Formal Reliability Analysis of Protective Systems in Smart Grids

Awais Mahmood, Osman Hasan,
Hassan Raza Gillani and Yassar Saleem
School of Electrical Engineering and Computer Science
National University of Sciences and Technology (NUST)
Islamabad, Pakistan
Email: {10beeamahmood,osman.hasan,
08beerazagillani,10beeysaleem}@seecs.nust.edu.pk

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

***Abstract*—Given the enormous amount of random and uncertain parameters that affect the performance of smart grids, compared to traditional power grids, a rigorous reliability analysis holds a vital role in ensuring the safe operation of this safety-critical domain. Based on such an analysis, appropriate protective systems are designed and included in the smart grid systems. Traditionally, the reliability analysis of smart grids is done using numerical methods and computational intelligence based techniques. However, none of these traditional analysis techniques can guarantee absolute accuracy of the load flow analysis results due to their inherent incompleteness. As a more accurate alternative, we propose to use probabilistic model checking, i.e., a formal analysis method for Markovian models, for conducing the load flow analysis of smart grids. In particular, the paper provides a reliability assessment of smart grid components with backup protection using the PRISM model checker. Our results have shown significant improvement in terms of completeness and precision compared to the results obtained via numerical methods for the same load flow analysis problems.**

I. Introduction

Smart grids utilize communication infrastructure along with computers to provide a two-way flow of power and information with the aim of increasing the reliability, efficiency and user controllability of power distribution systems. However, the presence of both information and communication technology (ICT) infrastructure and traditional power distribution equipment, like lines, cables, and transformers, in smart grids and their inherent randomness, including variable loads, peak consumption times and renewable energy sources with generation capacity depending on varying weather conditions, make them quite prone to errors. Therefore, it is customary to integrate protective components in smart grids to ensure reliable operation in the presence of the above-mentioned uncertainties and random failures. It is very important to assess the level of protection in a smart grid as an ineffective protection system may lead to disastrous consequences, like power outages, in worst case consequences.

Reliability analysis for traditional grids is a mature field but the reliability analysis of smart grids still has a lot of room for improvement and research. The biggest challenge is the high computational requirements, due to the involvement of two-way communication, distributed renewable energy resources and variations in network configurations along with peak loads, for attaining results with reasonable accuracy. For example, the usage of consumer appliances depends on weather conditions and the time of the day. The distributed generation and usage of storage cells also plays a key role in varying the electrical demand. The smart grid components usually fail randomly and these failing components may either be fixed by self-repair or require manual repair to restore their operation. Some components may also have back-up protection. Similarly, the influence of electricity prices on the energy demand cannot be neglected as higher prices usually result in the reduction of energy consumption. Moreover, in smart grids, the consumers are more cautious about costs since they can get the real-time tariffs using smart meters. Time-of-Use (TOU) pricing scheme, which offers low off peak rates, encourages consumers to shift their loads to off peak hours. Moreover, electric vehicles (EVs) also greatly influence load profiles since their charging consumes a significant amount of energy and thus is recommended to be done in the off peak times. The reliability analysis must also cater for smart-grid specific behaviors, like component protection, controllable generation, automatic response and source demand dynamic equilibrium [8].

There are various techniques available for reliability analysis of smart grid protection systems including, numerical and simulation, methods. However, the numerical methods are mainly based on some iterative approaches that generate approximate results mainly because the precision of the results is a function of the number of iterations. Simulations are primarily based on observing the results for a subset of all possible cases and thus the results can never be termed as complete. Thus both of the above-mentioned techniques are quite scalable and user-friendly but cannot guarantee the absolute accuracy of the analysis results. The main reasons behind the inaccuracies in the result include the usage of computer-arithmetic based models, which contain round-off errors, and the sampling based nature of the analysis, i.e., the models are analyzed for a subset of all possible scenarios due to limited computational resources. Hence, it is possible that a system bug may not be detected during these analyses. Moreover, due to the usage of pseudo random numbers for developing the system models, simulation cannot capture the true random behaviors, such as frequent changes in renewable energy generation, variations in network configurations and the peak loads, which are quite frequently encountered in

smart grids. Given the safety-critical nature of smart-grids, the accuracy of load flow analysis results is the most desirable feature, since an undetected fault in the smart grid system can have major impact. For example, the analysis inaccuracy limitations have been reported as the main causes behind the 2003 Northeast blackout in the United States and Canada [12] which approximately affected 55 Million people.

Formal methods [9] are capable of overcoming the above-mentioned inaccuracy limitation and have been successfully used to guarantee correctness of many real-world software, hardware and physical systems. However, to the best of our knowledge, no prior work regarding the reliability analysis of protective systems of smart grids exists so far. In order to fill this gap, we propose to use probabilistic model checking [7], which is a widely used formal method for analyzing Markovian models, to ensure accurate results in the domain of load flow analysis of smart grids. For illustrating the effectiveness of this idea, we utilize the probabilistic model checker PRISM to conduct the reliability of smart grid components, which can be installed either at the transmission or the distribution side [2], with backup protection. This reliability analysis is an integral step smart grid analysis as the reliability values of these components can be used to minimize the stress on the overall smart grid and thus schedule system maintenance to ensure safe operation cost-effectively.

II. Related Work

Formal methods have been widely used to analyze smart grids, mainly due to the dire need of accurate analysis in this domain. Chen et. al. [4] studied the structural design and performance of a smart grid substation communication network and evaluated its reliability by utilizing the Reliability Block Diagrams (RBD) and Fault Tree (FT) reliability modeling techniques. Similarly, Walfer et. al [15] extended the capabilities of the analytical reliability analysis method, by combining pivotal decomposition method with RBD and Markov modeling techniques, for the dependability analysis of smart grids. Niyato et. al [11] carried out the reliability and redundant design analysis for a smart grid wireless communication system using RBDs. Similarly, Yu et. al [14] proposed a generic FT-based reliability analysis method for industrial grids by considering the failure effects of Variable Frequency Devices (VFD), which are power electronic devices widely utilized to increase system efficiency and reduce losses. Colored Petri Nets (CPN) have also been used to model dynamic RBDs (DRBDs) [13], which are used to describe dynamic reliability behavior of systems. CPN verification tools, based on model checking principles, are then used in turn to verify behavioral properties of the DRBDs models to identify design flaws [13]. Zhanjun et. al [18] utilized Petri Nets (PN) to analyze the fault diagnosis model for a smart substation. Similarly, Zeng et. al [17] carried out the Stochastic Petri Net (SPN) based reliability and availability analysis of control center networks, which provide the interconnectivity and continuous monitoring by using Wide Area Network (WAN) for smart grid substations. The authors of [17] also discussed, the methods to reduce the state-space explosion problem for the case of large smart grids. Similarly, probabilistic model checking has been used for the development of a distributed probabilistic-control hybrid automata for analyzing smart grid applications [6], the performance and energy consumption evaluation of smart grids [16], and the reliability analysis of protective relays in power distribution systems [1]. However, the focus of none of the above-mentioned formal methods have been on analysing the reliability of protection systems of smart grids, which is the main focus of the current paper..

III. Formal Verification Methods and the PRISM Model Checker

There is a dire need to ensure the accuracy of reliability analysis in smart grids as an undetected bug, or wrong performance estimation, may lead to a significant financial loss or the loss of human lives in the worst cases. However, none of the above-mentioned existing analysis techniques used for reliability analysis can be termed as error-free. Due to their inherent precision, formal verification methods [5] are increasingly being used in verifying safety and financial-critical systems these days and thus can be used to overcome the inaccuracy limitations of reliability analysis as well.

The main idea behind formal verification methods is to construct a computer based mathematical model of the given system and formally verify, within a computer, that this model meets rigorous specifications of intended behavior. Due to the mathematical nature of the analysis, the analysis can be guaranteed to be faultless [9]. The added benefits of formal verification methods come mainly at the cost of formalizing the given models and properties, which becomes quite challenging for real-world systems.

Model Checking [3] is one of the most commonly used formal verification method and is primarily used to verify reactive systems, i.e., the systems that exhibit a behavior that is dependent on time and their environment. The inputs to a model checker include the finite-state model of the system that needs to be analyzed along with the intended system properties, which are expressed in temporal logic. The model checker automatically verifies if the properties hold for the given system while providing an error trace in case of a failing property. The main verification principle behind model-checking is to construct a precise state-based model of the given system and exhaustively verify the given property for each state of this model. The analysis is automatic, which is why model checking is one of the most widely used formal verification technique. On the other hand, model-checking is limited to systems that can only be expressed as finite state machines. Another major limitation of the model checking approach is state space explosion. The state space of a system can be very large, or sometimes even infinite. Thus, it becomes computationally impossible to explore the entire state space with limited resources of time and memory. This problem is usually resolved by working with abstract, less complex, models of the system by somewhat compromising the accuracy of the analysis.

PRISM is a probabilistic model checker for the analysis of random systems [10]. The random systems are modeled using the state-based PRISM language and their properties are specified as probabilistic properties of the states or in terms of rewards. A model is identified by specifying the type of analysis, i.e, continuous time markov chain (*CTMC*), discrete time markov chain (*DTMC*), markov decision process (*mdp*), stochastic multi-player games (*smg*), etc. The behavior of the

model is then identified as *modules*, in which the state chain is modeled as per the transitions. The transitions can be labeled by *variables* which can have global as well as local scope. The behavior of each module is described by a set of commands. For example,

$$[]\ present\ state \rightarrow probability_1 : (nextstate_1) + probability_2 : (nextstate_2) + \cdots \quad probability_n : (nextstate_n);$$

A very useful feature of PRISM is the ability to judge state probabilities, which allows us to judge the probabilities of different states of the model after a certain period of time or a specific number of iterations. For example,

$$P=?\ [\ F=5\ s=7\ ]$$

allows us to obtain, the probability when State is equal to 7 (s=7) at time unit equal to 5 (F=5). Similarly,

$$S=?\ [\ \text{“unavailable”}\ \&\ \text{“not needed”}\ ]$$

means the steady-state probability for state being unavailable AND not needed.

IV. Formal Reliability Analysis of a Protection System for SMART Grid

Consider a smart grid component with back up protection given in Figure 1 [2]. The protection system mainly consists of a transmission line component C, which is surrounded by circuit breakers (CB) and switches (S). They are controlled by protective relays at $stationsA$ and B. Transducers and communications among different protective devices are also used for more stability. All of these protective measures will be collectively referred to as protection or P. The backup protection system is labeled as X which will take the control of C in isolation in case P fails.

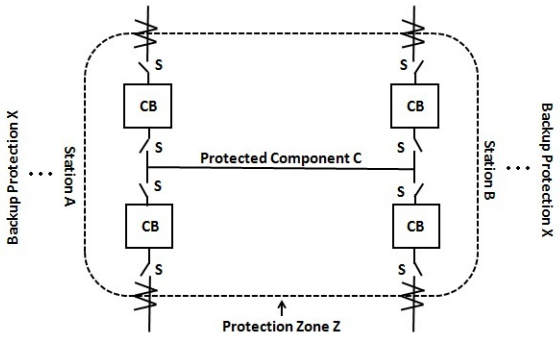

Figure 1: Protected Smart Grid Component in a Zone

A. Probabilistic Properties

Some of the significant probability computations are mentioned below.

- The most undesirable event in our system is the one when both P and C are down. Since the P is not ready to respond as well so this event is usually termed as the “abnormal unavailability”[2].

$$abnormal\ unavailability = P_4 + P_8 \qquad (1)$$

The behavior is abnormal because before State 4, C is always UP, but in State 4 both C and P go DN simultaneously. In State 8, backup protection isolates the faulty C as P is still DN. The property *S=? [s=4 | s=8]* asseses the probability associated with the abnormal unavailability event.

- The second most undesirable event in our system occurs when P is unavailable at a point when it is needed. Hence, C is UP and P is unable to respond. This will help in calculating the duration of time, in which P is unable to work while C is UP.

$$Unavailability\ of\ P = P_3 + P_5 \qquad (2)$$

The property used to implement this probability is, *S=? [s=3 | s=5]*

The continuous time markov chain of the system, given in Figure 1, is provided in Figure 2.

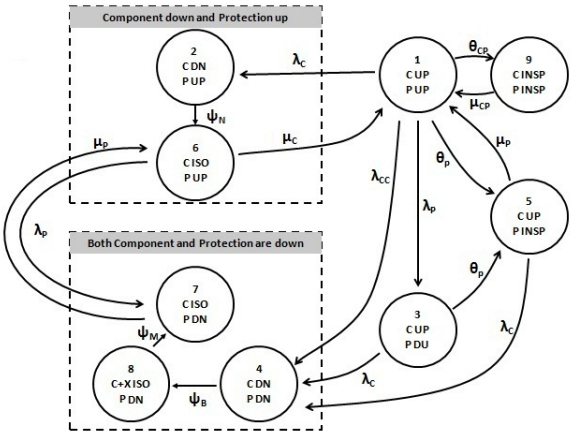

Figure 2: CTMC for the Smart Grid Component of Figure 1, where λ_c: component failure rate, λ_p: protection failure rate, λ_{cc}: component and protection common failure, μ_c: component repair rate, μ_p: protection repair rate, μ_{cp}: component and protection repair rate, θ_{cp}: component and protection inspection rate, θ_p: protection inspection rate, ψ_n: normal switching rate of protection, ψ_m: manual switching rate for component isolation, ψ_b: backup switching rate for protective system, C: component, P: protection, UP: object is good, DN: object in announced failure, DU: object in unannounced failure, ISO: object is isolated, INSP: object is in inspection

State 1 is the initial state where both C and P are UP and running. When C goes down (DN), the system enters the State 2 for a short time while P detects the failure and the system moves to State 6. If the failure is removed then the State 1 is restored, otherwise it will move to State 7 where P goes DN. When P goes in the unannounced failure (DU) in State 1 the system moves to State 3. In this state if C goes DN then the system moves to State 4, otherwise the P goes for INSP and

system enters in State 5. Similarly, in State 5, if P is repaired the system get into State 1, or else if P goes DN it enters State 4. Since, in State 4, both C and P are DN, so as soon it enters in this state, the backup protection will isolate the C while P is still DN and hence the system moves to State 8. Now, X must be restored while C and P should be repaired so the system goes into State 7. From there, if P goes UP the system will move into State 6. State 9 represents the planned maintenance of C and P.

B. Verification Results

We have used PRISM 4.1.beta2 running on an INTEL core-i5 M460 2.53 GHz processor with 2 GB memory as our platform for the analysis. Besides presenting our results, we also present some discussions about the strengths of PRISM in this particular example to emphasize upon the usefulness of using formal methods in the case of analyzing reliability.

Figure 3(a) shows the abnormal unavailability curves for different values of component failure rate (λ_c). This plot shows that on the basis of component failure rate, an optimum inspection interval can be determined for the protection system. The optimum value for protection inspection interval will be calculated before the action of back up protection system. In the curve for λ_c = 2 failures (f)/yr, the minima is found at 1025 hours ($\approx$ 43 days). After this minimum value, the curve rises again depicting the role of backup protection. The system operators should inspect and maintain the component before this situation. It is also obvious from the curves that the abnormal unavailability for higher rates is greater. The abnormal unavailability for different values of protection failure rate (λ_p) is shown in Figure3(b). The optimum inspection interval is calculated in the same manner as described previously. In the graph, for λ_p = 0.02 f/yr, the curve shows its minima at 2000 hours $\approx$ 83 days. Hence, for the specified value of λ_p, the protection must be inspected after 83 days. It can also be seen in the graph that as the failure rate increases the optimum inspection interval decreases and the abnormal unavailability for higher rates is greater.

Figure 3(c) shows the abnormal unavailability for different values of protection repair rate (μ_p). The optimum inspection interval and abnormal unavailability decrease as repair rate increases. Repair rate also indicates the number of inspections performed in a unit time. For example, if μ_p = 0.05 repair(r)/hr then it will take 20 hours to complete 1 repair. In the curve for μ_p = 1 r/hr, the optimum protection inspection interval becomes 300 hours $\approx$ 13 days.

Figure 3(d) shows the effect of protection failure rate (λ_p) on the unavailability of protection system when it is needed. It can help the designer in determining the optimum inspection interval before the protection goes down. For example, when λ_p = 0.01 f/yr, the optimum inspection interval would be 5000 hours $\approx$ 208 days. It can also be observed that for higher failure rates the probability of unavailability of protection system increases.

PRISM model checker was found to be a very helpful tool for this analysis. It allows plotting curves for different values of more than one variable on the same graph. One such graph produced by PRISM, for a sweep of λ_p and μ_p for 20 different series is shown in Figure3(e). It can be seen that when λ_p is the least, i.e, 0.01 f/yr, the inspection interval is largest and it decreases as the value of λ_p increases. For λ_p = 0.01 f/yr and μ_p = 0.04 r/hr, the optimum inspection interval would be 45 hours. This proves to be very helpful in analyzing a complex system where a number of design parameters are involved for efficient functionality of the system, which is typically the case for the reliability analysis of smart grids. It is also observed from the curves that as the repair rates increase, the optimum inspection interval decreases, which makes perfect sense because computerized inspections will be done more quickly with the advancement in technology. PRISM allows us to obtain state probabilities after certain number of iterations or a specified time . State probabilities of the model, shown in Figure 2, are given in Table I. This data indicates that the probability of being in State 1, which is our initial and the most desirable state, is 97% for a sufficiently long time.

Table I: Steady State Probabilities for the model in Figure 2

State No.	Steady State Probabilities
1	0.9724105562818497
2	2.569578041066133 x 10^{-10}
3	0.007381276835334171
4	5.927521197913861 x 10^{-11}
5	0.019593745247079058
6	5.885623476042611 x 10^{-4}
7	1.3047831631722975 x 10^{-5}
8	1.2760293038810163 x 10^{-5}
9	5.068756727861908 x 10^{-8}

The above-mentioned model was analyzed using the numerical approach in [2] . Due to the iterative nature of numerical methods, our results can be considered to be slightly more accurate given the rigorous nature of model checking. Moreover, the analysis was quite expensive in terms of computational resource utilization. On the other side, PRISM has been shown to be more efficient both in terms of number of computations and computational timeas for calculating steady state probabilities, given above, and 672407 iterations were performed in 4.68 seconds. Moreover, we have been able to obtain many results that could not be assessed using numerical techniques. For example, state probabilities cannot be judged using numerical methods. Moreover, probability of "Unavailability of Protection" was not plotted in the original case study but it was necessary to be analyzed because the component's life is highly dependent on availability of protection.

V. CONCLUSIONS

Reliability analysis of the protection systems of a smart gird plays a vital role in safe and effective working of the smart grid system and a number of analysis methods have been used in this domain. However, most of the existing reliability analysis techniques compromise on the accuracy of the reliability analysis due to their inherent nature. As an accurate analysis approach, we propose to use probabilistic model checking for conducting the safety-critical reliability analysis of the protection systems of smart grids in this paper. The main contributions of the paper include a modular approach to construct Markovian models for generic smart grid components, with back-up protection, and thus using

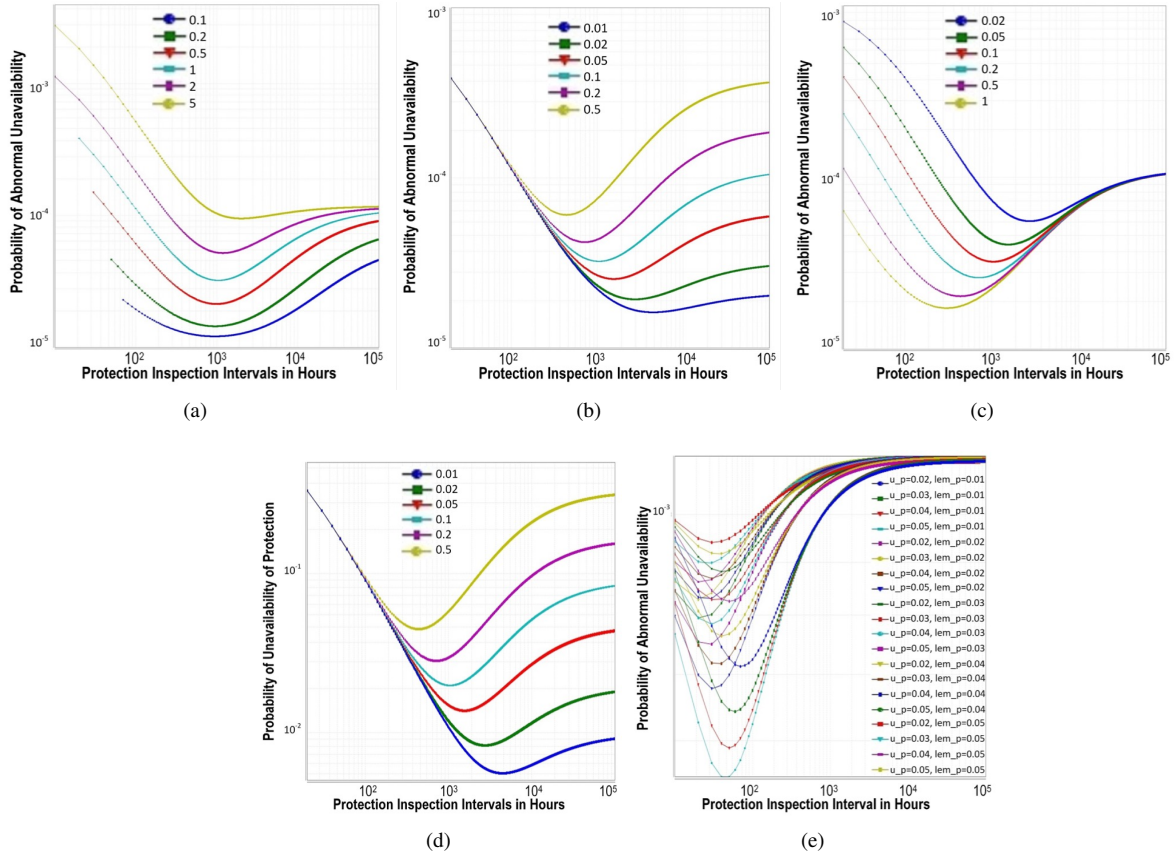

Figure 3: Probability of unavailability against the inspection interval for variation in (a) λ_c (b) λ_p (c) μ_p (d) u λ_p (e) λ_p and μ_p.

probabilistic model checking to analyze the system-level safety and reliability of smart grid systems. Our results have been found to be more rigorous and were less heavy in terms of computational requirements and CPU time requirements compared to the corresponding numerical method based results.

REFERENCES

[1] K. Adil, H. Ali, A. Tariq, and O. Hasan. *Formal Methods for Industrial Critical Systems: 18th International Workshop, FMICS 2013, Madrid, Spain, September 23-24, 2013. Proceedings*, chapter Formal Reliability Analysis of Protective Relays in Power Distribution Systems, pages 169–183. Springer, 2013.

[2] P.M. Anderson and S.K. Agarwal. An improved model for protective-system reliability. *Reliability*, 41(3):422–426, 1992.

[3] C.Baier and J.Katoen. *Principles of Model Checking*. MIT Press, 2008.

[4] L. Chen, K. Zhang, Y. Xia, and G. Hu. Scheme design and real-time performance analysis of information communication network used in substation area backup protection. In *Power Engineering and Automation Conference*, pages 1–4, 2012.

[5] A. Hall. Realising the benefits of formal methods. *Universal Computer-Science*, 13(5):669–678, 2007.

[6] A. Platzer J. Martins and J. Leite. Statistical model checking for distributed probabilistic-control hybrid automata with smart grid applications. In *Formal Methods and Software Engineering*, volume 6991 of *LNCS*, pages 131–146. Springer, 2011.

[7] G. Norman J. Rutten, M. Kwiatkowska and D. Parker. *Mathematical techniques for analyzing concurrent and probabilistic systems*. AMS, 2004.

[8] W.B. Powell J. Si, A.G. Barto and D.C. Wunsch et al. *Handbook of learning and approximate dynamic programming*. IEEE, 2004.

[9] J.Abrial. Faultless systems:Yes we can! *Computer*, 42(9):30–36, 2009.

[10] M. Kwiatkowska, G. Norman, and D. Parker. PRISM: Probabilistic symbolic model checker. In *Computer performance evaluation: modelling techniques and tools*, pages 200–204. Springer, 2002.

[11] D. Niyato, P. Wang, and E. Hossain. Reliability analysis and redundancy design of smart grid wireless communications system for demand side management. *Wireless Communications, IEEE*, 19(3):38–46, 2012.

[12] K. Poulsen. Tracking the blackout bug, 2004. http://www.securityfocus.com/news/8412.

[13] R. Robidoux, H. Xu, L. Xing, and M. Zhou. Automated modeling of dynamic reliability block diagrams using colored petri nets. *Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions on*, 40(2):337–351, 2010.

[14] J.Pan R.Yu, Y.Chen and R.W.Vesel. Generic reliability evaluation method for industrial grids with variable frequency drives. *Wireless Communications, IEEE*, 5(4B):83–88, 2013.

[15] J. Wäfler and P.E. Heegaard. A combined structural and dynamic modelling approach for dependability analysis in smart grid. In *Symposium on Applied Computing*, SAC '13, pages 660–665. ACM, 2013.

[16] E. Yuksel, H. Zhu, H.R. Nielson, H. Huang, and F. Nielson. Modelling and analysis of smart grid: A stochastic model checking case study. In *Theoretical Aspects of Software Engineering (TASE)n*, pages 25–32, 2012.

[17] R. Zeng, Y. Jiang, C. Lin, and X. Shen. Dependability analysis of control center networks in smart grid using stochastic petri nets. *Parallel and Distributed Systems, IEEE Transactions on*, 23(9):1721–1730, 2012.

[18] G. Zhanjun, C. Qing, and L. Zhaofei. Fault diagnosis method for smart substation. In *Advanced Power System Automation and Protection (APAP)*, volume 1, pages 427–430, 2011.