2014 IEEE 15th International Symposium on High-Assurance Systems Engineering

Towards Comprehensive Modeling of Reliability for Smart Grids: Requirements and Challenges

Koosha Marashi and Sahra Sedigh Sarvestani
Department of Electrical and Computer Engineering
Missouri University of Science & Technology
Rolla, Missouri 65409
Email: {koosha.marashi,sedighs}@mst.edu

***Abstract*—Smart grids utilize computation and communication to improve the efficacy and dependability of power generation, transmission, and distribution. As such, they are among the most critical and complex cyber-physical systems. The success of smart grids in achieving their stated goals is yet to be rigorously proven. In this paper, our focus is on improvements (or lack thereof) in reliability. We discuss vulnerabilities in the smart grid and their potential impact on its reliability, both generally and for the specific example of the IEEE-14 bus system. We conclude the paper by presenting a preliminary Markov imbedded systems model for reliability of smart grids and describe how it can be evolved to capture the vulnerabilities discussed.**

***Keywords*—cyber-physical systems; reliability modeling; vulnerability analysis; smart grid;**

I. Introduction

Tight coupling of a complex physical system with computation and communication results in a cyber-physical system (CPS). Modern critical infrastructure systems, e.g., smart grids, intelligent water distribution networks, or health information networks, are examples of CPSs that exhibit significant dependence on the cyber components. The application of digital technologies (i.e., microprocessor-based measurement and control, communications, computing, and information systems) is expected to improve the reliability, security, interoperability, and efficiency of critical infrastructures, while reducing environmental influences and promoting economic growth [1]. Verifying the success of CPSs in increasing the reliability, resiliency, flexibility, and efficiency of physical systems is an increasingly urgent task, given the ubiquitous use of CPSs in critical applications. Impairment of components in the cyber infrastructure is very likely to have consequences for the physical system, and ultimately, could degrade its functionality or cause a complete breakdown. Our past work has illustrated such failure propagation for power and water CPSs, respectively [2], [3].

The focus of this paper is on the CPS domain of smart grids. The high complexity of the electric power grid has motivated the use of cyber infrastructure to fortify its operation, culminating in the development of smart grids. In the modern power grid, the required intelligence is based on the integration of current-carrying components (e.g., generators and transmission lines) and power electronics with computing and communication.

Smart grids are among the most critical and ubiquitous CPSs, whose design aims at achieving fault tolerance, security and decentralized control. Therefore, developing a reliability model that captures effects of impairments in both the physical infrastructure and the cyber control would help engineers to design a dependable, efficient electric delivery system. In this study, we survey requirements for developing a comprehensive reliability model for smart grids and challenges in providing and using required analytical data. In our past work, we have developed a quantitative model that achieves the same task; i.e., integrated cyber-physical modeling of reliability; for a specific case - the IEEE-118 bus system [4], [5]. Our model is based on the Markov Imbeddable Systems (MIS) technique [6]. The focus of this paper is on generalization of our preliminary model to other systems - a task that is far from trivial considering the complexity of even a very limited Smart Grid. We present this generalization in the context of the IEEE-14 bus system. This is a step back in scale (from our previous modeling of the IEEE-118), but several steps forward in complexity and applicability, as we account for a broad range of control and communication techniques and describe the requirements for representing them in the model.

The remainder of this paper is organized as follows. Section II presents a summary of related literature. Section III presents the methodology for developing a reliability model and Section IV describes the elements that should be represented in a comprehensive reliability model for smart grids. Challenges on developing a reliability model for the example of IEEE-14 are presented in Section V. It also reviews susceptible domains in this example. Finally, Section VI concludes the study and outlines the future work.

II. Related Work

Modeling and prediction of non-functional attributes such as reliability, security, and interoperability can be useful in increasing the dependability of critical infrastructures. The CPSs underlying these complex systems exhibit significant heterogeneity, which makes it difficult to develop a unified model that captures their behavior. Furthermore, accurate modeling requires understanding of the joint dynamics of embedded computers, software, networks, and physical processes [7]. Despite increasing activity in research related to CPSs, such models are still scarce, and primarily qualitative [8], [9].

Providing reliable power delivery has always been an essential requirement in the design and maintenance of power generation and distribution systems. As such, studies on the reliability of electric power grids are abundant. In Ref. [10], authors investigate the main challenges in modeling the reliability

978-1-4799-3466-9/14 $31.00 © 2014 IEEE
DOI 10.1109/HASE.2014.23

of the power grid. The authors study computational limitations, availability of suitable analytical models, and conceptual difficulties in defining appropriate metrics. Another related study is Ref. [11] which mainly focuses on reliability of power transmission systems. The paper investigates the reliability of a system of two parallel transmission lines, given the distribution functions for the uptime and downtime of each. Ref. [12] describes an analytical approach and a Monte Carlo simulation technique for evaluating the reliability indices of distribution systems using a method of representing a non-exponentially distributed state by a combination of stages, each of them is exponentially distributed.

In Ref. [13], Zio and Golea use a graph-theoretical approach to model the reliability of the power grid. The goal is to find the most vulnerable nodes and edges with respect to attacks and accidental failures. They have formulated the reliability model considering both electrical (impedance of transmission lines) and reliability (probability of failure in network components) indices. The paper also shows that other weighted indicators can be defined as complements to the topological indicators to quantify the criticality of network components.

The authors of Ref. [14] have analyzed and compared the effect of installing network automation devices on reliability indices such as the System Average Interruption Frequency Index, System Average Interruption Duration Index, and Average System Interruption Duration Index. They have investigated the use of several network automation devices that can be utilized to prevent failures or minimize subsequent effects. Examples are circuit reclosers or switch gear with breaker functions and remote-controlled disconnectors.

In the study presented in Ref. [15], the authors propose two approaches; namely, Stochastic Activity Networks (SAN), and Stochastic Well-formed Nets (SWN) to modeling and quantification of the interdependency between the electrical and information infrastructures. The main idea is to analyze the performance of the electric power system when encountering a cyber-attack. In a similar study, the performance of the system is qualitatively evaluated [16].

IEEE-14 is a popular bus system and is used in many studies. One example is Ref. [17], which investigates cascading failures while considering the power flow capacities of transmission lines. In another study presented in Ref. [18], the authors study the effect of installing UPFC devices on the IEEE-14 system. They determine the consequences of single-line contingencies in terms of increase in the power flow of transmission lines and occurrence of voltage violations in buses, and try to mitigate these effects by installing UPFCs at optimal locations of the grid. The work presented in Ref. [19] is related, as it illustrates the computation of real-time reliability of the network based on the reliability of transmission lines and the concept of cascading failure. All of the aforementioned studies consider failures in only the physical infrastructure of the grid. Furthermore, very limited (if any) computation and communication is assumed or reflected.

The work presented in our paper builds upon our earlier work on reliability modeling of cyber-physical smart grids [2], [20], [21]. The differentiating factor between our work and the studies presented earlier in this section is our consideration of the role of the cyberinfrastructure. Earlier studies have considered grids with very limited computing and computation, essentially physical power generation and distribution infrastructures. Models that reflect the interdependence between cyber and physical components have been of a qualitative nature. In contrast, our work aims at developing a single integrated quantitative reliability model that captures impairments in both physical and cyber infrastructures for smart grids. In our previous work we used a hardware-in-the-loop simulator to investigate the IEEE-118 bus system (which has 118 buses and 186 transmission lines). As briefly outlined in Section V, we studied failure scenarios for specific type of cyber control - Flexible AC Transmission System (FACTS) devices, which adjust the flow of power to prevent outage of transmission lines as a result of overload. Our current focus, as described in this paper, is generalizing our earlier reliability model by expanding the scope of failures considered from FACTS devices to control algorithms, measurement systems, operators, and the communication network. In the interest of clarity, we illustrate these concepts for the IEEE-14 bus system.

III. Markov Chain Imbeddable Structure

The overall reliability of a smart grid as a CPS is a function of the respective reliabilities of its elements, including both physical components, e.g., generators and transmission lines, and cyber components, e.g., control software, communication links, FACTS devices, and sensors. As such, we chose the MIS technique [6] - an analytical method for reliability evaluation of systems with interdependent components - as the mathematical foundation for our proposed reliability model. Our past and current work has this foundation in common; they differ considerably in the scope of components (and hence failures) considered.

The MIS model requires identification of "Functional" and "Failed" states of the system, and computes the system reliability as the probability of being in one of the "Functional" states. The state of a system with n components can be represented by an n-dimensional binary vector, S, each element of which reflects the operational state (functional or failed) of one component. 2^n such vectors exist, reflecting all possible states. Let $\mathbf{\Pi_0}$ denote a vector of probabilities, where $Pr(Y_0 = S_i)$ is the probability of the system initially being in state S_i. In a normal system, the initial state would be S_0, which represents a system with no component failures.

$$\mathbf{\Pi_0} = [Pr(Y_0 = S_0), Pr(Y_0 = S_1), \ldots, Pr(Y_0 = S_N)]^T \tag{1}$$

Furthermore, for a given component, l, the matrix Λ_l represents the state transition probabilities of the system as a function of l. In other words, each element $p_{ij}(l)$ in the matrix Λ_l represents the probability that the system will switch from state S_i to state S_j due to the failure of component l.

Finally, a vector $\mathbf{u}$ is defined, with length equal to the number of states, where each element has a value of 1 if the corresponding state is considered a "Functional" state for the system, and 0 otherwise. The overall reliability of the n-component system can be expressed as:

$$R = (\mathbf{\Pi_0})^T \left(\prod_{l=\mathbf{1}}^{n} \mathbf{\Lambda}_l \right) \mathbf{u} \quad (2)$$

IV. Structure and Components of Smart Grids

Rapid developments in generation and consumption of power are causing increasing stress on distribution networks. Among other benefits, cyber control brings more efficient use of the limited capacity available. However, each additional component used in this cyber control is a potential source of failure, and the net effect of this increased vulnerability and complexity on the overall reliability of the grid requires careful examination. A comprehensive reliability model should be able to consider every potential source of failure and reflects its effect on the overall system state. The remainder of this section enumerates the main categories of components that comprise a smart grid and can affect its operation by causing or decreasing the likelihood of failure. The categories are depicted in Figure 1.

A. Physical (Electrical) Infrastructure Components

Electric delivery systems are primarily composed of current-carrying components, including generators and transmission lines. Reliability analysis is often performed by classifying the physical (electrical) infrastructure into hierarchical levels where generation, transmission, and distribution facilities form levels I to III, respectively [22]. However, in the advanced electric power grid, Distributed Energy Resources (DERs) are considered generation facilities that are dispersed throughout the electricity network. DERs are small power generation plants that generate extra electricity and supplement the electricity supply from bulk generation plants. Although DERs enhance the reliability and availability of the electric power grid, their addition complicates reliability analysis. However, in many studies, transmission lines are assumed to be the main sources of vulnerability, as generation units and similar components typically have enough backup to compensate for their failures [11], [21]. With this assumption, reliability analysis of a power grid usually entails tripping transmission lines, one-at-a-time, and inspecting the resulting state of the system in terms of power flow overloads and voltage violations. This process is also referred to as $N-1$ *contingency analysis*. A typical assumption is that the failure of more than one transmission line will degrade the system to an unusable state. Our previous work has shown this assumption to be untrue - up to three lines could fail without causing a cascade [5]. As consider concurrent failure of multiple transmission lines in determining the state (functional or failed) of the smart grid.

B. Control Devices

Power flow control has traditionally relied on generator control and voltage regulation by means of tap-changing and phase-shifting transformers. Phase-shifting transformers have been used to regulate active power in transmission networks, but are often found to be ineffective, as they operate with permanently fixed angles and lack the adaptability shown by variable tapping [23]. In addition, series reactors are used to reduce power flow and conversely, series capacitors are used to increase the power flow. In general, series compensation is switched on and off according to load and voltage conditions. Until recently, these solutions served well the needs of the electricity supply industry.

FACTS devices are a recent technological development in electrical power systems. The FACTS concept is based on the incorporation of power electronic devices into the high-voltage side of the network, to make it electronically controllable. Early developments of the FACTS technology were in power electronic versions of the phase-shifting and tap-changing transformers. These controllers, together with the electronic series compensator, can be considered the first generation of FACTS devices. The Unified Power Flow Controller (UPFC), the Static Compensator (STATCOM), and the Interphase Power Controller (IPC) are more recent developments [23]. The hardware-in-the-loop simulator used in our previous work included UPFCs. Generalization of our model requires relaxation of this constraint and is one of the objectives of our current efforts.

C. Communication

One important feature of smart grids is the integration of high-speed and reliable data communication networks to manage the complex power grid effectively and intelligently [24]. The communication backbone of power systems is responsible for information exchange among distributed power devices to assist the functioning of management systems. The reliability of power management is hence contingent on a reliable communication backbone. In other words, power systems cannot operate correctly unless reliable communication takes place among intelligent electronic devices. Communication networks used in smart grids are typically of three types: wide-area networks, field area networks, and home area networks.

Wide-area networks form the communication backbone that connects the highly-distributed smaller networks (micro-grids) that contribute to the power systems. When the control centers are located far from the substations or consumers, real-time measurements taken at the electrical devices are transported to the control centers through wide-area networks. In the reverse direction, the wide-area networks transport commands from control centers to the electric devices.

Field area networks are typically used as communication facilities for distribution systems. The main information sources to be monitored and controlled by the distribution management system at the control center include the electrical measurement devices on the distribution feeders and transformers, electronic devices capable of executing control commands from distribution management systems, DERs in the distribution systems, plug-in electric vehicle charging stations, and smart meters at customer premises form. The power system applications operating in the distribution domain utilize field area networks to exchange this information.

Home area networks are needed in the customer domain to implement monitoring and control of smart devices on customer premises and to implement functionalities such as automatic metering. Within the customer premises, a secure two-way communication called Energy Services Interface (ESI) exchange information between the utility and the customer.

These networks may be implemented using public (e.g., the Internet) and/or non-public networks. Both public and

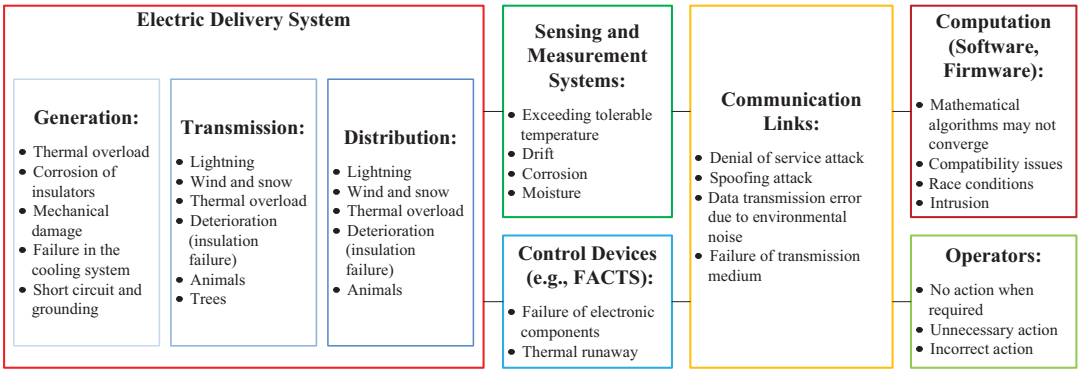

Fig. 1. Vulnerabilities of smart grids.

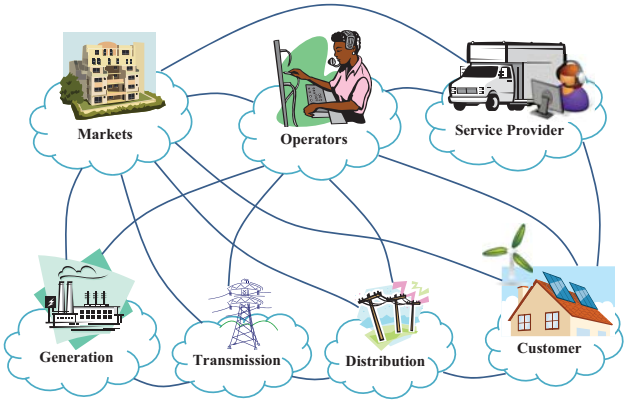

Fig. 2. Communication in a smart grid (adapted from [1]).

non-public networks will require implementation and maintenance of appropriate security assurance to support smart grids. Examples of where communications may go through the public networks include: customer to third-party providers, bulk generators to grid operators, markets to grid operators, and third-party providers to utilities [1]. To effectively manage these complex power system, a communication infrastructure is required to coordinate the distributed functions across the entire power system, the constituents of which can be broadly categorized into the following domains, which are also depicted in Figure 2.

Generation: Generation units communicate with the market domain through a market services interface over the Internet, and with the operation domain over the wide-area network. The information communicated to other domains includes key parameters such as generation capacity and shortage. The generation domain is composed of electrical equipment including remote terminal units, programmable logic controllers, equipment monitors, and fault recorders.

Transmission: To achieve self-healing and enhance wide-area situational awareness and control, a significant amount of data is captured from the grid and sent to the control centers. The control centers in turn send responses to devices in remote substations. Prompt detection of transmission contingencies is critical to ensure satisfactory power quality and service. The common method of automated transmission line monitoring is installing sensors along the lines to collect real-time status information, which is relayed through transceivers associated with the sensors until it reaches a measurement collection site connected to the wide area networks used for communication with the control office.

Distribution: Distribution networks interact with many different entities, such as DERs, plug-in electric vehicles, automatic metering infrastructure, and sensors with communication capability. The distribution domain takes the responsibility of delivering electricity to energy consumers according to user demands and energy availability. In order to provide high-quality electricity, the stability of this domain is monitored and controlled.

Operation: The operation domain communicates over field-area and wide-area networks in the distribution and transmission domains to obtain information about power system activities such as monitoring, control, fault management, maintenance, analysis, and metering. The information is obtained using the Supervisory Control And Data Acquisition (SCADA) systems.

Market: Effective communications between the bulk producers of electricity, the DERs, and the market is essential to match the production of electricity with its demand.

Customer: The customer domain is electrically connected to the distribution domain and communicates with the distribution, operation, service provider, and market domains. A communication network within the customer premises is required to allow exchange of data and control commands between the utility and the smart customer devices. These facilities support applications such as remote load control, DER monitoring and control, in-home display support for customer usages, reading of non-energy meters, and integration with building management systems [25].

Service Provider: Service providers communicate with the operation domain to obtain metering information and for situational awareness and system control. They must also communicate with home area networks in the customer domain through the energy services interface to provide smart services such as management of energy use and home energy generation.

A broad range of network technologies can be used for

communications in the transmission, distribution and customer domains in the smart grid, but none of them suits every application. The network technologies available to smart grid applications are as follows:

Wireline Networks: Dedicated wireline cables can be used to construct data communication networks that are separate from electrical power lines. These dedicated networks require extra investment for cable deployment, but can offer higher communication capacity and shorter communication delay.

Power Line Communication (PLC): Power lines are mainly used for electrical power transmission, but they can also be utilized for data communication. Power line communication systems operate by sending modulated carrier signals over power transmission wires. One method of PLC is Broadband over Power Line (BPL), which is a system for two-way transmission of data over the electrical distribution wiring of a metropolitan area.

Wireless Networks: Advances in wireless networking technology can potentially eliminate the need for installation of wirelines. However, wireless networks usually provide short-distance connections with comparatively low data rates, due to transmission attenuation and environmental interference.

D. Measurement Systems

Advanced sensing and measurement technologies acquire and extract information from data and enhance multiple aspects of power system management. These technologies evaluate the health of equipment and the integrity of the grid. In the context of smart grids, enhanced measurement and control potentially allows the system to operate closer to its physical limits and increases its efficiency [26].

For better wide-area situational awareness, regional transmission operators require considerable information about the state of the power grid. This is achieved by real-time use of data acquired by specialized electrical sensors - Phasor Measurement Units (PMUs)- at substations. PMU devices capture current and voltage phasor information from the electrical buses at selected substations at sample rates of up to 60 Hz. The information received from PMUs is used by energy management systems at control centers for improved state estimation, monitoring, control, and protection. Many in the power systems engineering community believe that the Northeast blackout of 2003 could have been contained within a much smaller area if a wide-area phasor measurement network had been deployed [27]. Of the many sensing and measurement technologies currently under development, Wide-Area Measurement System (WAMS) - which is comprised of PMUs - may have the greatest potential for enhancing grid reliability [28].

In the customer domain, Automatic Metering Infrastructure (AMI) provides two-way communication capability for interaction between the utility companies and end customer premises equipped with smart meters. These are mainly used to automatically gather metering information from the customer side (automatic meter reading) thereby reducing operational costs. AMI can further facilitate remote power-quality monitoring of and outage detection for customer premises.

Another instrument in modern sensing and measurement technology is Dynamic Line Rating (DLR), which measures the ampacity - or electrical current capacity - of lines in real time using temperature sensors to allow accurate dynamic rating of overhead lines. It is believed that a DLR system delivers 10% to 30% additional grid capacity, 90% of the time. Moreover, temperature sensing is used in fiber-optic temperature monitoring systems that provide direct, real-time measurement of hot spots in small and medium transformers, thus addressing utility concerns about the safety and reliable operation of high-voltage equipment.

E. Computation

The evolution and use of decentralized control significantly complicates analysis of the large-scale distributed networks. It also necessitates that communication links and data transfer functions be considered alongside computing elements in reliability analysis. Software engineering has enabled the development of nearly-perfect computer programs that utilize control algorithms to optimize the functionality of a CPS. However, software faults (due to limitations in mathematical algorithms for specific sets of data or maliciously induced by intrusion) lead to system failures and should be considered in the reliability model.

F. Operators

If proper planning criteria are followed, most modern power systems are designed to be able to operate safely and in a stable fashion with minor contingencies. However, depending on the severity of a failure event, the system may enter into an emergency state where a human operator needs to take an action. Human error can cause catastrophic failure [29], [30], and should be considered in any reliability model.

V. Case Study - the IEEE-14 Bus System

The work presented in Ref. [21], which serves as the basis for the current study, proposes a quantitative CPS reliability model and demonstrates its usefulness for the example of the IEEE-118 bus system. Our earlier model considered outage of transmission lines (single-line contingencies) and various failure scenarios of FACTS devices. We utilized a hardware-in-the-loop simulator to identify the "Functional" and "Failed" states of the system, with "failure" being defined as a single-line contingency that leads to a cascading failure of other lines. We used the MIS technique to aggregate the state information into a reliability model that reflects failures in both physical and cyber components. As an example of our method, the reliability model for an IEEE-118 smart grid with seven UPFC devices configured in "fail-bypass" mode is given in Equation (3) - a reduced form that assumes all transmission lines and all FACTS devices, respectively, are equally reliable.

$$R_{sys} = p_L^{186} + p_L^{185} q_L * (117 + p_F^2 + 2p_F q_F + 2q_F^2) \quad (3)$$

In Equation (3), p_L and q_L are the reliability and unreliability of transmission lines, respectively; $q_L = 1 - p_L$. Similarly, p_F and q_F represent the reliability and unreliability of FACTS devices, respectively.

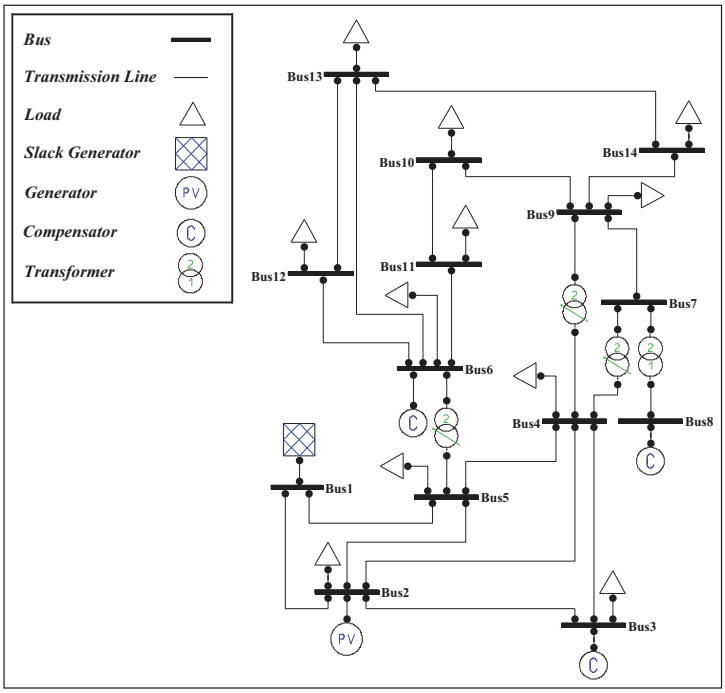

Fig. 3. The IEEE-14 bus system.

As discussed in Sections I and II, our preliminary model has a number of limitations. The hardware-in-the-loop simulator did not allow us to investigate the failure of all components of the cyber network - we could only carry out fault injection for the FACTS devices. The very nature of the simulator constrained our work to the IEEE-118 bus system - a very complex, but nonetheless fixed topology. In extending our earlier work, we have selected the IEEE-14 bus system as a simpler topology that facilitates visualization and understanding of the model. As in the case of the IEEE-118, the IEEE-14 bus system is a commonly-used test system with 14 buses and 20 transmission lines. Other studies that investigate the IEEE-14 bus system [17]–[19] are briefly described in Section II. Figure 3 depicts a single-line diagram of the IEEE-14 bus system. A cyber-physical reliability model should reflect the effect of any possible failure - whether physical or cyber in origin. To be comprehensive, it should be able to accommodate the inclusion of a vast array of components in the cyberinfrastructure. Figure 4 reflects our vision of a sophisticated IEEE-14 bus smart grid that includes measurement and control devices. The remainder of this section enumerates and discusses vulnerabilities in this CPS.

Transmission lines: *[physical domain]* - Transmission lines are fragile parts of the electric delivery system, as it is not always possible to invest in redundant lines. Studying the outage of transmission lines is essential in reliability evaluation of any power grid.

FACTS devices: *[actuators interfacing cyber domain to the physical]* - three Static Synchronous Series Compensator (SSSC) devices (computer-controlled power electronics) are installed in our example on lines l_{1-5}, l_{2-3}, and l_{2-4}. SSSC is connected in series with the AC system and its output current is adjusted to control the nodal voltage magnitude. The failure of an SSSC device could initiate cascading failures.

Communication paths: *[information exchange links between the physical and cyber domains]* - Several communication paths are required to connect the FACTS devices, PMUs, DLR, control center and operator station. Failure of a link in any of these paths, where accidental or maliciously induced, could significantly affect the functionality of the grid.

PMUs: *[meters in the cyber domain]* - Four PMUs are installed on the network to measure voltage magnitude and angle in real-time. These PMUs, which are critical in the sense of network observability, may stop sending measurements to the control center, or may send incorrect values. We carried out the PMU placement based on the method introduced in Ref. [31].

DLR: *[meters in the cyber domain]* - A DLR measurement system is installed on the line between bus 1 and bus 2 (l_{1-2}), which carries a large amount of power, to measure its capacity of this line. Failure of this DLR may overload the line (l_{1-2}) and initiate a cascading failure.

Control algorithms: *[backbone of cyber domain]* - Mathematical algorithms should control the power flow in the transmission lines to efficiently supply customers and prevent overload. Defective software can cause catastrophic problems by generating incorrect commands.

Operator: Operators need to intervene when unpredicted incidents occur to prevent subsequent failures. Human error is always a possibility. We consider two categories of human error: "no action when required," "unnecessary action," and "incorrect action."

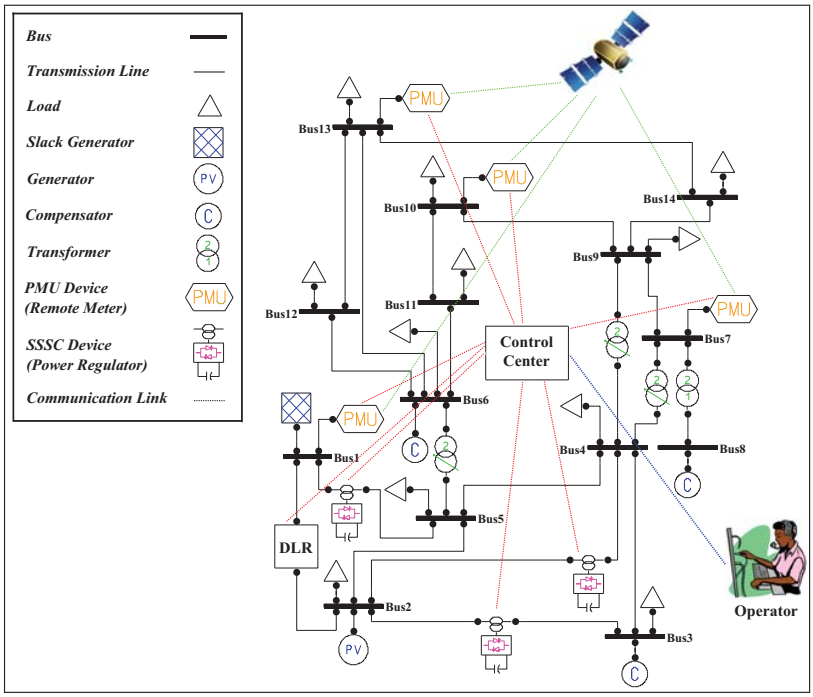

Fig. 4. An IEEE-14 smart grid.

Investigating the effects of failures in each of the aforementioned physical and cyber components leads to comprehensive contingency analysis that encompasses both the cyber and physical domains. Such contingency analysis is necessary for developing an integrated model for system reliability, where certain failure profiles are assumed for the various components, and the resulting "Failed" and "Functional" states are identified. The (very challenging) question to be answered here is whether the system can continue to operates correctly despite the failure of one or more specific components. Given the significant constraints on access to operational smart grids, simulation is a very typical alternative for gaining the information required. For the case of smart grids, such a simulator should be able to reflect the failure of components from both the cyber and physical domains. It should also allow the user to manipulate the information exchanged between these two domains. Furthermore, it is an advantage if the simulator provides or facilitates the development of modules as new technologies are developed. To this end, we are considering Power System Analysis Toolbox (PSAT), as the power grid simulator for our future work. PSAT [32] is an open-source MATLAB-based software package for analysis and design of electric power systems. It includes conventional analyses and simulations and supports a number of electronic control devices, such as FACTS, PMU, and AVR. Its open-source nature is instrumental to fault injection and manipulation of information exchange between the components.

VI. Conclusions and Future Work

Recent studies have illustrated that design of large-scale systems based on criteria derived from worst-case analysis is overly conservative and leads to inefficient use of resources [33]. Probabilistic techniques that reflect a wide range of operational conditions can be utilized instead to determine, not only the severity and consequences of a failure, but also the probability of its occurrence. Designing for safe and sustainable operation under the most likely scenarios is far more efficient. Prediction of the reliability of a system is instrumental to efficiency and robustness. We carry out this vital task for smart grids - among the most critical large-scale systems.

The work presented in this paper discusses ongoing efforts that build on and eliminate the limitation of our work on reliability modeling of an IEEE-118 smart grid system. We are planning to generalize our past work by using simulation software capable of representing a broad range of systems, rather than the hardware-in-the-loop simulator that constrained our earlier work to a fixed topology and design. The case study for our ongoing work is a cyber-physical incarnation of the IEEE-14 bus system, designed by us to facilitate comprehensive investigation of smart grids by considering failures in measurement systems, control algorithms, communication links; as well as human error in operator intervention. We use the PSAT computer simulation framework to observe the effect of impairments in each component of the cyber infrastructure of our IEEE-14 smart grid.

Three ultimate objectives or our work are to i) recognize susceptible domains in critical infrastructure systems, ii) guide investments to eliminate or alleviate these vulnerabilities, and iii) develop a routine to automatically mitigate failures, resulting in an increase in safety and a decrease in costs. The consequent reliance on intelligent control can lead to more efficient utilization of vital resources by critical systems.

REFERENCES

[1] "NIST framework and roadmap for smart grid interoperability standards, release 1.0," National Institute of Standards and Technology, Tech. Rep., January 2010.

[2] A. Faza, S. Sedigh, and B. McMillin, "Integrated cyber-physical fault injection for reliability analysis of the smart grid," in *Computer Safety, Reliability, and Security*, 2010, vol. 6351, pp. 277–290.

[3] J. Lin, S. Sedigh, and A. Hurson, "Ontologies and decision support for failure mitigation in intelligent water distribution networks," in *Proceedings of the 45th Hawaii International Conference on System Sciences (HICSS-45)*, Grand Wailea, Maui, Hawaii, January 2012.

[4] A. Faza, S. Sedigh, and B. McMillin, "An integrated cyber-physical reliability model for the smart grid," *Reliability Engineering and System Safety*, under review.

[5] ——, "A case study in quantitative analysis of cyber-physical systems: reliability of the electric power grid," *IEEE Transactions on Reliability*, under review.

[6] W. Kuo and M. Zuo, *Optimal Reliability Modeling: Principles and Applications*. Wiley, 2003.

[7] P. Derler, E. Lee, and A.-S. Vincentelli, "Modeling cyber-physical systems," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 13–28, 2012.

[8] T. Crenshaw, E. Gunter, C. Robinson, L. Sha, and P. Kumar, "The simplex reference model: Limiting fault-propagation due to unreliable components in cyber-physical system architectures," in *Proceedings of the 28th IEEE International Real-Time Systems Symposium (RTSS '07)*, December 2007, pp. 400–412.

[9] L. Xie and M. Ilic, "Module-based modeling of cyber-physical power systems," in *Distributed Computing Systems Workshops, 2008. ICDCS '08. 28th International Conference on*, 2008, pp. 513–518.

[10] J. Endrenyi, M. Bhavaraju, K. Clements, K. Dhir, M. McCoy, K. Medicherla, N. Reppen, L. Saluaderi, S. Shahidehpour, C. Singh, and J. Stratton, "Bulk power system reliability concepts and applications," *IEEE Transactions on Power Systems*, vol. 3, no. 1, pp. 109–117, February 1988.

[11] C. Dichirico and C. Singh, "Reliability analysis of transmission lines with common mode failures when repair times are arbitrarily distributed," *IEEE Transactions on Power Systems*, vol. 3, no. 3, pp. 1012–1019, August 1988.

[12] S. Asgarpoor and M. Mathine, "Reliability evaluation of distribution systems with nonexponential down times," *IEEE Transactions on Power Systems*, vol. 12, no. 2, pp. 579–584, May 1997.

[13] E. Zio and L. Golea, "Analyzing the topological, electrical and reliability characteristics of a power transmission system for identifying its critical elements," *Reliability Engineering & System Safety*, vol. 101, no. 0, pp. 67 – 74, May 2012.

[14] J. Haakana, J. Lassila, T. Kaipia, and J. Partanen, "Comparison of reliability indices from the perspective of network automation devices," *IEEE Transactions on Power Delivery*, vol. 25, no. 3, pp. 1547–1555, May 2010.

[15] M. Beccuti, S. Chiaradonna, F. D. Giandomenico, S. Donatelli, G. Dondossola, and G. Franceschinis, "Quantification of dependencies between electrical and information infrastructures," *International Journal of Critical Infrastructure Protection*, vol. 5, no. 1, pp. 14 – 27, March 2012.

[16] J.-C. Laprie, K. Kanoun, and M. Kaâniche, "Modelling interdependencies between the electricity and information infrastructures," in *Computer Safety, Reliability, and Security*, ser. Lecture Notes in Computer Science, F. Saglietti and N. Oster, Eds. Springer Berlin Heidelberg, 2007, vol. 4680, pp. 54–67.

[17] X. Li, A. Dwivedi, and X. Yu, "Assessing cascading failure in power networks based on power line correlations," in *Proceedings of the 4th International Conference on Power Engineering, Energy and Electrical Drives (POWERENG)*, 2011, pp. 1–6.

[18] H. I. Shaheen, G. Rashed, and S. Cheng, "Optimal location and parameters setting of UPFC based on GA and PSO for enhancing power system security under single contingencies," in *2008 IEEE Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century*, Pittsburgh, PA, July 2008, pp. 1–8.

[19] W. Qin, F. Meng, W. Zhang, and J. Zhang, "Transmission lines operating reliability evaluation based on real-time power flow," in *Proceedings of the 10th International Power and Energy Conference (IPEC)*, Ho Chi Minh City, December 2012, pp. 606–610.

[20] A. Faza, S. Sedigh, and B. McMillin, "Reliability modeling for the advanced electric power grid," in *Proceedings of the 26th International Conference on Computer Safety, Reliability and Security, SAFECOMP '07*, vol. 4680, September 2007, pp. 370–383.

[21] ——, "Reliability analysis for the advanced electric power grid: From cyber control and communication to physical manifestations of failure," in *Proceedings of the 28th International Conference on Computer Safety, Reliability and Security, SAFECOMP '09*, vol. 5775, September 2009, pp. 257–269.

[22] R. Billinton and R. Allan, *Reliability Assessment of Large Electric Power Systems*, ser. Power Electronics and Power Systems. Springer, 1988.

[23] E. Acha, H. Ambriz-Pérez, C. Fuerte-Esquivel, and C. Angeles-Camacho, *FACTS: Modelling and Simulation in Power Networks*. Wiley, 2004.

[24] "IEEE recommended practice for data communications between remote terminal units and intelligent electronic devices in a substation," *IEEE Std 1379-2000*, pp. 1–72, 2001.

[25] Y. Wang, W. Li, and J. Lu, "Reliability analysis of wide-area measurement system," *IEEE Transactions on Power Delivery*, vol. 25, no. 3, pp. 1483–1491, March 2010.

[26] A. Dominguez-Garcia, "Reliability modeling of cyber-physical electric power systems: A system-theoretic framework," in *Power and Energy Society General Meeting, 2012 IEEE*, San Diego, CA, July 2012, pp. 1–5.

[27] P. Mazza and Climate Solutions (Organization), *Powering Up the Smart Grid: A Northwest Initiative for Job Creation, Energy Security and Clean, Affordable Electricity*. Climate Solutions, 2005.

[28] "Modern Grid v1.0: A Systems View of the Modern Grid: Appendix B2: Advanced Sensing, Metering, and Measurement," National Energy Technology Laboratory, Tech. Rep., March 2007.

[29] P. Pyy, K. Laakso, and L. Reiman, "A study on human errors related to NPP maintenance activities," in *Human Factors and Power Plants, 1997. Global Perspectives of Human Factors in Power Generation., Proceedings of the 1997 IEEE Sixth Conference on*, 1997, pp. 12/23–12/28.

[30] R. Duffey and T. Ha, "The probability and timing of power system restoration," *Power Systems, IEEE Transactions on*, vol. 28, no. 1, pp. 3–9, 2013.

[31] T. Baldwin, L. Mili, J. Boisen, M. B., and R. Adapa, "Power system observability with minimal phasor measurement placement," *IEEE Transactions on Power Systems*, vol. 8, no. 2, pp. 707–715, May 1993.

[32] F. Milano, "An open source power system analysis toolbox," *IEEE Transactions on Power Systems*, vol. 20, no. 3, pp. 1199–1206, August 2005.

[33] E. Vaahedi, W. Li, T. Chia, and H. Dommel, "Large scale probabilistic transient stability assessment using B.C. Hydro's on-line tool," *Power Systems, IEEE Transactions on*, vol. 15, no. 2, pp. 661–667, 2000.