Reliability Analysis of Smart Grids Using Formal Methods

Mohamed Abdelghany and Sofiène Tahar

Contents

1 Introduction . . . 2
1.1 Reliability Modeling Methods . . . 3
1.2 Reliability Analysis Methods . . . 4
2 Problem Statement . . . 5
3 Proposed Solution . . . 5
4 State of the Art . . . 6
4.1 Event Tree Reliability Analysis . . . 6
4.2 Cause-Consequence Diagram Reliability Analysis . . . 7
4.3 Functional Block Diagram Reliability Analysis . . . 8
4.4 Monte Carlo Simulation Reliability Analysis . . . 8
4.5 Reliability Analysis in HOL4 Theorem Proving . . . 9
4.6 Formal Reliability Analysis of Smart Power Grids . . . 10
5 Proposed Methodology . . . 11
6 Smart Grid Power System Applications . . . 12
7 Conclusions . . . 15
References . . . 15

Abstract

Smart grids (SG) are complex integrated electric networks, where failures in any zone of the network can cause widespread catastrophic disruption of supply. In recent years, there has been a significant proliferation in the use of renewable energy sources, such as wind/solar systems, for SG power generation due to global warming, pollution, as well as economic and energy security concerns. However, the main obstacle that these energy systems face is their intermittent

M. Abdelghany (✉) · S. Tahar
Department of Electrical and Computer Engineering, Concordia University, Montreal, QC, Canada
e-mail: m_eldes@ece.concordia.ca; tahar@ece.concordia.ca

M. Fathi et al. (eds.), *Handbook of Smart Energy Systems*,
https://doi.org/10.1007/978-3-030-72322-4_81-1

nature, which greatly affects their ability to deliver constant power to the grid. While this raises several reliability-related concerns, 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. Therefore, in this chapter, we propose a novel approach that uses formal methods for the accurate and sound reliability analysis of SG systems. This new methodology overcomes the incompleteness of simulation-based analysis and the error-proneness of manual mathematical analysis. In particular, we use higher-order logic (HOL) theorem proving, which is a computer-based mathematical reasoning tool, where we developed a library of fundamental concepts of reliability analysis techniques, such as event trees, functional block diagrams, and cause-consequence diagrams. This library allowed us to conduct formal system-/subsystem-level reliability analysis and determine absolute accuracy of important SG reliability indices, such as system/customer average interruption frequency and duration (SAIFI, SAIDI, and CAIDI), as well as energy indices, such as Energy not Supplied Index (ENS) and loss of energy expectation (LOEE). In order to demonstrate the effectiveness of our proposed methods, we conducted the formal system-/subsystem-level reliability analysis of the standard IEEE 3/39/118-bus electrical power generation/transmission/distribution networks. The results of the proposed formal analysis are extremely useful for the electrical power planners/designers to accurately quantify SG reliability improvements and satisfy the total demand within acceptable risk levels.

Keywords

Power system reliability · Smart grids · Renewable energy resources · Formal methods · SAIFI · SAIDI · CAIDI · ENS · LOLE · LOEE

1 Introduction

Due to the complex and integrated nature of real-world smart grids (SG) (Keyhani and Albaijat 2012), as shown in Fig. 1, failures in any part of the network can cause catastrophic accidents, such as severe damage of expensive equipment, serious injury to people, and huge economic loss. Therefore, the central safety inquiry in SG power systems is to identify all possible risk consequences given that one or more sudden events could happen at system/subsystem level. Spare or redundant critical components in highly critical SGs have been inbuilt in order to ensure adequate and acceptable continuity of power service without failures. However, major discussion points regarding reliability during the decision-making process at critical design stage are as follows (Bucher et al. 2013): (1) How much redundancy and at what cost? (2) Should the reliability be increased, maintained at existing levels, or allowed to degrade? (3) On what accuracy should the decision be made? It is evident that reliability and economics are related to each other, as shown in Fig. 2a (Allan 2013), i.e., increased investment ΔC, is required in order to improve

reliability ΔR. The increment cost of reliability $\Delta C/\Delta R$ is one of the ways of deciding whether an investment in the SG power system is worth it or not. The basic concept of reliability-cost/reliability-worth assessment can be presented by the cost/reliability curves, as shown in Fig. 2b (Allan 2013). It can be observed that as reliability increases, the investment cost generally increases, while the consumer costs associated with failures decrease. From the reliability analysis of SGs, we can obtain an *optimum* target level of reliability and costs, as shown in Fig. 2b (Allan 2013). Therefore, to make decision-making of the optimal design for a specific SG power system, planners/designers require a probabilistic risk assessment at the critical design stage.

1.1 Reliability Modeling Methods

Since the late 1960s, various types of reliability modeling methods (Čepin 2011) have been developed to determine the probabilistic risk assessment of SG power systems. These include predominantly graph theory-based approaches such as fault trees (FT) (Javadi et al. 2011), reliability block diagrams (RBD) (Boussahoua and Elmaouhab 2019), event trees (ET) (Muzik and Vostracky 2018), cause-consequence diagrams (CCD) (Andrews and Ridley 2002), and functional block diagrams (FBD) (Papazoglou 1998a), as shown in Fig. 3. FTs mainly provide a graphical model, using logic gates OR/AND/NOT, for analyzing the factors causing a complete SG system failure upon their occurrences only (see Fig. 3). On the other hand, RBDs provide a schematic structure, using series/parallel configurations, for analyzing the success relationships of SG system components that keep the entire power system reliable only (Fig. 3). In contrast to FTs and RBDs, ETs provide

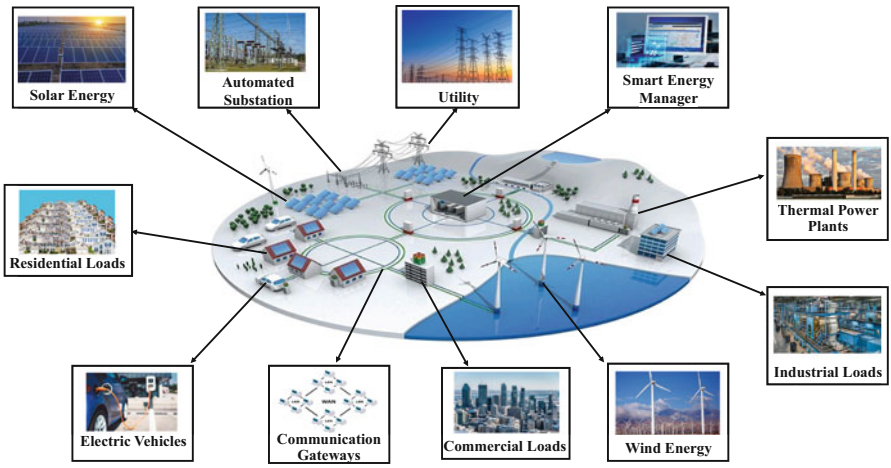


Fig. 1 A smart grid power system

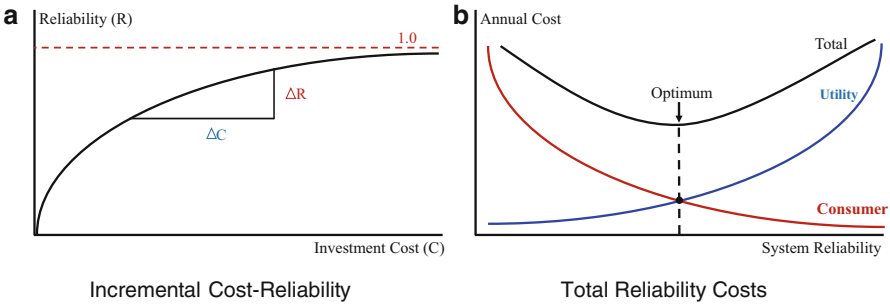


Fig. 2 Smart grid cost-reliability relationship. (**a**) Incremental cost reliability. (**b**) Total reliability costs

a complete risk tree model for all possible complete/partial failure and success-consequence scenarios at the system level simultaneously so that one of these possible sudden events can occur in the entire SG system, as shown in Fig. 3. More recently, an approach has been proposed to conduct ET analysis in conjunction with FTs to identify all subsystem failure events in a critical SG system and their cascading dependencies on the entire power network. This analysis method is known as cause-consequence analysis, using a combined hierarchical structure of cause-consequence diagrams (CCD), as shown in Fig. 3. Moreover, ET analysis can be used to associate failure and success events with all subsystems of the safety-critical SG power grid in more complex hierarchical structures, such as functional block diagrams (FBD). An FBD (Fig. 3) is a graphical representation of the detailed SG functionality and the functional relationship between all its subsystems (i.e., generation, transmission, and distribution) that are represented as functional blocks (FB). All subsystem-level ETs associated with their corresponding FBs are then composed together to build a subsystem-level ET model of a given smart power grid system under reliability study. Therefore, the probabilistic risk assessment of the occurrence of consequence accident events using ETs/CCDs/FBDs can be used for all required system-/subsystem-level improvements and satisfy the total reliability demand within acceptable risk levels.

1.2 Reliability Analysis Methods

The reliability analysis of SG power systems can be calculated using a variety of methods, among them analytically based paper-and-pencil methods and sampling-based Monte Carlo simulation (MCS) methods being the most popular. The former one represents the system by a mathematical model and evaluates the reliability indices from this model manually using direct numerical solutions. However, when real-world smart power grids with complex operating procedures have to be modeled, the resulting analysis can therefore lose some of its significance due to the possibility of human error-proneness, and it was a very cumbersome

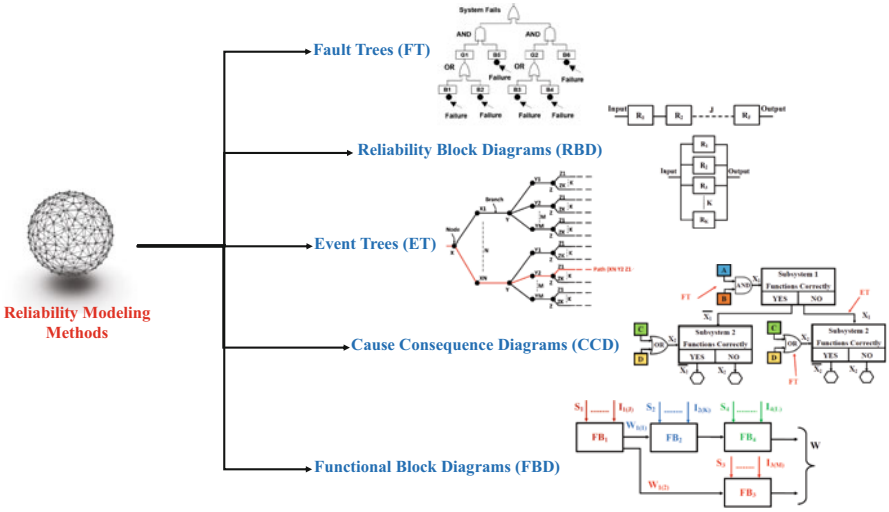


Fig. 3 Reliability modeling methods of smart grid power systems

effort to perform reliability analysis manually. For that reason, many of designers use sampling-based MCS approach for faster computation, which uses random algorithms to predict the real functional behavior of critical SG systems and estimate the average value of reliability parameters.

2 Problem Statement

The existing analysis methods for reliability assessment of critical SG systems compromise the accuracy or completeness of the reliability parameter evaluation during the design stage. Therefore, this could lead to undesirable inaccuracies in the obtained risk results, which can be deemed fatal for SG power systems that consequently could lead to the occurrence of unexpected sudden failures. The smallest error in the safety-critical smart power grids can cause disastrous consequences in human lives as well as huge financial losses. A more accurate and safer way to the error-prone informal reasoning of the predictive reliability evaluation would be the use of formal mathematical verification as per recommendations of safety standards, such as IEC 61850 (Mackiewicz 2006) and ISO 26262 (Palin et al. 2011).

3 Proposed Solution

In this chapter, we propose a novel approach that uses formal methods (Hasan and Tahar 2015), based on theorem proving, for accurate and sound ET-/FBD-/CCD-based reliability analysis of large-scale SG systems. The proposed formal

analysis technique allows us to perform a predictive verification of all possible SG system-/subsystem-level failure and reliability probabilistic risk expressions simultaneously. Theorem proving is a formal verification technique (Hasan and Tahar 2015), which is used for conducting the proof of mathematical theorems constructed in higher-order logic (HOL) (Hasan and Tahar 2015) based on computerized proof tools, called theorem provers. In particular, we use HOL4, which is a well-known interactive theorem prover with the ability of verifying a wide range of mathematical HOL expressions. The main advantage of using HOL formulation form is that all defined functions and verified theorems are *generic*, which allow us to use them for any given input system data and for $\mathcal{N}$ system components. Moreover, the main characteristic of HOL4 is that its core consists only of a few axioms and inference rules and any further theorem should be verified based on proven theorems. This ensured the soundness of the SG system model analysis. Moreover, since the system properties are proven mathematically within HOL4, no approximation is involved in the analysis results. These features make HOL4 suitable for carrying out the reliability analysis of the safety-critical SG power systems, which require sound verification results. To the best of our knowledge, this is the first work that develops a library for the mathematical modeling and reasoning framework of system-/subsystem-level consequence risk analysis (based on ETs, FBDs, and CCDs) using HOL4 and that uses library on real-world SG power system applications, where we provide significant improvements compared to all existing reliability analysis methods in terms of scalability, expressiveness, accuracy, and time.

4 State of the Art

In this section, we present all the related literature review and the proposed novel framework in this chapter.

4.1 Event Tree Reliability Analysis

Event tree (ET) reliability analysis has been developed in the mid-1970s (Rasmussen 1974) for the probabilistic risk assessment of all possible sudden accident risks that can occur in nuclear power plants in the generation sector of power systems. Then, in the late 1990s, Papazoglou in Papazoglou (1998b) was the first researcher to lay down the mathematical foundations of ETs to replace their graphical representation for probabilistic risk analysis of nuclear power plants. Since that time, many researchers have analyzed SG power systems using ETs for the probabilistic risk assessment at the design stage. For instance, Dialynas and Koskolos (1994) used ET analysis to model the operational consequence behavior of the high-voltage direct current (HVDC) power transmission system components as well as to deduct all possible system failure and reliability modes simultaneously. Muzik and Vostracky (2018) used the notion of ETs in analyzing

all emergency risk possibilities of a microgrid (MG) power system near the city of Pilsen, Czech Republic. Phulpin et al. in (2011), used the ET analysis results to improve the control strategy of HVDC transmission power flow and consequently the system sustainability aftermath of a large disturbance. In (2004), Peplow et al. used an ET diagram to evaluate the probability of all possible consequences of sudden accident events or terrorist attacks causing the contamination with radioactive material, which would make a large surrounding area uninhabitable for thousands of years. Ku and Cha, in (2011), used graph theory of ETs to determine some significant reliability indices of catenary of electric railways. However, the reliability analysis done in all the abovementioned work is done purely analytically based using a paper-and-pencil approach. A major limitation in the mathematical manual approach is the possibility of human error-proneness for large-scale real-world SG systems as well as the cumbersome effort and large amounts of time to perform the reliability analysis manually. On the other hand, there exist several commercial software tools for building the graph theory of ETs for probabilistic risk assessment of critical SG systems, such as ITEM (ITEM Software 2021) and Isograph (Isograph Software 2021). However, these commercial tools also require from the user to manually draw the ET model based on *two states* only of each component (*success or failure*) due to an explosion of outcome possible test cases. This limitation could be not suitable for real-world complex SG power systems that usually require to assign *multistates* of complete/partial failure and reliability events to each component.

4.2 Cause-Consequence Diagram Reliability Analysis

There exist some techniques that have been developed for subsystem-level reliability analysis of SG power systems. For instance, Papadopoulos et al. in (2011) have developed a software tool called *HiP-HOPS* (Hierarchically Performed Hazard Origin and Propagation Studies) for subsystem-level failure analysis to overcome classical manual failure analysis of complex SG systems and prevent human errors. HiP-HOPS can automatically generate the subsystem-level fault tree (FT) model and perform failure modes, effects, and critical analyses (FEMCA) from a given subsystem models, where each subsystem component is associated with its failure rate or failure probability (Papadopoulos et al. 2011). Currently, HiP-HOPS lacks the modeling of *multistate* system components and also cannot provide generic mathematical expressions that can be used to predict the reliability of an SG system based on any probabilistic distribution, like exponential/Weibull/Poisson (Kabir et al. 2019). Similarly, Jahanian in (2019) has proposed a new technique called failure mode reasoning (FMR) for identifying and quantifying the failure modes for SG power systems at the subsystem level. However, according to Jahanian (2019), the soundness of the FMR approach needs to be proven mathematically. On the other hand, cause-consequence diagram (CCD) reliability analysis typically uses FTs to analyze failures at the subsystem levels combined with an ET consequence diagram to integrate their cascading failure/reliability dependencies on the entire

system (Andrews and Ridley 2002). CCDs are categorized into two general methods for the ET linking process with the FTs (Čepin 2011): (1) small ET diagram and large subsystem level FT and (2) large ET diagram and small subsystem-level FT. Both methods are used for the probabilistic risk assessment of industrial applications. For example, Andrews and Ridley, in (2002), used the former method of CCD reliability analysis (i.e., small ET and large FTs) to determine all the probabilistic risk assessment of high-integrity protection systems (HIPS). Also Andrews, in (2001), used latter approach (i.e., large ET and small FTs) to determine all possible complete/partial failure and reliability events at the subsystem level of a pressure tank system that contains a motor control center (MCC) with a start-up and shutdown sequence in addition to its required operational phase. In (2006), Vyzaite et al. applied both methods the CCD method for reliability analysis of non-repairable phased missions at the subsystem level. However, the subsystem-level CCD reliability analysis done in all the abovementioned framework is done purely analytically based using a paper-and-pencil approach. This implies that it is very difficult to apply the manual CCD analysis on complex SG power systems, where planners/designers require n-level cause-consequence analysis corresponding to n-subsystems (i.e., n-level ET model and n-level FT models).

4.3 Functional Block Diagram Reliability Analysis

In the late 1990s, Papazoglou developed the fundamentals of FBD subsystem-level reliability analysis in Papazoglou (1998a) for more hierarchical ET structures, which is done purely analytically using the mathematical manual paper-and-pencil approach. For instance, Papakonstantinou et al., in (2013), used FBD analysis to determine all safety classes of a boiling water reactor (BWR) and steam turbine generator in a nuclear power plant generation system. Since that time, FBD analysis has not improved much due to the complexity that planners/designers are facing of building complex ET structure models manually during the design stage. A computer simulation program can be written in any modern language to automate the FBD reliability analysis proposed by Papazoglou. However, both of these analysis methods either lack detailed proof steps and are not scalable for *n-level* reliability analysis of real-world complex SG systems or use approximation algorithms for faster computation. Therefore, these approaches could introduce undesirable inaccuracies that can be deemed fatal for SG power systems.

4.4 Monte Carlo Simulation Reliability Analysis

Due to the limitations of the analytically mathematical manual approach, planners and designers started to consider sampling-based Monte Carlo simulation (MCS) for faster reliability analysis computation, which is built-in behind based on predictive consequence analysis using random algorithms to estimate the probability of failure and reliability (Allan 2013). For instance, in (1994), Billinton and

Sankarakrishnan used the random-based MCS to predict the reliability studies of a composite generation and transmission systems containing HVDC link. In (2001), Shelemy and Swatek used MCS to model of the performance of Manitoba Hydro Nelson River HVDC transmission lines. Bae et al., in (2012), proposed a technique to evaluate the reliability of distribution systems with multiple interconnected microgrids (MG) based on MCS. In (2013), Ranjbar used MCS-based reliability assessment method for reliability analysis of hybrid integrated MGs. In (2015), Shi and Bazzi applied MCS to determine the reliability of MGs for high penetration photovoltaic (PV) and wind turbine (WT) clean renewable energy systems. In Ansari et al. (2016), the authors used MCS to evaluate the reliability of smart power grids including various types of distributed green generation and energy storage systems (ESS) as well as prioritized loads to be supplied. Nanou et al., in (2016), used the MCS method to enhance power dispatch control under stochastic operating conditions for multiterminal HVDC transmission power grids. In (2000), Bevilacqua et al. used MCS to perform a predictive FEMCA analysis at the subsystem level of electrical power plants in a smart power grid. However, MCS-based reliability analysis approaches lack the rigor of detailed proof steps for reliability indices and may not be scalable for large-scale SG systems due to an explosion of the generated test cases, which requires a large amount of computing time. A more accurate and safer way to the error-prone informal reasoning of the predictive reliability evaluation would be the use of formal mathematical verification, which we propose in this chapter.

4.5 Reliability Analysis in HOL4 Theorem Proving

Only a few work have previously considered using formal methods for reliability analysis of SG power systems. For instance, Nỳvlt and Rausand in (2012) 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 (Nỳvlt and Rausand 2012). However, according to the same authors, they are not able to obtain verified expressions from the generated ET model (Nỳvlt and Rausand 2012). Ortmeier et al. in (2005) developed a framework for Deductive Cause-Consequence Analysis(DCCA) using a model checker SMV to verify the CCD proof obligations. However, according to the authors, there is a problem of showing the completeness of DCCA due to the exponential growth of the number of proof obligations with complex systems that need cumbersome proof efforts (Ortmeier et al. 2005). To overcome all the abovementioned limitations of existing analysis methods, we are proposing a novel approach of using theorem proving to obtain a verified system-/subsystem-level failure and reliability probabilistic expressions.

Prior to this work, proposed in this chapter, there were three notable projects for building formal infrastructures in HOL to formally model and analyze FTs and RBDs. For instance, Ahmad (2017) used the HOL4 theorem prover to formalize ordinary (static) FT and RBD structures. Elderhalli (2019) had formalized dynamic

versions of FTs and RBDs in HOL4. These formalizations have been used for the reliability analysis of several engineering systems. However, they formally analyze either a critical system static/dynamic failure or static/dynamic success only. Conversely, in this chapter, we developed a formally verified ET/CCD/FBD library in HOL4, which allowed us to a analyze all possible complete/partial failure and success-consequence risk events simultaneously at system and subsystem level, which makes our framework the first of its kind.

4.6 Formal Reliability Analysis of Smart Power Grids

Only a few researchers have recently considered using formal methods to analyze the reliability of SGs. For instance, Mahmood et al., in (2016), developed a framework for the reliability assessment of power grid components (Fang et al. 2011) with backup protection using the probabilistic model checker PRISM. Similarly, in (2013), Khurram et al. presented a foundational model for relay-based protected components in power distribution systems using the PRISM model checker. Also, in (2017), Sugumar et al. were the first to use formal analysis via the UPPAAL model checker (Larsen et al. 1997) to design and validate the energy management system (EMS) for a microgrid (MG) system that consists of high penetration of solar PV systems. Also, Sugumar et al., in (2019), used UPPAAL for the verification of a supervisory EMS, which provides much stronger confidence in the correctness of the EMS design than conventional approaches. Recently, Badings et al., in (2021), used model checking for the predictive verification of smart grids (SG) incorporating WTs and ESSs to overcome the need for sampling-based MCS and to be used by transmission system operator (TSO). However, all the abovementioned model-checking tools face a combinatorial blowup of the state space, commonly known as the state explosion problem (Hasan and Tahar 2015). Moreover, in (2017), Li et al. used the formal analysis, based on the continuous reachability analyzer (CORA) MATLAB toolbox, for the predictive verification of networked MG systems' stability in the presence of heterogeneous uncertainties induced by high penetration of RES generation. However, CORA has a limit of only providing probabilistic failure/reliability expressions of integrated $\mathcal{N}$ MGs at each MG component level.

On the other hand, theorem proving has been successfully utilized for the formal reliability analysis of smart power grids. For instance, Ahmad et al. in (2020a) used theorem proving to generate a capacity outage probability table (COPT) (Allan 2013) in order to estimate the overall capacity of the generation system. Also, Ahmad et al. in (2020b) used RBDs/FTs to determine the reliability/failure of various intelligent embedded devices for an automated substation. However, the work in Ahmad et al. (2020b) is limited to formally analyzing either the failure or the reliability of smart power grids compared to the work we propose which provides a comprehensive formal analysis considering both failure and success risk states of smart power grid components simultaneously at the system/subsystem level.

5 Proposed Methodology

Figure 4 depicts an overview of the proposed novel methodology for SG reliability analysis. This methodology allows us to formally verify system-/subsystem-level failure and reliability expressions for SG power systems, which can be evaluated and used in critical decision analysis. The core component of this methodology is the HOL4 libraries of ETs, FBD, and CCDs as depicted in container, enclosed by a box. The first step in our proposed methodology is the SG power system diagram, description, and its subsystem specifications provided by the reliability engineers. The second step is to choose which technique is suitable for the SG power system reliability analysis, i.e., either using ET analysis for system-level analysis or using FBD/CCD for subsystem-level analysis, as shown in Fig. 4. To perform the formal system-level ET analysis using our core ET library (ET structure, reduction properties, and probabilistic theorems), the reliability engineer has to provide the reliability requirements for the SG power system under reliability study, as shown in Fig. 4 with green arrows. While performing the formal subsystem-level FBD analysis using our FBD library (FBD structure, FBD-ET translation, and probabilistic theorems), the user has to model the SG subsystem-level FBD with all its decomposed FBs, as shown in Fig. 4 with blue arrows. Similarly, using our CCD library (CCD structure, CCD reduction, and probabilistic theorems) requires the SG subsystem RBD or FT models, as shown in Fig. 4 with red arrows. Based on our rich new ET/FBD/CCD definitions and novel formulations, proposed in this research work, a user with some basic knowhow about HOL4 can easily *verify* all possible system-/subsystem-level safety classes of reliability and failure consequence expressions based on any given probabilistic distribution, like exponential/Weibull/Poisson, corresponding to the given SG power system description.

The last step is the probabilistic computation of the formally verified reliability/failure expressions using new defined standard metalanguage (SML) functions. We can use the verified probabilistic results to determine significant reliability and energy indices (Keyhani and Albaijat 2012), such as forced outage rate (FOR), System Average Interruption Frequency Index (SAIFI), System Average Interruption Duration Index (SAIDI), Customer Average Interruption Duration Index (SAIDI), Average Service Availability Index (ASAI), Average Service Unavailability Index (ASUI), Energy not Supplied Index (ENS), Average System Curtailment Index (ASCI), loss of load expectation (LOLE), loss of energy expectation (LOEE), and Energy Index of Reliability (EIR), to help the planners/designers in making effective decisions at the critical design stage. Lastly, we propose a new Functional Block Diagram and Event Tree Modeling and Analysis ($\mathbb{FETMA}$) Software for industrial engineers, which is mainly build based on our verified mathematical equations in HOL4 to overcome the limitations of all existing analysis methods. In order to demonstrate the practical effectiveness of our proposed methodology, we use our framework to conduct a formal system-/subsystem-level reliability and safety analysis of real-world smart power systems in the major sectors (Keyhani and

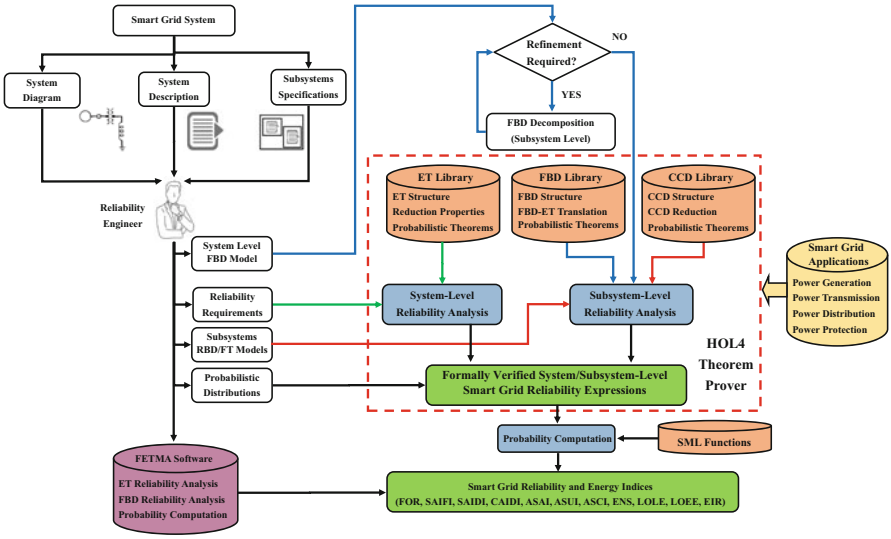


Fig. 4 Proposed methodology

Albaijat 2012), (i) power generation plants, (ii) power transmission grids, (iii) power distribution networks, and (iv) power protection systems, as shown in Fig. 4.

6 Smart Grid Power System Applications

In this section, we utilize our proposed novel methodology on real-world SG power system applications, as follows:

- In Abdelghany and Tahar (2020), we conducted the formal system-level ET reliability analysis of the standard IEEE 3-bus composite bulk power system incorporating 50% distributed renewable energy resources (RES) systems, as shown in Fig. 5. Also, we performed the predictive verification of some significant reliability indices, such as SAIFI, SAIDI, and CAIDI, for the entire power grid.
- In Abdelghany et al. (2021), we conducted the formal system-level ET reliability analysis of different load locations in the standard IEEE 118-bus transmission line system representing a portion of the American electric power system (in the Midwestern USA), as shown in Fig. 6. Moreover, we determined an important SG energy indices, such as ENS, ASCI, LOLE, LOEE, and EIR, for the transmission power system under reliability study.
- In Abdelghany and Tahar (2021), we conducted the formal subsystem-level CCD reliability analysis of the IEEE 39-bus electrical power network incorporating 50% truly carbon-neutral or emission-free green power generation, as shown

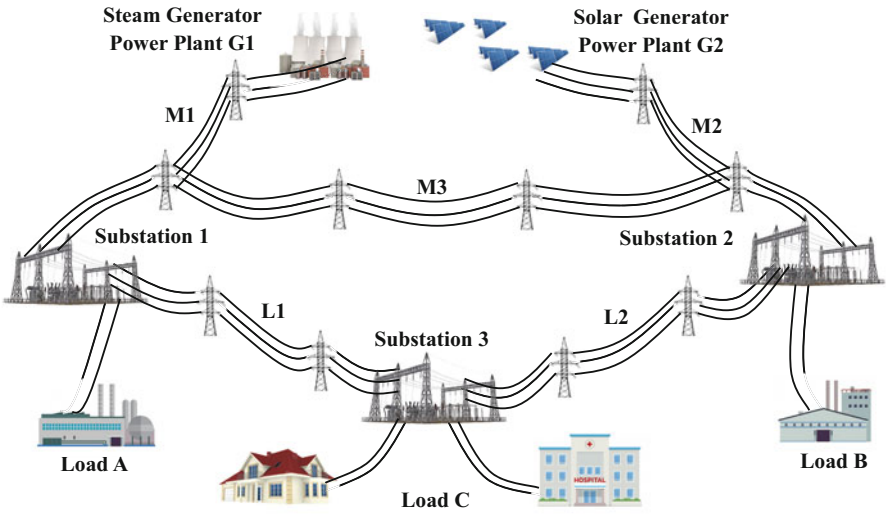


Fig. 5 IEEE 3-Bus Composite Bulk Power System

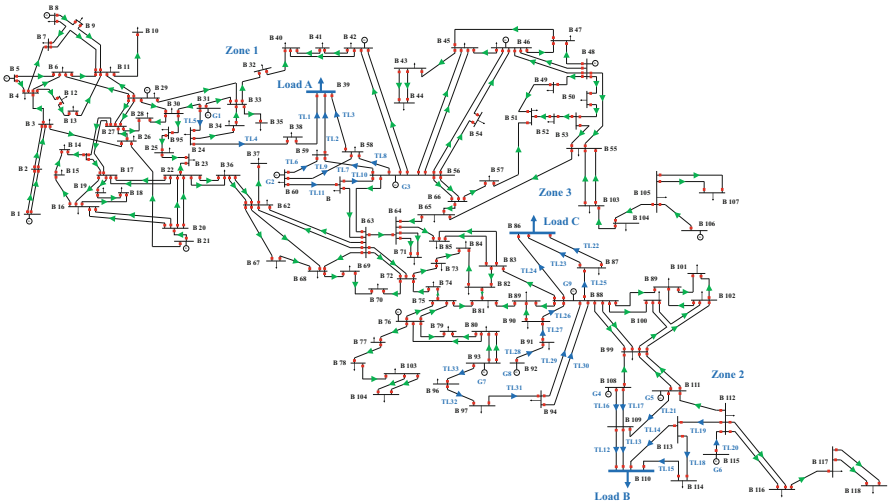
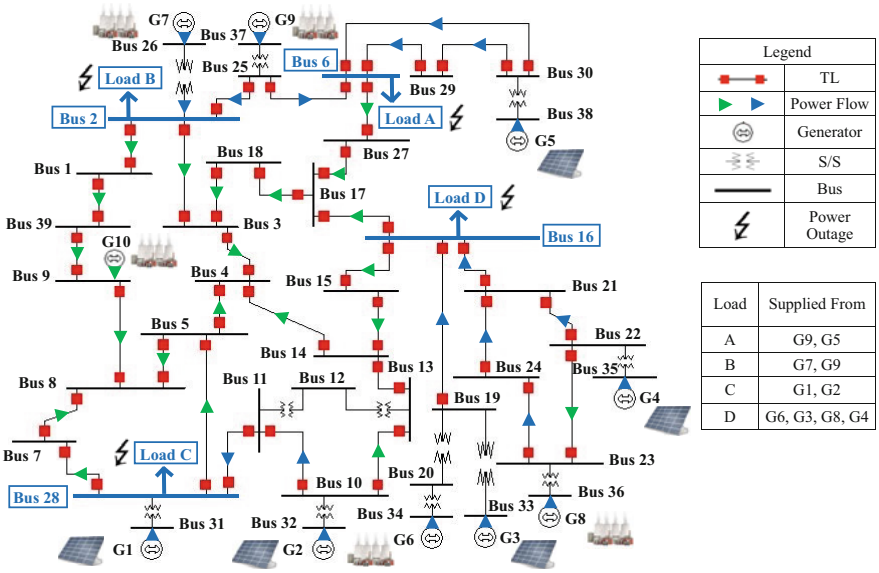


Fig. 6 IEEE 118-bus transmission power grid system

in Fig. 7. Also, we automatically generated the forced outage rate (FOR) probabilistic expressions of all power generation units and the network reliability index SAIDI complex expression at each generation subsystem level.

– In Abdelghany et al. (2020), we apply our FETMA software on a probabilistic risk ET analysis of the distance protection fault tripping circuits in different zones of SG power transmission lines, as shown in Fig. 8. We built a decision tree describing the process of selecting the redundancy for critical transmission



Load	Supplied From
A	G9, G5
B	G7, G9
C	G1, G2
D	G6, G3, G8, G4

Fig. 7 IEEE Standard 39-bus generation network

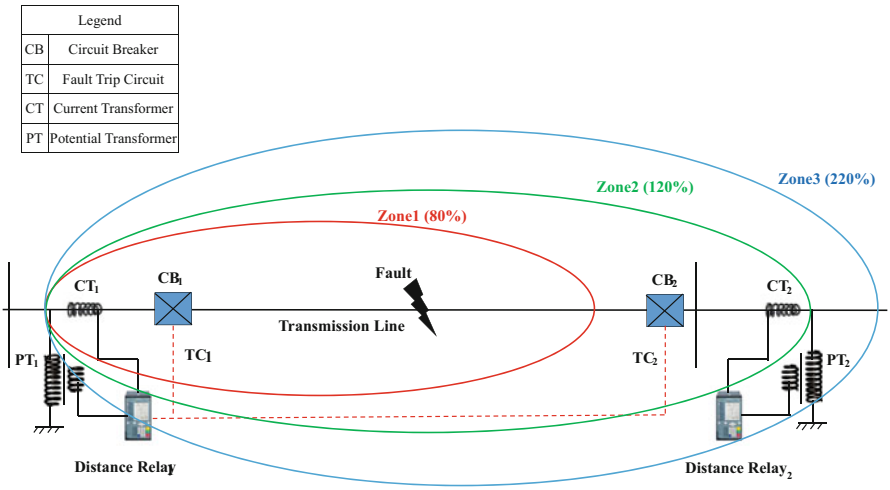


Fig. 8 Power transmission distance protection

protection components. Moreover, the CPU time for the transmission protection step-wise ET analysis in FETMA is much faster than existing tools, like the commercial Isograph ET analysis tool.

7 Conclusions

We proposed a novel methodology based on formal methods to conduct the predictive verification of system-/subsystem-level reliability analysis of smart grids (SG) as an accurate alternate analysis approach. For that purpose, we built a formally verified complete library using HOL4 theorem proving for analyzing large-scale reliability risk modeling methods, i.e., event trees (ET), cause-consequence diagrams (CCD), and functional block diagrams (FBD). We demonstrated the practical effectiveness of our proposed methods by conducting the formal system-/subsystem-level reliability analysis of the standard IEEE 3-bus composite bulk power system, IEEE 118-bus transmission system, IEEE standard 39-bus generation network, and power transmission distance protection scheme. Moreover, we accurately determined significant reliability and energy indices, such as SAIFI, SAIDI, CAIDI, ASAI, ASUI, ENS, ASCI, LOLE, LOEE, and EIR.

References

M. Abdelghany, S. Tahar, Event tree reliability analysis of electrical power generation network using formal techniques, in *Electric Power and Energy Conference* (IEEE, Edmonton, 2020), pp. 1–7

M. Abdelghany, S. Tahar, Cause-consequence diagram reliability analysis using formal techniques with application to electrical power networks. IEEE Access **9**, 23929–23943 (2021)

M. Abdelghany, W. Ahmad, S. Tahar, S. Nethula, ETMA: an efficient tool for event trees modeling and analysis, in *IEEE International Systems Conference* (IEEE, Montreal, 2020), pp. 1–8

M. Abdelghany, W. Ahmad, S. Tahar, Event tree reliability analysis of safety critical systems using theorem proving. IEEE Syst. J. (2021). [Online]. Available: https://doi.org/10.1109/JSYST.2021.3077558

W. Ahmad, Formal dependability analysis using higher-order-logic theorem proving. Ph.D. dissertation, National University of Sciences and Technology, Islamabad, 2017

W. Ahmad, O. Hasan, F. Awwad, N. Bastaki, S. Hasan, Formal reliability analysis of an integrated power generation system using theorem proving. IEEE Syst. J. **14**(4), 4820–4831 (2020a)

W. Ahmad, O. Hasan, S. Tahar, Formal reliability and failure analysis of ethernet based communication networks in a smart grid substation. Form. Asp. Comput. **32**(1), 71–111 (2020b)

R. Allan, *Reliability Evaluation of Power Systems* (Springer Science & Business Media, New York, 2013)

J. Andrews, Reliability of sequential systems using the cause-consequence diagram method. J. Process Mech. Eng. **215**(3), 207–220 (2001)

J. Andrews, L. Ridley, Application of the cause-consequence diagram method to static systems. Reliab. Eng. Syst. Saf. **75**(1), 47–58 (2002)

O. Ansari, N. Safari, C. Chung, Reliability assessment of microgrid with renewable generation and prioritized loads, in *Green Energy and Systems Conference* (IEEE, 2016), pp. 1–6

T. Badings, A. Hartmanns, N. Jansen, M. Suilen, Balancing wind and batteries: towards predictive verification of smart grids, in *NASA Formal Methods Symposium* (Springer, 2021), pp. 1–18

M. Bevilacqua, M. Braglia, R. Gabbrielli, Monte Carlo simulation approach for a modified FMECA in a power plant. Qual. Reliab. Eng. Int. **16**(4), 313–324 (2000)

Z. Bie, P. Zhang, G. Li, B. Hua, M. Meehan, X. Wang, Reliability evaluation of active distribution systems including microgrids. IEEE Trans. Power Syst. **27**(4), 2342–2350 (2012)

R. Billinton, A. Sankarakrishnan, Adequacy assessment of composite power systems with HVDC links using Monte Carlo simulation. IEEE Trans. Power Syst. **9**(3), 1626–1633 (1994)

B. Boussahoua, A. Elmaouhab, Reliability analysis of electrical power system using graph theory and reliability block diagram, in *Algerian Large Electrical Network Conference* (IEEE, 2019), pp. 1–6

M. Bucher, R. Wiget, G. Andersson, C. Franck, Multiterminal HVDC networks – what is the preferred topology? IEEE Trans. Power Delivery **29**(1), 406–413 (2013)

M. Čepin, *Assessment of Power System Reliability: Methods and Applications* (Springer Science & Business Media, London, 2011)

E. Dialynas, N. Koskolos, Reliability modeling and evaluation of HVDC power transmission systems. IEEE Trans. Power Delivery **9**(2), 872–878 (1994)

Y. Elderhalli, Dynamic dependability analysis using HOL theorem proving with application in multiprocessor systems. Ph.D. dissertation, Concordia University, 2019

X. Fang, S. Misra, G. Xue, D. Yang, Smart grid – the new and improved power grid: a survey. IEEE Commun. Surv. Tutor. **14**(4), 944–980 (2011)

O. Hasan, S. Tahar, Formal verification methods, in *Encyclopedia of Information Science and Technology* (IGI Global, 2015), pp. 7162–7170

Isograph Software, 2021. [Online]. Available: https://www.isograph.com

ITEM Software, 2021 [Online]. Available: https://itemsoft.com/eventtree.html

H. Jahanian, Failure mode reasoning, in *International Conference on System Reliability and Safety* (IEEE, 2019), pp. 295–303

M. Javadi, A. Nobakht, A. Meskarbashee, Fault tree analysis approach in reliability assessment of power system. J. Multidiscip. Sci. Eng. **2**(6), 46–50 (2011)

S. Kabir, K. Aslansefat, I. Sorokos, Y. Papadopoulos, Y. Gheraibia, A conceptual framework to incorporate complex basic events in HiP-HOPS, in *Model-Based Safety and Assessment*, vol. 11842 (Springer, 2019), pp. 109–124

A. Keyhani, M. Albaijat, *Smart Power Grids* (Springer Science & Business Media, Berlin/Heidelberg, 2012)

A. Khurram, H. Ali, A. Tariq, O. Hasan, Formal reliability analysis of protective relays in power distribution systems, in *Formal Methods for Industrial Critical Systems* (Springer, Berlin/Heidelberg, 2013), pp. 169–183

B. Ku, J. Cha, Reliability assessment of catenary of electric railway by using FTA and ETA analysis, in *Environment and Electrical Engineering* (IEEE, 2011), pp. 1–4

K. Larsen, P. Pettersson, W. Yi, UPPAAL in a nutshell. Int. J. Softw. Tools Technol. Transfer **1**(1–2), 134–152 (1997)

Y. Li, P. Zhang, P. Luh, Formal analysis of networked microgrids dynamics. IEEE Trans. Power Syst. **33**(3), 3418–3427 (2017)

R. Mackiewicz, Overview of IEC 61850 and benefits, in *Power Engineering Society General Meeting* (IEEE, Montreal, 2006), pp. 623–630

A. Mahmood, O. Hasan, H. Gillani, Y. Saleem, S. Hasan, Formal reliability analysis of protective systems in smart grids, in *Region 10 Symposium* (IEEE, 2016), pp. 198–202

V. Muzik, Z. Vostracky, Possibilities of event tree analysis method for emergency states in power grid, in *International Scientific Conference on Electric Power Engineering* (IEEE, 2018), pp. 1–5

S. Nanou, O. Tzortzopoulos, S. Papathanassiou, Evaluation of an enhanced power dispatch control scheme for multi-terminal HVDC grids using Monte-Carlo simulation. Electric Power Syst. Res. **140**, 925–932 (2016)

O. Nỳvlt, M. Rausand, Dependencies in event trees analyzed by petri nets. Reliab. Eng. Syst. Saf. **104**, 45–57 (2012)

F. Ortmeier, W. Reif, G. Schellhorn, Deductive cause-consequence analysis. IFAC Proc. Vol. **38**(1), 62–67 (2005)

R. Palin, D. Ward, I. Habli, R. Rivett, ISO 26262 safety cases: compliance and assurance, in *IET Conference on System Safety*, Birmingham (2011), pp. 1–6

Y. Papadopoulos, M. Walker et al., Engineering failure analysis and design optimisation with HiP-HOPS. Eng. Failure Anal. **18**(2), 590–608 (2011)

N. Papakonstantinou, S. Sierla, B. O'Halloran, Y. Tumer, A simulation based approach to automate event tree generation for early complex system designs, in *Design Engineering Technical Conferences and Computers and Information in Engineering Conference*, vol. 55867 (American Society of Mechanical Engineers, 2013), pp. 1–10

I. Papazoglou, Functional block diagrams and automated construction of event trees. Reliab. Eng. Syst. Safety **61**(3), 185–214 (1998a)

I. Papazoglou, Mathematical foundations of event trees. Reliab. Eng. Syst. Saf. **61**(3), 169–183 (1998b)

D. Peplow, C. Sulfredge et al., Calculating nuclear power plant vulnerability using integrated geometry and event/fault-tree models. Nucl. Sci. Eng. **146**(1), 71–87 (2004)

Y. Phulpin, J. Hazra, D. Ernst, Model predictive control of HVDC power flow to improve transient stability in power systems, in *International Conference on Smart Grid Communications* (IEEE, 2011), pp. 593–598

A. Ranjbar, Reliability analysis of modern hybrid micro-grids. Ph.D. dissertation, The University of Texas at Dallas, 2013

N. Rasmussen, *Reactor Safety Study: An Assessment of Accident Risks in US Commercial Nuclear Power Plants*, vol. 7 (NTIS, 1974)

S. Shelemy, D. Swatek, Monte Carlo simulation of lightning strikes to the nelson river HVDC transmission lines, in *International Conference on Power System Transients* (2001), pp. 1–6

X. Shi, A. Bazzi, Fault tree reliability analysis of a micro-grid using Monte Carlo simulations, in *Power and Energy Conference* (IEEE, 2015), pp. 1–5

G. Sugumar, R. Selvamuthukumaran et al., Formal validation of supervisory energy management systems for microgrids, in *Industrial Electronics Society* (IEEE, 2017), pp. 1154–1159

G. Sugumar, R. Selvamuthukumaran, M. Novak, T. Dragicevic, Supervisory energy-management systems for microgrids: modeling and formal verification. IEEE Ind. Electron. Mag. **13**(1), 26–37 (2019)

G. Vyzaite, S. Dunnett, J. Andrews, Cause-consequence analysis of non-repairable phased missions. Reliab. Eng. Syst. Saf. **91**(4), 398–406 (2006)