Interdependency Modeling in Smart Grid and the Influence of ICT on Dependability

Jonas Wäfler, Poul Heegaard

Interdependency Modeling in Smart Grid and the Influence of ICT on Dependability

Jonas Wäfler and Poul E. Heegaard

Norwegian University of Science and Technology
N-7491 Trondheim, Norway
{Jonas.Waefler, Poul.Heegaard}@item.ntnu.no

Abstract. The smart grid is a complex system consisting of interdependent power grid and information and communication (ICT) components. Complex systems have different properties than simple networks and give raise to new risks and failure types. In this paper, we study the dependencies in smart grid and the influence ICT may have on the dependability. We start with giving a categorization of the smart grid components and define state machines for these categories and for smart grid services. Then we investigate their interactions and interdependencies from a dependability perspective. Further, we investigate the positive and negative effects ICT can have on the dependability of the system. Finally, we introduce a meta-model which incorporates the information about the states of the components and services to create a state estimator for the smart grid considering ICT and power components.

1 Introduction

The reliability analysis of power grids has traditionally not included the state of supporting information and communication technology (ICT) infrastructure [1–3]. However, in the last ten years several authors pointed out the need of studying the power grid as complex network by including the cyber or ICT part in the analysis [1, 4, 5]. This complex network is called *cyber-physical* system or more general *system of systems*.

Theoretical results indicate the importance of analyzing the power grid (PG) and its supporting ICT together in one common model as a *system of systems*. It has been shown for interdependent random graphs that *system of systems* have different properties than simple systems [6]. Additionally, with an increasing number of interconnections and therefore a higher interdependency between the systems the vulnerability to random failures increases also [7].

A classification of particular types of failures which are caused by the interdependency of systems is put forward by [8]. Failures are classified as *cascading*, *escalating* and *common cause* failures depending on the interaction of the systems. Studies of major power grid incidents show that these interdependency effects between the PG and the ICT already exist in the current power grid [6,9,10]. A chain of cascading failures, i.e. failures in one system that trigger failures in another system, was a major reason for the large blackout in Italy in

2003 [6]. And an escalating failure, i.e. independent failures in the systems that amplify each other, was an important reason why the blackout in the US in 2003 could become so large [9]. Another analysis of the disturbances in the US power grid from 1979 to 1995 found that "*problems in real-time monitoring and operating control system, communication system, and delayed restoration contribute to a very high percentage of large failures*" [10]. The smart grid will rely even stronger on ICT than the legacy power grid, therefore, it can be expected that these effects will become even stronger.

The smart grid has the potential to increase the reliability of the power supply with new services like self-healing and demand response, which may reduce downtime and increase dependability [11]. However, misbehaving ICT and interdependency effects between ICT and PG have to be analyzed carefully and included into the dependability analysis, otherwise the results may be inaccurate and could lead to false conclusions about the system.

An interdependency model for the electricity and information infrastructure was presented in [12]. Using four to five different states for both infrastructures the model accommodates the three new failure types of *system of systems* as described in [8]. The model contains interesting features like passive and active latent errors; however, it is very high-level and the repair is not covered in details. Both power grid and ICT components are repaired in one step at the same time.

In 2009 an interdependency model for the power grid was put forward to illustrate the effect ICT can have on the reliability of the whole power grid [1]. In this model, both ICT and PG have a binary state variable and can either be in a normal or abnormal state leading to a four state model. The model is very conceptual and concentrates mostly on the transitions. Because of the high abstraction level most details are hidden within the states.

A more detailed approach is taken by [13] by introducing a three-level assessment hierarchical architecture consisting of a device, network and service level. Each level has its own properties and is modeled individually.

In this paper, we start bottom-up with the components constituting the smart grid and give a categorization based on their use of ICT. We then give state machines for the components and services and explain their interactions from a dependability perspective. Further, we discuss the positive and negative effects ICT can have on the dependability of the system. Finally, we introduce a metamodel which incorporates the information about the states of the components and services to create a state estimator for the smart grid considering ICT and power components.

2 Components and Services in the Smart Grid

The power grid consists of the power infrastructure on the one hand and of intelligent devices and a communication infrastructure to control and monitor it on the other hand. We categorize all components of the power grid into five categories as shown in Fig. 1. Category A contains power components with no communication means and no software like power lines and mechanical power

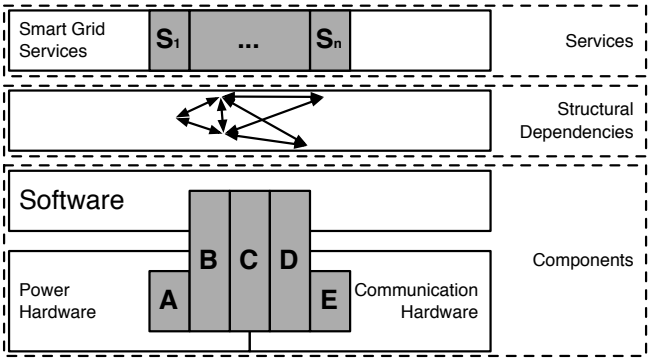

Fig. 1: Services and components of smart grids.

devices. Category B contains power components that are configurable but run autonomous and have no communication means like certain distributed energy resources. Category C contains software controlled power components with communication means like intelligent electronic devices used for monitoring and controlling the power grid. Category D contains software controlled communication components like routers. Category E contains communication components with no software like communication cables. It is important to note that some devices can be in several categories like a power cable which is also used as carrier of a PLC (power line communication) signal. Such structural dependencies can be the cause for common cause failures.

Devices in the categories B, C and D are in the following called intelligent devices. Components in A and E are called hardware (HW) components. Power HW components like power lines and transformers build the physical connections in the power grid between production sites and loads. The intelligent devices and the communication HW components are needed to operate the whole grid.

Smart grid services run on top of these components and they need a certain subset of components and other smart grid services to work. This partial dependency is called in the following *structural dependency*. The services are used to operate the power grid and include power delivery, monitoring, control, protection and more advanced services like demand response.

The biggest change in the transition from the legacy power grid to the smart grid will lie in the increase of software capabilities of B and C components and the quantitative increase of C components. In other words, the components become more intelligent and there will be more intelligent electronic devices to increase the system awareness and control, especially in the distribution grid. The latter will also lead to an increase of D and E devices in the smart grid. Additionally, the transition to the smart grid will change the power grid services. On the one hand, they are extensions to existing services like an increased monitoring and controlling in the distribution grid. On the other hand, they introduce new functionalities like smart metering or demand response.

2.1 State Machines for Components and Services

In the following we present state machines for components and services. The states are on a high level and different failure modes are not differentiated. For a quantitative analysis separate states for the considered failure modes have to be created and transition rates or probabilities assigned to the transitions.

Hardware components are modeled with two states as seen in Fig. 2. They can either be in a working state *ok* or a failed state F. Repair can happen after the monitoring system detected a failure or it can happen before when the failure is only temporary and disappears on its own.

Intelligent devices on the other hand, have a more complex failure behavior. First, we differentiate between *errors* and *failures*, as described in [14]. A fault can trigger an error in a device but only when the provided service is incorrect it becomes a failure. Differentiating errors and failures allows for example to model intermittent failures. While the failure disappears for some time, the responsible error does not. Second, a failure may be either passive (F_p) or active (F_a), depending on their behavior. We use the following definition similar to [12]:

passive failure: The device works incorrectly in a passive way, i.e. it does not respond when needed (e.g. not sending monitoring data, not responding to a control signal, not triggering a breaker when needed).

active failure: The device works incorrectly in an active way, i.e. it functions but not as intended (e.g. sending wrong monitoring data, executing the wrong control command, triggering self-healing when not necessary).

The corresponding errors are accordingly termed *passive errors (E_p)* and *active errors (E_a)*. A device may also directly change its state from *ok* to F_p for example if parts of the hardware fail.

The devices are controlled by highly capable software which may cause harm to the system if working incorrectly. Due to the potential complexity of designing, configuring and updating such devices, faults are likely and errors may reside undiscovered in a device for a long time. Faults can be unintentional like design and configuration faults but also intentional like viruses/worms, intrusions and sabotage. Design, configuration or maintenance errors like software bugs, erroneous configuration/reconfiguration or the distribution of a faulty software update will affect potentially many devices at the same time. Failures may propagate on their own like in the case of a virus or a worm. The degree of the spreading depends on the detection and repair time.

The state of smart grid services may depend on the working and operational state of certain components, their structural dependencies, other services and on the input or the situation the system is in. The working states of a component are the states described above, the operational states are states in normal operation which can have an influence on a service. For example an open breaker which was opened by an undetected failure in an IED may cause the disconnection of parts of the grid and a state change for a service. The reason for the state change is the operational state of the breaker and only indirectly a failure. A service is said to be in the failed state F if the service produces incorrect output.

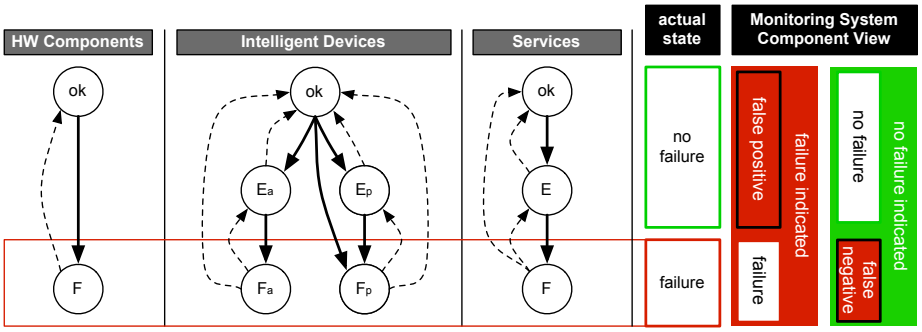

Fig. 2: State machines for components and services and the perception of their state in the monitoring system.

If components fail which are necessary to create correct output but the output itself is not yet incorrect, then the service is in the error state E. For example, consider a protection service which is responsible for opening breakers in a high overload situation. This service relies on protection devices installed throughout the power grid. The failure of one of these devices is already critical if there are no redundant devices. However, as long as there is no overload in which this specific device is needed to operate the service does not produce wrong output, hence the service is in the error state E while the device itself is in a failed state. In the error state the failure probability is much higher than in the working state. It is not the same as a failed state because for dependability analysis this state is considered as *not failed*. The monitoring system may detect the device failure and initiate the repair before the service fails.

2.2 Interactions

The components and services are highly depending on each other. The transitions between the states depend theoretically on the state of all the other components and services at a given time. For practical analysis of large systems the states may be modeled as depending only on the state of a subset of all components and services which are either geographically or logically close. In the following, we discuss the influence components can have on other components or services depending on their states.

Influence of HW Components

F A failure may increase the load on other HW components and the probability for them to fail. This is especially the case for power HW components. Intelligent components may fail if a power HW component fails and there is no other power source (transition into F_p).

Influence of Intelligent Devices

$\mathbf{E}_a$ and $\mathbf{E}_p$ Errors have by definition no effect on other components.

$\mathbf{F}_a$ An active failure may cause a change in the operational status in another component, e.g. opening a breaker, increasing power production instead of decreasing. This may lead to a critical situation and eventually even to a hardware failure or a service failure. An active failure may also cause errors and failures in other ICT components, e.g. by spreading harmful configuration or virus. It can also cause a smart grid service to not function properly.

$\mathbf{F}_p$ A passive failure may cause a smart grid service to not function properly because for example necessary information is not delivered or information is not received and processed by the component. A passive failure may also lead to a failure in a power grid HW component, e.g. by not alarming the control center about a critical situation which could lead to an overload failure.

Influence of Services

E An error has by definition no effect on other components or services.

F A failure can cause problems for the components or services relying on the output of this service. It may provoke a critical situation end eventually even to a failure in a component. For example, if the service *demand response* is increasing the loads instead of decreasing. If this happens in a distribution grid with a high number of charging electrical vehicles it could lead to an overload in that particular area and eventually even to a blackout, i.e. a failure of the power delivery service.

2.3 Perception of Components and Services

The monitoring system has its own perception of the system which is not the same as the actual state of the system. This is because the monitoring system is also just a service which can fail. The monitoring system can either indicate *failure* or *no failure*. The error states are considered as *no failure* as the delivered service is per definition still correct. As shown in Fig. 2 the indication can be wrong, i.e. be a *false positive* if a failure is indicated when there is none or be a *false negative* if no failure is indicated when there is indeed one.

The deviation of the indication in the monitoring system from the actual state is critical. If false positives are frequent it may cause high costs for the clarification of the cause and eventually to a loss of trust. False negatives may prolong the time a component or service stays in the failed state which decreases the dependability of the system. The longer a component is in the failed state the longer the negative interactions described above take place and more state changes in other components may happen.

2.4 Techniques for Quantitative Analysis

A difficulty when modeling the smart grid for quantitative analysis is that it consists of dynamic parts, i.e. the components with their state machines, and

structural parts, i.e. the structural dependencies between services and components. This becomes clearer when considering the smart grid services. The working and failed state of a given service may be described by a fault tree, where the events are failures of components or other services. This fault tree represents the structural dependency of the given service. The dynamic parts are the different failure modes leading to the events, i.e. failure of components or services.

A straight forward way of quantitatively analyzing a service is by creating markov models for each individual component and computing with them the dependability parameters needed for the fault tree. In this way, both availability and reliability of a service can be computed. However, this method assumes all events or state changes to be independent which is a very strong assumption and usually not true in real systems.

A way of including dependencies between components in an analytical model has been proposed in [15]. It starts with a reliability block diagram, i.e. a structural model which is equivalent to a fault tree and has the same independence assumption. The dependencies are then included by either isolating them or by using a combination of pivotal decomposition and markov chain. This method is most useful if the number of dependent components is small.

Another solution is to use a stochastic reward net (SRN) [16] which is an extension of a stochastic Petri net. The state machines from Fig. 2 can be used as a basis for the SRN in which the individual components and services are modeled as tokens. The transitions in SRN may be enabled by boolean functions on the markings of states and the transition rates may also depend on the marking of states. This allows to create a small model for a complex problem. However, this holds only if the components or services are treated as anonymous. If the identity of the different components and services become important, the model becomes more complex as well.

If the two mentioned methods are unpractical then a simulation may also be used for quantitative analysis.

3 Role of ICT in the Smart Grid

ICT components and services have a large potential for supporting the operation of a smart grid and increasing its dependability. The software part allows for smarter decision making processes and the communication allows for sharing information. Both are important for the most fundamental services: monitoring and controlling. An optimal monitoring system shows the actual state of the system with as little delay as possible and minimizes the discrepancy between perceived and real state. Precise data can help to operate the system in an optimal state and reduce errors and failures in the first place. For example, exact monitoring data in the distribution grid may optimize its use, maintenance and replacement, i.e. not wasting capacity or wearing the infrastructure unnecessarily out and preventively initiate repair or replacement before an incident happens. In case of a failure the monitoring service helps to detect and localize the failure. The reparation time may also be shortened by finding an optimal repair strat-

egy, by self-healing or by enabling the repair or mitigation by remote control, e.g. by isolating a line failure and possibly reconnect disconnected loads by an alternative route to reduce the impact of the failure.

By aggregating the data from the components new insights can be gained. For example, by finding patterns for failures which might improve error and failure prevention or failure detection. With a wide-area monitoring and control, enabled by communication, the optimal strategy for operation can be found for a certain area or the whole grid and not only for the local component. In case of an incident a coordinated protection or isolation scheme may prevent a propagation of the failure in the system.

While ICT can help to improve dependability, it can also have a negative effect. Passive failures in monitoring lead to a mismatch between perception and reality. A critical situation or failure may not be detected due to the missing data. In a controlling service a passive failure in a component leads to the disregard of the control signal. If no acknowledgment message is used this stays undetected and a mismatch between the assumed state of the component and the real state arises.

Passive failures reduce the potential improvement of ICT. The total failure of an ICT service nullifies its effect and intuitively one may conclude that additional ICT services will either improve the dependability of the whole system or at least keep the status quo. However, this is a dangerous conclusion because of two reasons. First, if services or controllers blindly rely on the service a passive failure may have a worse effect as not having the service at all. In the former case there is a strong assumption that the service works correct, in the latter case there is no correctness assumption and nobody is left with a false sense of security. Second, active failures may trigger new failures which would not exist without the specific service or ICT component.

Active failures in monitoring lead to a mismatch between perception and actual state and eventually even to undesired decisions and actions. For example, wrong information about the status of a breaker or the load of a line can trigger the isolation of a power grid part and lead to an unnecessary outage. Active failures in controlling lead also to a mismatch of perception and actual state but have in addition a direct effect on some components. Examples are protection devices initiating a protection process, breakers opening or closing, or the sending of wrong control signals. Frequent active failures of ICT components may negate the positive effect ICT can have and lead to an overall negative effect.

Last but not least, ICT plays a big enough role in the smart grid to qualify it as *system of systems*, which have particular interdependency effects and failure types, i.e. *Cascading Failure*, *Escalating Failure*, and *Common Cause Failure* [8].

4 Aggregated view for the Control Center

In the legacy power grid the control centers for the power grid and the communication system are usually separated. However, as new failure paths emerge in the smart grid which originate in or include ICT components, it becomes crucial

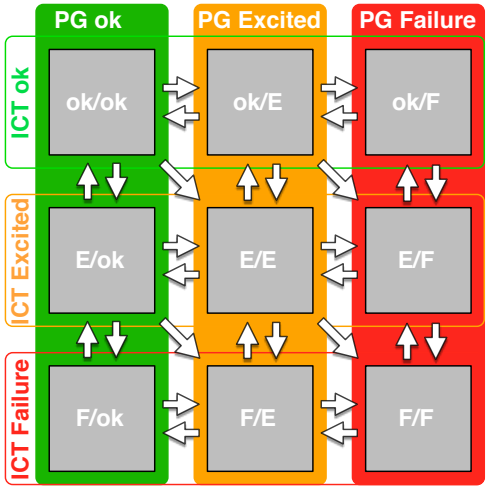

Fig. 3: Meta-model for smart grid.

to incorporate the information of both into the state estimation of the whole smart grid. This allows an early detection of possible failures coming from the ICT components.

In the following, we propose a meta-model to describe the state of the whole system for the control center. The meta-model is an aggregation and interpretation of the information from the monitoring system to determine the criticality level of the system. It has two axis using the states of the power grid (PG) and the ICT, see Fig. 3. The most important service in the power grid is the power delivery to the customers. The state of this service plus the state of supporting components are used to determine the power grid (PG) state. On the other hand, the states of ICT components and services are used together with a logic which indicates which services are critical to determine the state of the ICT system.

The model follows a service-centric approach. *Failure* means a service is not delivered correctly and action has to be taken immediately. *Excited* means that the service may run soon into a critical situation. More detailed, the states of the two axis are defined as:

PG ok: The system operates normally.
PG Excited: All customers are powered but the system is excited (N-1 redundancy is harmed, the load is critical, etc.)
PG Failure: At least one customer is disconnected from the power supply.

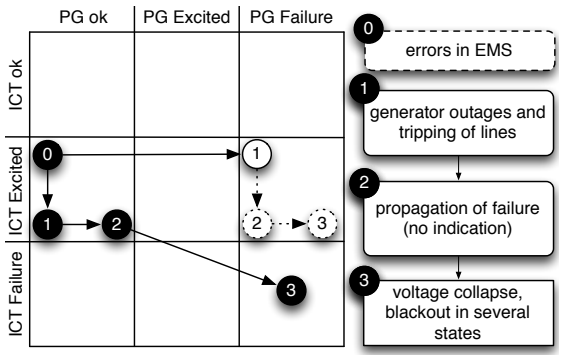

Fig. 4: Events in ICT and PG during an escalating failure in the US in 2003 as seen by the control center. The black disks indicate the information about the events as it happened. The white disks show how it could have been with a working detection mechanism, may be stopping the chain after event 1 or 2.

ICT ok: The ICT system operates normally.
ICT Excited: All critical ICT services are delivered correctly but the system is excited (non-critical components failed, congestion in the system)
ICT Failure: Some critical ICT services are incorrectly delivered.

The nine states are then created by the intersections of this two axis. Both excited states denote states of the system where the corresponding system is still working correctly but the stability and robustness is decreased. They are a key factor in the meta-model because the system may be much weaker than in the failure-free state and failures may propagate.

The states are as perceived by the control center and can be wrong as discussed above. These monitored states should be as close to the real states as possible. The fast detection of failures reduces the risk that the failure can propagate or cascade to other components. Monitoring should also be reliable to reduce the risk of having false positives and false negatives.

The meta-model is a highly condensed view of the whole grid to create a clear and easy understandable warning system. Due to the aggregation it is highly scalable. In large systems or in presence of autonomous structures like micro grids it may be useful to use several meta-models.

4.1 Applications

The primary application for the proposed meta-model is the state indication of the smart grid for the control center as explained above. However, there are additional applications.

In ex post incident analysis the meta-model can be used to show the basic cause and effect chains in a clear way and study alternative scenarios. In Fig. 4 we give an example of such an analysis by showing the events of an escalating failure in the US in 2003 [9]. In short, several generators had an outage, which

led to a tripping of several lines. When that happened, the energy management systems (EMS) of the two responsible network operators were not fully functional and the failure could propagate in the PG and ended in a voltage collapse and a blackout spanning several federal states. In the figure, the black disks indicate the information the control center had during the events. The control center knew about the reduced functionality of the EMS but did not learn about the outage in the power grid until it was too late. The white disks indicate the information the control center would have had if the monitoring system had worked. The first outage could have been detected and the failure perhaps isolated which could have stopped the chain of events.

As an extension of the ex post incident analysis the meta-model can also serve as a tool to visualize and illustrate interdependencies in two systems. The new failure types propagation, escalation and common cause failures can be explained in an intuitive way and new failure paths are revealed.

5 Conclusion

The wide introduction of ICT changes the way the smart grid may fail. It is necessary to consider the states of both the ICT and the PG in the dependability analysis due to the following reasons:

- Dependability analysis for smart grid services yield inaccurate results if the possible non-functioning or malfunctioning of ICT is not included. ICT can have special dynamics like failure propagation within the system and active latent errors, which can have a strong effect on the smart grid.
- ICT plays a big enough role in the smart grid to qualify it as *system of systems*, which introduces particular interdependency effects and failure types. In individual models it is difficult to include those.

In this paper we categorized the smart grid components and services and showed the interactions between them. We motivated that their state and especially the state of the ICT components and services will play an important role in the dependability analysis of smart grids. We proposed a meta-model which takes this into account and combines the states of ICT and power grid components and services. It can be used as a tool for the control center to estimate the state of the smart grid. The proposed meta-model facilitates the understanding of the mechanisms of previous incidents by tracing their trajectories in the model. The simple structure creates an intuitive model that allows explaining the interdependencies and new failure types that are created by connecting systems. Understanding the risks is the first step to make a system more dependable and secure.

This work is meant to generally describe dependencies in the smart grid and to create a basis for future work. Future work will focus on specific interactions and interdependencies of components and services. We are especially interested in studying the new failure modes and evaluating and quantifying the dependability effects of new smart grid services.

References

1. D. Kirschen and F. Bouffard, "Keeping the lights on and the information flowing," *IEEE Power and Energy Magazine*, vol. 7, no. 1, pp. 50–60, Jan. 2009.
2. A. Bose, "Models and techniques for the reliability analysis of the smart grid," in *Proc. IEEE PES General Meeting, Minneapolis, USA*, Jul. 2010, pp. 1–5.
3. C. Singh and A. Sprintson, "Reliability assurance of cyber-physical power systems," in *2010 IEEE PES General Meeting, Minneapolis, USA*, Jul. 2010, pp. 1–6.
4. M. Amin, "National infrastructure as complex interactive networks," in *Automation, control and complexity*, T. Samad and J. Weyrauch, Eds. New York, USA: Wiley, 2000, pp. 263–286.
5. R. G. Little, "Toward more robust infrastructure: Observations on improving the resilience and reliability of critical systems," in *Proc. of 36th Annual Hawaii International Conference on System Sciences (HICSS'03) - Track 2 - Volume 2*, 2003, pp. 58–66.
6. S. V. Buldyrev, R. Parshani, G. Paul, H. E. Stanley, and S. Havlin, "Catastrophic cascade of failures in interdependent networks," *Nature*, vol. 464, no. 7291, pp. 1025–1028, Apr. 2010.
7. R. Parshani, S. V. Buldyrev, and S. Havlin, "Critical effect of dependency groups on the function of networks," *Proc. National Academy of Sciences of the United States of America*, vol. 108, no. 3, pp. 1007–1010, Jan. 2011.
8. S. Rinaldi, J. Peerenboom, and T. Kelly, "Identifying, understanding, and analyzing critical infrastructure interdependencies," *IEEE Control Systems*, vol. 21, no. 6, pp. 11–25, Dec. 2001.
9. G. Andersson *et al.*, "Causes of the 2003 major grid blackouts in north america and europe, and recommended means to improve system dynamic performance," *IEEE Trans. Power Syst.*, vol. 20, no. 4, pp. 1922–1928, Nov. 2005.
10. Z. Xie, G. Manimaran, V. Vittal, A. G. Phadke, and V. Centeno, "An information architecture for future power systems and its reliability analysis," *IEEE Trans. Power Syst.*, vol. 17, no. 3, pp. 857–863, Aug. 2002.
11. V. V. Vadlamudi, R. Karki, G. H. Kjølle, and K. Sand, "Challenges in smart grid reliability studies," in *Proc. 12th Int. Conf. on Probabilistic Methods Applied to Power Systems (PMAPS), Istanbul, Turkey*, June 2012.
12. J.-C. Laprie, K. Kanoun, and M. Kaâniche, "Modelling interdependencies between the electricity and information infrastructures," in *Proc. SAFECOMP, Nuremberg, Germany*, 2007, pp. 54–67.
13. R. Zhang, Z. Zhao, and X. Chen, "An overall reliability and security assessment architecture for electric power communication network in smart grid," in *Power System Technology (POWERCON), 2010 International Conference on*, Oct. 2010, pp. 1 –6.
14. A. Avizienis, J. C. Laprie, B. Randell, and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing," *IEEE Trans. Dependable and Secure Computing*, vol. 1, no. 1, pp. 11–33, Mar. 2004.
15. J. Wäfler and P. E. Heegaard, "A combined structural and dynamic modelling approach for dependability analysis in smart grid," in *Proceedings 28th ACM Symposium on Applied Computing (SAC), Coimbra, Portugal*, March 2013, pp. 660–665.
16. J. K. Muppala, G. Ciardo, and K. S. Trivedi, "Stochastic reward nets for reliability prediction," in *Communications in Reliability, Maintainability and Serviceability*, 1994, pp. 9—20.