# Reliability Modeling of Cyber-Physical Electric Power Systems: A System-Theoretic Framework

Alejandro D. Domínguez-García, *Member, IEEE*

***Abstract*—This paper proposes a framework for developing systematic reliability analysis tools to address planning and operation challenges of future electric power systems. These systems are undergoing a radical transformation in structure and functionality enabled by new technologies, e.g., advanced communication and control, renewable-based generation, and advanced power electronics. The added functionality comes with side effects of increased system complexity and the introduction of new sources of uncertainty in systems already inherently complex. Current reliability analysis tools are inadequate to capture the impacts of integrating this new technology. Without proper reliability analysis tools, poorly understood, unreliable and unsafe systems will result, leading to catastrophic consequences if deployed. Thus, it is key to create systematic analytical tools to capture the impacts of new technology integration on power system reliability. In this paper, the discussion focuses on tools for quantifying power system reliability when there is coupling between cyber and physical components, and there is coupling between system dynamics and component stress.**

## I. Introduction

Electrical energy systems worldwide are undergoing a radical transformations in structure and functionality driven by a quest to increase efficiency and reliability. Such transformations are enabled by the introduction of new technologies such as advanced communication and control applications, integration of new generation sources, e.g., wind, photovoltaics (PV), new loads, such as plug-in hybrid electric vehicles (PHEV), and advanced power electronics devices for power-flow control, such as flexible AC transmission systems (FACTS). However, added functionality provided by the integration of new technologies comes with side effectsincreasing system complexity and the introduction of new sources of uncertainty at all levels in systems that are already inherently complex.

Current reliability engineering tools, although effective for today's electric power systems, are inadequate to engineer the reliability of next generation power systems, as they cannot capture the impacts of integrating the aforementioned technologies. For example, in bulk power transmission, increased communication and control potentially increase system responsiveness to disturbances and allow system operation closer to physical limits for increased efficiency [1], [2], [3], [4]. In this regard, next generation electric power systems envisioned under the US DOE *Smart Grid* initiative and its European counterpart *Electricity Networks of the Future*, are truly *cyber-physical systems*,[1] where the functions of the physical resources encompass one or more of the following: generation, transmission and consumption of electrical energy; and the computational (cyber) resources in tight coordination, with the physical resources, monitor and control the entire system. However, existing reliability analysis tools cannot characterize the tight coupling between this communication and control infrastructure and the physical components responsible for generation, transmission and utilization of electrical energy, and consequently, the impacts of faults in the communication and control infrastructure on the overall system operation [6], [7]. Without adequate tools to address the impact of integrating new technologies, ad-hoc system designs will likely result, leading to the deployment of poorly understood and unreliable systems, which could have catastrophic consequences.

In this paper, we propose a framework for developing systematic analytical tools that properly capture the impact of new technology integration on system reliability of large-scale electric power grids, such as the bulk power transmission system. In particular, we focus on tool development for 1) quantifying impacts of coupling between cyber and physical components on system reliability, and 2) quantifying impacts of coupling between system dynamics and component stress on the overall system reliability. On each of these two fronts, we next discuss several issues that need to be addressed.

*1) Coupling between cyber and physical components:* Although the operation of most modern electric power systems is dependent on a cyber infrastructure of sensing, communication, and control devices (from now on, cyber components), conventional analysis methods do not address the coupling of this infrastructure and the system physical components. Some progress has been made in developing analytical methods and simulation tools to explicitly model this coupling. For example, the authors of [8] have expanded the classical model of a power system to include additional variables representing delayed versions of certain state variables of the original classical model, with the purpose of characterizing the impact of these random delays in delivering true measurements. In [9], the author developed a computer tool to simulate the effect of delays in communication systems and the impacts of wide-area control schemes on system dynamics. More recent efforts have focused on co-simulation approaches to understand the interaction between physical and cyber layers, which rely on combining well-established simulation tools for physical systems and communication systems [10], [11].

The author is with the ECE Department of the University of Illinois at Urbana-Champaign. E-mail: aledan@ILLINOIS.EDU.

This work has been supported in part by NSF under Career Award ECCS-CAR-0954420.

[1] Cyber-physical systems refer to engineered systems with a tight integration and coordination between computational and physical components [5].

Conventional reliability analysis techniques have focused on quantifying the effects of faults in physical components, e.g., power sources and transmission lines, on system reliability. For large power systems, the pioneering work of Allan, Billinton, Endrenyi, and Singh, among others, set the foundation for the techniques widely used in the power industry to assess power system reliability (see, e.g., [12] and the references therein). Today, these tools are also applied to smaller systems, e.g., distribution systems (see, e.g., [13]). However, while faults in physical components are reasonably well understood, there is no systematic definition and characterization of faults in cyber components and their effect on system reliability.

*2) Coupling between system and component stress:* The concept of operating electric power systems with large margins is being challenged. Within the context of the Smart Grid vision, increased communication and control is envisioned as an aid to enable system operation closer to its physical limits. In the aerospace domain, digital control has allowed the design of fighter aircraft that are aerodynamically unstable, e.g., F-16, in order to achieve increased maneuverability [14]. While operating electric power systems closer to their margins may increase their efficiency, it is necessary to understand the implications of margin reduction on system reliability.

When systems are operated with large margins, it is usually assumed that component failure behavior is unaffected by the evolution of system dynamics (see, e.g., [15]). Component failure mechanisms are modeled as random variables describing the time to occurrence of each particular failure mechanism. The time-to-fault occurrence is usually characterized by the well-known concept of failure rate, which is either constant if the time to fault occurrence is exponentially distributed or time-dependent, as in the case of a Weibull distribution. However, this failure rate is assumed independent of the system dynamic continuous evolution—an assumption that needs to be revisited in order to understand the effect of system dynamics on each individual component and how the stress of individual components over time affects system dynamics.

In nuclear reactor risk analysis, previous attempts to characterize the interplay between system dynamics and component failure behavior resulted in a framework commonly referred to as *dynamic probabilistic risk assessment* (DPRA) (see, e.g.,[16], [17] and the references therein). While the mathematical formulation is very elegant, it is not practical for gaining analytical insights into the problem, as the resulting differential equations do not admit analytical solutions even for simplified systems. Monte Carlo simulation approaches based on discretizing the system dynamic evolution variables have been proposed to obtain solutions [17]. In the context of power system security (operational reliability) analysis, a similar framework tailored to power systems was developed in [18]. This framework has drawbacks similar to those of DPRA, and its ability to handle large-scale systems has not been demonstrated. Neither of these methods can handle operational uncertainty, i.e., uncontrolled and unpredictable change in the demand or in the supply, which is basic to understanding the random variability of renewable energy resources.

## II. A Framework for Reliability Modeling of Cyber-Physical Electrical Energy Systems

To address the problems discussed in Section I, we tailor tools developed in the control field for analysis of hybrid and switched systems to the unique structural features of electrical energy systems. This hybrid/switched system view of electrical energy system was first introduced in [19].

It is well accepted that the behavior of many electrical energy systems is governed by the interaction of continuous dynamics and discrete events. In general, the continuous dynamics of electric power systems are usually represented by a differential-algebraic equation [20]. However, as stated in [19], it is possible to solve (locally) the algebraic equations and substitute into the differential equations to obtain a ordinary differential equation. Thus, in this paper, it is assumed, without loss of generality, that the dynamic behavior of electric power systems can be described by a switched state-space model:

$$\Gamma : \begin{cases} \dot{x} = f_\sigma(x,u), \\ y = h_\sigma(x,u), \end{cases} \tag{1}$$

where $\sigma : [0,\infty) \to \mathcal{Q}$, called the switching signal, indicates the active subsystem at every time, $\mathcal{Q}$ called "index set", and $f_q$, $h_q$, with $q \in \mathcal{Q}$, define, respectively, the evolution of the continuous dynamics and the observation equation of each subsystem in (1). As discussed in [21], this switched state-space description can be obtained from a more general hybrid systems description if the discrete behavior governed by the switching signal is known. Component faults will be thought of as switching between the subsystems in (1), the occurrence of which can be modeled, for example, as a random variable representing the time to fault and usually characterized by so-called *failure rate* [15].

### A. Coupling between Cyber and Physical Elements

Historically, reliability analysis of electric power systems has focused on understanding the effect of faults in the physical layer, however, as discussed in Section I, faults in the cyber components can be as harmful for the system as physical failures. For example, in Fig. 1, assume the phasor measurement unit (PMU) measuring the voltage of load bus 7 stops sending measurements to the control center. Then, assuming this measurement is critical in the sense of network observability [], it is then likely, that the voltage in this bus can no longer be maintained within its specified range. Thus, no physical fault has occurred, yet the system cannot provide an appropriate voltage level to load bus 7. Communication delays and intermittent faults are more elaborate examples of faults in the cyber layer.

While faults in physical components are well understood, there is no systematic definition and characterization of faults in cyber components of electric power systems and their impacts on overall system reliability. For example, assume that the PMU considered above starts sending measurements intermittently due to an internal fault. The effect of this type of intermittent fault on the reliability of electric power systems has not been previously addressed. The setup for defining and characterizing this fault is summarized as follows.

***Example 1:*** Consider the system in Fig. 1; this system is a 3-machine, 9-bus abstraction of the Western Electricity Coordinating Council (WECC) [20], where the classical one-line diagram representing the system physical elements is complemented with a simplified representation of its supporting control and communication infrastructure. The purpose is to reliably provide power to the three load buses, and maintain stable operation and the voltage of the three load buses within a certain range. An intermittent fault in one of the PMUs will cause the system to switch back and forth between two different dynamical systems. Even if both systems are stable, it is well known that the resulting switched system can be unstable, i.e., the system exhibits some emergent behavior that the original subsystems did not have. Under this fault the behavior of the system can be described by

$$\dot{x} = f_\sigma(x), \tag{2}$$

where $x$ is the vector of machine dynamic variables (including machine speed and angle for each machine), and the switching signal $\sigma : [0, \infty) \to \mathcal{Q}$ indicates when the fault is active and when it is not; thus the set $\mathcal{Q}$ contains only two elements, and therefore the corresponding $f_q$ describes the system dynamics for both non-faulty and faulty configurations. If the time structure of the fault is completely unknown (equivalent to the time structure of $\sigma$ being completely unknown), results in stability of switched systems under arbitrary switching can be applied to characterize the system behavior under this fault. For example, if the two systems in (2) share a common Lyapunov function, then the system is stable despite the presence of this intermittent fault [21]. Other results can be used to establish stability if we have more information on the time structure of the intermittent fault. For example, we know that once the sensor stops sending measurements to the controller, it will fail to send measurements for at least $\tau_1$ units of time, and when the sensor is sending measurements, it will keep sending them for at least $\tau_2$ units of time. If it turns out that both systems in (2) are stable, then the system remains stable under this intermittent fault if the values of the individual Lyapunov functions at the beginning of each time interval for each active subsystem in (2) form a decreasing sequence [21]. There are other results involving the concepts of *dwell-time* and *average dwell-time* (concepts that capture the notion that the switching between subsystems is slow enough [21]) that could be applied to characterize this fault. Finally, if the evolution of the fault is described as a random process, then stability statements under this particular fault can be made using stability results of randomly switched systems [22]. □

There are several issues that need to be further investigated. For example, the previous example focused on a system with no disturbances, and the reliability-related question was to understand the impacts of intermittent faults in cyber components on the stability of the system. Assume the system has inputs representing disturbances, e.g. loads can be modeled as current sources. Further assume that those inputs are not constant but are subject to uncontrolled random variations; however, it is known they can not exceed certain values. In this context, and in the presence of an intermittent fault such as the one described in the previous example, rather than focusing on quantifying the effect of the fault on the stability of the system, the interest might be to assess whether or not the voltage of the load buses remain within certain bounds. The characterization of this fault can be cast into the framework of input-to-state stability (ISS) for switched systems, for which there are several available results. For example, see [23], [24] for conditions for a switched system to be ISS under "slow switching," given all the individual subsystems are ISS. Very recently, conditions for ensuring ISS of switched systems when not all the individual subsystems are ISS was established [25].

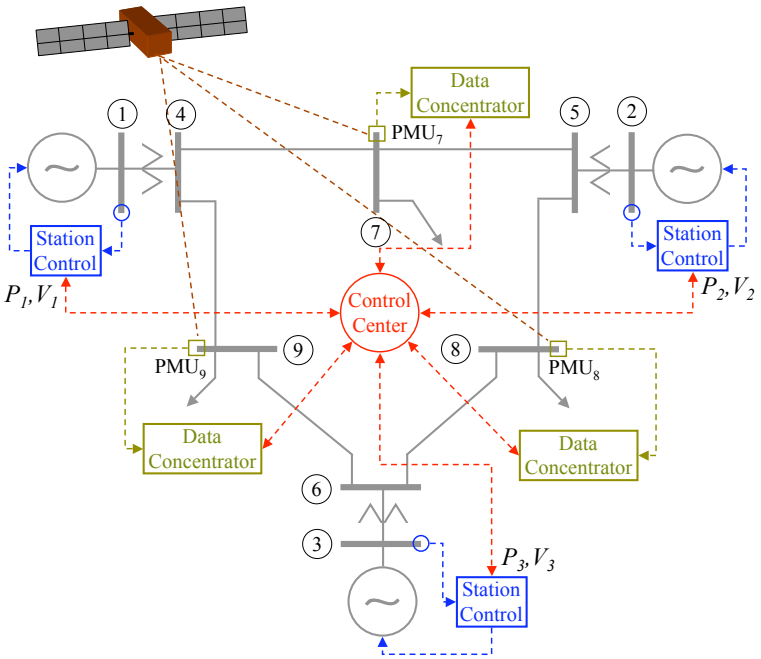


Fig. 1. WECC 3-machine, 9-bus system including communication and control infrastructure.

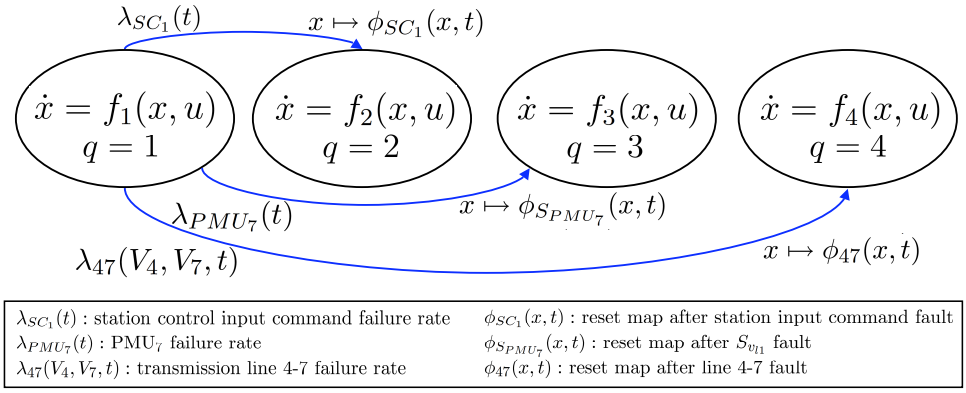


Fig. 2. Snapshot of the SHS-based reliability model of the system in Fig. 1.

### *B. Coupling between System Dynamics and Component Stress*

Markov chains are among the most powerful formalisms used for quantitatively analyzing the reliability of a system [26], and are widely used in reliability analysis of electric power systems [27]. They can easily capture failure sequences in which the order of component failures matters, different repair strategies, common-mode failures, and state-dependent failure rates that other modeling formalisms cannot, e.g., fault trees and reliability block diagrams. A Markov chain is often described graphically by a directed graph. In the context of reliability modeling, each node corresponds to a system configuration reached after a unique sequence of component failures, and the edges represent transitions between configurations triggered by failures (or repairs).

However, the conventional use of Markov chains in reliability analysis cannot explicitly handle the coupling between system continuous dynamics and component failure behavior. It is possible to discretize the continuous system dynamics and, for each particular configuration (faulty and non-faulty), develop individual Markov chains describing the system dynamics, and then embed these chains into the Markov chain describing the transitions among configurations caused by faults. This approach, while technically correct, would result in an explosion of the resulting Markov chain state-space. Thus, it is important to develop a scalable framework, amenable for computer implementation and expressive enough to characterize the coupling between system dynamics and component failure behavior. Dependence of component failure rates on system dynamic variables (and time), operational uncertainty, nonlinear continuous dynamics, and sudden jumps of certain state variables caused by a fault will be included. Modeling formalisms developed in the area of stochastic hybrid systems (SHS) are a promising tool to address the problem. An example of one such formalism, namely the stochastic hybrid systems modeling and analysis framework developed by Hespanha [28], [29], is discussed next.

***Example 2:*** In the context of reliability modeling, in Hespanha's framework, the discrete mode $q$ can take values in some finite set $\mathcal{Q}$, the elements of which represent both fault-free system configurations and configurations reached after a sequence of faults (very much like the states in a Markov reliability model). For the system of Fig. 1, as displayed in Fig. 2, $q = 1$ denotes the non-faulted configuration, $q = 2$ is a configuration where the generator on bus 1 stops receiving commands from the control center, $q = 3$ is a configuration where the PMU$_7$ stops sending measurements to the control center, and $q = 4$ a configuration where the transmission line between bus 4 and bus 7 failed open-circuit. For each $q$, the evolution of the continuous dynamics is modeled by a stochastic differential equation, which captures operational uncertainty. In the system of Fig. 1, operational uncertainty can occur in the three load buses, and we can assume without loss of generality that their time evolution follows a white Gaussian process. Thus, as shown in Fig. 2, this system's continuous dynamics is described by

$$\dot{x} = f_q(x,u),\ q \in \mathcal{Q}, \tag{3}$$

where $x$ is the vector of state variables (including machine angles and speeds), $u$ is a vector of independent white Gaussian processes, and $f_q$ is a vector field defining the system dynamics. The transitions among different modes are triggered by random events representing component faults, very much like the transitions in a Markov reliability model, with the peculiarity that these transitions can be a function of time, the discrete mode and the continuous dynamics. They are unlike conventional Markov reliability modeling, where the transitions (which are also associated with component failure rates) are, at most, a function of time and the discrete mode. Thus, as displayed in Fig. 2, the transition intensity $\lambda_{i,j}(q,x,t)$ between modes $i$ and $j$ corresponds to the failure rate of the component that causes each particular transition. The functional relation between the component failure rate and the system continuous variables is the key feature of this modeling framework that allows an explicit representation of the interaction between the system dynamic behavior and component failure mechanisms. Finally, after a fault causing a transition between two modes occurs, a reset map determines the new value of the continuous state variables after the transition. This allows the possibility of sudden jumps in the continuous dynamics variables caused by a particular fault. Once this SHS-based reliability model is formulated, it is necessary to obtain the evolution of the joint probability density function of $q$ and $x$. □

The literature in SHS modeling frameworks is extensive [30], [31], [32]. Depending on the nature of each system, there might be other frameworks than Hespanha's that more appropriately capture particular system features. For example, certain systems might not be subject to operational uncertainty, so the continuous dynamics are modeled by a deterministic differential equation instead of a stochastic differential equation, although the transitions among different modes are stochastic. The nature of other systems might be such that faults in the system components never cause the continuous state variables to jump, although a stochastic differential equation is needed to capture operational uncertainty.

## III. Concluding Remarks

We believe that the proposed framework provides powerful tools for engineering more reliable, more efficient, and more responsive electrical energy systems. The methods and tools developed will also help to broaden the understanding of cyber-physical systems. Cyber-physical systems have been identified as a research priority within the US. Recently, many workshops addressed priorities in the research agenda for cyber-physical systems [33], [34], [35], [36], [37], [38]. Next generation electric power system will be true cyber-physical systems, where the functions of the physical resources encompass one or more of the following: generation, transmission and consumption of electrical energy. The computational (cyber) resources in tight coordination, with the physical resources, monitor and control the entire system.

## References


[1] G. Gross, A. Bose, C. DeMarco, M. Pai, J. Thorp, and P. Varaiya, "White paper on real-time security monitoring and control of power systems," August 1999.

[2] Z. Xie, G. Manimaran, V. Vittal, A. Phadke, and V. Centeno, "An information architecture for future power systems and its reliability analysis," *IEEE Transactions on Power Systems*, vol. 17, no. 3, pp. 857–863, Aug 2002.

[3] K. Tomsovic, D. Bakken, V. Venkatasubramanian, and A. Bose, "Designing the next generation of real-time control, communication, and computations for large power systems," *Proceedings of the IEEE*, vol. 93, no. 5, pp. 965–979, May 2005.

[4] C. Hauser, D. Bakken, and A. Bose, "A failure to communicate: next generation communication requirements, technologies, and architecture for the electric power grid," *IEEE Power and Energy Magazine*, vol. 3, no. 2, pp. 47–55, March-April 2005.

[5] E. Lee, "Cyber-physical systems: Design challenges," University of California, Berkeley, EECS Department, Tech. Rep. UCB/EECS-2008-8, January 2008.

[6] M. Amin, "Modeling and control of complex interactive networks [guest editorial]," *IEEE Control Systems Magazine*, vol. 22, no. 1, pp. 22–27, Feb 2002.

[7] 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, January-February 2009.

[8] S. Carullo and C. Nwankpa, "Experimental validation of a model for an information-embedded power system," *IEEE Transactions on Power Delivery*, vol. 20, no. 3, pp. 1853–1863, July 2005.

[9] S. Sarawgi, "A simulation tool for studying the effects of special protection systems and communications on power system stability," Master's thesis, Washington State University, Pullman, WA, 2004.

[10] K. Hopkinson, X. Wang, R. Giovanini, J. Thorp, K. Birman, and D. Coury, "EPOCHS: a platform for agent-based electric power and communication simulation built from commercial off-the-shelf components," *IEEE Transactions on Power Systems*, vol. 21, no. 2, pp. 548–558, May 2006.

[11] A. T. Al-Hammouri, M. S. Branicky, and V. Liberatore, "Co-simulation tools for networked control systems," in *Proc of the 11th international workshop on Hybrid Systems: Computation and Control*. Berlin, Heidelberg: Springer-Verlag, 2008, pp. 16–29.

[12] R. Allan, R. Billinton, A. Breipohl, and C. Grigg, "Bibliography on the application of probability methods in power system reliability evaluation," *IEEE Transactions on Power Systems*, vol. 14, no. 1, pp. 51–57, Feb 1999.

[13] R. Brown, Ed., *Electric Power Distribution Reliability*. New York, NY: Marcel Dekker, 2002.

[14] J. Tomayk, "Computers take flight," NASA, Washington, DC, Tech. Rep. NASA SP-2000-4224, 2000.

[15] M. Rausand and A. Høyland, *System Reliability Theory*, 2nd ed. New York, NY: John Wiley and Sons, 2004.

[16] A. Amendola, "Event sequences and consequence spectrum: A methodology for probabilistic transient analysis," *Nuclear Science An Engineering*, vol. 77, no. 3, pp. 297–315, March 1981.

[17] P. Labeau, C. Smidts, and S. Swaminathan, "Dynamic reliability: Towards an integrated platform for probabilistic risk assessment," *Journal of Reliability Engineering and System Safety*, vol. 68, no. 3, pp. 219–254, June 2000.

[18] F. Wu and Y.-K. Tsai, "Probabilistic dynamic security assessment of power systems-i: Basic model," *IEEE Transactions on Circuits and Systems*, vol. 30, no. 3, pp. 148–159, Mar 1983.

[19] I. Hiskens and M. Pai, "Hybrid systems view of power system modelling," in *Proc. IEEE International Symposium on Circuits and Systems*, Geneva, Switzerland, 2000.

[20] P. Sauer and A. Pai, *Power System Dynamics and Stability*. Upper Saddle River, NJ: Prentice Hall, 1998.

[21] D. Liberzon, *Switching in Systems and Control*. Boston, MA: Birkhauser, 2003.

[22] D. Chatterjee, "Studies on stability and stabilization of randomly switched systems," Ph.D. dissertation, University of Illinois at Urbana-Champaign, Urbana, IL, 2007.

[23] W. Xie, C. Wen, and Z. Li, "Input-to-state stabilization of switched nonlinear systems," *IEEE Transactions on Automatic Control*, vol. 46, no. 7, pp. 1111–1116, Jul 2001.

[24] L. Vu, D. Chatterjee, and D. Liberzon, "Input-to-state stability of switched systems and switching adaptive control," *Automatica*, vol. 43, no. 4, pp. 639–646, April 2007.

[25] M. Mueller, "Input-to-state stability and related concepts for switched systems and fault coverage," Master's thesis, University of Illinois at Urbana-Champaign, Urbana, IL, 2009.

[26] M. Malhotra and K. Trivedi, "Power-hierarchy of dependability-model types," *IEEE Transactions on Reliability*, vol. 43, no. 3, pp. 493–502, 1994.

[27] J. Endenyi, *Reliability Modeling in Electric Power Systems*. Chichester, England: John Wiley & Sons, 1978.

[28] J. Hespanha, "Polynomial stochastic hybrid systems," in *Hybrid Systems: Computation and Control*, M. Morari and L. Thiele, Eds. Berlin: Springer-Verlag, Mar. 2005, no. 3414, pp. 322–338.

[29] ——, "Modeling and analysis of stochastic hybrid systems," *IEE Proc. Control Theory and Applications, Special Issue on Hybrid Systems*, vol. 153, pp. 520–535, 2007.

[30] M. Davis, Ed., *Markov Models and Optimization*. London, UK: Chapman & Hall, 1993.

[31] G. Pola, M. Bujorianu, J. Lygeros, and M. Benedetto, "Stochastic hybrid models: An overview," in *Proc. of the IFAC Conference on Analysis and Design of Hybrid Systems*, 2003.

[32] J. Lygeros, C. Tomlin, and S. Sastry. (2008, December) Hybrid systems: Modeling, analysis and control. Berkeley, CA.

[33] (2006, November) National workshop—beyond SCADA: Cyber-physical systems. Alexandria, VA.

[34] (2006, November) National workshop on new directions for high confidence software platforms for cyber-physical system technologies. Alexandria, VA.

[35] (2008, April) National workshop on automotive cyber-physical systems. Troy, MI.

[36] (2008, November) National workshop for research on high confidence transportation cyber-physical systems: Automotive, aviation, and rail. Vienna, VA.

[37] (2009, June) Workshop on new research directions for high confidence future energy cyber-physical systems. Baltimore, MD.

[38] (2009, July) National workshop on future directions in cyber-physical systems security. Gateway Center, NJ.