Formal Verification of Fault Isolation and Restoration Algorithms in Smart Grid

Sohaiba Iqbal and Osman Hasan
School of Electrical Engineering and Computer Science (SEECS)
National University of Sciences and Technology (NUST)
Islamabad, Pakistan
{sohaiba.iqbal,osman.hasan}@seecs.nust.edu.pk

Syed Rafay Hasan
Department of Electrical and Computer Engineering
Tennessee Technological University
Cookeville, TN, USA
shasan@tntech.edu

***Abstract*—The efficacy of smart grid based modern power systems is primarily dependent on two way communication mechanisms for fault isolation and restoration of the grid. These systems are of critical nature and also have direct impact on customers in terms of down time. Many algorithms for effective fault restoration have been proposed. However, the requirement of physical testing of these algorithms against all possible cases has been a bottleneck for their timely deployment. To overcome this challenge, we propose a formal quantitative analysis in this paper. We argue that if we can formally model these algorithms, which can incorporate the randomness of the faults, then their verification can be reduced to the validation of their formal properties. To facilitate this process, we have identified a set of functional properties based on the working description of a given fault restoration algorithm. These properties are represented using the Linear Temporal Logic (LTL) operators that are available in PRISM, which is a probabilistic model checker. For illustration purposes, we use the PRISM model checker to model and analyze a real-world scenario of fault isolation and restoration while considering some key factors, like capacity of substations, fault occurrence at different load locations and efficient load balancing among substations.**

***Index Terms*—Fault restoration, Load balancing, Formal Modeling and Formal Verification.**

I. Introduction

We are facing numerous challenges with the ever-increasing demand of electric power all across the world. As per a recently published report [19] on the international energy outlook from U.S. energy information administration, electricity demand is expected to grow tremendously in many Asian countries, which are not member of Organization for Economic Co-operation and Development (OECD) due to the tremendous rise in the standard of living, demand of heating, cooling, lighting and appliances. Conventional grid is typically used to carry power from central generation units to a huge number of customers. Since it lacks communication between the customer and utility, it is very challenging for the utility to know the requirements of the customer in real-time, which may result in system failures and large-area blackouts [14], [16]. Recently, smart grid [15], also called as the intelligent or future grid, has emerged as a promising concept to solve the energy crisis of this era. It enables two way information and electricity flow between the customer and utility to generate an advanced automated and distributed energy system. Therefore, electric efficiency, safety and reliability can significantly be improved by smart grids [15].

Distribution systems are evolving towards self-healing systems which can quickly identify and isolate faulted components and restore supply to the affected customers with little human intervention [8]. A self-healing mechanism can reduce the outage times and improve the continuity of supply; however, such an improvement requires a fast fault location method and also a communication and measurement infrastructure [1]. Traditionally, distribution systems present the final link between utilities and customers. In most cases, a distribution network is operated in radial configuration for a simple design, low cost, supportive protection scheme, simple protection coordination, and minimizing the possibility of fault currents. However, continuity of supply requires normal operation for all components between the supply and the load. Hence, distribution networks have poor reliability as a failure of any component may cause an interruption for all loads that are downstream to the faulty zone [2].

Distribution system restoration following a fault is an important area of research in smart grids. When there is a fault in the system, some of the loads are interrupted for some time during the fault. Therefore, a strategy is required to restore the out of service loads by immediately isolating the faulted portion of the line. In the radial distribution feeder, many criteria have to be considered in developing the post fault restoration strategy. Some of the criteria include that the feeders should always maintain the radial topology and none of the feeders should be overloaded, i.e., the feeders should not exceed their current carrying capability limits. Moreover, in modern multi-micro gird and possible non-radial topologies we envision that many more criteria require further investigation [15].

Almost all the present day distribution systems include remote controlled automatic sectionalizers and circuit breakers. These intelligent devices have opened up the avenues to implement the automatic methods for fault location identification, fault isolation and system restoration processes. Due to the advancement of distribution automation in the recent years, the reliability of the system can be improved by restoring the supply to the system after severe faults [18]. All these algorithms have been tested on the physical systems. However, there is a consensus among researchers that it is not possible

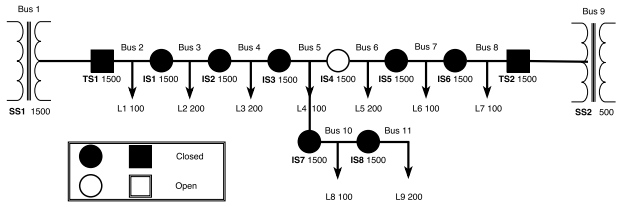

Fig. 1: Normal Distribution Feeder

to physically test the power restoration algorithm against all the possible cases [7], [8]. With the added features in the smart power systems (especially the smart features, which require two way communications) many more probable failure scenarios are possible [9], [10]. Some work has been done on the probabilistic failure analysis of the wireless sensor network in the transmission systems [11]. In [12], the voltage disturbance due to distributed generations (DG) penetration has been analyzed using probabilistic methods, but it is not been modeled and verified from the distribution management system (DMS) perspective. Distributed generation involves small-scale technologies to produce electricity close to the power requirements of end users. To overcome this challenge, we propose a formal quantitative analysis in this paper. The proposed formal analysis framework can incorporate the probabilistic nature of fault scenario in the grid and thus the resulting impact model can be effectively utilized for verification of fault restoration algorithms of DMS. For this purpose, we propose to use probabilistic model checking for modeling and verification of fault restoration algorithms. We have identified a set of desired functional properties based on the working description of a given fault restoration algorithms. These properties are represented by the Linear Temporal Logic (LTL) operators that are available in the PRISM model checker. The PRISM model checker provides quantitative information about these properties, which can play a vital role in developing effective fault restoration algorithms. Our proposed properties include the probability of fault restoration within some expected time and the probability of loads remain not served due to insufficient capacity of a substation. We have analyzed the effectiveness of the proposed methodology with a typical scenario of fault occurrence in a case study.

II. Preliminaries

A. Probabilistic Model Checking

Probabilistic model checking [5] is an extension of traditional model-checking techniques [21] for the integrated analysis of both qualitative and quantitative properties of systems that exhibit stochastic behavior. A model checker exhaustively searches all possible input and state conditions for failures and ensures 100 % completeness of analysis results. One of the drawbacks of model checking is the extensive utilization of memory due to large state-space of some systems, which sometimes leads to state-space explosion problem. This problem is usually resolved by developing abstract models or by using approximate model checking.

B. PRISM Model Checker

PRISM [5] is a widely used probabilistic model checker for formal modeling and analysis of schemes or systems that exhibit probabilistic or random behavior. The probabilistic behavior of systems is basically captured based on the Reactive Modules formalism [4]. PRISM supports modern algorithms and symbolic data structures based on Binary Decision Diagrams (BDDs) and Multi-Terminal Binary Decision Diagrams (MTBDDs) along with statistical model checking using its discrete events based simulation engine. The verification of Markov processes, i.e., continuous-time Markov chains (CTMC), discrete-time Markov chains (DTMC), Markov decision processes (MDP), and probabilistic timed automata (PTA) is also one of the distinguished features of this tool.

C. Fault Isolation and Restoration System

A simple sample distribution feeder is taken as an example system to demonstrate the restoration strategies. The feeder comprises of substations, tie-switches (TS) and isolation switches (IS) and the loads as shown in Fig. 1. It should be noted that "TS" connects a feeder with a substation. Also, "IS" provides a switchable component sectionalizing of the feeder. The normal circuit topology of the example system considered is as shown in Fig. 1. The current carrying capacity of each substation transformer, switches and current drawn by each loads are shown here. In the normal state, the substation SS1 is serving all the loads of the system. As distribution system is a complex structure, it should be noticed that the substations SS2, SS3 and SS4 are serving other branches of the system which are not part of the Fig. 1 [18].

III. Proposed Fault isolation and Restoration (FIR) Model

This section describes our proposed formal model for the Fault Isolation and Restoration (FIR) for smart grid. The major components identified to make this model are as follows:

1) Substations: The substations are responsible for providing power to the customers so that they have a fixed capacity in terms of ampere rating with a constant voltage.
2) Customers/Loads: Represents a facility, where the demand of power arises. Loads are considered to be constant power.

These components are used as inputs to the proposed (FIR) model. Now these components are described in detail below:

A. Substation in our model

A substation is primarily used to transform voltage. In our proposed FIR model, we assume that substations are always available and operational to meet the required needs. This assumption is made to evaluate the quality of the underlying FIR plan in smart grid as, in the case of unavailability of substations; the required demand of customers can never be fulfilled. Our model also incorporates substation capacity increment as this event can happen with a relatively high probability during load serving and load balancing.

B. Loads in our model

The load is defined as the facility that generates the demand to receive power from the substations. The successful and timely delivery of power to the required loads or customers is the only way to lessen the impact of fault occurrence in a scenario where the severity and frequency of fault is rising.

Algorithm 1 : Case_Fault_restoration

Input:

$switch\_close\_ISi$;Set of isolation switches in the distribution feeder $[IS1...ISi]$, $IS1$ represents close state of isolation switch 1 where range is from 1 to i

$switch\_close\_TSt$;Set of Tie switches in the distribution feeder $[TS1...TSt]$, $TS1$ represents Tie switch 1 where range is from 1 to t

$SS_n : [0 : C]$; substation current carrying capacity $[SS_1...SS_n]$, SS_1 and SS_n represents substation 1 and substation n respectively

$l : [1 : L]$; load to be served $[L_1...L_l]$, L_1 represents Load 1 where range is from 1 to l

$i : [1 : IS]$; Number of isolation switches

$t : [1 : TS]$; Number of Tie switches.

$Prob1, [pow(e, (-lambda * t))]$; probability of fault occurrence following exponential distribution

Fault Isolation:

0: **if** $Faultoccur = 0 \& Ll\_flag = false \& Ll\_flag = false$ **then**

0: $1/2 : (Ll\_flag = true) + 1/2 : (Ll\_flag = true)$;

0: $Ll\_flag = true -> Prob1 : (Faultoccur = 1) + 1 - Prob1(Faultoccur = 0)$;

where Faultoccur is occurrence of fault and L_l is any load ranging from 1 to L;

0: $Ll\_flag = true \& (switch\_close\_ISi = true) -> (switch\_close\_ISi = false)$;

0: **end if**

Substation Serving Loads:

0: $(Faultoccur = 1) \& (Ll\_flag = true) \& (switch\_close\_TSt = false) \rightarrow (switch\_close\_TSt = true) \& (Load\_SS_n = ceil(L_l)) \& (SS_n = ceil(SS_n - L_l)) \& (recovery\_time = recovery\_time + 1)$;

where $Load\_SS_n$ represents number of loads a substation n will handle after fault occurrence and recovery_time is the time to recover from the fault and SS_n is the remaining capacity of substation

0: $(switch\_close\_TSt = true) \& (Load\_SS_n = ceil(L_l)) \& (SS_n >= (ceil(L_l + L_l))) \rightarrow (Load_S S_n = ceil(L_l + L_l)) \& (recovery\_time = recovery\_time + 1)$

where SS_n represents substation capacity.

0: $switch\_close\_TSt = true) \& (Load\_SS_n = ceil(L_l + L_l)) \& (SS_n >= (ceil(L_l + L_l + L_l))) \rightarrow (Load_S S_n = ceil(L_l + L_l + L_l)) \& (recovery\_time = recovery\_time + 1))$;

Switch Over:

0: $(Ll\_flag = true) \& (Ll\_fault = 0) \rightarrow 1/2 : (Ll\_fault = 1) + 1/2 : (Ll\_fault = 2) \& (switch\_close_I Si = true) \& (switch\_close\_ISi = true) \& (switch\_close\_ISi = true) \& (switch\_close\_ISi = true)$ =0

IV. Probabilistic Modeling in PRISM

We selected Markov decision processes (MDP) to develop the formal model for fault isolation and restoration because it allows us to capture both probabilistic and non-deterministic aspects of the model. MDPs provide a mathematical structure for modeling scenarios where conclusions are partially random and partially under the control of the person making decisions. In our model, probabilistic factors include single and multiple fault occurrences while non-deterministic factors include fault isolation. This model can be used to analyze properties by varying different parameters in PRISM.

The inputs of the model are described in the $Input$ part of Algorithm 1 [17] where, `I`, `T` and `L` represents the total number of isolation switches, tie switches and loads, respectively. Similarly, `i` represents a specific isolation switch, `t` represents a specific tie switch and `l` represents a specific load with values ranging `1` to `I`, `1` to `T` and `1` to `L`, respectively. Fault

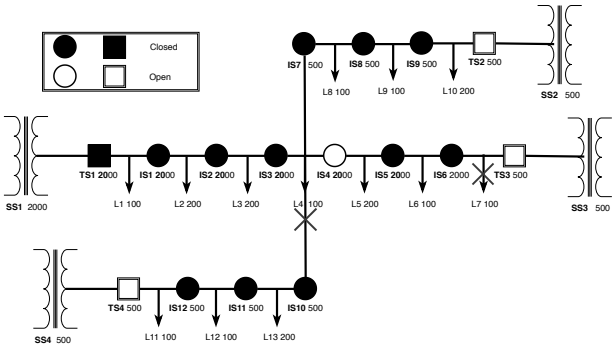

Fig. 2: Fault occurrence at Load 4 and Load 7

restoration includes the coverage of events that can be taken up after the occurrence of a fault.

The first step is fault isolation, which is represented by flags, i.e. `Ll_flag`, and are selected non-deterministically in our model as shown in the $Fault\ Isolation$ part of Algorithm 1. The next step is the fault occurrence check `Faultoccur` based on the load's flag and exponential probability distribution. Exponential distribution is considered for modeling the period of low failure risk areas. It is most widely used to model the failure probabilities of electronic components that usually do not wear out until long after the expected life of their products. The modeling of fault occurrence step in PRISM results in opening of immediate isolation switches `switch_close_ISi = false` as shown in the $FaultIsolation$ part of Algorithm 1. Afterwards, each substation serves its respective loads, $Load\_SS_n$ and `recovery_time`, are estimated in the $SubstationServingLoads$ part of Algorithm 1.

Multiple fault occurrence is shown in the $SwitchOver$ part of Algorithm 1. This represents the occurrence of another fault, i.e., at some load location either after previous fault is fully recovered `Ll_fault = 2` or in the presence of previous fault `Ll_fault = 1`. To handle multiple substations the model also incorporates the concept of module renaming which allows duplication of existing modules.

V. Case Study

To demonstrate the effectiveness of the proposed analysis methodology, we analyze a typical scenario of fault occurrence. The fault event, based on its occurrence at load, is analyzed as a case study while assuming that a fault occurrs at Load (4) and Load (7) as shown in Figure 2. The isolation of fault at loads is represented by flags, i.e., `L4_flag` and `L7_flag` and are selected in a non-deterministic way in our model as shown in Algorithm 1.

The next step is to check the fault occurrence `Faultoccur` based on the load's flag and exponential probability distribution. This results in opening of the immediate isolation switches switch_close_IS3, switch_close_IS4, switch_close _IS7, switch_close_IS10. This activity is handled in the Fault Isolation part of Algorithm 1.

Afterwards, each substation serves its respective loads,

Load_SS2 and recov ery_time, as estimated by the Substation Serving Loads part of Algorithm 1.

Multiple fault occurrences are handled in Switch Over part of Algorithm 1. This represents the occurrence of another fault, i.e., at load L7 either after previous fault is fully recovered L7_fault = 2 or in the presence of previous fault L7_fault = 1.

A. Property Specification

The first step of formal verification is to develop the fault restoration model while identifying its substations, isolation switches, tie switches and loads. After modeling, a set of functional properties based on the working description of the model is identified. The model performance parameters, i.e., the probability of fault occurrence and the probability of loads that are not served due to multiple occurrence of faults are used to analyze the impact on the substation capacity. The modeling parameters and performance parameters are translated into a MDP model. PRISM, based on the given LTL properties, formally verifies the MDP model and provides the quantitative information. This quantitative information can play a vital role in developing effective fault restoration model.

We assume that the capacity of a substation ranges from s_1 to s_n. In case of a fault, the algorithm initially isolates it by opening the immediate isolation switches and performs load balancing to ensure that the loads get equally distributed among the available substations. In order to perform the load balancing, the algorithm iteratively evaluates the remaining percentage capacity of available substations against each increment in the served load. After that, if another fault occurs at some other load location the algorithm utilizes the remaining substation capacity for fault restoration strategy. We analyze the probability of loads, which are not served either because of failure of a previous fault recovery within the expected time or due to insufficient capacity of substations. Another analysis is performed on the probability of requiring increased substation capacity due to multiple fault occurrences at different locations.

We provide a set of properties to formally analyze the functionality of the model with respect to a fault. For instance, we evaluated the probability of loads that are not served due to insufficient substation capacity:

$$P =?[F \;\; Loads\_notserved \;\; = false \;\; \& \;\; recovery\_time \;\; <= expected\_time] \quad (1)$$

Property 1 corresponds to the loads that are not served because of multiple fault occurrence. Loads_notserved in Property 1 is set to false and represents the loads of particular substation that are not served. Similarly, recovery_time represents the time it takes to recover faults and is less than or equal to the expected time expected_time. Expected time is computed by taking into account the best and the worst case scenarios of the given model and the recovery time is the approximate time computed by the number of steps involved in the fault occurrence and load balancing in PRISM. The best and worst case scenarios occurs when the substation has the maximum capacity for load balancing after fault occurrence and the substation does not have enough capacity, respectively.

$$P =?[F \;\; SS1 \;\; < sumofloads\_SS1 \;\; \& \;\; SS1 = SS1 + ceil(sumofloads\_SS1 - Load\_SS1)] \quad (2)$$

Property 2 corresponds to the probability of a substation to serve the loads connected to it having capacity ranging from s_1 to s_n. Here s_1 is the lower capacity limit and s_n is the upper capacity limit. the number of loads served by a substation after fault is represented by Loads_SS1. Similarly, sumofloads_SS1 is the sum of all the loads that are supposed to be served by Substation 1. The capacity of a substation that is updated upon each load serving is represented by SS1.

B. Verification

As explained, the normal topology of a distribution feeder can be interrupted by a single or multiple faults. There can be two scenarios, i.e., both L4 and L7 faults occur simultaneously or one of them (say L7) may occur after the recovery of the other one (say L4). In our model, we have incorporated both of these scenarios by evaluating the probability of loads that are not served against the following parameters:

1) Fault occurrence time: It is the time at which the fault occurs at a specific load location.
2) Fault recovery time: It is the approximate time of fault recovery provided by the algorithm with respect to its total number of iterations.
3) Expected time: It is the approximate time within which the fault is expected to be recovered and it is the average time computed by the algorithm by taking into account its best and worst case scenarios.

We have used Property 1 to evaluate the probability of loads that are not served within the expected time of 10 units, where expected time of 10 units is the average time computed by the algorithm by taking into account its best and worst case scenarios. The corresponding output is depicted in Figure 3, which exhibits a decreasing trend as the time duration increases of the probability of loads that are not served within the expected time.

The substations have a range of capacity (i.e. SS_1 to SS_n). In this case study, we have assumed SS_1 as 0 units and SS_n as 15 units. The loads assigned to a specific substation can vary from (L_1 to L_l), which in this case study varies from L_1 to L_3 assuming each load to be of 5 units [7]. To evaluate the probability of requirement of increase in capacity of a substation to fulfill the demand of the assigned loads we have verified Property 2 by varying the capacity of the substation at different fault occurrence times ($i.e., T1 to T4, where T4 = 1000 units > T3 = 500 units > T2 = 100 units > T1 = 10 units$). The same trend is depicted in Figure 4, which exhibits a decreasing trend of the probability of increase in the capacity of a substation to

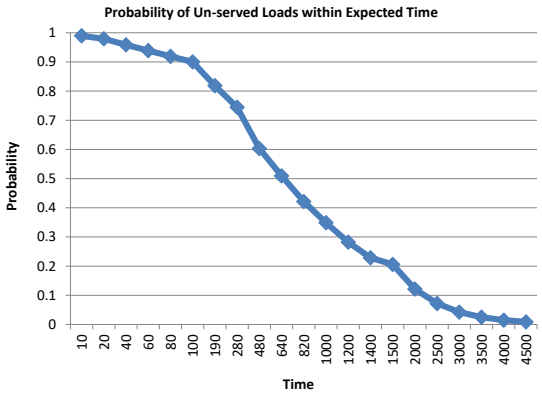

Fig. 3: Trend of Loads not served within Expected Time

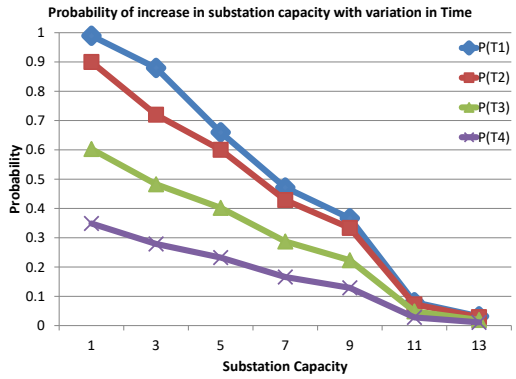

Fig. 4: Trend of increase in substation Capacity

fulfill the demand of all the assigned loads. As we increase the capacity of a substation, the probability of requiring increment in the capacity of a substation decreases for the assigned loads. Similarly, we can also observe that as the value of T increases, the probability of increase in the capacity of a substation decreases. The trend in Figure 4 depicts that there is a trade-off between T and S, and by using this model the power system engineer can select their desired probability of requirement of increase in capacity of a substation against fault occurrence time T and substation capacity S. A distinguishing feature of developing such a model is its basis on a formal semantic of systems as it allows the smart grid engineer to reason about very complex behavioral properties of the system using probabilistic model checking. We have considered random factors associated with fault restoration model in the analysis, including fault isolation, fault occurrence and loads that are not served due to insufficient capacity of substation. To the best of our knowledge, all these factors have not been investigated concurrently in any existing model.

VI. Conclusion

The main contribution of this paper includes the development of a formal model of Fault isolation and restoration. In modeling, a number of stochastic factors are considered, such as fault occurrence, fault isolation and loads that are not served due to insufficient substation capacity. A distinguishing feature of developing such a model is its basis on a formal semantic of systems as it allows the power system manager to reason about very complex behavioral properties of the system using probabilistic model checking. In order to illustrate the usefulness of the model, we used it to analyze a typical case study. The analysis results demonstrate the effectiveness of the model, which can be further extended to formally model and analyze and scale to modern multi-micro grid power systems.

References

[1] A. Bahmanyar, A. Estebsari, E. Pons, E. Patti, S. Jamali, E. Bompard, and A. Acquaviva, Fast fault location for fast restoration of smart electrical distribution grids, Smart Cities Conference (ISC2), 2016 IEEE International, 1–6, 2016, IEEE

[2] A. Zidan, M. Khairalla, A. Abdrabou, T. Khalifa, K. Shaban, A. Abdrabou, R. El Shatshat, and A.M. Gaouda, Fault detection, isolation, and service restoration in distribution systems: state-of-the-art and future trends, IEEE Transactions on Smart Grid, 8, 5, 2170–2185, 2017, IEEE

[3] 25 Worst Natural Disasters Ever Recorded https://www.eia.gov/outlooks/ieo/, 2022

[4] PRISM Modelchecker, http://www.prismmodelchecker.org/, 2022

[5] M. Kwiatkowska, G. Norman and D. Parker, PRISM 4.0: Verification of Probabilistic Real-time Systems, Computer Aided Verification, 2011, 585–591, Springer, LNCS, 6806

[6] M. Ismail, O. Hasan, T. Ebi, M. Shafique and J. Henkel, Formal verification of distributed dynamic thermal management, Computer-Aided Design (ICCAD), 2013 IEEE/ACM International Conference on, 248–255, 2013, IEEE

[7] S. Adhikari, F. Li, Q. Hu and Z. Wang, Heuristic optimal restoration based on constructive algorithms for future smart grids, Intelligent System Application to Power Systems, 1–6, 2011, ISA

[8] A. Zidan and E. F. El-Saadany, Service restoration in balanced and unbalanced distribution systems with high DG penetration, In Power and Energy Society General Meeting, 1–8, 2011, IEEE

[9] F. Xi, S. M. GuoliangXue, and D. Yang, Smart Grid—The New and Improved Power Grid: A Survey, In Power and Energy Society General Meeting, 1–37, 2011,

[10] D. R. Perrier and M. Trépanier, A Survey of Models and Algorithms for Emergency Response Logistics in Electric Distribution Systems, Technical Report, 1–8, 2010,

[11] E. Yüksel, F. Nielson and H. Huang, Modelling Chinese Smart Grid: A Stochastic Model Checking Case Study, International Symposium on Theortetical Aspects of Software Engineering, 25–32, 2012, IEEE

[12] C. Su, Stochastic Evaluation of Voltages in Distribution Networks with Distributed Generation using detailed Distribution Operation Models, Power Systems, IEEE Transactions, 786–795, 2010, IEEE

[13] I. Colak, Introduction to smart grid, Smart Grid Workshop and Certificate Program (ISGWCP), International, 1–5, 2016, IEEE

[14] J. Romero, Blackouts Illuminate India's Power Problems, IEEE spectrum, 49, 10, 2012, IEEE

[15] X. Fang, S. Misra, G. Xue and D. Yang, Smart Grid—The New and Improved Power Grid: A Survey, IEEE communications surveys & tutorials, 14, 4, 944–980, 2012, IEEE

[16] A. Y. Salik, M.U. Sardar, O. Hasan, S.R. Hasan, and F. Awwad, Formal Verification of Demand Response Based Home Energy Management Systems in Smart Grids, Innovative Smart Grid Technologies, 2017.

[17] S. Adhikari, F. Li, Q. Hu, Z. Wang, Heuristic Optimal Restoration based on Constructive Algorithms for Future Smart Grids, Intelligent System Application to Power Systems, 1–6, 2011, IEEE

[18] Adhikari, Sarina and Li, Fangxing and Wang, Zhenyuan, Constructive back-feed algorithm for online power restoration in distribution systems, Power & Energy Society General Meeting, 1–5, 2009, IEEE

[19] International Energy Outlook 2016, 2022, www.eia.gov/outlooks/ieo/electricity.cfm

[20] T. Herault, R. Lassaigne, F. Magniette, and S. Peyronnet,, Approximate Probabilistic Model Checking, Verification, Model Checking and Abstract Interpretation, Springer, 2937, 73-84, 2004

[21] O. Hasan and S. Tahar, Formal Verification of Tail Distribution Bounds in the HOL Theorem Prover, Mathematical Methods in the Applied Sciences, 32, 4, 480–504, 2009, Wiley Online Library