Event Tree Reliability Analysis of Electrical Power Generation Network using Formal Techniques

Mohamed Abdelghany, Waqar Ahmad, and Sofiène Tahar [1]

***Abstract*—In recent years, there has been a significant proliferation in the use of Renewable Energy Sources (RES), such as wind/solar systems, for power generation. However, the main obstacle that these resources face is their intermittent nature, which greatly affects their ability to deliver constant power to the power network. This raises several reliability-related concerns and existing sampling-based simulation tools, such as the Monte-Carlo approach, cannot guarantee absolute accuracy of the reliability analysis results due to their inherent incompleteness. In this paper, we propose to use formal techniques based on theorem proving to conduct the reliability analysis of electric grids as an accurate alternate approach. In particular, we use the HOL4 theorem prover, which is a computer-based mathematical reasoning tool. We demonstrate the effectiveness of our proposed approach by analyzing the reliability of the IEEE 39-bus power grid incorporating RES power plants and and also determine its reliability indices, such as System Average Interruption Frequency and Duration ($\mathcal{SAIFI}$ and $\mathcal{SAIDI}$). To assess the accuracy of our proposed approach, we compare our results with the commercial reliability analysis tool Isograph and the MATLAB toolbox based on Monte-Carlo approach.**

***Index Terms*—Power Grids, Reliability Analysis, Event Trees, Formal Methods, Theorem Proving, Monte-Carlo, SAIFI, SAIDI.**

I. Introduction

Electrical power grid is an interconnected network for delivering electricity from producers to customers. The power grid system consists of three major sectors [1]: (i) generating stations; (ii) transmission grid; and (iii) distribution system. According to the policy of Renewable Energy Network for the 21^{st} Century (REN21) [2], generating power from Renewable Energy Sources (RES), such as solar and wind, has become a mandatory requirement to be the best alternative for expanding fossil fuel generators [3]. The endeavor is to use 100% RES for power generation by 2050 due to global warming, pollution, and other environmental issues, as well as economic and energy security concerns [4]. A major challenge in power grids incorporating RES is to keep them stable and reliable from all disturbances and failures that could happen due to the intermittent nature of RES. Therefore, it is a dire need to develop reliability analysis techniques for electric grids consisting of RES power plants making them more resilient to costly blackouts and enable back-up decisions [5].

[1] M. Abdelghany, W. Ahmad, and S. Tahar are with the Department of Electrical and Computer Engineering, Concordia University, Montreal, Canada. {m_eldes,waqar,tahar}@ece.concordia.ca

Several reliability analysis techniques exist [5], such as Fault Trees (FT), Reliability Block Diagrams (RBD) and Event Trees (ET), which can quantify the probabilities of failure and success in electric grids. The fundamental idea in these techniques is to effectively capture the overall system reliability in terms of components' failure characteristics. FTs mainly provide a graphical model for analyzing the factors causing a system failure upon their occurrences. On the other hand, RBDs allow us to model the success relationships of complex systems. ETs provide a detailed system view with all possible operating states, i.e., success and failure.

Traditionally, ET analysis is carried out by using paper-and-pencil-based approaches or computer tools based on Monte-Carlo Simulation (MCS). Commercial ET simulation tools, such as ITEM [6], ReliaSoft [7], and Isograph [8], have been widely used in analyzing electrical grids (e.g., in [9]). A major limitation in both of the above approaches is the possibility of introducing inaccuracies in the ET analysis either due to human infallibility or the approximation errors due to pseudo-random numbers in the simulation tools. Moreover, simulation tools do not provide the mathematical expressions that can be used to predict the reliability of a given power grid based on any probabilistic distributions and failure rates. A more safe way is to substitute the error-prone informal reasoning of ET-based reliability analysis by formal mathematical proofs as per recommendations of safety standards, such as IEC 61850 [10] and ISO 26262 [11].

In this paper, we propose to use formal techniques [12] based on theorem proving for the formal reliability ET analysis-based of electrical power grids, which provides us the ability to obtain a *verified* failure/operating consequence expression. Theorem proving is a formal verification technique, which is used for conducting the proof of mathematical theorems based on a computerized proof tool [12]. In particular, we use HOL4 [13], which is an interactive theorem prover with the ability of verifying a wide range of mathematical expressions constructed in higher-order logic (HOL). We recently developed a formally verified algebra for ETs implemented in HOL4 [14], which allows us to formally model and analyze all possible system-level success and failure relationships. Using this formal ET algebra, in this paper we conduct the formal ET-based reliability analysis of a standard IEEE 39-bus electric grid

978-1-7281-6489-2/20/$31.00 ©2020 IEEE

system consisting of wind and solar power plants (50% RES). Subsequently, we formally determine its System Average Interruption Frequency Index ($\mathcal{SAIFI}$) and System Average Interruption Duration Index ($\mathcal{SAIDI}$), which describe the average frequency and duration of interruptions in a specific power grid, respectively [15]. Moreover, in order to ensure the accuracy of our proposed analysis, we compare our results with the commercial Isograph ET analysis tool [8] and MATLAB MCS-based algorithm for reliability analysis [16].

The rest of the paper is organized as follows: In Section II, we describe some preliminaries to facilitate the understanding of the rest of the paper. Section III summarizes the fundamentals of ETs. In Section IV, we describe the formal ET-based reliability analysis of electrical power grids. In Section V, we present the formal ET analysis-based of the IEEE 39-bus electric grid system. Section VI provides a comparison between our formal ET-based reliability evaluation with Isograph and MATLAB. Lastly, Section VII concludes the paper.

II. Preliminaries

In this section, we briefly summarize the fundamentals of HOL4 to facilitate the understanding of the rest of the paper.

A. HOL4 Theorem Proving

Theorem proving is a widely used formal technique based on a computerized proof system. HOL4 [13] is an interactive theorem prover that can verify mathematical expressions constructed in HOL. In general, given a safety-critical system, such as a power grid, to be formally analyzed, we first model its structure mathematically, then using the HOL4 theorem prover, several properties of the system can be verified based on this mathematical model. The main feature in HOL4 is that its core consists only of four axioms and eight inference rules. Any further lemmas or theorems should be formally verified based on these axioms and rules or based on previously proven theorems. This ensured the soundness of the system model analysis. Moreover, since the system properties are proven mathematically within HOL4, no approximation is involved in the analysis results.

B. Probability Theory in HOL4

Measure space is defined mathematically as (Ω, Σ, and μ), where Ω represents the sample space, Σ represents a σ-algebra of subsets of Ω, and μ represents a measure with the domain Σ. A probability space is a measure space (Ω, Σ, and Pr), where Ω is the complete sample space, Σ is the corresponding event space containing all events of interest, and Pr is the probability measure of the sample space as 1. The HOL4 theorem prover has functions `p_space`, `events`, and `prob`, which return the corresponding Ω, Σ, and Pr, respectively.

III. Event Tree Analysis

An ET diagram is a graphical model that enumerates all possible combinations of system components failure and success states. An ET starts by an Initiating Event (IE) called *node* and then all possible scenarios of an event are drawn as *branches*. For instance, consider a Microgrid [17] consisting of one wind-turbine generator (G) and two transmission lines (TL) to supply a load X, as shown in Fig. 1. Assuming that each component in the grid has two operational states, i.e., operating or failing. The ET *four* step-analysis are as follows [18]:

1) *Generation*: Construct a complete ET diagram that draws all possible scenarios, known as *paths*. Each *path* consists of a unique sequence of events. Fig. 2 depicts 8 paths (0-7) with all possible scenarios that can occur.
2) *Reduction*: Model the accurate functional behavior of a system by deleting some specific branches corresponding to the occurrence of certain events, which are known as *Complete Cylinders* (CCs) [18]. These cylinders are ET *paths* consisting of $\mathcal{N}$ events and are conditional on the occurrence of $\mathcal{K}$ *Conditional Events* (CEs) in their respective paths. They are typically referred to as CCs with respect to $\mathcal{K}$. For instance, if the generator G fails, then the whole grid fails regardless of the status of the rest of the components, i.e., TL_1 and TL_2, as shown in Fig. 2. The paths 4-7 are CCs with respect to G_F.
3) *Partitioning*: This step is essential as we are only inter-

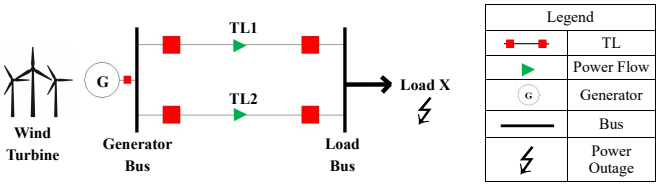


Fig. 1: Schematic of an Example Microgrid

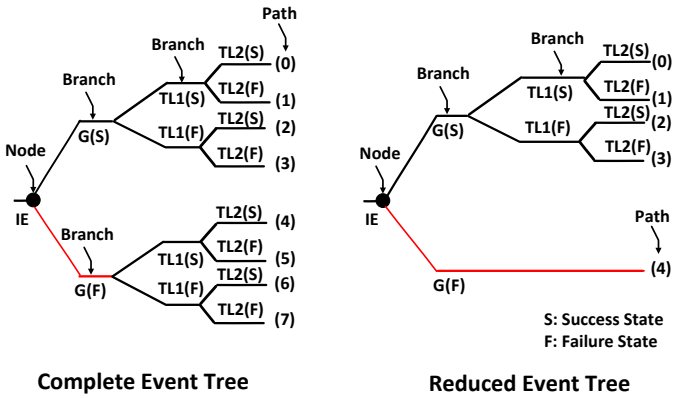


Fig. 2: A Sample Microgrid ET Diagrams

ested in the occurrence of certain events according to the system failure and success events. For instance, suppose we are only focusing on the failure of the Microgrid, then the ET paths 3 and 4 are taken from the reduced ET.

4) *Probabilistic analysis*: Lastly, evaluate the probabilities of ET paths based on the occurrence of a certain event. These probabilities represent the likelihood of each scenario that can possibly occur. Each path is disjoint implying that *only one* path can occur at a particular instance of time. If all events in an ET are mutually independent, then the probability of any ET path can be computed by simply multiplying the individual probabilities of all events in a path. For example, the probability of the grid failure in Fig. 2, i.e., paths 3 and 4, can be evaluated as:

$$\mathcal{P}(\mathrm{Grid}_F) = \mathcal{P}(\mathrm{G}_S) \times \mathcal{P}(\mathrm{TL}_{1F}) \times \mathcal{P}(\mathrm{TL}_{2F}) + \mathcal{P}(\mathrm{G}_F) \quad (1)$$

where $\mathcal{P}(\mathcal{X}_F)$ is the unreliability function or the probability of failure for a component $\mathcal{X}$ and $\mathcal{P}(\mathcal{X}_S)$ represents the correct functioning of the component, i.e. 1 - $\mathcal{P}(\mathcal{X}_F)$.

IV. ET Modeling and Analysis in HOL4

In this section, we briefly describe our proposed formal ET-based reliability analysis of electrical power grids in HOL4.

A. ET Formal Modeling

An ET structure is formally modeled by defining a new semantic function `ETREE` in HOL4 that can mathematically yield a corresponding ET diagram as follows [14]:

1) `ETREE (NODE L)`: it takes a list, identified by an ET type constructor `NODE`, then it returns the union of all elements of the given list.
2) `ETREE (BRANCH X L)`: it takes an event `X` and a list, identified by an ET type constructor `BRANCH`, then it performs the intersection of the event `X` with the union of all events of the list.

Based on this approach, we could express any generic, complete, scalable, and sequential ET model for a given electrical power grid consisting of $\mathcal{N}$ components as:

a) Step 1 (Generation): An event outcome space ($\mathcal{W}$) in the ET analysis [18] represents a list of all possible scenarios of modes of operation of a power grid critical-components. For instance, consider a grid having two events, say E_1 and E_2, with two event outcome spaces $\mathcal{W}_1$ and $\mathcal{W}_2$, respectively. The Cartesian product ($\bigotimes$) of these event outcome spaces returns a list of ($\mathcal{N}_1 \times \mathcal{N}_2$) pairs containing all possible outcome pairs for the occurrence of E_1 and E_2 together (i.e., $\mathcal{W}_1 \bigotimes \mathcal{W}_2$). Now, by using the concept of Cartesian product, a generic function $\bigotimes_{\mathrm{L}}^{\mathcal{N}}$ is defined that takes an arbitrary list of event outcome spaces (L = [[$\mathcal{W}_1$]; [$\mathcal{W}_2$];...; [$\mathcal{W}_{\mathcal{N}-1}$]]) and the last event outcome space list ($\mathrm{L}_{\mathcal{N}}$ = [$\mathcal{W}_{\mathcal{N}}$]), and then automatically generates a corresponding complete ET diagram [14]. For instance, we can generate mathematically the complete ET model, as shown in Fig. 2, in HOL4 as:

```
⊢ MICROGRID_COMPLETE_ET
  [G_S; G_F; TL_1S; TL_1F] [TL_2S; TL_2F] =
  ETREE (NODE
  ([[G_S; G_F]; [TL_1S; TL_1F]] ⊗_L^N [TL_2S; TL_2F])
```

b) Step 2 (Reduction): To perform the ET reduction process, it is needed to extract all possible paths from a given ET model and then apply the deletion operation. This is done by first defining a recursive function $\bigotimes_{\mathrm{paths}}^{\mathcal{N}}$ in HOL4 that returns a list containing all possible ET paths [14]. Now, to perform multiple reduction operations on an ET model, a function $\boxtimes^{\mathcal{N}}$ is defined in HOL4, which takes the output of $\bigotimes_{\mathrm{paths}}^{\mathcal{N}}$, a list of ET path numbers to be reduced and their conditional events. Upon this, the actual ET after reducing the paths 4-7, as shown in Fig. 2, can be obtained in HOL4 as:

```
⊢ MICROGRID_REDUCED_ET
  [G; TL_1] [TL_2] [[4-7]] [[G ↓]] =
  ETREE (NODE ((↑↓ [G; TL_1]) ⊗_paths^N (↑↓ [TL_2]))
                ⊠^N [[4-7]] [[G ↓]])
```

where the function $\uparrow\downarrow$ takes a list of $\mathcal{N}$ components and assigns failure and success events $\downarrow$ and $\uparrow$ to each grid component, respectively. The function failure event $\downarrow$ or Cumulative Distribution Function (CDF) takes a component X and returns a set of all the values less or equal to a value t, i.e., $X \leq t$, while the success function $\uparrow$ is the complement of the failure function $\downarrow$, i.e., $X > t$.

c) Step 3 (Partitioning): A partitioning function $\boxplus$ is defined to extract a collection of ET paths specified in an index list. For instance, the failure paths of the Microgrid, i.e., paths 3 and 4, as shown in Fig 2, can be extracted in HOL4 as:

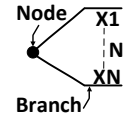
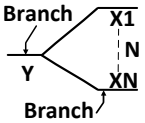
```
⊢ MICROGRID_FAILURE
  [G; TL_1] [TL_2] [[4-7]] [[G ↓]] [3;4] =
  ETREE (NODE
  ([3;4] ⊞ (MICROGRID_REDUCED_ET
            [G; TL_1] [TL_2] [[4-7]] [[G ↓]])))
```

B. ET Formal Probabilistic Analysis

For the formal probabilistic assessment of each path occurrence in the ET diagram, HOL4 probabilistic properties for the ET `NODE` and `BRANCH` constructors are provided in Table I [14]. These expressions are verified assuming p is a valid probability space, all associated events in the given list are drawn from the events space p, each pair of node events in the list is mutually exclusive, and lastly each pair of branch events in the list is mutually independent. The function $\sum_{\mathcal{P}}$ sums the probabilities of events for a given list.

In the rest of the paper, we will assume that the failure/success states of each solar/wind farm is exponentially

TABLE I: ET HOL4 Probabilistic Theorems

ET Constructor	Probabilistic Theorem
	`prob p (ETREE (NODE` $X_{\mathcal{N}}$`)) = ` $\sum_{\mathcal{P}}$ `p` $X_{\mathcal{N}}$
	`prob p (ETREE (BRANCH Y` $X_{\mathcal{N}}$`)) = (prob p Y) ×` $\sum_{\mathcal{P}}$ `p` $X_{\mathcal{N}}$

distributed [19]. To illustrate the applicability of our proposed approach, in the next section, we present the formal ET step-analysis of an electrical power grid and verify its reliability indices ($\mathcal{SAIFI}$ and $\mathcal{SAIDI}$), which are commonly used as reliability indicators by electric power utilities.

V. Electrical Power 39-Bus Grid System

Consider a standard *IEEE 39-bus* electrical power grid system consisting of 10 (5 renewable and 5 conventional) generators (G), 39 Buses (Bus), and 46 transmission lines (TL), and three different loads A, B and C, as shown in Fig. 3 [20]. For power grids safety assessment, reliability engineers have been dividing the electric grid into three main hierarchical levels [21]: (a) generation systems; (b) composite generation and transmission systems; and (c) distribution systems. We can use our proposed methodology for the formal reliability analysis of any hierarchical level in the electrical grid. In this case study, we focus on the generation part only, i.e., hierarchical level I. There are two types of RES power generation in the power grid (Fig. 3): (i) solar photo-voltaic (PV) power plants $G_{1,2,5}$; and (ii) wind-turbine power plants $G_{7,9}$. Using the Optimal Power Flow (OPF) optimization [22], we can determine the flow of electricity from generators to consumers in the power grid. For instance, if we consider load A, then according to the OPF it is supplied from G9 and G5 only, as shown in Fig. 3.

A. Formal ET Model

a) Step 1: Assume that each power generator has two operational states, i.e., operating or failing. Using our ET formalization described in Section VI, we can formally specify the complete ET model of the IEEE 39-bus electric grid. There is a total of 32 paths for the 5 wind/solar farms that mainly affect the reliability of loads A, B and C, modeled in HOL4 as:

Definition 1:

```
⊢ POWER_GRID_COMPLETE_ET [G9;G5;G7;G1] [G2] =
  ETREE (NODE
  (↑↓ [G9;G5;G7;G1]) ⊗ᴸ^𝒩 (↑↓ [G2]))
```

We can formally *verify* the complete ET model of the electrical power network, in HOL4 as:

Theorem 1:

```
⊢ POWER_GRID_COMPLETE_ET [G9;G5;G7;G1] [G2] =
  ETREE (NODE
    [BRANCH (G9 ↑)
       [BRANCH (G5 ↑) ...; BRANCH (G5 ↓) ...];
     BRANCH (G9 ↓)
       [BRANCH (G5 ↑) ...; BRANCH (G5 ↓) ...]])
```

b) Step 2: Assuming that if *one* wind/solar power plant fails, then its supplied load will be disconnected from the grid, i.e., *load-shedding*, to maintain the stability of frequency in the whole grid and hence prevent it from a blackout [23]. Therefore, based on that assumption, the complete ET obtained above can be reduced from 32 paths (0-31) to 15 paths (0-14), as shown in Fig. 4. For example, the paths from 16 to 31, where both G9 and G1 fail and consequently the load-shedding of all loads A, B and C, then the likelihood of occurrence of these paths is equal to the probabilities of G9 and G1 failures only regardless of the status of other generators, i.e., G5, G7 and G2. We can formally model and verify the actual ET model of the electrical grid, as shown in Fig. 4, in HOL4 as:

Definition 2:

```
⊢ POWER_GRID_REDUCED_ET [G9;G5;G7;G1] [G2]
  [[16-31];...] [[G9 ↓; G1 ↓];...] =
  ETREE (NODE
  ((↑↓ [G9;G5;G7;G1]) ⊗ᵖᵃᵗʰˢ^𝒩 (↑↓ [G2]))
  ⊠^𝒩 [[16-31];...] [[G9 ↓; G1 ↓];...])
```

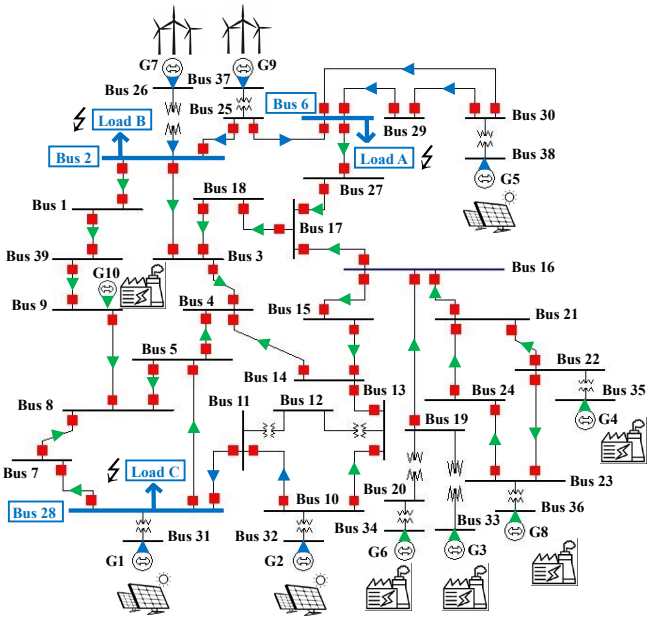


Fig. 3: IEEE 39-bus Electrical Power Grid [20]

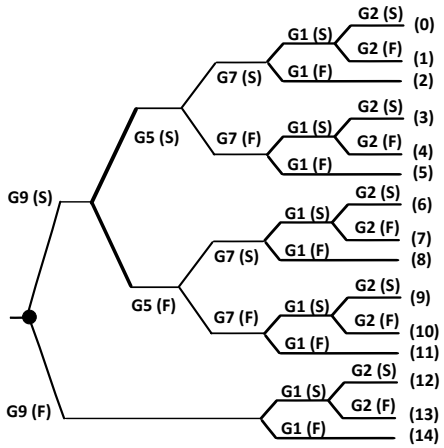


Fig. 4: Reduced ET of the Electrical Power Grid

Theorem 2:

```
⊢ POWER_GRID_REDUCED_ET [G9;G5;G7;G1] [G2]
  [[16-31];...] [[G9 ↓; G1 ↓];...] =
  ETREE (NODE
   [BRANCH (G9 ↑)
    [BRANCH (G5 ↑)
     [BRANCH (G7 ↑)
       [BRANCH (G1 ↑) [G2 ↑; G2 ↓]; G1 ↓];
      BRANCH (G7 ↓)
       [BRANCH (G1 ↑) [G2 ↑; G2 ↓]; G1 ↓]];
     BRANCH (G5 ↓)
      [BRANCH (G7 ↑)
       [BRANCH (G1 ↑) [G2 ↑; G2 ↓]; G1 ↓];
       BRANCH (G7 ↓)
       [BRANCH (G1 ↑) [G2 ↑; G2 ↓]; G1 ↓]]];
    BRANCH (G9 ↓)
     [BRANCH (G1 ↑) [G2 ↑; G2 ↓]; G1 ↓]])
```

c) Step 3: Typically, we are only interested in the occurrence of certain events in ET that affect certain paths. For instance, if we consider the failure of load A, then paths 6-14 are obtained (Fig. 4). Similarly, a different set of paths can be obtained by observing different failures in the power grid as:

a. $\mathcal{P}(\text{Load}_A \lightning) = \sum_{\mathcal{P}(paths 6,7,8,9,10,11,12,13,14)}$
b. $\mathcal{P}(\text{Load}_B \lightning) = \sum_{\mathcal{P}(paths 3,4,5,9,10,11,12,13,14)}$
c. $\mathcal{P}(\text{Load}_C \lightning) = \sum_{\mathcal{P}(paths 1,2,4,5,7,8,10,11,13,14)}$

B. Reliability Indices Assessment

We can also determine the System Average Interruption Frequency Index ($\mathcal{SAIFI}$), and the System Average Interruption Duration Index ($\mathcal{SAIDI}$), which are used by design engineers to indicate the average frequency and duration of customers experiencing a sustained outage. $\mathcal{SAIFI}$ is defined as the total number of customer interruptions (power outage $\lightning$) over the total number of customers served, while $\mathcal{SAIDI}$ is defined as the sum of all customer interruption durations over the total number of customers served [15]:

$$\mathcal{SAIFI} = \frac{\sum_{\mathcal{P}(\mathcal{X}_{\lightning}) \times \text{CN}_{\mathcal{X}}}}{\sum_{\text{CN}_{\mathcal{X}}}} \tag{2}$$

$$\mathcal{SAIDI} = \frac{\sum_{\mathcal{P}(\mathcal{X}_{\lightning}) \times \text{MTTR}_{\mathcal{X}} \times \text{CN}_{\mathcal{X}}}}{\sum_{\text{CN}_{\mathcal{X}}}} \tag{3}$$

where $\text{CN}_{\mathcal{X}}$ is the number of customers at $\mathcal{X}$ while $\text{MTTR}_{\mathcal{X}}$ is the mean-time-to-repair the failure that occurred at $\mathcal{X}$.

a) $\mathcal{SAIFI}$: We define a function $\sum_{\lightning}$ in HOL4 that models the numerator of Equation 2, which is the sum of multiplying the probabilities of failures at different locations in the power grid with the number of customers that are affected by these failures. Each probability of failure is obtained by extracting a certain collection of ET paths (ET partitioning) from the reduced ET model (ET reduction). Then, we formally define a generic function $\mathcal{SAIFI}$ that represents the division of $\sum_{\lightning}$ over the total number of customers at all those locations, in HOL4 as:

Definition 3:

$$\vdash \mathcal{SAIFI}\ \texttt{L}\ \texttt{L}_{\mathcal{N}}\ \texttt{N}_{\mathcal{N}}\ \texttt{CE}_{\mathcal{N}}\ \texttt{E}_{\mathcal{N}}\ \texttt{CN}_{\mathcal{N}}\ \texttt{p} = \frac{\sum_{\lightning}\ \texttt{L}\ \texttt{L}_{\mathcal{N}}\ \texttt{N}_{\mathcal{N}}\ \texttt{CE}_{\mathcal{N}}\ \texttt{E}_{\mathcal{N}}\ \texttt{CN}_{\mathcal{N}}\ \texttt{p}}{\sum \texttt{CN}_{\mathcal{N}}}$$

where

- $\texttt{L}$: List of wind/solar generators modes
- $\texttt{L}_{\mathcal{N}}$: Last generator modes
- $\texttt{N}_{\mathcal{N}}$: List of complete cylinders
- $\texttt{CE}_{\mathcal{N}}$: List of conditional events
- $\texttt{E}_{\mathcal{N}}$: List of events partitioning paths
- $\texttt{CN}_{\mathcal{N}}$: List of customer numbers

b) $\mathcal{SAIDI}$: Similarly, we formally define a function $\sum_{\lightning}^{T}$ in HOL4 to sum all customer interruption durations. Then, we formally define a generic function $\mathcal{SAIDI}$ by dividing the output of $\sum_{\lightning}^{T}$ over the total number of customers served as described in Equation 3, in HOL4 as:

Definition 4:

$$\vdash \mathcal{SAIDI}\ \texttt{L}\ \texttt{L}_{\mathcal{N}}\ \texttt{N}_{\mathcal{N}}\ \texttt{CE}_{\mathcal{N}}\ \texttt{E}_{\mathcal{N}}\ \texttt{MTTR}_{\mathcal{N}}\ \texttt{CN}_{\mathcal{N}}\ \texttt{p} = \frac{\sum_{\lightning}^{T}\ \texttt{L}\ \texttt{L}_{\mathcal{N}}\ \texttt{N}_{\mathcal{N}}\ \texttt{CE}_{\mathcal{N}}\ \texttt{E}_{\mathcal{N}}\ \texttt{MTTR}_{\mathcal{N}}\ \texttt{CN}_{\mathcal{N}}\ \texttt{p}}{\sum \texttt{CN}_{\mathcal{N}}}$$

where $\texttt{MTTR}_{\mathcal{N}}$ is the list of MTTRs.

The assessment of $\mathcal{SAIFI}$ and $\mathcal{SAIDI}$ for the Grid (G) shown in Fig. 3 can be written mathematically as:

$$\mathcal{SAIFI}_G = \frac{\mathcal{P}(\text{Load}_A \lightning) \times \text{CN}_{\text{Load}_A} + \dots}{\text{CN}_{\text{Load}_A} + \text{CN}_{\text{Load}_B} + \text{CN}_{\text{Load}_C}} \tag{4}$$

$$\mathcal{SAIDI}_G = \frac{\mathcal{P}(\text{Load}_A \lightning) \times \text{MTTR}_{\text{Load}_A} \times \text{CN}_{\text{Load}_A} + \dots}{\text{CN}_{\text{Load}_A} + \text{CN}_{\text{Load}_B} + \text{CN}_{\text{Load}_C}} \tag{5}$$

Using the ET probabilistic properties (Table I) with the assumption that the failure and success states of the generators are exponentially distributed, we can formally verify the above-expressions of $\mathcal{SAIFI}_G$ and $\mathcal{SAIDI}_G$ in HOL4 as:

Theorem 3:

$$\vdash \mathcal{SAIFI}\ (\uparrow\downarrow\ [\mathrm{G9};\ \mathrm{G5};\ \mathrm{G7};\ \mathrm{G1}])\ (\uparrow\downarrow\ [\mathrm{G2}])\ [[16\text{-}31];\ldots]\ [[\mathrm{G9}\downarrow;\ \mathrm{G1}\downarrow];\ldots]\ [[6\text{-}14];[3\text{-}5;\ 9\text{-}14];\ [1;2;4;5;7;8;10;11;13;14]]\ [\mathrm{CN\_LoadA};\ \mathrm{CN\_LoadB};\ \mathrm{CN\_LoadC}]\ p =$$

$$\frac{\begin{aligned}&(e^{(-\lambda_{G9}t)} \times (1 - e^{(-\lambda_{G5}t)}) \times e^{(-\lambda_{G7}t)} \times e^{(-\lambda_{G1}t)} \times \\ &e^{(-\lambda_{G2}t)} + \ldots) \times \mathrm{CN\_LoadA} + \\ &(e^{(-\lambda_{G9}t)} \times e^{(-\lambda_{G5}t)} \times (1 - e^{(-\lambda_{G7}t)}) \times e^{(-\lambda_{G1}t)} \times \\ &e^{(-\lambda_{G2}t)} + \ldots) \times \mathrm{CN\_LoadB} + \\ &(e^{(-\lambda_{G9}t)} \times e^{(-\lambda_{G5}t)} \times e^{(-\lambda_{G7}t)} \times e^{(-\lambda_{G1}t)} \times \\ &(1 - e^{(-\lambda_{G2}t)}) + \ldots) \times \mathrm{CN\_LoadC}\end{aligned}}{(\mathrm{CN\_LoadA} + \mathrm{CN\_LoadB} + \mathrm{CN\_LoadC})}$$

Theorem 4:

$$\vdash \mathcal{SAIDI}\ (\uparrow\downarrow\ [\mathrm{G9};\ \mathrm{G5};\ \mathrm{G7};\ \mathrm{G1}])\ (\uparrow\downarrow\ [\mathrm{G2}])\ [[16\text{-}31];\ldots]\ [[\mathrm{G9}\downarrow;\ \mathrm{G1}\downarrow];\ldots]\ [[6\text{-}14];[3\text{-}5;\ 9\text{-}14];\ [1;2;4;5;7;8;10;11;13;14]]\ [\mathrm{MTTR\_LoadA};\ \mathrm{MTTR\_LoadB};\ \mathrm{MTTR\_LoadC}]\ [\mathrm{CN\_LoadA};\ \mathrm{CN\_LoadB};\ \mathrm{CN\_LoadC}]\ p =$$

$$\frac{\begin{aligned}&(e^{(-\lambda_{G9}t)} \times (1 - e^{(-\lambda_{G5}t)}) \times e^{(-\lambda_{G7}t)} \times e^{(-\lambda_{G1}t)} \times \\ &e^{(-\lambda_{G2}t)} + \ldots) \times \mathrm{MTTR\_LoadA} \times \mathrm{CN\_LoadA} + \\ &(e^{(-\lambda_{G9}t)} \times e^{(-\lambda_{G5}t)} \times (1 - e^{(-\lambda_{G7}t)}) \times e^{(-\lambda_{G1}t)} \times \\ &e^{(-\lambda_{G2}t)} + \ldots) \times \mathrm{MTTR\_LoadB} \times \mathrm{CN\_LoadB} + \\ &(e^{(-\lambda_{G9}t)} \times e^{(-\lambda_{G5}t)} \times e^{(-\lambda_{G7}t)} \times e^{(-\lambda_{G1}t)} \times \\ &(1 - e^{(-\lambda_{G2}t)}) + \ldots) \times \mathrm{MTTR\_LoadC} \times \mathrm{CN\_LoadC}\end{aligned}}{(\mathrm{CN\_LoadA} + \mathrm{CN\_LoadB} + \mathrm{CN\_LoadC})}$$

To further facilitate the exploitation of our proposed approach for power grid reliability engineers, we defined an *Auto_$\mathcal{SAIFI}$_ML* and *Auto_$\mathcal{SAIDI}$_ML* Standard Meta Language (SML) functions that can numerically evaluate the above-*verified* expressions of $\mathcal{SAIFI}$ and $\mathcal{SAIDI}$. In the sequel, we compare our results with the commercial Isograph tool [8] and MCS-based algorithm using MATLAB [16] to ensure the accuracy of our computations.

VI. Experimental Results and Discussion

Considering the failure rates of the solar PV power plants ($G_{1,2,5}$) are 0.22 per year with MTTR of 80 hours [24]. Similarly, the failure rates of the wind-turbine power plants ($G_{7,9}$) are 0.35 per year with MTTR of 35 hours [25]. Also assuming the number of customers served $\mathrm{CN}_{\mathrm{Load}_A}$, $\mathrm{CN}_{\mathrm{Load}_B}$, and $\mathrm{CN}_{\mathrm{Load}_C}$ are 2500, 900, and 1800 customers, respectively. The reliability study is undertaken for 5 years, i.e., t = (8760 × 5) hours. We first analyze the power grid using the Isograph ET analysis tool and then using the MCS-based MATLAB toolbox. It is important to mention that Isograph requires from the users to manually draw the actual ET model and assign the probability to each event, as shown in Fig. 5. Fig. 6 and Fig. 7 show the MATLAB MCS results of $\mathcal{SAIFI}$ and $\mathcal{SAIDI}$, respectively. The comparison in the

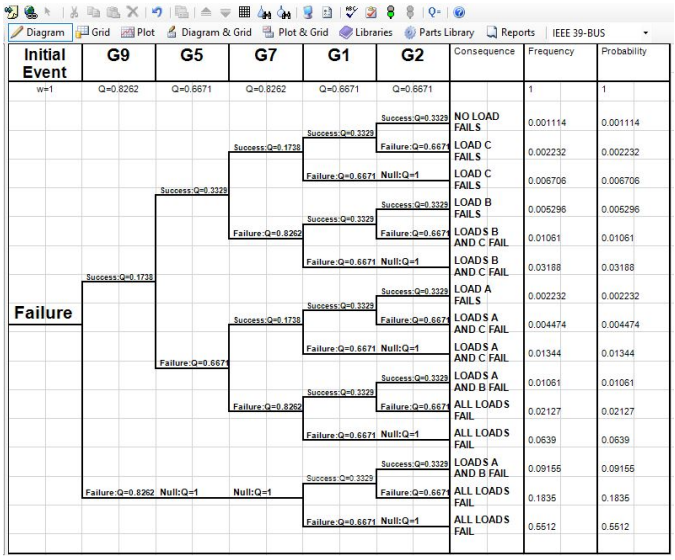


Fig. 5: Isograph: Electric Grid ET Model

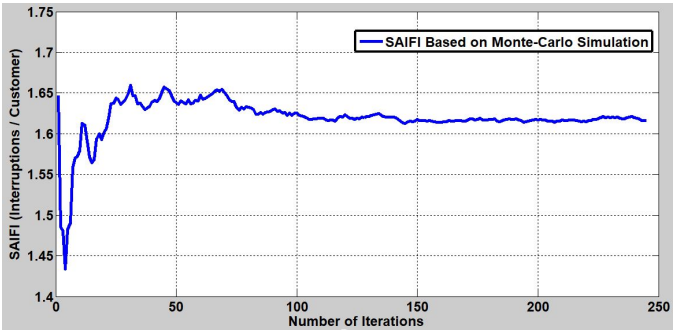


Fig. 6: MATLAB: Electric Grid $\mathcal{SAIFI}$ Result

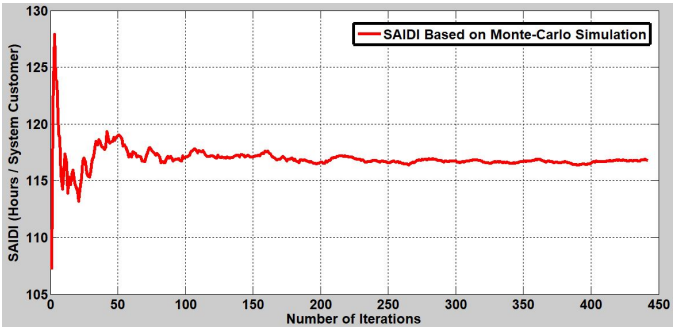


Fig. 7: MATLAB: Electric Grid $\mathcal{SAIDI}$ Result

evaluation of electrical power grid reliability indices $\mathcal{SAIFI}$ and $\mathcal{SAIDI}$ using all the techniques is presented in Table II.

It can be observed that the reliability indices obtained from our analysis are approximately equivalent to the corresponding ones calculated using Isograph. On the other hand, MATLAB MCS-based uses a random-based algorithm, which estimates different results of $\mathcal{SAIFI}$ and $\mathcal{SAIDI}$ every generation of a random number with errors between 4-11%. This clearly demonstrates that our analysis is not only providing the correct results but also with formally proven reliability expressions (Theorems 3 and 4) compared to existing simulation tools. Moreover, the CPU time for the evaluation of the reliability indices ($\mathcal{SAIFI}$ and $\mathcal{SAIDI}$) evaluation using the SML functions is much faster than Isograph (4.5X) and MATLAB (10X), as shown in Table II. The experiments were performed on core i5, 2.20 GHz, Linux VM with 1 GB of RAM.

TABLE II: $\mathcal{SAIFI}$ and $\mathcal{SAIDI}$ Comparison

Power Grid Reliability Indices	**Isograph Analysis**	**MATLAB Analysis**	**HOL4 Analysis**
$\mathcal{SAIFI}$ (Interruptions/Customer)	1.7749	1.6162	1.7748947863
$\mathcal{SAIDI}$ (Hours/Customer)	120.9387	116.7960	120.9387397546
CPU Time (Seconds)	2.752	6.074	0.592

By performing the formal ET step-analysis of a real-world 39-bus electrical power grid, we demonstrated the practical effectiveness of the proposed approach using HOL4 theorem prover, which will help power grid engineers to meet the desired quality requirements. Moreover, our proposed methodology can be used to analyze larger scale ET models of other power grid applications, such as Smart power systems [26].

VII. Conclusions

In this paper, we proposed a formal methodology using HOL4 theorem proving to conduct the reliability analysis of electrical power grids as an accurate alternate approach. We demonstrated the practical effectiveness of the proposed approach by performing the formal ET-based reliability analysis of the standard IEEE 39-bus electrical grid and formally determine its System Average Interruption Frequency and Duration Indices ($\mathcal{SAIFI}$ and $\mathcal{SAIDI}$), We also compared the results obtained from our analysis with those from the commercial ET analysis tool Isograph and the MATLAB Monte-Carlo simulation. As future work, we plan to provide the formal component-level reliability analysis of electrical grids, which will enable us to analyze the cascading dependencies with many sub-system levels, based on our proposed framework.

References

[1] A. Keyhani and M. Albaijat, *Smart Power Grids*. Springer Sci. & Bus. Media, 2012.

[2] R. Adib, H. E. Murdock, F. Appavou *et al.*, "Renewables 2015 Global Status Report," *REN21 Secretariat, Paris, France*, 2015.

[3] D. Connolly, H. Lund, and M. Mathiesen, B. V.and Leahy, "The First Step Towards a 100% Renewable Energy-System for Ireland," *Applied Energy*, vol. 88, no. 2, pp. 502–507, 2011.

[4] H. Lund and B. V. Mathiesen, "Energy System Analysis of 100% Renewable Energy Systems—The Case of Denmark in Years 2030 and 2050," *Energy*, vol. 34, no. 5, pp. 524–531, 2009.

[5] M. Čepin, *Assessment of Power System Reliability: Methods and Applications*. Springer Sci. & Bus. Media, 2011.

[6] ITEM, 2020. [Online]. Available: https://itemsoft.com/eventtree.html

[7] ReliaSoft, 2020. [Online]. Available: https://www.reliasoft.com

[8] Isograph, 2020. [Online]. Available: https://www.isograph.com

[9] V. Muzik and Z. Vostracky, "Possibilities of Event Tree Analysis Method for Emergency States in Power Grid," in *Electric Power Eng. Conf.* IEEE, 2018, pp. 1–5.

[10] R. E. Mackiewicz, "Overview of IEC 61850 and Benefits," in *Power Syst. Conf. and Expo.*, Montreal, Canada, 2006, pp. 623–630.

[11] R. Palin, D. Ward, I. Habli, and R. Rivett, "ISO 26262 Safety Cases: Compliance and Assurance," in *Syst. Safety*. Birmingham, UK: IET, 2011, pp. 1–6.

[12] O. Hasan and S. Tahar, "Formal Verification Methods," in *Encyclopedia of Inform. Sci. and Technology*. IGI Global, 2015, pp. 7162–7170.

[13] HOL Theorem Prover, 2020. [Online]. Available: https://hol-theorem-prover.org

[14] M. Abdelghany, W. Ahmad, and S. Tahar, "A Formally Verified HOL4 Algebra for Event Trees," 2020. [Online]. Available: http://arxiv.org/abs/2004.14384

[15] R. N. Allan, *Reliability Evaluation of Power Systems*. Springer Sci. & Bus. Media, 2013.

[16] W. Li, *Reliability Assessment of Electric Power Systems Using Monte Carlo Methods*. Springer Sci. & Bus. Media, 2013.

[17] N. Hatziargyriou, H. Asano, R. Iravani, and C. Marnay, "Microgrids," *Power and Energy Magazine*, vol. 5, no. 4, pp. 78–94, 2007.

[18] I. A. Papazoglou, "Mathematical Foundations of Event Trees," *Rel. Eng. & Syst. Safety*, vol. 61, no. 3, pp. 169–183, 1998.

[19] O. Hasan, N. Abbasi, B. Akbarpour, S. Tahar, and R. Akbarpour, "Formal Reasoning About Expectation Properties for Continuous Random Variables," in *Formal Methods*, ser. LNCS 5850. Springer, 2009, pp. 435–450.

[20] G. Bhatt and S. Affljulla, "Analysis of Large Scale PV Penetration Impact on IEEE 39-Bus Power System," in *Riga Technical University Conf. on Power and Elect. Eng.* IEEE, 2017, pp. 1–6.

[21] S. Xu, Y. Qian, and R. Q. Hu, "On Reliability of Smart Grid Neighborhood Area Networks," *IEEE Access*, vol. 3, pp. 2352–2365, 2015.

[22] D. Gan, R. J. Thomas, and R. D. Zimmerman, "Stability-Constrained Optimal Power Flow," *IEEE Trans. on Power Syst.*, vol. 15, no. 2, pp. 535–540, 2000.

[23] M. Marzband, M. M. Moghaddam, M. F. Akorede, and G. Khomeyrani, "Adaptive Load Shedding Scheme for Frequency Stability Enhancement in Microgrids," *Electric Power Syst. Research*, vol. 140, pp. 78–86, 2016.

[24] R. M. Moharil and P. S. Kulkarni, "Reliability Analysis of Solar PhotoVoltaic System using Hourly Mean Solar Radiation Data," *Solar Energy*, vol. 84, no. 4, pp. 691–702, 2010.

[25] P. J. Tavner, J. Xiang, and F. Spinato, "Reliability Analysis for Wind Turbines," *Int. J. for Progress and Applicat. in Wind Power Conversion Technology*, vol. 10, no. 1, pp. 1–18, 2007.

[26] R. Karki, R. Billinton, and A. K. Verma, *Reliability Modeling and Analysis of Smart Power Systems*. Springer Sci. & Business Media, 2014.