Event Tree Reliability Analysis of Safety-Critical Systems Using Theorem Proving

Mohamed Abdelghany, *Member, IEEE*, Waqar Ahmad, *Member, IEEE*, and Sofiène Tahar, *Senior Member, IEEE*

***Abstract*—Event tree (ET) analysis is widely used as a forward deductive safety analysis technique for decision-making at the design stage of safety-critical systems, such as smart power grids. An ET is a schematic diagram representing all possible complete/partial reliability and failure consequence events in a system so that one of these events can occur. In this article, we propose to use formal techniques based on theorem proving for the formal modeling and step-analysis of ET diagrams. To this end, we develop a formalization in higher order logic enabling the mathematical modeling of the graphical diagrams of ETs and the formal analysis of system-level failure/reliability. We propose new mathematical ET probabilistic formulations, based on a generic *list*-datatype, which are capable of analyzing large scale ETs that consist of $\mathcal{N}$ *multistate* system components and enable the formal ET probabilistic analysis for any given probabilistic distribution. We demonstrate the practical effectiveness of the proposed ET formalization by performing the formal reliability analysis of a standard IEEE 118-bus electrical power grid system and also formally determine its reliability indices, such as system/customer average interruption frequency and duration (SAIFI, SAIDI, and CAIDI). To assess the accuracy of our proposed approach, we compare our formal ET analysis results for the grid with those obtained by MATLAB Monte Carlo simulation, the commercial Isograph software as well as manual paper-and-pencil analysis.**

***Index Terms*—Customer average interruption duration indices (CAIDI), event tree (ET), HOL4, Isograph, reliability, system average interruption duration indices (SAIDI), system average interruption frequency index (SAIFI), smart power grids, theorem proving.**

I. Introduction

A. Motivation

NOWADAYS, the fulfillment of stringent safety requirements for critical systems, such as smart power grids [1] and the automotive industry [2], has been encouraging design engineers to use formal techniques as per recommendations of safety standards, such as IEC 61 850 [3] and ISO 26 262 [4]. Therefore, it is required to build necessary formal support for rigorous reliability analysis so that they become an essential step in the design process and ensure the delivery of a trusted service without failures [5]. Several reliability modeling techniques have been developed, such as fault trees (FT) [6], reliability block diagrams (RBD) [7], and event trees (ET) [8], for analyzing critical systems. FTs and RBDs are used to either analyze the factors causing a system failure or the success relationships of a system only, respectively. In contrast to FTs and RBDs, ETs provide a system risk analysis with all possible complete/partial failure and success events that can occur in a form of a tree structure. The results of the ET analysis are extremely useful for reliability analysts as ETs provide a more detailed system view compared to FTs and RBDs.

B. Literature Review

Papazoglou [8] was the first researcher to lay down the mathematical foundations of ETs in the late 1990s. He described the process of ET analysis in the following *four* main steps.

1) *Generation:* construct a complete ET model.
2) *Reduction:* removal of unnecessary ET branches.
3) *Partitioning:* extract a collection of ET paths according to the system failure and success events.
4) *Probabilistic analysis:* evaluate the probabilities of ET paths based on the occurrence of certain events.

But the analysis of ETs proposed in [8] is done purely manually using a paper-and-pencil approach. A major limitation in the manual approach is the possibility of human errors. On the other hand, there exist several simulation-based ET analysis tools, such as ITEM [9], ReliaSoft [10], and Isograph [11], which have been widely used to determine all possible complete/partial failure and success consequence scenarios of real-world systems, like electrical power grids [12], nuclear power plants [13], and electric railways [14]. However, simulation-based analysis approaches lack the rigor of detailed proof steps and may not be scalable for large systems due to an explosion of the test cases. On the other hand, simulation approaches generally use approximate random-based algorithms, such as MATLAB Monte Carlo simulation (MCS) [15], for faster computation, which could introduce undesirable inaccuracies that can be deemed fatal for safety-critical systems. A safer way is to substitute the error-prone informal reasoning of ET analysis for safety-critical systems by formal mathematical proofs.

Only a few works have previously considered using formal techniques to model and analyze ETs. For instance, Nỳvlt and Rausand in [16] used Petri nets for ET analysis to model the complete/partial system-level failure and success consequence events. The authors proposed a new method based on P-invariants to obtain a model of cascading dependencies in ETs [16]. However, according to the same authors, they are not able to obtain verified equations from the generated ET model [16]. For that purpose, we propose to use formal techniques, based on theorem proving, for the ET-based reliability analysis of safety-critical systems, which provides us the ability to obtain *verified* failure and operating consequence expressions.

Manuscript received November 24, 2020; revised March 4, 2021; accepted April 25, 2021. Date of publication May 31, 2021; date of current version June 13, 2022. *(Corresponding author: Mohamed Abdelghany.)*

The authors are with the Department of Electrical and Computer Engineering, Concordia University, Montreal, QC H4B 1R6, Canada (e-mail: m_eldes@ece.concordia.ca; waqar@ece.concordia.ca; tahar@ece.concordia.ca).

Digital Object Identifier 10.1109/JSYST.2021.3077558

Theorem proving is a formal verification technique [17], which is used for conducting the proof of mathematical theorems constructed in higher order logic (HOL) [18] based on a computerized proof tool. In particular, we use HOL4 [19], which is a well-known interactive theorem prover with the ability of verifying a wide range of mathematical HOL expressions. To the best of our knowledge, this is the first article, which develops a modeling and reasoning framework for ETs using theorem proving.

C. Contribution and Article Organization

In this article, we endeavor to formalize the *four* steps of ET analysis using the HOL4 proof assistant, i.e., *generation*, *reduction*, *partitioning,* and *probabilistic analysis*. We present two syntactically different, but semantically equivalent formalizations for ET analysis, using *set* and *list*-datatypes, respectively. The former *set*-datatype ET formalization is described by Papazoglou [8], however, it cannot mimic the graphical model of an ET consisting of an initiating node and branches since the elements in sets are orderless. The ordering is important in *Steps* 3 and 4 (*reduction* and *partitioning* processes) of the ET analysis. In the latter approach, the *list*-datatype inherently preserves the index of its member elements and naturally captures the graphical structure of ETs. Also, from our experience, the reasoning about ET reduction and partitioning properties using the *set*-datatype is quite cumbersome and significantly slow compared to the *list*-datatype especially when the ET diagram becomes tremendously large. For that purpose, we propose to use the *list*-datatype that inherently preserves the index of its member elements and naturally captures the graphical structure of ETs. Moreover, our proposed formulations provide the modeling of an arbitrary scale ET diagrams that consist of $\mathcal{N}$ *multistate* system components and based on any probabilistic distributions, which makes our framework the first of its kind. To demonstrate the practical effectiveness of the proposed ET formalization, we conduct the formal ET analysis of a standard IEEE 118-bus electrical power grid system. Subsequently, we formally determine its system average interruption frequency index (SAIFI) and system/customer average interruption duration Indices (SAIDI and CAIDI), which describe the average frequency and duration of interruptions in a specific electrical power grid, with respect to the system and customers, respectively [20]. Subsequently, to ensure the validity of our proposed analysis, we compare our formal ET analysis results with those obtained by the commercial tool Isograph, manual paper-and-pencil step-wise analysis and MATLAB MCS-based analysis.

1) Novel Contributions of the Article: The main novel contributions in this article using the HOL4 theorem prover can be summarized as follows.

- Development of a *rigorous analysis methodology* that can model mathematically the graphical diagrams of ETs and perform formally the system-level reliability analysis of the given safety-critical system
- Providing new *generic* modeling and probabilistic formulations that are capable of analyzing complex ETs that consist of $\mathcal{N}$ *multistate* system components and is based on any given probabilistic distribution and failure rates
- Proving the *soundness*, with respect to the original ET definitions by Papazoglou [8], of our newly proposed formalization of ETs using a new defined datatype, `EVENT_TREE`
- Application on a real-world IEEE standard 118-bus electrical power grid system with the *verification* of its important reliability indices (SAIFI, SAIDI, and CAIDI) and *validation* of our results with manual paper-and-pencil, Isograph, and MATLAB analysis

2) Organization of the Article: The rest of the article is organized as follows. In Section II, we briefly summarize the basics of HOL4 theorem proving and the fundamentals of ETs. An overview for our proposed methodology is described in Section III. In Section IV, we present the details of our HOL4 formalization of ETs using the *set*-datatype. Section V describes the formalization of ETs by developing a new recursive datatype `EVENT_TREE`, which we use for ET reduction, partitioning, and formal probabilistic analysis. In Section VI, we present the formal ET-based reliability of a standard 118-bus electrical grid. In Section VII, we provide a comparison of our formal SAIFI, SAIDI, and CAIDI analysis results with those of the Isograph software, paper-and-pencil, and MATLAB MCS approaches. Lastly, Section VIII concludes the article.

TABLE I
HOL4 SYMBOLS AND FUNCTIONS

HOL4 Symbol	Standard Symbol	Meaning
{x | P(x)}	$\{\lambda x.\ P(x)\}$	Set of all x such that $P(x)$
λx. t	$\lambda x.\ t$	Function that maps x to $t(x)$
h :: L	$cons$	Add a new element h to a list L
EL n L	$element$	n^{th} element of list L

II. PRELIMINARIES

In this section, we summarize the basics of the HOL4 theorem proving and the fundamentals of the ET to facilitate the understanding of the rest of the article.

A. HOL4 Theorem Proving

Theorem proving [17] is used as a formal verification approach for conducting the proof of mathematical theorems based on a computerized proof system. HOL4 [19] is an interactive theorem prover with the ability of verifying mathematical expressions constructed in HOL. In general, given a critical-system to be formally analyzed, we model the system mathematically, then using the HOL4 theorem prover, several reliability indices of the system can be verified based on this mathematical model. The main feature in HOL4 is that its core consists only of a few axioms and inference rules and any further lemma/theorem should be verified based on 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. Table I provides some commonly used HOL4 symbols and functions that we will use in this article.

The probability theory in HOL4 is built on the *measure space* and *probability space* concepts [21]. 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 the events of interest, and *Pr* is the probability measure of the sample space as 1. The HOL4 theorem prover has a rich library

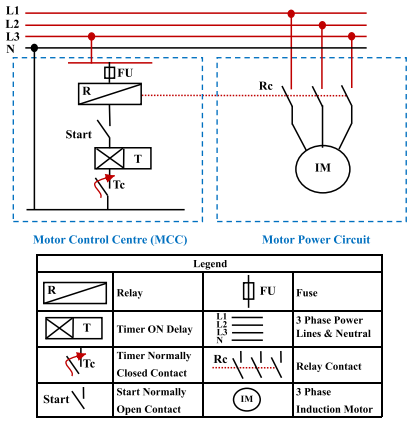

Fig. 1. Schematic of an example MCC.

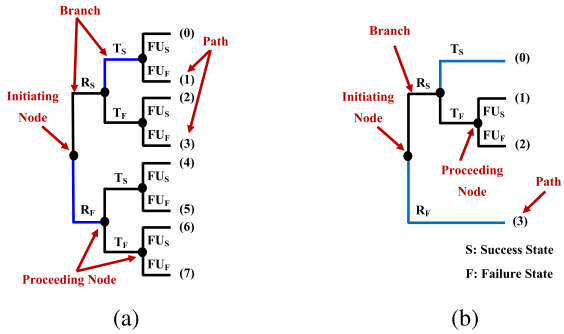

Fig. 2. Sample MCC ET diagrams. (a) Complete ET. (b) Reduced ET.

of probabilities, including the functions `p_space`, `events` and `prob`. Given a probability space p, these functions return the corresponding Ω, Σ, and Pr, respectively. The cumulative distribution function (CDF) is defined as the probability of the failure event where a random variable X has a value less or equal to a value t, i.e., $\mathcal{P}(X \leq t)$. This definition can be been formalized in HOL4 as [21]

```
⊢ CDF p X t = distribution p X {y | y ≤ t}
```

where the function `distribution` takes three inputs: 1) a probability space p; 2) a random variable X; 3) a set of real numbers, then returns the probability of the variable X acquiring all the values of the given set in probability space.

B. Event Tree (ET) Analysis

ET is a widely used probabilistic risk assessment technique that can model all possible system-level complete/partial reliability and failure consequence events in the form of a tree structure [8]. An ET diagram starts by an *Initiating Node* from which all possible consequence scenarios of a sudden event that can occur in the safety-critical system are drawn as *Branches* connected to *Proceeding Nodes* so that *only one* of these scenarios can occur. As an example, consider a motor control Center (MCC) system [22] consisting of three components Relay R, Timer T, and Fuse FU, as shown in Fig. 1. The MCC is designed to control an induction motor (IM) and let it run for a specific period of time then stops. The power circuit of IM is energized by the closure of the relay contact R_c, as shown in Fig. 1. The relay contact works after the user presses the *Start* button that energizes the relay R and at the same time energizes an ON-delay timer T. The timer T opens its contact T_c after a specific period of time t and consequently the IM stops. If the IM is overloaded, then the fuse FU melts and protects both MCC and IM from damage. Assume that each component in the MCC has two operational states, i.e., operating or failing. Papazoglou [8] defined the ET *four* step-analysis as follows.

1) *Generation:* Model a complete ET diagram that draws all possible consequence scenarios, called *paths*. Each consequence *path* consists of unique events associated with it, i.e., all ET paths are distinct. Fig. 2(a) depicts eight unique paths (0–7) with all possible scenarios that can occur in the MCC. For instance, if the Relay contact functions correctly or not, i.e., Success (S) or Fail (F), then the next MCC components are considered in order, i.e., Timer and Fuse, respectively. Each path in the ET ends with either motor fails or operates correctly.
2) *Reduction:* Model the actual ET of the system in the sense that the unnecessary paths should be removed from a complete ET. This can be done by deleting some specific nodes/branches corresponding to the occurrence of certain events, which are known as complete cylinders (CCs) [23]. These cylinders are ET *paths* consisting of $\mathcal{N}$ events and they 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 critical-component relay R fails (R_F) then the whole MCC system fails regardless of the status of the rest of the components, i.e., Timer and Fuse, as shown in Fig. 2(b). Therefore, the paths 4–7 are CCs with respect to R_F. Similarly, if both Relay and Timer work correctly as designed (R_S and T_S), then the motor functions correctly regardless of the status of the Fuse. So, the paths 0 and 1 are CCs with respect to R_S and T_S.
3) *Partitioning:* Dividing the ET paths according to the system failure and success events. For instance, suppose we are only focusing on the complete failure (CF) of the MCC in Fig. 2(b) to function correctly, then the ET paths 2 and 3 only are taken from the set of reduced ET paths.
4) *Probabilistic analysis:* Eventually, calculate the probabilities of the ET paths based on the occurrence of a certain event. These probabilities represent the likelihood of each sequence that is possible to occur in a system so that *only one* can occur [8]. This implies that all ET paths are disjoint, i.e., the failure and success states cannot occur at the same instant. Assuming that all events in an ET are mutually independent that the probability of any ET path can be computed by multiplying the individual probabilities of all the events associated with it [8]. For example, the probability of the MCC complete failure in Fig. 2(b) (ET paths 2 and 3) can be expressed mathematically as

$$\mathcal{P}(\mathrm{MCC}_{CF}) = \mathcal{P}(\mathrm{R}_S) \times \mathcal{P}(\mathrm{T}_F) \times \mathcal{P}(\mathrm{FU}_F) + \mathcal{P}(\mathrm{R}_F) \tag{1}$$

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

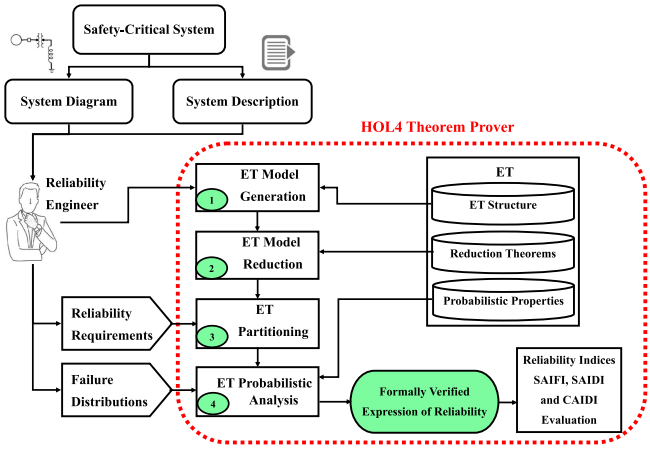

Fig. 3. Methodology for formal probabilistic ET analysis.

III. Methodology

Fig. 3 depicts an overview of the proposed methodology for the formal ET analysis based on HOL4 theorem proving. This methodology allows us to formally *verify* failure/operating consequence expressions corresponding to the given critical-system diagram and its description. The core component of this methodology is the HOL4 formalization of ETs, proposed in this article, as depicted in containers, enclosed by a box, as shown in Fig. 3. The first step in our proposed methodology is a safety-critical system design provided by the reliability engineers and the construction of its complete ET model. The second step is to formally model the obtained ET model in the previous step using our core ET formalization and the reduction of irreverent nodes and branches. The next step is to partition the ET model according to the reliability requirements of the given system and also assign the failure distributions, like Exponential/Weibull/Poisson to each system component to perform the probabilistic analysis. Based on our rich library of ET lemmas and theorems, proposed in this article, a user with some basic knowhow about HOL4 can easily verify the corresponding complete/partial reliability or failure probability expressions. The last step is to formally verify the expressions of a given system failure/operating reliability indices, such as SAIFI, SAIDI, and CAIDI, based on formal ET analysis. By applying the above-mentioned steps, we provide a rigorous verification methodology for analyzing critical systems, such as smart power grids, based on formal ET reliability analysis.

In the next section, we describe the formalization of ETs using the *set* and the *list* data-types, respectively. The reason for using the *set* theory is that most of the mathematical foundations of ETs from the work of Papazoglou [8] are built on sets. However, the ordering of events in ET paths is important during the *Steps* 2 and 3 of the ET analysis. Therefore, a sequence-preserving formalization of ETs in the *list* theory should be adopted. In order to ensure the correspondence of the *set* and *list* theory-based ET formalizations, we formally verify the equivalence between them.

IV. ET Formalization Using Sets

An event outcome space ($\mathcal{W}$) is referred to as a set of all possible scenarios of an initiating event (IE) or modes of operation of a system critical-component, which must satisfy the following constraints according to Papazoglou [8].

1) *Distinct:* All outcomes in $\mathcal{W}$ must be unique.
2) *Disjoint (mutually exclusive):* Any pair of events from a set $\mathcal{W}$ cannot occur at the same time.
3) *Finite:* $\mathcal{W}$ must consist of a finite number of elements

$$\mathcal{W} = \{\omega_j\} \qquad j = 1, 2, \ldots, \mathcal{N}. \tag{2}$$

For example, the event outcome spaces $\mathcal{W}_R$, $\mathcal{W}_T$, $\mathcal{W}_{FU}$ corresponding to all components of the MCC system (see Section II-B) are $\{\mathrm{R}_S, \mathrm{R}_F\}, \{\mathrm{T}_S, \mathrm{T}_F\}, \{\mathrm{FU}_S, \mathrm{FU}_F\}$, respectively, satisfying all ET constraints distinct, disjoint, and finite. We formalize the above-mentioned $\mathcal{W}$ constraints in HOL4 as follows:

Definition 1:

$\vdash \Omega\ \mathcal{W} = \{x |\ x \in \mathcal{W} \wedge$ `FINITE` $\mathcal{W} \wedge$ `disjoint` $\mathcal{W}\}$

where $\mathcal{W}$ is a set of *events* representing the possibilities resulting from an IE or modes of operation of a system component in HOL4. The elements in a set are intrinsically distinct, and thus, ensuring the constraint (a). The function `disjoint` ensures that each pair of elements in a given set $\mathcal{W}$ is mutually exclusive satisfying constraint (b). The HOL4 function `FINITE` guarantees that the set of event outcome space must consist of a finite number of elements, as indicated by constraint (c).

Consider a system 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 set 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., $\mathcal{W}_1 \bigotimes \mathcal{W}_2$). In ETs, an intersection operation is performed on each member of these pairs to obtain a valid event outcome space. In other words, the resulting event outcome space from the Cartesian product of two event outcome spaces also satisfies the above-mentioned constraints. We formalize this concept in HOL4 as follows.

We first define a function $\bigcap^{\otimes}$ that takes two different event outcome spaces $\mathcal{W}_1$ and $\mathcal{W}_2$ and then constructs a set by performing all possible intersection scenarios on the given elements of $\mathcal{W}_1$ and $\mathcal{W}_2$ as follows:

Definition 2:

$\vdash \mathcal{W}_1 \bigcap^{\otimes} \mathcal{W}_2 =$ `{x ∩ y | x ∈` $\Omega\ \mathcal{W}_1 \wedge$ `y ∈` $\Omega\ \mathcal{W}_2$`}`

Next, we ensure that the obtained duets from Definition 2 are mutually exclusive. For instance, consider two arbitrary outcomes $(\omega_{1^{\frown}m} \cap \omega_{2n})$ and $(\omega_{1^{\frown}k} \cap \omega_{2^{\frown}l})$ at least $(m \neq k)$ or $(n \neq l)$ must be true. So, we define the function $\bigotimes$ that applies the function $\bigcap^{\otimes}$ on the given event outcome spaces $\mathcal{W}_1$ and $\mathcal{W}_2$ and also the function `disjoint` to ensure that each pair of elements is mutually exclusive as follows:

Definition 3:

$\vdash \mathcal{W}_1 \bigotimes \mathcal{W}_2 =$

`{x |` $x \in \mathcal{W}_1 \bigcap^{\otimes} \mathcal{W}_2 \wedge$ `disjoint (`$\mathcal{W}_1 \bigcap^{\otimes} \mathcal{W}_2$`)}`

Now, we can define a generic function $\bigotimes^{\mathcal{N}}$ as proposed by Papazoglou [8] that can take an arbitrary set of event outcome spaces and generates the corresponding ET diagram (i.e., $\mathcal{W}_1 \bigotimes \mathcal{W}_2 \bigotimes \cdots \bigotimes \mathcal{W}_{\mathcal{N}}$). For this purpose, we use the HOL4 function `ITSET` that can recursively apply $\bigotimes$ on a given set of event outcome spaces as follows:

Definition 4:

$\vdash \mathcal{S} \bigotimes^{\mathcal{N}} \mathcal{W}_{\mathcal{N}}$ = ITSET ($\lambda \mathcal{W}_1\ \mathcal{W}_2.\ \mathcal{W}_1 \bigotimes \mathcal{W}_2$) $\mathcal{S}\ \mathcal{W}_{\mathcal{N}}$

where $\mathcal{S}$ is a *set* containing all event outcome spaces till $\mathcal{N}-1$ (i.e., $\mathcal{S} = \{\mathcal{W}_1, \mathcal{W}_2, \ldots, \mathcal{W}_{\mathcal{N}-1}\}$) and $\mathcal{W}_{\mathcal{N}}$ represents the last event outcome space. In order to verify the correctness of the defined functions $\bigotimes$ and $\bigotimes^{\mathcal{N}}$, we formally verify the following *commutative* and *associative* properties, by utilizing the existing HOL4 functions INSERT and DELETE to insert and delete an element or event outcome space $\mathcal{W}_1$ from a given set of event outcome spaces $\mathcal{S}$, respectively, in HOL4 as follows:

Theorem 1:

$\vdash$ ($\mathcal{W}_1$ INSERT $\mathcal{S}$) $\bigotimes^{\mathcal{N}}$ $\mathcal{W}_{\mathcal{N}}$ =
($\mathcal{S}$ DELETE $\mathcal{W}_1$) $\bigotimes^{\mathcal{N}}$ ($\mathcal{W}_1 \bigotimes \mathcal{W}_{\mathcal{N}}$)

Theorem 2:

$\vdash$ ($\mathcal{W}_1$ INSERT $\mathcal{S}$) $\bigotimes^{\mathcal{N}}$ $\mathcal{W}_{\mathcal{N}}$ =
$\mathcal{W}_1 \bigotimes$ (($\mathcal{S}$ DELETE $\mathcal{W}_1$) $\bigotimes^{\mathcal{N}}$ $\mathcal{W}_{\mathcal{N}}$)

The order of events in a path is irrelevant when evaluating the probabilities of a given path [23], e.g., the probability of path (R_S, T_F, FU_F) in (1) is exactly equivalent to the probability of path (FU_F, T_F, R_S) due to the commutative property of intersection and the events independence. However, it is important to preserve the order of events in ET paths during *Steps* 2 and 3 (*reduction* and *partitioning*) of the ET analysis [8] while the elements in the sets are orderless. A possible way to resolve the problem of ordering in the *set*-datatype is by assigning a unique number to each set element representing a branch during the ET modeling. However, when an ET becomes tremendously large, the set-based reasoning is quite cumbersome and significantly slow compared to the *list*-datatype. For that purpose, we propose the formalization of ETs using the *list* theory in the HOL4 theorem prover.

V. ET Formalization Using Lists

In this section, we present all four ET analysis steps using the *list* datatype, which preserves the order of the elements.

A. ET Modeling Formalization

We start the formalization of ETs by developing a new recursive datatype EVENT_TREE in HOL4 as follows:

Hol_datatype EVENT_TREE =
ATOMIC of (event) | NODE of (EVENT_TREE list) |
BRANCH of (event) (EVENT_TREE)

where the new datatype EVENT_TREE consists of *three* basic ET constructors ATOMIC, NODE and BRANCH. The basic ET constructor ATOMIC takes a single event while the basic ET constructor NODE takes a recursive EVENT_TREE-typed list and lastly the basic ET constructor BRANCH takes an event and a recursive EVENT_TREE-typed. A semantic function is then defined that can yield a corresponding ET diagram as follows:

Definition 5:

$\vdash$ ETREE (ATOMIC X) = X $\wedge$
ETREE (NODE (h::L)) =
ETREE h $\cup$ (ETREE (NODE L)) $\wedge$
ETREE (BRANCH Y Z) = Y $\cup$ ETREE Z

The function ETREE takes the constructors defined by the datatype EVENT_TREE to mathematically model the ET diagram. If the function ETREE takes a success/fail event X, identified by a type constructor ATOMIC, then it returns the event X. If the function ETREE takes an arbitrary list (h::L) of type EVENT_TREE, identified by a type constructor NODE, then it returns the union of the head of the list (h) after applying the function ETREE and the recursive call of the NODE constructor with the rest of the list (L). Similarly, if the function ETREE takes a success/fail event Y and a proceeding ET Z of type EVENT_TREE, identified by a type constructor BRANCH, then it performs the intersection of the event Y with the ET Z after applying the function ETREE. To have a clear understanding, we can use the defined function ETREE to describe mathematically the nodes and branches for the MCC system shown in Fig. 2(b) as follows.

1) Initiating node of R states:
ETREE (NODE [R_S;R_F]) = $\mathrm{R}_S \cup \mathrm{R}_F$.
2) Branch T_F with a proceeding node of FU states:
ETREE (BRANCH T_F (NODE [FU_S;FU_F])) = $\mathrm{T}_F \cap \mathrm{FU}_S \cup \mathrm{T}_F \cap \mathrm{FU}_F$.
3) ET Path 2 of branch R_S with subbranches T_F and FU_F:
ETREEE (BRANCH R_S (BRANCH T_F FU_F)) = $\mathrm{R}_S \cap \mathrm{T}_F \cap \mathrm{FU}_F$.

Moreover, we define a *generic* function ET_{PATH} in HOL4 to obtain a specific path in the ET model consisting of $\mathcal{N}$ branch events. This was done in HOL4 by using the HOL4 recursive function FOLDL that recursively applies the BRANCH ET constructor on a given list of different $\mathcal{N}$ branch events as follows:

Definition 6:

$\vdash$ ET_{PATH} p (EVENT_1::$\mathrm{EVENT}_{\mathcal{N}}$) =
FOLDL
(λa b. ETREE (BRANCH a b)) EVENT_1 $\mathrm{EVENT}_{\mathcal{N}}$

To formally define a function that can model a complete ET of $\mathcal{N}$ multistate system components, similar to Definition 4, we start by defining a function that can model an ET diagram for two consecutive NODE lists, say L_1 and L_2, in HOL4 as follows:

Definition 7:

$\vdash$ $\mathrm{L}_1 \bigotimes_{\mathrm{L}} \mathrm{L}_2$ =
MAP (λa. MAP (λb. ETREE (BRANCH a b)) L_2) L_1

where the function $\bigotimes_{\mathrm{L}}$ takes two different EVENT_TREE-typed lists and returns an EVENT_TREE-typed list by recursively mapping the BRANCH constructor on each element of the first NODE list paired with the entire second NODE list using the HOL4 mapping function MAP.

Now, we can define a *generic* function $\bigotimes_{\mathrm{L}}^{\mathcal{N}}$ that takes an arbitrary list of $\mathcal{N}$ event outcome spaces and generates a corresponding complete sequential ET diagram. For this purpose, we utilize the HOL4 function FOLDR that recursively maps $\bigotimes_{\mathrm{L}}$ on a given list of event outcome spaces as follows:

Definition 8:

$\vdash$ L $\bigotimes_{\mathrm{L}}^{\mathcal{N}}$ $\mathrm{L}_{\mathcal{N}}$ = FOLDR ($\lambda \mathrm{L}_1\ \mathrm{L}_2.\ \mathrm{L}_1 \bigotimes_{\mathrm{L}} \mathrm{L}_2$) $\mathrm{L}_{\mathcal{N}}$ L

where L is a *list* of all given event outcome spaces till $\mathcal{N}-1$ (i.e., L = [[$\mathcal{W}_1$], [$\mathcal{W}_2$],..., [$\mathcal{W}_{\mathcal{N}-1}$]]) and $\mathrm{L}_{\mathcal{N}} = [\mathcal{W}_{\mathcal{N}}]$. For instance, we can define the complete ET model for the MCC system shown in Fig. 2(b), in HOL4 as

$\vdash$ MCC_COMPLETE_ET [[R_S;R_F];[T_S;T_F]; [FU_S;FU_F]]
= ETREE (NODE
([[R_S;R_F];[T_S;T_F]] $\bigotimes_{\mathrm{L}}^{\mathcal{N}}$ [FU_S;FU_F])

We can formally verify the above complete ET model of the MCC system, in HOL4 as

```
⊢ MCC_COMPLETE_ET [[R_S;R_F];[T_S;T_F]; [FU_S;FU_F]]
  = ETREE
    (NODE
      [BRANCH R_S
        (NODE [BRANCH T_S (NODE [FU_S;FU_F]);
               BRANCH T_F (NODE [FU_S;FU_F])]);
      BRANCH R_F
        (NODE [BRANCH T_S (NODE [FU_S;FU_F]);
               BRANCH T_F (NODE [FU_S;FU_F])])])
```

To covers all constraints of the event outcome space (*distinct*, *disjoint*, and *finite*) on each list of the given $\mathcal{N}$ event outcome space lists, as described in (2), we define a recursive *predicate* function $\Omega_C^{\mathcal{N}}$, in HOL4 as follows:

Definition 9:

```
⊢ Ω_C^N (W::W_N) ⇔
  ALL_DISTINCT W ∧ disjoint W ∧ Ω_C^N W_N
```

where the function ALL_DISTINCT ensures that each pair of elements in each given list is distinct satisfying constraint (a) in (2). The disjoint ensures that each pair of elements in each list is mutually exclusive satisfying constraint (b). The elements in a list are intrinsically finite, and thus, ensuring the constraint (c). In order to ensure the *soundness* of our new proposed list formalization with respect to the *set* one, we formally verify the equivalence between Definitions 3 and 7 and Definitions 4 and 8, in HOL4 as follows:

Theorem 3:

```
⊢ Ω_C^N [L_1;L_2] ⇒ ETREE (NODE (L_1 ⨂_L L_2)) =
                    ⋃ ((set L_1) ⨂ (set L_2))
```

Theorem 4:

```
⊢ Ω_C^N (L_N::L) ⇒ ETREE (NODE (L ⨂_L^N L_N)) =
                   ⋃ ((set L) ⨂^N (set L_N))
```

B. ET Reduction and Partitioning Formalization

In ET analysis [8], *Step 2 (Reduction)* is used to model the accurate functional behavior of systems in the sense that the irrelevant ET paths should be removed from a complete ET of a system to reduced its number of ET test cases. Therefore, in HOL4 we define a reduction function $\boxtimes$ on event outcome spaces that takes a list of ET paths *L*, which is the output of Definition 8, a list of ET path numbers *N* to be reduced and their *K* conditional events *CE* and returns a reduced ET list as follows:

Definition 10:

```
⊢ L ⊠ N CE p =
  LUPDATE (ET_PATH p CE) (LAST N)
          (DELETE_N L (TAKE (LENGTH N-1) N))
```

where the functions LUPDATE, LAST, and TAKE are the HOL4 *list* theory functions to update an element, extract the last element and take a collection of elements, respectively. The function DELETE_N recursively deletes *N* elements from a given list corresponding to the paths that should be removed from a complete ET of a system in order to model the accurate functional behavior of safety-critical systems. To ensure the correctness of the system reduced ET model after the deletion process, we formally verify that the length of the new ET list after reduction is equal to the length of complete ET model minus the number of paths that were deleted, in HOL4 as follows:

Theorem 5:

```
⊢ INDEX_LT_LEN N (L ⨂_L^N L_N) ∧ LENGTH N ≥ 1 ⇒
  LENGTH ((L ⨂_L^N L_N) ⊠ N CE p) =
  LENGTH (L ⨂_L^N L_N) − LENGTH N + 1
```

where the function INDEX_LT_LEN ensures that each index in the given list *N* is less than the length of the ET list.

To perform multiple reduction operations on a given ET model, we define the following recursive reduction function $\boxtimes^{\mathcal{N}}$, using Definition 10, in HOL4 as follows:

Definition 11:

```
⊢ L ⊠^N (N::Ns) (CE::CEs) p =
  (L ⊠ N CE p) ⊠^N Ns CEs p.
```

Upon this, the actual ET of the MCC after reducing the paths 0, 1, and 4–7, as shown in Fig. 2(b), can be obtained in HOL4 as follows:

```
⊢ MCC_REDUCED_ET
  [R;T;FU] [[0;1];[4-7]] [[R↑;T↑];[R↓]] =
  ETREE (NODE ((↑↓ [R;T]) ⨂_L^N (↑↓ [FU]))
        ⊠^N [[0;1];[4-7]] [[R↑;T↑];[R↓]])
```

where the function ↑↓ takes an arbitrary list of $\mathcal{N}$ components and assigns complete failure and complete success states ↓ and ↑ to each system component, respectively. The function failure event ↓ or CDF (see Section II-A) 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 ↑ is the complement of the function ↓, i.e, $X > t$. Also, we can formally verify the above reduced ET model of the MCC system, in HOL4 as follows:

```
⊢ MCC_REDUCED_ET
  [R;T;FU] [[0;1];[4-7]] [[R↑;T↑];[R↓]] =
  ETREE
    (NODE
      [BRANCH R↑ [T↑;BRANCH T↓ [FU↑;FU↓]];
       R↓]).
```

After the ET reduction process, the next step is the partitioning of the ET paths space according to the system reliability requirements. We define a partitioning function ⊞ to extract a collection of ET paths specified in the index list *N* as follows:

Definition 12:

```
⊢ N ⊞ L = MAP (λa. EL a L) N.
```

For instance, the complete failure paths of the MCC, i.e., paths 2 and 3, as shown in Fig 2(b), can be extracted in HOL4 as follows:

```
⊢ MCC_COMPLETE_FAILURE [2;3] [R;T;FU]
                [[0;1];[4-7]] [[R↑;T↑];[R↓]] =
  ETREE (NODE
   ([2;3] ⊞ MCC_REDUCED_ET [R;T;FU]
              [[0;1];[4-7]] [[R↑;T↑];[R↓]]))
```

C. ET Probabilistic Analysis Formalization

The last step in the ET analysis [23] is to determine the probability of each ET path occurrence. For that purpose, we developed new *generic* probabilistic properties for NODE, BRANCH, ET_{PATH}, and $\bigotimes_{\mathrm{L}}^{\mathcal{N}}$ that are based on any probabilistic distributions. These properties can be used to easily evaluate the probabilities of all possible scenarios of large scale ET diagrams that consist of $\mathcal{N}$ system components and each component consists of $\mathcal{M}$-states. Each of these probabilistic properties has been *formally verified* in the HOL4 theorem prover as described in the sequel.

Property 1: The probability of $\mathcal{N}$ events in an ET initiating node is verified as the sum of probabilities associated with the events of the given list, i.e., mutually exclusive, in HOL4 as follows:

Theorem 6:

$\vdash$ prob_space p $\wedge$ $\Omega_C^{\mathcal{N}}$ L $\wedge$
$\forall$y. y $\in$ L $\Rightarrow$ y $\in$ events p
$\Rightarrow$ prob p (ETREE (NODE L)) = $\sum$ (PROB_LIST p L)

The first assumption in the above theorem ensures that *p* is a valid probability space. The next assumption is quite similar to the one described in Theorem 3 to ensure all ET constraints of the event outcome space (*distinct*, *disjoint*, and *finite*). The last assumption ensures that all *multistate* events in a node belong to the events space. The function PROB_LIST takes an arbitrary list of events $[Z_1, Z_2, Z_3, \ldots, Z_N]$ and returns a list of probabilities associated with the elements of the list [prob p Z_1, prob p Z_2, prob p Z_3, ..., prob p Z_N], while the function $\sum$ takes a list $[X_1, X_2, X_3, \ldots, X_N]$ and returns the sum of the list elements $X_1 + X_2 + X_3 + \cdots + X_N$.

Property 2: The probability of events in ET branches connected to proceeding nodes is verified as the multiplication of each branch failure/success event probability with the sum of the probabilities for the next node events, in HOL4 as follows:

Theorem 7:

$\vdash$ prob_space p $\wedge$ MUTUAL_INDEP p (X::L) $\wedge$
$\Omega_C^{\mathcal{N}}$ L $\wedge\forall$y. y $\in$ (X::L) $\Rightarrow$ y $\in$ events p
$\Rightarrow$ prob p (ETREE (BRANCH X (NODE L))) =
(prob p X) $\times$ $\sum$ (PROB_LIST p L)

where the predicate function MUTUAL_INDEP ensures that all events in each path of an ET are mutually independent.

Property 3: The probability of an ET path consisting of $\mathcal{M}$ events can be verified as the multiplication of the individual probabilities of all $\mathcal{M}$ events associated with it, in HOL4 as follows:

Theorem 8:

$\vdash$ prob_space p $\wedge$ MUTUAL_INDEP p $\text{EVENTS}_{\mathcal{M}}$ $\wedge$
$\forall$y. y $\in$ $\text{EVENTS}_{\mathcal{M}}$ $\Rightarrow$ y $\in$ events p
$\Rightarrow$ prob p (ET_{PATH} p $\text{EVENTS}_{\mathcal{M}}$) =
$\prod$ (PROB_LIST p $\text{EVENTS}_{\mathcal{M}}$)

where the function $\prod$ takes a list $[Y_1, Y_2, Y_3, \ldots, Y_N]$ and returns the product of the list elements $Y_1 \times Y_2 \times Y_3 \times \cdots \times Y_N$.

Property 4: A complex *2-D generic* ET probabilistic formulation for extracting a collection of $\mathcal{N}$ paths and each path is associated with different $\mathcal{M}$ events from an ET model is verified as the sum of the recursive multiplication of individual probabilities for all its ET paths, in HOL4 as follows:

Theorem 9:

$\vdash$ prob_space p $\wedge$ MUTUAL_INDEP p $\text{PATHS}_{\mathcal{N}}$ $\wedge$
disjoint (MAP (λa. ET_{PATH} p a) $\text{PATHS}_{\mathcal{N}}$) $\wedge$
ALL_DISTINCT (MAP (λa. ET_{PATH} p a) $\text{PATHS}_{\mathcal{N}}$)
$\Rightarrow$ prob p
(ETREE
(NODE
(MAP (λa. ET_{PATH} p a) $\text{PATHS}_{\mathcal{N}}$))) =
$\sum$ (MAP (λa. $\prod$ (PROB_LIST p a)) $\text{PATHS}_{\mathcal{N}}$)

Property 5: A generic probabilistic formulation for the function $\bigotimes_{\text{L}}^{\mathcal{N}}$ is verified, in HOL4 as follows:

Theorem 10:

$\vdash$ prob_space p $\wedge$ $\Omega_C^{\mathcal{N}}$ ($\text{L}_{\mathcal{N}}$::L) $\wedge$
MUTUAL_INDEP p ($\text{L}_{\mathcal{N}}$::L) $\wedge$
$\forall$y. y $\in$ ($\text{L}_{\mathcal{N}}$::L) $\Rightarrow$ y $\in$ events p
$\Rightarrow$ prob p (ETREE (NODE (L $\bigotimes_{\text{L}}^{\mathcal{N}}$ $\text{L}_{\mathcal{N}}$))) =
$\prod$ ($\sum_{\text{Prob}}^{\text{2D}}$ p ($\text{L}_{\mathcal{N}}$::L))

where the function $\sum_{\text{Prob}}^{\text{2D}}$ is used to recursively apply the functions PROB_LIST and $\sum$ on a given two dimensional list.

Remark that all above-mentioned ET new probabilistic formulations have been *formally verified* in HOL4, where the proof-script amounts to about 4000 lines of HOL4 code, which can be downloaded for use from [24]. In the next section, we present the formal ET analysis of a standard IEEE 118-bus electrical power grid and determine its reliability indices to illustrate the applicability of our proposed approach.

VI. Electrical Power 118-Bus Grid System

A smart power grid [1] is an interconnected network for delivering electricity from producers to consumers. The power grid system consists of three main zones [25]: 1) generating stations that produce electric power; 2) transmission lines that carry power from sources to loads; and 3) distribution lines that connect individual consumers. Due to the complex and integrated nature of the electrical power network, failures in any zone of the power system can cause widespread catastrophic disruption of supply [26]. With respect to the power-outage-causes study domain, the majority of the outages in the power grid are the result of accident events that occur on the grid transmission side [27]. Despite the huge investment in upgrading the cyber-infrastructure of the smart power grids, blackouts are still the common occurrence every year around the world [28]. Therefore, there is a dire need to develop reliability analysis techniques for electric power grids making them more resilient to costly blackouts and enable back-up decisions [29]. Using our proposed ET formalization, we can model the ET for any power grid consisting of $\mathcal{N}$ transmission lines and $\mathcal{M}$ customers. Consider a standard IEEE 118-bus electrical power grid test case representing a portion of the American electric power system (in the Midwestern US) [30] consisting of 19 generators (G), 186 transmission lines (TL), and 91 loads, as shown in Fig. 4. Assuming the study is undertaken for three major loads A, B, and C with the number of customers served CN_A, CN_B, and CN_C, respectively. Using the optimal power flow (OPF) optimization [31], we can determine the flow of power from generators to consumers A, B, and C in the transmission power network, as shown in Fig. 4.

A. Formal ET Model

Step 1: Using our novel *generic* ET formalization described in Section V, we can assign different multistate models, as shown in Fig. 5 [29], to each TL of the transmission power network for reliability analysis. We consider each TL (TL_1–TL_{33}) shown in Fig. 4 to be represented by a two state model, i.e., Success $\uparrow$ or Fail $\downarrow$. Therefore, we can formally describe the complete ET models of all TLs that affect the reliability of loads A, B, and C (2048, 1024, and 4096 test cases, respectively), in HOL4 as follows:

Definition 13:

$\vdash$ IEEE_118_BUS_COMPLETE_ET_LOAD_A
[TL_1;TL_2;TL_3;TL_4;TL_5;TL_6;TL_7;TL_8;TL_9;TL_{10}]
[TL_{11}] =
ETREE (NODE
($\uparrow\downarrow$ [TL_1;TL_2;TL_3;TL_4;TL_5;
TL_6;TL_7;TL_8;TL_9;TL_{10}]) $\bigotimes_{\text{L}}^{\mathcal{N}}$ ($\uparrow\downarrow$ [TL_{11}]))

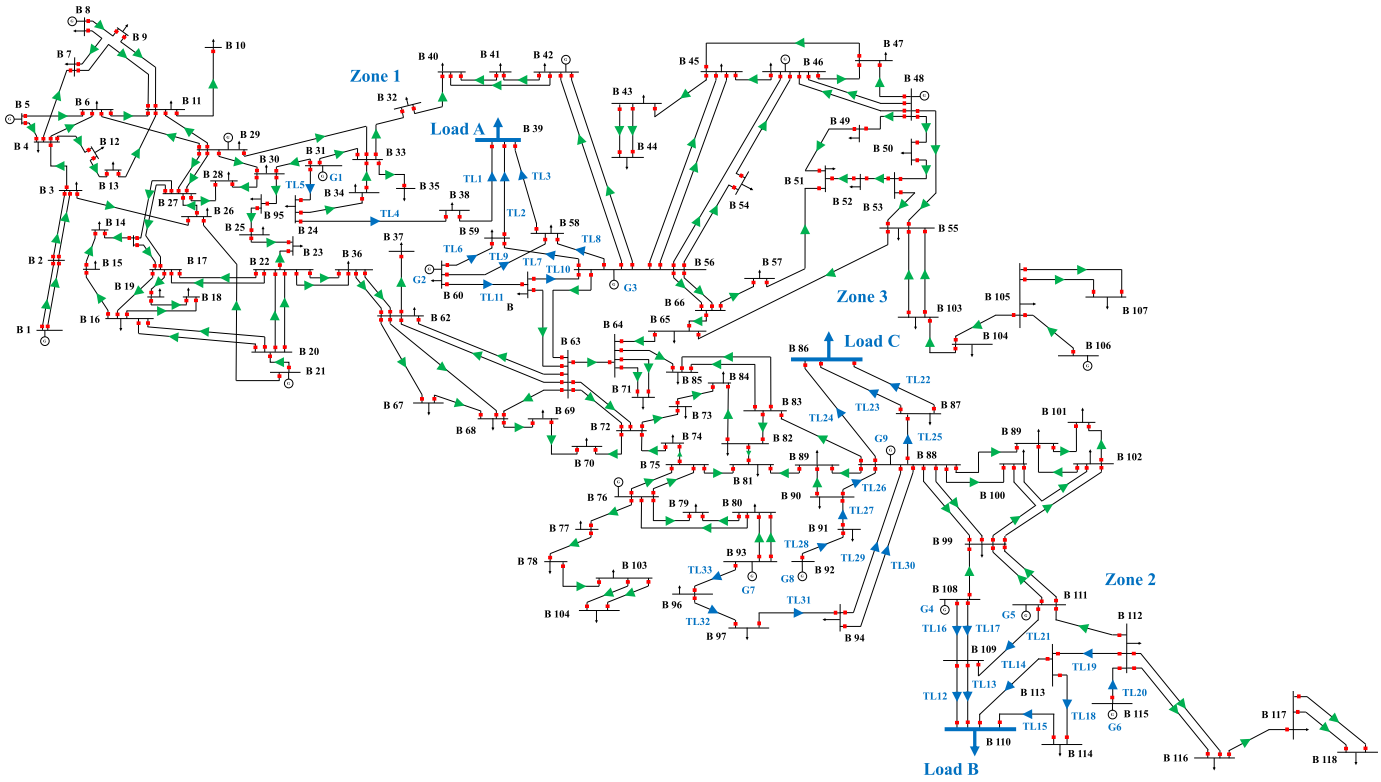

Fig. 4. IEEE 118-bus electrical power grid system.

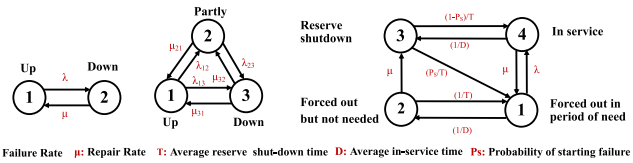

Fig. 5. Multistate models for reliability studies.

Definition 14:

$$\vdash \texttt{IEEE\_118\_BUS\_COMPLETE\_ET\_LOAD\_B}\ [\mathrm{TL}_{12};\mathrm{TL}_{13};\mathrm{TL}_{14};\mathrm{TL}_{15};\mathrm{TL}_{16};\mathrm{TL}_{17};\mathrm{TL}_{18};\mathrm{TL}_{19};\mathrm{TL}_{20}]\ [\mathrm{TL}_{21}] = \texttt{ETREE (NODE}\ (\uparrow\downarrow [\mathrm{TL}_{12};\mathrm{TL}_{13};\mathrm{TL}_{14};\mathrm{TL}_{15};\mathrm{TL}_{16};\mathrm{TL}_{17};\mathrm{TL}_{18};\mathrm{TL}_{19};\mathrm{TL}_{20}]) \otimes_{\mathrm{L}}^{\mathcal{N}} (\uparrow\downarrow [\mathrm{TL}_{21}]))$$

Definition 15:

$$\vdash \texttt{IEEE\_118\_BUS\_COMPLETE\_ET\_LOAD\_C}\ [\mathrm{TL}_{22};\mathrm{TL}_{23};\mathrm{TL}_{24};\mathrm{TL}_{25};\mathrm{TL}_{26};\mathrm{TL}_{27};\mathrm{TL}_{28};\mathrm{TL}_{29};\mathrm{TL}_{30};\mathrm{TL}_{31};\mathrm{TL}_{32}]\ [\mathrm{TL}_{33}] = \texttt{ETREE (NODE}\ (\uparrow\downarrow [\mathrm{TL}_{22};\mathrm{TL}_{23};\mathrm{TL}_{24};\mathrm{TL}_{25};\mathrm{TL}_{26};\mathrm{TL}_{27};\mathrm{TL}_{28};\mathrm{TL}_{29};\mathrm{TL}_{30};\mathrm{TL}_{31};\mathrm{TL}_{32}]) \otimes_{\mathrm{L}}^{\mathcal{N}} (\uparrow\downarrow [\mathrm{TL}_{33}]))$$

Step 2: The complete ET models of all loads A, B, and C, obtained above, can be reduced in the sense that the irrelevant paths are removed to model the exact logical behavior of the electrical grid system and reduced the number of test cases. To have a clear understanding, consider the generation of nuclear power plants (G_1–G_9) are installed with a full capacity of 4000 MW/generator and the demand for loads A, B, and C is 2400 MW/load [32]. Assuming the generators and the transmission lines (TL_1–TL_{33}) are loaded to 90% and 70% of their full capacity, respectively, so that if a sudden TL failure occurs and one of the generators is cutoff, then the power utility can utilize the reservoir in other generators along with the full capacity loading of other TLs to apply around 15% *load-shedding* [33] only, but the failure of two main TLs causes a complete load shutdown, and thereupon the electric utility can maintain the stability [34] of the rest of the power grid and prevent the whole grid to be subject to an undesirable complete blackout. For instance, the ET paths of both TL_{22} and TL_{23} fail for load C is equal to the probabilities of TL_{22} and TL_{23} failures only regardless of the status of other TLs as load C is completely disconnected from the grid. Using our formal reduction properties presented in Section V, we can describe and verify all actual ET models of loads A (97 paths from 0 to 96), B (59 paths from 0 to 58), and C (81 paths from 0 to 80) [24]. For example, we can obtain the actual ET of the main TLs that affect load C, i.e., 80 ET paths out of a total of 4096 test cases (from 0 to 4095), in HOL4 as follows:

Definition 16:

$$\vdash \texttt{IEEE\_118\_BUS\_REDUCED\_ET\_LOAD\_C}\ [\mathrm{TL}_{22};\mathrm{TL}_{23};\mathrm{TL}_{24};\mathrm{TL}_{25};\mathrm{TL}_{26};\mathrm{TL}_{27};\mathrm{TL}_{28};\mathrm{TL}_{29};\mathrm{TL}_{30};\mathrm{TL}_{31};\mathrm{TL}_{32}]\ [\mathrm{TL}_{33}]\ \texttt{[[3072-4095];...]}\ \texttt{[[}\mathrm{TL}_{22}\downarrow;\ \mathrm{TL}_{23}\downarrow\texttt{];...]} = \texttt{ETREE (NODE}\ (\uparrow\downarrow [\mathrm{TL}_{22};\mathrm{TL}_{23};\mathrm{TL}_{24};\mathrm{TL}_{25};\mathrm{TL}_{26};\mathrm{TL}_{27};\mathrm{TL}_{28};\mathrm{TL}_{29};\mathrm{TL}_{30};\mathrm{TL}_{31};\mathrm{TL}_{32}]) \otimes_{\mathrm{L}}^{\mathcal{N}} (\uparrow\downarrow [\mathrm{TL}_{33}])) \boxtimes^{\mathcal{N}} \texttt{[3072-4095];...]}\ \texttt{[[}\mathrm{TL}_{22}\downarrow;\ \mathrm{TL}_{23}\downarrow\texttt{];...])}$$

Step 3: Typically, we are only interested in the occurrence of certain events in the ET models. For instance, a different

collection of the ET paths can be obtained by observing different failure levels for each load in the power grid as

1) $Prob_1(\text{Load}_A \lightning(\textit{Complete Failure} 100\%)) = \sum_{\text{ET}_{\text{Paths}}} (18, 20, 21, 23-25, 27-29, 30, 33-36, \ldots, 85, 87, 88-96)$
2) $Prob_2(\text{Load}_{A\lightning}(\textit{Load-Shedding}\ 15\%)) = \sum_{\text{ET}_{\text{Paths}}} (2, 3, 5, 8, 9, 11, 13, 14-17, 19, 31, 32, 37, \ldots, 78, 80, 82, 86)$
3) $Prob_3(\text{Load}_{B\lightning}(\textit{Complete Failure}\ 100\%)) = \sum_{\text{ET}_{Paths}} (5-8, 14-17, 23-26, 32-37, 42-47, 52-58)$
4) $Prob_4(\text{Load}_{B\lightning}(\textit{Load-Shedding}\ 15\%)) = \sum_{\text{ET}_{Paths}} (3, 4, 9-13, 18-22, 27-31, 38-41, 48-51)$
5) $Prob_5(\text{Load}_{C\lightning}(\textit{Complete Failure}\ 100\%)) = \sum_{\text{ET}_{\text{Paths}}} (14-18, 20-24, 26-31, 33-40, 42, 43, \ldots, 70, 72-80)$
6) $Prob_6(\text{Load}C_{\lightning}(\textit{Load-Shedding}\ 15\%)) = \sum_{\text{ET}_{\text{Paths}}} (1-3, 5-7, 9-13, 19, 25, 32, 41, 44, 47, 51, 61, 65, 69, 71)$

B. Reliability Indices Assessment

We can determine the SAIFI and SAIDI and CAIDI, which are used by design engineers to indicate the average frequency and duration of customers experience a sustained outage. SAIFI is defined as the total number of customer interruptions (power outage $\lightning$) over the total number of customers served. SAIDI is defined as the sum of all customer interruption durations over the total number of customers served while CAIDI is defined as the sum of all customer interruption durations over the total number of customer interruptions indicating the average outage duration that any customer would experience [35]

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

$$\text{SAIDI} = \frac{\sum_{\mathcal{P}(\mathcal{X}_{\lightning})\times \text{MTTR}_{\mathcal{X}}\times \text{CN}_{\mathcal{X}}}}{\sum_{\text{CN}_{\mathcal{X}}}}, \quad \text{CAIDI} = \frac{\text{SAIDI}}{\text{SAIFI}} \tag{4}$$

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

SAIFI . We define a generic function SAIFI in HOL4 in three parts as follows:

Definition 17:

```
⊢ ∑_Load↯ L L_N N_N CE_N (E::E_N) (CN::CN_N) p =
(λa b.
prob p
(ETREE (NODE (a ⊞ (L ⊗_L^N L_N) ⊠^N N_N CE_N)))
   × b) E CN + ∑_Load↯ L L_N N_N CE_N E_N CN_N p
```

where L, $\text{L}_{\mathcal{N}}$, $\text{N}_{\mathcal{N}}$, $\text{CE}_{\mathcal{N}}$, $\text{E}_{\mathcal{N}}$, and $\text{CN}_{\mathcal{N}}$ are the lists of load TL modes, load last TL modes, complete cylinders, conditional events, events partitioning paths, and affected customer numbers, respectively. The function $\sum_{Load}\lightning$ represents the sum of multiplying the probabilities of failures at a certain load in the electrical 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). For multiple ET models corresponding to different loads in the transmission network, we define a generic function $\sum_{Grid}\lightning$ that recursively applies $\sum_{Load}\lightning$ on each load ET in the power grid to sum the total number of grid customer interruptions as follows:

Definition 18:

```
⊢ ∑_Grid↯ (L::L_All) (L_N::L_N_All) (N_N::N_N_All)
     (CE_N::CE_N_All) (E_N::E_N_All) (CN_N::CN_N_All) p =
  ∑_Load↯ L L_N N_N CE_N E_N CN_N p +
  ∑_Grid↯ L_All L_N_All N_N_All CE_N_All E_N_All CN_N_All p
```

Lastly, we can define the function SAIFI that represents the division of $\sum_{Grid}\lightning$ over the total number of customers, as described in (3) as follows:

Definition 19:

```
⊢ SAIFI L_All L_N_All N_N_All CE_N_All E_N_All CN_N_All p =
  ∑_Grid↯ L_All L_N_All N_N_All CE_N_All E_N_All CN_N_All p
  ─────────────────────────────────────────────────────────
                    ∑ CN_N_All
```

SAIDI: Similarly, we formally define a function $\sum_{Grid}^{T}\lightning$ in HOL4 to sum all grid customer interruption durations. Then, we formally define a function SAIDI by dividing the output of $\sum_{Grid}^{T}\lightning$ over the total number of customers served, as described in (4), in HOL4 as follows:

Definition 20:

```
⊢ SAIDI L_All L_N_All N_N_All CE_N_All E_N_All MTTR_N_All CN_N_All p
=
  ∑_Grid^T↯ L_All L_N_All N_N_All CE_N_All E_N_All MTTR_N_All CN_N_All p
  ──────────────────────────────────────────────────────────────────────
                          ∑ CN_N_All
```

where MTTR_{All} is the list of all MTTRs.

CAIDI : Lastly, we formally define a function CAIDI by dividing the output of SAIDI (Definition 20) over SAIFI (Definition 19), as described in (4), in HOL4 as follows:

Definition 21:

```
⊢ CAIDI L_All L_N_All N_N_All CE_N_All E_N_All MTTR_N_All CN_N_All p
=
  SAIDI L_All L_N_All N_N_All CE_N_All E_N_All MTTR_N_All CN_N_All p
  ─────────────────────────────────────────────────────────────────
  SAIFI L_All L_N_All N_N_All CE_N_All E_N_All CN_N_All p
```

The assessment of SAIFI and SAIDI for the Grid (G) shown in Fig. 4 can be written mathematically as

$$\text{SAIFI}_G = \frac{\begin{array}{l} Prob_1 \times \text{CN}_A + Prob_2 \times (15\%\ \text{CN}_A) + \\ Prob_3 \times \text{CN}_B + Prob_4 \times (15\%\ \text{CN}_B) + \\ Prob_5 \times \text{CN}_C + Prob_6 \times (15\%\ \text{CN}_C) \end{array}}{\text{CN}_A + \text{CN}_B + \text{CN}_C} \tag{5}$$

$$\text{SAIDI}_G = \frac{\begin{array}{l} Prob_1 \times \text{MTTR}_A \times \text{CN}_A + \\ Prob_2 \times \text{MTTR}_A \times (15\%\ \text{CN}_A) + \\ Prob_3 \times \text{MTTR}_B \times \text{CN}_B + \\ Prob_4 \times \text{MTTR}_B \times (15\%\ \text{CN}_B) + \\ Prob_5 \times \text{MTTR}_C \times \text{CN}_C + \\ Prob_6 \times \text{MTTR}_C \times (15\%\ \text{CN}_C) \end{array}}{\text{CN}_A + \text{CN}_B + \text{CN}_C} \tag{6}$$

In this article, we assumed that the failure and success states of all TLs in the 118-bus electrical power grid are continuous exponentially distributed [36], where the distribution is well known as *memoryless* and is routinely used in the reliability analysis of real-world power system applications to determine

the probability of failure ($\mathcal{P}(X \leq t)$) and the probability of success ($\mathcal{P}(X > t)$) for each system component over a time period of interest. This can be formalized in HOL4 as follows:

Definition 22:

```
⊢ EXPONENTIAL_ET_DISTRIB p X λ_X =
    ∀ t. 0 ≤ t ⇒ (CDF p X t = 1 - e^(-λ_X t))
```

where λ_X is the failure rate of the variable X and t is a time index. Using our new proposed ET probabilistic formulations (Section V-C), we can formally verify the above-expressions of SAIFI_G and SAIDI_G for the power grid, in HOL4 as follows:

Theorem 11:

```
⊢ SAIFI
   [↑↓ [TL_1;TL_2;TL_3;TL_4;TL_5;TL_6;
        TL_7;TL_8;TL_9;TL_10];
    ↑↓ [TL_12;TL_13;TL_14;TL_15;TL_16;
        TL_17;TL_18;TL_19;TL_20];
    ↑↓ [TL_22;TL_23;TL_24;TL_25;TL_26;
        TL_27;TL_28;TL_29;TL_30;TL_31;TL_32]]
   [↑↓ [TL_11]; ↑↓ [TL_21]; ↑↓ [TL_33]]
   [[[512-2048];...]; [[256-1023];...];
    [[3072-4095];...]]
   [[[TL_1 ↓; TL_2 ↓];...]; [[TL_12 ↓; TL_13 ↓];...];
    [[TL_22 ↓; TL_23 ↓];...]]
   [[[18,20,21,...,88-96];[2,3,5,...,80,82,86]];
    [[5-8,14-17,...,52-58];[3,4,...,48-51]];
    [[14-18,20-24,...,72-80];[1-3,5-7,...,71]]]
   [[CN_A; 15% CN_A]; [CN_B; 15% CN_B];
    [CN_C; 15% CN_C]] p =
```

$$\frac{\begin{array}{l}(\mathrm{e}^{(-\lambda_{TL_1}t)} \times \mathrm{e}^{(-\lambda_{TL_2}t)} \times \mathrm{e}^{(-\lambda_{TL_3}t)} \times \mathrm{e}^{(-\lambda_{TL_4}t)} \times \\ (1-\mathrm{e}^{(-\lambda_{TL_5}t)}) \times \mathrm{e}^{(-\lambda_{TL_6}t)} \times \mathrm{e}^{(-\lambda_{TL_7}t)} \times \\ (1-\mathrm{e}^{(-\lambda_{TL_8}t)}) \times (1-\mathrm{e}^{(-\lambda_{TL_9}t)}) + \ldots) \times \mathrm{CN}_A + \\ (\mathrm{e}^{(-\lambda_{TL_1}t)} \times \mathrm{e}^{(-\lambda_{TL_2}t)} \times \cdots \times \mathrm{e}^{(-\lambda_{TL_6}t)} \times \mathrm{e}^{(-\lambda_{TL_7}t)} \times \\ (1-\mathrm{e}^{(-\lambda_{TL_8}t)}) \times (1-\mathrm{e}^{(-\lambda_{TL_9}t)}) + \ldots) \times 15\%\ \mathrm{CN}_A + \\ (\mathrm{e}^{(-\lambda_{TL_{12}}t)} \times \mathrm{e}^{(-\lambda_{TL_{13}}t)} \times \mathrm{e}^{(-\lambda_{TL_{14}}t)} \times \mathrm{e}^{(-\lambda_{TL_{15}}t)} \times \\ \mathrm{e}^{(-\lambda_{TL_{18}}t)} \times (1-\mathrm{e}^{(-\lambda_{TL_{19}}t)}) + \ldots) \times \mathrm{CN}_B + \\ (\mathrm{e}^{(-\lambda_{TL_{12}}t)} \times \mathrm{e}^{(-\lambda_{TL_{13}}t)} \times \mathrm{e}^{(-\lambda_{TL_{14}}t)} \times (1-\mathrm{e}^{(-\lambda_{TL_{15}}t)}) \times \\ \mathrm{e}^{(-\lambda_{TL_{19}}t)} \times \cdots \times \mathrm{e}^{(-\lambda_{TL_{17}}t)} + \ldots) \times 15\%\ \mathrm{CN}_B + \\ (\mathrm{e}^{(-\lambda_{TL_{22}}t)} \times \mathrm{e}^{(-\lambda_{TL_{23}}t)} \times (1-\mathrm{e}^{(-\lambda_{TL_{24}}t)}) \times \\ (1-\mathrm{e}^{(-\lambda_{TL_{25}}t)}) + \ldots) \times \mathrm{CN}_C + \\ (\mathrm{e}^{(-\lambda_{TL_{22}}t)} \times (1-\mathrm{e}^{(-\lambda_{TL_{23}}t)}) \times \mathrm{e}^{(-\lambda_{TL_{24}}t)} \times \mathrm{e}^{(-\lambda_{TL_{25}}t)} \times \\ \mathrm{e}^{(-\lambda_{TL_{26}}t)} \times \cdots \times \mathrm{e}^{(-\lambda_{TL_{33}}t)} + \ldots) \times 15\%\ \mathrm{CN}_C\end{array}}{\mathrm{CN}_A + \mathrm{CN}_B + \mathrm{CN}_C}$$

Theorem 12:

```
⊢ SAIDI
   [↑↓ [TL_1;TL_2;TL_3;TL_4;TL_5;TL_6;
        TL_7;TL_8;TL_9;TL_10];
    ↑↓ [TL_12;TL_13;TL_14;TL_15;TL_16;
        TL_17;TL_18;TL_19;TL_20];
    ↑↓ [TL_22;TL_23;TL_24;TL_25;TL_26;
        TL_27;TL_28;TL_29;TL_30;TL_31;TL_32]]
   [↑↓ [TL_11]; ↑↓ [TL_21]; ↑↓ [TL_33]]
   [[[512-2048];...]; [[256-1023];...];
    [[3072-4095];...]]
   [[[TL_1 ↓; TL_2 ↓];...]; [[TL_12 ↓; TL_13 ↓];...];
    [[TL_22 ↓; TL_23 ↓];...]]
   [[[18,20,21,...,88-96];[2,3,5,...,80,82,86]];
    [[5-8,14-17,...,52-58];[3,4,...,48-51]];
    [[14-18,20-24,...,72-80];[1-3,5-7,...,71]]]
   [MTTR_A; MTTR_B; MTTR_C]
   [[CN_A; 15% CN_A]; [CN_B; 15% CN_B];
    [CN_C; 15% CN_C]] p =
```

$$\frac{\begin{array}{l}(\mathrm{e}^{(-\lambda_{TL_1}t)} \times \mathrm{e}^{(-\lambda_{TL_2}t)} \times \mathrm{e}^{(-\lambda_{TL_3}t)} \times \mathrm{e}^{(-\lambda_{TL_4}t)} \times \\ (1-\mathrm{e}^{(-\lambda_{TL_5}t)}) \times \mathrm{e}^{(-\lambda_{TL_6}t)} \times \mathrm{e}^{(-\lambda_{TL_7}t)} \times \\ (1-\mathrm{e}^{(-\lambda_{TL_8}t)}) \times (1-\mathrm{e}^{(-\lambda_{TL_9}t)}) + \ldots) \times \mathrm{MTTR}_A \times \mathrm{CN}_A + \\ (\mathrm{e}^{(-\lambda_{TL_1}t)} \times \mathrm{e}^{(-\lambda_{TL_2}t)} \times \cdots \times \mathrm{e}^{(-\lambda_{TL_7}t)} \times (1-\mathrm{e}^{(-\lambda_{TL_8}t)}) \times \\ (1-\mathrm{e}^{(-\lambda_{TL_9}t)}) + \ldots) \times \mathrm{MTTR}_A \times 15\%\mathrm{CN}_A + \\ (\mathrm{e}^{(-\lambda_{TL_{12}}t)} \times \mathrm{e}^{(-\lambda_{TL_{13}}t)} \times \mathrm{e}^{(-\lambda_{TL_{14}}t)} \times \mathrm{e}^{(-\lambda_{TL_{15}}t)} \times \\ \mathrm{e}^{(-\lambda_{TL_{18}}t)} \times (1-\mathrm{e}^{(-\lambda_{TL_{19}}t)}) + \ldots) \times \mathrm{MTTR}_B \times \mathrm{CN}_B + \\ (\mathrm{e}^{(-\lambda_{TL_{12}}t)} \times \mathrm{e}^{(-\lambda_{TL_{13}}t)} \times \mathrm{e}^{(-\lambda_{TL_{14}}t)} \times (1-\mathrm{e}^{(-\lambda_{TL_{15}}t)}) \times \\ \mathrm{e}^{(-\lambda_{TL_{19}}t)} \times \cdots \times \mathrm{e}^{(-\lambda_{TL_{17}}t)} + \ldots) \times \mathrm{MTTR}_B \times 15\%\mathrm{CN}_B + \\ (\mathrm{e}^{(-\lambda_{TL_{22}}t)} \times \mathrm{e}^{(-\lambda_{TL_{23}}t)} \times (1-\mathrm{e}^{(-\lambda_{TL_{24}}t)}) \times \\ (1-\mathrm{e}^{(-\lambda_{TL_{25}}t)}) + \ldots) \times \mathrm{MTTR}_C \times \mathrm{CN}_C + \\ (\mathrm{e}^{(-\lambda_{TL_{22}}t)} \times (1-\mathrm{e}^{(-\lambda_{TL_{23}}t)}) \times \mathrm{e}^{(-\lambda_{TL_{24}}t)} \times \mathrm{e}^{(-\lambda_{TL_{25}}t)} \times \\ \mathrm{e}^{(-\lambda_{TL_{26}}t)} \times \cdots \times \mathrm{e}^{(-\lambda_{TL_{33}}t)} + \ldots) \times \mathrm{MTTR}_C \times 15\%\mathrm{CN}_C\end{array}}{\mathrm{CN}_A + \mathrm{CN}_B + \mathrm{CN}_C.}$$

Using Theorems 11 and 12, we can also verify the CAIDI index for the electrical grid [24]. In order to maximize the exploitation of our proposed new formulations by the reliability engineers, in the next section, we defined a couple of standard meta language (SML) functions that can numerically evaluate the above-verified expressions of reliability indices SAIFI, SAIDI, and CAIDI of the 118-bus electrical power grid. In order to ensure the accuracy of our computations, in the sequel, we compare our results with those obtained by the commercial Isograph ET software, by manual paper-and-pencil analysis and by MATLAB MCS.

VII. Experimental Results and Discussion

Considering the failure rates λ_{TL_1}-λ_{TL_4}, λ_{TL_5}-λ_{TL_8}, λ_{TL_9}-$\lambda_{TL_{11}}$, $\lambda_{TL_{12}}$-$\lambda_{TL_{15}}$, $\lambda_{TL_{16}}$-$\lambda_{TL_{18}}$, $\lambda_{TL_{19}}$-$\lambda_{TL_{21}}$, $\lambda_{TL_{22}}$-$\lambda_{TL_{25}}$, $\lambda_{TL_{26}}$-$\lambda_{TL_{29}}$, $\lambda_{TL_{30}}$-$\lambda_{TL_{33}}$ are 0.2, 0.5, 0.3, 0.25, 0.4, 0.15, 0.35, 0.29, 0.45 per year with an average MTTR of 30 hours [30]. Also assuming the number of customers CN_A, CN_B, and CN_C to be 12 000, 9000, and 11 000 customers, respectively. The reliability study is undertaken for five years, i.e., $t = (8760 \times 5)$ hours. Based on the given data, we can evaluate SAIFI, SAIDI, and CAIDI for the 118-bus grid (see Fig. 4) using: 1) SML functions; 2) Isograph software; 3) MATLAB MCS; 4) paper-and-pencil.

1) *SML functions:* We define SML functions [24], which can numerically evaluate the *verified* HOL4 expressions of SAIFI, SAIDI, and CAIDI, as shown in Fig. 6.

```
val it = (): unit
> SAIFI for 5 Years = 0.6569484469 Interruptions / System Customer
val it = (): unit
> SAIDI for 5 Years = 19.708453419 Hours / System Customer
val it = (): unit
> CAIDI for 5 Years = 30.0 Hours / Customer Interruption
*** Emacs/HOL command completed ***
U:**-  *HOL*          Bot L1585  (Comint:run +1)
```

Fig. 6. SML functions: SAIFI, SAIDI, and CAIDI results.

2) *Isograph software:* The commercial Isograph ET analysis software provides many powerful features, including user-friendly editors and the coloring of diagram elements for easier viewing [11]. It is important to mention that Isograph requires from the user to manually draw the actual ET model based on *two-states* only of each system component (*success or failure*). After that, the user has to assign the probability of each branch failure event $\mathcal{P}(X_F)$ and Isograph calculates automatically the probability of the other success branch (1 - $\mathcal{P}(X_F)$). Finally, the consequences of all paths, i.e., no load fails, all loads fail, etc., should be added by the user. After running the ET model, Isograph calculates the probability of each individual path and the frequency of each path occurrence. However, the important feature of partitioning an ET with respect to an event occurrence (*Step 3* in Fig. 3) and then to calculate its corresponding probability is not available in Isograph or any other ET analysis tool. For that reason, we used the manual calculation for evaluating the paths probabilities that represent the occurrence of the load failure events.
3) *MATLAB MCS:* Using the MATLAB software based on a random-based MCS algorithm, we can examine and predict the real behavior patterns to estimate the expected or average value of the various reliability indices. The steps followed in this technique are as [37] follows.
   a) Read the values of failure rate λ in *f/hours* and repair time *r* in hours for each component.
   b) Generate a random number *U*.
   c) Calculate the predicted next time to fail (*TTF*) and time to repair (*TTR*) from the equations

$$TTF = \frac{-\ln U}{\lambda} \quad TTR = \frac{-\ln U}{r}. \tag{7}$$

   d) Repeat the above iterative process till the number of iterations exceeds 1e5 or the variance σ is less than 1e-5.

It is evident from the above description that the MCS technique is depending on the sampling approach. Therefore, we obtain different results of SAIFI, SAIDI, and CAIDI reliability indices every run of the algorithm depending on the generated random number with a tolerance error between 4%–9%. Plots of the estimates are extremely valuable and are one of the significant merits of MCS. So, for example, Fig. 7 shows the best estimated results of SAIFI in MATLAB for the electrical power grid system based on the MCS approach with the least errors.

A comparison between all techniques, i.e., SML functions, Isograph software, MATLAB MCS, and manual analysis, in the assessment of different reliability indices SAIFI (Interruptions/Customer), SAIDI (Hours/Customer), and CAIDI (Hours/Customer Interruption) for the 118-bus electrical power grid system is presented in Table II.

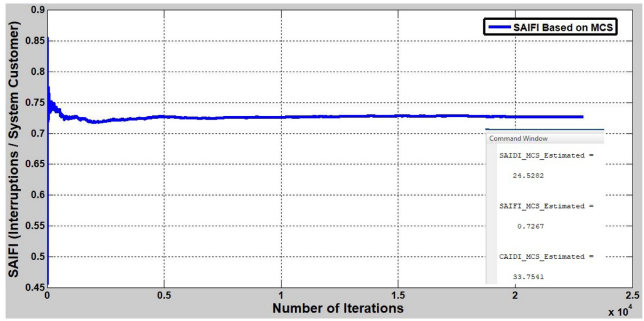

Fig. 7. MATLAB MCS: SAIFI result.

TABLE II
COMPARISON OF SAIFI, SAIDI, AND CAIDI

Power Grid Indices	Manual Analysis	Isograph Analysis	MATLAB Analysis	HOL4 Analysis
SAIFI	0.65695	0.6579	0.7267	0.656948446
SAIDI	19.70845	19.8592	24.5282	19.708453419
CAIDI	29.99991	30.1857	33.7541	30.000000000
CPU Time (Seconds)	–	47.205	153.916	9.477

It can be noticed that the reliability indices SAIFI, SAIDI, and CAIDI of the 118-bus electrical power grid system obtained from our analysis are approximately equivalent to the corresponding ones calculated using the Isograph ET software tool and our manual paper-and-pencil ET analysis. Note that during the manual analysis and due to the large size of the case study, some errors that we inadvertently made were caught through one-to-one comparison with the HOL4 verified results. On the other hand, MATLAB MCS uses a random-based algorithm, which estimates different results of SAIFI, SAIDI, and CAIDI at every generation of a random number with errors between 4%–9%. This clearly elucidates that our analysis is not only providing the correct results but also *formally proven* reliability expressions (Theorems 11 and 12) compared to existing techniques. Therefore, our proposed approach provides the *first mechanical computation* of ET probabilities ever, augmented with the rigor of the HOL4 theorem prover for accurate system-level reliability analysis. Moreover, the CPU time for the 118-bus electrical power grid system using the SML functions is much faster than Isograph (5X) and MATLAB MCS (15X), as shown in Table II. The experiments were performed on core i5, 2.20 GHz, running under Linux VM with 1 GB of RAM.

In a nutshell, by applying our formal ET step-analysis on a standard 118-bus electric grid system and obtaining its reliability indices SAIFI, SAIDI, and CAIDI, we showed the *practical validation* of our proposed methodology in the HOL4 theorem prover, which will help electrical power planners/designers to accurately quantify electric power grid reliability improvements and satisfy the total required demand within acceptable risk levels. Moreover, our approach can be used in-conjunction with the existing power system reliability analysis softwares to provide a validation of their SAIFI, SAIDI, and CAIDI results. Also, our proposed methodology can be used to analyze larger scale ET models of other complex power system applications, such

as microgrids connected and synchronized with the centralized power grid (macrogrid) [38], and smart grids [39].

VIII. Conclusion

In this article, we described the HOL4 formalization of ETs step-analysis using a generic *list* data-type. We defined the `NODE` and `BRANCH` concepts, which can be used to model an arbitrary level of ET diagram consisting of $\mathcal{N}$ system components. We developed a formal approach to reduce ET branches and partition ET paths based on the occurrence of certain events. Also, our proposed approach provides new mathematical formulations that can perform ET probabilistic analysis of *multistate* system components and based on any given probabilistic distribution, which are features not existing in any other ET commercial tool. In order to check the correctness of the proposed equations, we have verified them using the HOL4 theorem prover. The proposed ET formalization enables safety engineers to perform different levels of ET reliability/failure analysis for safety-critical systems, such as smart power grids, within the sound environment of HOL4. For illustration purposes, we conducted the formal ET analysis of a standard 118-bus electrical power grid system and also verified its reliability indices SAIFI, SAIDI, and CAIDI. We also compared our formal analysis results with those obtained from commonly used approaches, including paper-and-pencil analysis, MATLAB MCS, and a commercial software tool. As a future work, we plan to formalize functional block diagrams (FBD) [23], which enable us to perform ET analysis for hierarchical systems with $\mathcal{N}$ subsystem levels. Therefore, we can *verify* complete/partial reliability and failure consequence expressions at the subsystem level corresponding to the given complex critical-system description, based on our proposed ET formalization in the HOL4 theorem prover.

References

[1] A. Keyhani and M. Albaijat, *Smart Power Grids*. New York, NY, USA: Springer-Verlag, 2012.

[2] S. Ili, A. Albers, and S. Miller, "Open innovation in the automotive industry," *RD Manage.*, vol. 40, no. 3, pp. 246–255, 2010.

[3] R. E. Mackiewicz, "Overview of IEC 61850 and benefits," in *Proc. Power Syst. Conf. Expo.*, 2006, pp. 623–630.

[4] R. Palin, D. Ward, I. Habli, and R. Rivett, "ISO 26262 safety cases: Compliance and assurance," in *Proc. IET Conf. System Saf.*, 2011, pp. 1–6.

[5] M. Bozzano and A. Villafiorita, *Design and Safety Assessment of Critical Systems*. Boca Raton, FL, USA: Auerbach Publications, 2010.

[6] M. Towhidnejad, D. R. Wallace, and A. M. Gallo, "Fault tree analysis for software design," in *Proc. 27th NASA Goddard Softw. Eng. Workshop*, 2002, pp. 24–29.

[7] A. Brall, W. Hagen, and H. Tran, "Reliability block diagram modeling-comparisons of three software packages," in *Proc. Rel. Maintainability Symp.*, 2007, pp. 119–124.

[8] I. A. Papazoglou, "Mathematical foundations of event trees," *Rel. Eng. Syst. Saf.*, vol. 61, no. 3, pp. 169–183, 1998.

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

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

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

[12] V. Muzik and Z. Vostracky, "Possibilities of event tree analysis method for emergency states in power grid," in *Proc. Elect. Power Eng. Conf.*, 2018, pp. 1–5.

[13] D. E. Peplow, C. D. Sulfredge, R. L. Sanders, R. H. Morris, and T. A. Hann, "Calculating nuclear power plant vulnerability using integrated geometry and event/fault-tree models," *Nucl. Sci. Eng.*, vol. 146, no. 1, pp. 71–87, 2004.

[14] B. H. Ku and J. M. Cha, "Reliability assessment of Catenary of Electric railway by using FTA and ETA analysis," in *Proc. Environ. Elect. Eng.*, 2011, pp. 1–4.

[15] W. Li, *Reliability Assessment of Electric Power Systems Using Monte Carlo Methods*. New York, NY, USA: Springer-Verlag, 2013.

[16] O. Nývlt and M. Rausand, "Dependencies in event trees analyzed by petri nets," *Rel. Eng. System Saf.*, vol. 104, pp. 45–57, 2012.

[17] O. Hasan and S. Tahar, "Formal verification methods," in *Encyclopedia of Information Science and Technology*. Hershey, PA, USA: IGI Global, 2015, pp. 7162–7170.

[18] J. Van Benthem and K. Doets, "Higher-order logic," *Handbook Philos. Log.*, vol. 1, pp. 189–243, 2001.

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

[20] J. J. Grainger and W. D. Stevenson, *Power System Analysis*. New York, NY, USA: McGraw-Hill, 2003.

[21] O. Hasan, N. Abbasi, B. Akbarpour, S. Tahar, and R. Akbarpour, "Formal reasoning about expectation properties for continuous random variables," in *Formal Methods (Series LNCS 5850)*. New York, NY, USA: Springer, 2009, pp. 435–450.

[22] L. R. Olsen, J. A. Kay, and M. Van Krey, "Enhanced safety features in motor control centers and drives for diagnostics and troubleshooting," in *Proc. IAS Elect. Saf.*, 2015, pp. 1–9.

[23] I. A. Papazoglou, "Functional block diagrams and automated construction of event trees," *Rel. Eng. Syst. Saf.*, vol. 61, no. 3, pp. 185–214, 1998.

[24] M. Abdelghany, "Formalization of Event Trees: HOL4 Script," 2020. [Online]. Available: https://github.com/hvg-concordia/ET

[25] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart grid-the new and improved power grid: A survey," *IEEE Commun. Surveys Tut.*, vol. 14, no. 4, pp. 944–980, Fourth Quarter 2012.

[26] R. Karki, R. Billinton, and A. K. Verma, *Reliability Modeling and Analysis of Smart Power Systems*. New York, NY, USA: Springer-Verlag, 2014.

[27] E. C. Portante, S. F. Folga, J. A. Kavicky, and L. T. Malone, "Simulation of the September 8, 2011, San Diego Blackout," in *Proc. Winter Simul. Conf.*, 2014, pp. 1527–1538.

[28] S. Xu, Y. Qian, and R. Q. Hu, "On reliability of smart grid neighborhood area networks," *IEEE Access*, vol. 3, pp. 2352–2365, 2015.

[29] R. N. Allan, *Reliability Evaluation of Power Systems*. New York, NY, USA: Springer-Verlag, 2013.

[30] I. Pena, B. Martinez-Anido, and B. Hodge, "An extended IEEE 118-bus test system with high renewable penetration," *IEEE Trans. Power Syst.*, vol. 33, no. 1, pp. 281–289, Jan. 2018.

[31] V. Yadav and P. Ghoshal, "Optimal power flow for IEEE 30 and 118-bus systems using Monarch Butterfly optimization," in *Proc. Technol. Smart-City Energy Secur. Power*, 2018, pp. 1–6.

[32] R. Billinton and R. Allan, *Reliability Assessment of Large Electric Power Systems*. New York, NY, USA: Springer-Verlag, 2012.

[33] M. Marzband *et al.*, "Adaptive load shedding scheme for frequency stability enhancement in microgrids," *Elect. Power Syst. Res.*, vol. 140, pp. 78–86, 2016.

[34] D. Gan, R. J. Thomas, and R. D. Zimmerman, "Stability-constrained optimal power flow," *IEEE Trans. Power Syst.*, vol. 15, no. 2, pp. 535–540, May 2000.

[35] Y. G. Hegazy and M. A. Mostafa, "Reliability indices of electrical distributed generation systems," *IEEE Trans. Power Syst.*, vol. 4, no. 10, pp. 1785–1790, Aug. 2005.

[36] M. Çepin, *Assessment of Power System Reliability: Methods and Applications*. New York, NY, USA: Springer-Verlag, 2011.

[37] A. K. Pradhan *et al.*, "Implementation of Monte Carlo simulation to the distribution network for its reliability assessment," in *Innovation in Electrical Power Engineering, Communication, and Computing Technology*. New York, NY, USA: Springer, 2020, pp. 219–228.

[38] O. Egbue, D. Naidu, and P. Peterson, "The role of microgrids in enhancing macrogrid resilience," in *Proc. IEEE Smart Grid Clean Energy Technol.*, 2016, pp. 125–129.

[39] G. Boroojeni, H. Amini, and S. Iyengar, "Reliability in smart grids," in *Smart Grids: Security and Privacy Issues*. New York, NY, USA: Springer, 2017, pp. 19–29.