Reliability. *IEEE Trans. Smart Grid* **2019**, *10*, 105–115. [[CrossRef](#)]
12. Avizienis, A.; Laprie, J.C.; Randell, B.; Landwehr, C. Basic concepts and taxonomy of dependable and secure computing. *IEEE Trans. Dependable Secure Comput.* **2004**, *1*, 11–33. [[CrossRef](#)]
13. Trivedi, K.S.; Bobbio, A. *Reliability and Availability Engineering: Modeling, Analysis, and Applications*; Cambridge University Press: Cambridge, UK, 2017.
14. Silva, I.; Guedes, L.A.; Portugal, P.; Vasques, F. Reliability and Availability Evaluation of Wireless Sensor Networks for Industrial Applications. *Sensors* **2012**, *12*, 806–838. [[CrossRef](#)] [[PubMed](#)]
15. Wang, Y.; Sun, Q. Bayesian Network Technology to Analyze Fault Trees. In *Lecture Notes in Electrical Engineering, Proceedings of the First Symposium on Aviation Maintenance and Management-Volume II*; Wang, J., Ed.; Springer: Berlin/Heidelberg, Germany, 2014; Volume 297, pp. 87–94. [[CrossRef](#)]
16. Labib, A.; Harris, M. Learning how to learn from failures: The Fukushima nuclear disaster. *Eng. Fail. Anal.* **2015**, *47 Pt A*, 117–128. [[CrossRef](#)]
17. Araújo, J.R.; Silva, E.N.M.; Rodrigues, A.B.; da Silva, M.G. Assessment of the Impact of Microgrid Control Strategies in the Power Distribution Reliability Indices. *J. Control Autom. Electr. Syst.* **2017**, *28*, 271–283. [[CrossRef](#)]
18. Song, G.; Chen, H.; Guo, B. A Layered Fault Tree Model for Reliability Evaluation of Smart Grids. *Energies* **2014**, *7*, 4835–4857. [[CrossRef](#)]
19. Farzin, H.; Fotuhi-Firuzabad, M.; Moeini-Aghaie, M. Reliability Studies of Modern Distribution Systems Integrated With Renewable Generation and Parking Lots. *IEEE Trans. Sustain. Energy* **2017**, *8*, 431–440. [[CrossRef](#)]
20. Wang, Y.; Song, Z. Reliability Analysis of Distribution Network with Microgrid Based on Hybrid Energy Storage. In *Proceedings of the Chinese Intelligent Systems Conference, Mudanjiang, China, 14–15 October 2017*; Springer: Berlin, Germany, 2017, pp. 565–572.
21. LIU, W.; NIU, S.; XU, H. Optimal planning of battery energy storage considering reliability benefit and operation strategy in active distribution system. *J. Mod. Power Syst. Clean Energy* **2017**, *5*, 177–186. [[CrossRef](#)]
22. A survey of reliability assessment techniques for modern distribution networks. *Renew. Sustain. Energy Rev.* **2018**, *91*, 344–357. [[CrossRef](#)]
23. Sahner, R.A.; Trivedi, K.; Puliafito, A. *Performance and Reliability Analysis of Computer Systems: An Example-Based Approach Using the SHARPE Software Package*; Springer: Berlin, Germany, 2012.
24. Conseil International des Grands Eéseaux Électriques. Comité d'études C6. *Benchmark Systems for Network Integration of Renewable and Distributed Energy Resources: Task Force C6.04*; CIGRÉ: Paris, France, 2014.
25. Maier, M.; Levesque, M. Dependable Fiber-Wireless (FiWi) Access Networks and Their Role in a Sustainable Third Industrial Revolution Economy. *IEEE Trans. Reliab.* **2014**, *63*, 386–400. [[CrossRef](#)]

26. Kimani, K.; Oduol, V.; Langat, K. Cyber security challenges for IoT-based smart grid networks. *Int. J. Crit. Infrastruct. Prot.* **2019**, *25*, 36–49. [[CrossRef](#)]
27. Vaccaro, A.; Pisica, I.; Lai, L.; Zobia, A. A review of enabling methodologies for information processing in smart grids. *Int. J. Electr. Power Energy Syst.* **2019**, *107*, 516–522. [[CrossRef](#)]
28. Zeng, R.; Jiang, Y.; Lin, C.; Shen, X. Dependability Analysis of Control Center Networks in Smart Grid Using Stochastic Petri Nets. *IEEE Trans. Parallel Distrib. Syst.* **2012**, *23*, 1721–1730. [[CrossRef](#)]
29. Gamage, T.T.; Roth, T.P.; McMillin, B.M.; Crow, M.L. Mitigating Event Confidentiality Violations in Smart Grids: An Information Flow Security-Based Approach. *IEEE Trans. Smart Grid* **2013**, *4*, 1227–1234. [[CrossRef](#)]
30. Marashi, K.; Sarvestani, S. Towards Comprehensive Modeling of Reliability for Smart Grids: Requirements and Challenges. In Proceedings of the 2014 IEEE 15th International Symposium on High-Assurance Systems Engineering, Miami Beach, FL, USA, 9–11 January 2014; pp. 105–112. [[CrossRef](#)]
31. Desai, S.; Alhadad, R.; Chilamkurti, N.; Mahmood, A. A survey of privacy preserving schemes in IoT enabled Smart Grid Advanced Metering Infrastructure. *Clust. Comput.* **2019**, *22*, 43–69. [[CrossRef](#)]
32. Erol-Kantarci, M.; Mouftah, H. Energy-Efficient Information and Communication Infrastructures in the Smart Grid: A Survey on Interactions and Open Issues. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 179–197. [[CrossRef](#)]
33. Che, L.; Liu, X.; Shuai, Z.; Li, Z.; Wen, Y. Cyber cascades screening considering the impacts of false data injection attacks. *IEEE Trans. Power Syst.* **2018**, *33*, 6545–6556. [[CrossRef](#)]
34. Wang, H.; Ruan, J.; Wang, G.; Zhou, B.; Liu, Y.; Fu, X.; Peng, J. Deep Learning-Based Interval State Estimation of AC Smart Grids Against Sparse Cyber Attacks. *IEEE Trans. Ind. Inform.* **2018**, *14*, 4766–4778. [[CrossRef](#)]
35. Albasrawi, M.; Jarus, N.; Joshi, K.; Sarvestani, S. Analysis of Reliability and Resilience for Smart Grids. In Proceedings of the 2014 IEEE 38th Annual Computer Software and Applications Conference, Vasteras, Sweden, 21–25 July 2014; pp. 529–534. [[CrossRef](#)]
36. Avizienis, A.; Laprie, J.C. Dependable computing: From concepts to design diversity. *Proc. IEEE* **1986**, *74*, 629–638. [[CrossRef](#)]
37. Petre, L.; Sere, K.; Troubitsyna, E. *Dependability and Computer Engineering: Concepts for Software-intensive Systems*; Engineering Science Reference; IGI Global: Hershey, PA, USA, 2011.
38. Silva, I.; Leandro, R.; Macedo, D.; Guedes, L.A. A dependability evaluation tool for the Internet of Things. *Comput. Electr. Eng.* **2013**, *39*, 2005–2018. [[CrossRef](#)]
39. Muppala, J.; Fricks, R.; Trivedi, K. Techniques for System Dependability Evaluation. In *Computational Probability*; International Series in Operations Research & Management Science; Grassmann, W., Ed.; Springer: New York, NY, USA, 2000; Volume 24, pp. 445–479. [[CrossRef](#)]
40. Rausand, M.; Hsyland, A. *System Reliability Theory: Models, Statistical Methods, and Applications*, 2nd ed.; John Wiley & Sons, Inc.: Hoboken, NJ, USA, 2004; p. 644.
41. Rausand, M. *Reliability of Safety-Critical Systems: Theory and Applications*; John Wiley & Sons: Hoboken, NJ, USA, 2014.
42. Birnbaum, Z.W. *On the Importance of Different Components in a Multicomponent System*; Technical report; Washington Univ. Seattle Lab of Statistical Research: Seattle, WA, USA, 1968.
43. García Márquez, F.; Pliego Marugán, A.; Pinar Pérez, J.; Hillmanssen, S.; Papaelias, M. Optimal dynamic analysis of electrical/electronic components in wind turbines. *Energies* **2017**, *10*, 1111. [[CrossRef](#)]
44. Trivedi, K.S. *Probability and Statistics with Reliability, Queueing, and Computer Science Applications*, 2nd ed.; Wiley-Interscience: Hoboken, NJ, USA, 2001; p. 830.
45. Xing, L.; Amari, S.V. *Handbook of Performability Engineering*; Chapter Fault Tree Analysis; Springer: Berlin, Germany, 2008; pp. 595–617.
46. Choi, J.S.; Cho, N.Z. A practical method for accurate quantification of large fault trees. *Reliab. Eng. Syst. Saf.* **2007**, *92*, 971–982. [[CrossRef](#)]
47. Silva, I.M.D.D. Uma Metodologia Para Modelagem e Avaliação da Dependabilidade de Redes Industriais Sem Fio. Ph.D. Thesis, Universidade Federal do Rio Grande do Norte, Natal, Brazil, 2013.
48. Jain, T.; Kushwaha, D.; Misra, A. Optimization of the Quine-McCluskey Method for the Minimization of the Boolean Expressions. In Proceedings of the Fourth International Conference on Autonomic and Autonomous Systems (ICAS'08), Gosier, Guadeloupe, 16–21 March 2008; pp. 165–168. [[CrossRef](#)]

49. McDonald, J.D.; Wojszczyk, B.; Flynn, B.; Voloh, I. Distribution Systems, Substations, and Integration of Distributed Generation. In *Electrical Transmission Systems and Smart Grids: Selected Entries from the Encyclopedia of Sustainability Science and Technology*; Begovic, M.M., Ed.; Springer: New York, NY, USA, 2013; pp. 7–68. [[CrossRef](#)]
50. Tseng, C.C.; Chen, K.C. Organizing an optimal cluster-based ad hoc network architecture by the modified Quine-McCluskey algorithm. *IEEE Commun. Lett.* **2007**, *11*, 43–45. [[CrossRef](#)]



© 2019 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).