Direct Cyber-Power Interdependency Study on Microgrid Control

Bamdad Falahati and Roberto Costa
Schweitzer Engineering Laboratories, Inc.

Amin Kargarian
Louisiana State University

This paper was presented at the 2017 IEEE Power & Energy Society General Meeting, Chicago, Illinois, July 16–20, 2017, and can be accessed at: https://doi.org/10.1109/PESGM.2017.8274025.

Direct Cyber-Power Interdependency Study on Microgrid Control

Bamdad Falahati
Roberto Costa
Engineering Services
Schweitzer Engineering Laboratories, Inc.
Pullman, USA

Amin Kargarian
Division of Electrical & Computer Engineering
Louisiana State University
Baton Rouge, USA

***Abstract*—The control of a microgrid relies on intelligent electronic devices (IEDs) that continuously monitor the control system and run optimization algorithms to find the optimal stable condition. If any IED or communications network fails, the reliability of the microgrid is impacted. A cyber-power network is a combination of two heterogeneous networks, cyber and power, which are interconnected at certain points to create interdependencies. This paper discusses what happens when a control system fails and quantitatively evaluates the impact on microgrid reliability. Numerical results are presented to show the concept of interdependencies and to illustrate the impact of control system failure on the reliability of the microgrid.**

***Index Terms*—control strategies, interdependency, microgrid, power system reliability, and smart grid.**

I. Introduction

A cyber-power network is a combination of two heterogeneous networks, cyber and power, that are interconnected at certain points, which creates interdependencies. This generally means that the correct and appropriate operation of one element depends on the existence and proper function of other elements.

A microgrid is a power network that mostly relies on small and nondispatchable distributed generation sources that make its control more difficult and its logic and algorithms more complicated. Microgrid control encompasses many applications (e.g., power flow control, power/frequency and volt/VAR control, network reconfiguration, load sharing, and voltage fluctuation mitigation) that allow the microgrid to function stably [1] [2]. In such a small-scale power network, the loss of control leads to misoperation [2] [3], which makes the cyber network even more crucial.

In recent years, cyber networks have been used to take over control tasks in power systems, and control strategies have been widely implemented in intelligent electronic devices (IEDs). Fast and reliable communication is available between the IEDs. In such an environment, centralized and distributed algorithms can be implemented, depending on the application and control philosophy [4].

The uncertainty, unreliability, and unpredictability surrounding cyber networks are adversely affecting modern power systems. Techniques previously developed for power system reliability analysis and evaluation [5] need to be revisited for interdependent cyber-power networks because the two networks exhibit crucial differences [6]. Cyber failures, including failed digital devices, loss of communications, intrusion attempts, and anomalous changes in the status of switching devices, as well as the incorrect setting of digital relays, threaten the operation of the power network. These cyber failures need to be detected, simulated, and included in the reliability evaluation model [7].

Reference [8] proposes a vulnerability assessment method, which takes into account intrinsic characteristics of communications networks, such as interruption and latency. The communications network failure is quantified as the contribution of components to service failure. This information is used to illustrate the most vulnerable part of the entire network.

The reliability of communications systems based on network configuration is studied in [9] and [10], and quantified reliability evaluation methods are proposed for wide-area control systems. In [2], the impact of two important cyber failures on microgrid control—latency and loss of communications—is investigated. Simulation predicts the delay may be problematic for the control of microgrids. The developed method in [7] and [11] can be used to reveal the cause of cascading failures and evaluate overall studies to improve network reliability.

This paper discusses different modes of control in microgrids and applies a reliability assessment algorithm to incorporate the impact of cyber network failures on power networks. An optimization model is proposed to maximize the data connection in the cyber network with multiple data sources. Finally, microgrid reliability is numerically evaluated and results are compared with a sole-power infrastructure in which only the equipment fails.

II. Control in Microgrids

The idea for microgrids developed out of the need to use distributed generation and renewable energy while minimizing dependency on the bulk power system [12]. The main objective of microgrids is to supply reliable power to local consumers from sources that are either distributed generation sources or high-bandwidth batteries [13] [14].

The reliability and stability of microgrids are crucial and firmly rely on computer network and information data flow technologies. In general, renewable energy resources are small-

scale, intermittent, and nondispatchable [14] [15]. Maintaining constant frequency in a microgrid is more difficult than in the bulk power system because there is no slack bus, which usually exists in bulk power systems to provide the load-generation balance.

Figure 1 and Figure 2 show a simplified one-line diagram of a microgrid cyber-power network. The power network (shown in Figure 1) includes four distributed generation (DG) units and three loads. The cyber control network, shown in Figure 2, is a ring topology local-area network (LAN)/Ethernet network that includes real-time automation, protection, and control (RTAPC) devices; servers; and switches.

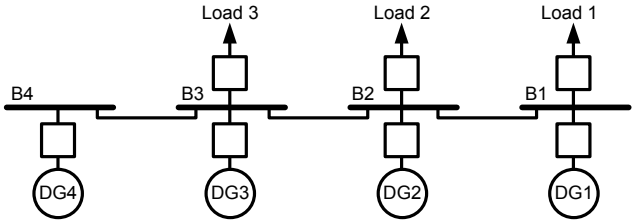

Figure 1. Schematic Diagram of Power Network in a Microgrid

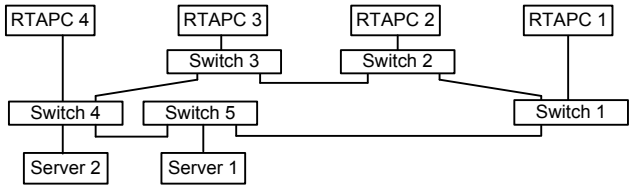

Figure 2. Schematic Diagram of Cyber Network in a Microgrid

A. Real-Time Automation, Protection, and Control

Microgrid control is part of a multitask IED that is, in reality, an RTAPC device. RTAPC devices manage microgrid resources to balance loads and generation. They continuously run real-time optimum energy management algorithms, with the objective of maximizing benefits and minimizing load curtailments and system losses.

B. Overall Control System

Typically, control and operation algorithms are implemented at the bay level inside the RTAPC unit of each bay, and a portion of the algorithms may be implemented inside a centralized reliable server (e.g., Server 1 or Server 2 in Figure 2). The decentralized control in each RTAPC unit allows for small, autonomous systems that communicate with each other [16]. On the other hand, centralized control is simpler to implement but may be more vulnerable to cyber faults and attacks, and a larger portion of the network may be impacted.

RTAPC units are responsible for transmitting real-time decisions as digital signals to breakers and sectionalizers to connect or disconnect the corresponding bay from the entire microgrid [17] [18].

Regardless of the control strategy, three modes of control exist in microgrids. These control modes are discussed in the following subsections.

1) Automatic Controls

Automatic controls refer to algorithms that the controller continuously runs or algorithms that the controller (not the operator) initiates. The control unit continuously monitors the network, collects data, and sends commands when required. The following subsections discuss the automatic controls required for a microgrid.

a) Power Frequency Control

The power frequency characteristics of distributed generation units provide the required active power to adjust the frequency in the microgrid. The control unit is responsible for maintaining the frequency in a microgrid by adjusting the synchronous generator according to its frequency droop characteristics and available storage units.

b) Volt/VAR Control

Voltage magnitude is highly dependent on and sensitive to reactive power. A lack or excessive amount of reactive power can cause undervoltage and overvoltage, respectively, in the equipment. The RTAPC unit can use voltage control strategies that consider the voltage and reactive power droop of the synchronous generator.

2) Operator-Initiated Controls

Some controls are initiated by the operator, and if prerequisites are satisfied, the RTAPC unit performs the sequence of operation (e.g., breaker switching). Operator-initiated controls are usually local or through a supervisory control and data acquisition (SCADA) system. Network reconfiguration and switching between islanded and grid-connected modes is a form of operator-initiated control [1].

3) Manual Controls

In manual mode, the sequential operation of breakers is disabled, and commands are run by an operator. The operator must open and close the circuit breakers manually, and the RTAPC units only check the satisfaction of the interlocks to perform the operation.

C. Loss-of-Control Situation

Losing data related to a feeder causes a loss-of-control situation and interrupts the operation of the corresponding feeder [2] because the central decision-maker neither knows how much energy is used by the corresponding load nor can manage the generating units to produce the required power.

Given the low inertia that characterizes microgrids, it is essential to have a load-shedding system that is capable of matching the load and generation in the islanded system. Loss of communication to a load causes the exclusion of that load from the load-shedding algorithm.

RTAPC controls each generator by adjusting exciter, governor, and operation modes (droop/isochronous). A loss of communication could result in RTAPC not being able to maintain the frequency, for example, when the generator is in isochronous mode.

In other words, communication between each controller and the servers is assumed as a prerequisite for keeping a feeder energized. Because each RTAPC unit is dedicated to

control each section in the microgrid, if the RTAPC unit does not receive data from the server and other RTAPC devices, all power elements in the corresponding section operate abnormally due to cyber connectivity issues.

III. Direct Cyber-Power Interdependency

Interdependencies are divided into two main categories: direct and indirect. Direct interdependency causes the failure or changes the behavior of the element in the power network [7]. Indirect interdependency does not cause the failure or change the behavior of the element, but will impact the performance of the element against the failure. Loss of control, it its nature, is direct interdependency, so this paper focuses solely on direct interdependencies.

A. Cyber-Power Link

A cyber-power interdependent network is modeled by a set of cyber-power links. A cyber-power link, formulated in (1), represents a physical or logical relationship between element γ in the cyber network and element δ in the power network. This means that if cyber element γ fails or does not receive the required data, power element δ stops working.

$$D = (\gamma : \delta) \tag{1}$$

Direct element-element interdependency (DEEI) refers to the interaction between elements that are physically and logically interconnected between cyber and power networks. The cyber element is connected to a power element through a cyber-power link. Therefore, failure of the cyber network means that the interconnected power elements stop working. DEEI is always found in points interconnected between the cyber and power networks.

For the proposed cyber-power network in Figure 1 and Figure 2, DEEI can be found between each RTAPC unit and corresponding power equipment. For example, the failure of RTAPC 1 in the cyber network leads to the inoperation of the physically connected Load 1 in the power network. On the other hand, failure of RTAPC 2 does not directly impact the operation of Load 1, which means that there is no DEEI between RTAPC 2 and Load 1. Table I lists all existing cyber-power links between the cyber and power network shown in Figure 1 and Figure 2, respectively.

TABLE I. Cyber-Power Links Between Cyber and Power Networks

Cyber-Power Link	Linked Elements
CP1	(RTAPC 1: Load 1)
CP2	(RTAPC 1: DG1)
CP3	(RTAPC 2: Load 2)
CP4	(RTAPC 2: DG2)
CP5	(RTAPC 3: Load 3)
CP6	(RTAPC 3: DG3)
CP7	(RTAPC 4: DG4)

B. Cyber Network Connectivity Check

In the cyber network, several elements are not directly connected to a power device. These elements may misoperate or fail, which impacts the operation of the power system. As mentioned previously, the cyber-power network is defined as a set of cyber-power links. The key factor is how the failure of a cyber element inside the cyber network that is not directly connected to the power element can be expressed by these cyber-power links. A more developed, sophisticated interdependency is direct network element interdependency (DNEI), which is defined in the following subsections. An optimization problem is also presented.

1) Definition and Examples

DNEI refers to the performance of one network causing failure or changing the specification of the elements in the other network [7]. To evaluate the impact of these failures, a network analysis is required to assess performance and find DNEI between the cyber and power network. If a failure inside the cyber network results in the cyber element in a specific cyber-power link losing data integrity to the entire cyber network, the corresponding power element in that cyber-power link stops working. In order to achieve correct communication, data from multiple sources need to be transmitted. If a source of data is redundant, receiving data from one of the redundant sources is sufficient.

Several DNEIs between the proposed cyber and power network exist in Figure 1. For example, the operator can successfully send a close or open command from the human-machine interface (HMI) to Load 2 if connectivity between the HMI and controller RTAPC 2 in the cyber network can be established. The failure of Switch 1 in the cyber network does not mean that the data stream cannot flow from the HMI to Load 2 because there is an alternative for the data transfer via Switch 3.

2) Optimization Model

The linear optimization problem formulated by (2), (3), (4), (5), and (6) is proposed to find the network nodes that lose data integrity and cause DNEI [18].

$$\text{Max} \sum_{b=1}^{N_B} \sum_{r=1}^{N_R} R_{rb} \tag{2}$$

S.t.

$$\sum_{j=1}^{N_J} \psi_{mj} \bullet T_{jb} = \sum_{s=1}^{N_S} \rho_{msb} \bullet S_{sb} - \sum_{r=1}^{N_R} \eta_{mrb} \bullet R_{rb} \quad \forall b, \forall m \tag{3}$$

$$0 \le R_{rb} \le 1 \quad \forall b, \forall r \tag{4}$$

$$S_{sb} \ge 0 \quad \forall b, \forall s \tag{5}$$

$$-\infty \le T_{jb} \le \infty \quad \forall b, \forall j \tag{6}$$

In these equations, R_{rb} is the data received at the data receiver *r* for the type of data source *b*. S_{sb} is the data supplied from data source *s* for the type of data source *b*. T_{jb} is the data transferred through the available communications channel *j* for the type of data source *b*. ψmj is the element of node-channel incidence matrix ψ in which $\psi mj = 1$ if the starting point of available communications channel *j* is node *m* and $\psi mj = -1$ if

the ending point of available channel *j* is node *m*; otherwise, ψmj = 0. ρmsb is the element of node-source incidence matrix ρ in which ρmsb = 1 if the data source *s* for the type of data source *b* is at node *m*; otherwise, ρmsb = 0. ηmrb is the element of node-receiver incidence matrix η in which ηmrb = 1 if the data receiver *r* for the type of data source *b* is at node *m*; otherwise, ηmrb = 0.

From the optimization viewpoint, R_{rb} is either 0 or 1. Thus, β_W is defined in (7) to determine whether the available data receiver $r = \gamma_W$ can successfully receive required data from required data sources (N_b). $\beta_W = 1$ represents DNEI, where the required data cannot be transferred to the data receiver *r*, which consequently causes the failure of power element δ_W.

$$\beta w = \begin{cases} 1 \text{ if } \sum_{b=1}^{N_B} R_{rb} < N_b \\ 0 \text{ if } \sum_{b=1}^{N_B} R_{rb} = N_b \end{cases} \quad (7)$$

IV. Cyber-Power Reliability Evaluation Algorithm

In this section, the proposed cyber-power reliability algorithm for DEEI and DNEI is presented.

A. Creating States of Cyber-Power Network

Each state (Φ_i) is defined in the form of an array, as shown in (8), in which each element refers to the status of a real device in the cyber and power networks.

$$\Phi_i = \left(\varphi_{i,1}, \varphi_{i,2}, ..., \varphi_{i,N_C}, \varphi_{i,N_C+1}, ..., \varphi_{i,N_C+N_P}\right) \quad (8)$$

$\varphi_{i,k}$ is the status of element *k* in state *i*. $\varphi_{i,k}$ can have two values: 0 and 1. $\varphi_{i,k} = 0$ means that element *k* is in service, and $\varphi_{i,k} = 1$ represents the outage of element *k*. N_C and N_P represent the total number of elements in both cyber and power networks, respectively. The probability of state *i* is calculated in (9), where λ_k and μ_k are the failure rate and repair rate of element *k*, respectively.

$$PR_{\Phi_i} = \prod_{k=1}^{N_C+N_P} \left(\frac{\lambda_k}{\lambda_k + \mu_k}\right)^{(1-\varphi_{ik})} \left(\frac{\mu_k}{\lambda_k + \mu_k}\right)^{\varphi_{ik}} \quad (9)$$

B. State Mapping

State mapping occurs when the cyber element in a cyber-power link does not receive data from all required nodes, which results in power network failure. In state mapping, the probability of a state completely transfers to another state [7]. In other words, if the interdependency in (1) exists, and cyber element γ is failed, then state mapping causes the mapping of state Φ_i to state Φ_i'. States Φ_i and Φ_i' are almost similar and related as shown in (10).

$$\varphi_{i,j}' = \begin{cases} \varphi_{i,j} & j \neq \delta \\ 1 & j = \delta \wedge \left(\varphi_{i,\gamma} = 1 \vee \beta_{i,\gamma} = 1\right) \end{cases} \quad (10)$$

Note that $\varphi_{i,\gamma} = \varphi_{i,\gamma}' = 1$ in both states. However, $\varphi_{i,\delta} = 1 - \varphi_{i,\delta}' = 0$. In the condition in (10), $\varphi_{i,\gamma} = 1$ represents DEEI and $\beta_{i,\gamma} = 1$ represents DNEI.

If state Φ_i is mapped to state Φ_i', as a result, the probability of Φ_i and Φ_i' are updated as shown in (11) and (12).

$$Pr_{\Phi_i'} = Pr_{\Phi_i} + Pr_{\Phi_i'} \quad (11)$$

$$Pr_{\Phi_i} = 0 \quad (12)$$

C. Reliability Indice Calculations

After finalizing the probability of all states, the amount of load shedding for each state is calculated [7]. The loss of load expectation (LOLE) is calculated as shown in (13), where *sgn* is the sign function, which is 1 and 0 when the input number is positive and zero, respectively.

$$LOLE = 8,760 \bullet \sum_i PR_{\Phi_i} \bullet \text{sgn}\left(LC_i^T\right) \text{ hrs/yr} \quad (13)$$

V. Numerical Evaluation

In this section, the LOLE of the proposed model for the cyber-power network shown in Figure 1 and Figure 2 is calculated. The capacity of generating units and load demands is listed in Table II. The capacity of all power lines is assumed to be 352 kVA and PF = 0.85. As failure and repair rates vary for different manufacturers and also depend on ambient conditions, failure and repair rates of power and cyber devices are arbitrarily selected. These are listed in Table III. To better compare the effect of DEEI and DNEI, the presented cyber-power network is evaluated for four different cases.

TABLE II. Generator and Load Data

Generator	Capacity (kW)	Load	Demand (kW)
DG1	80	Load 1	300
DG2	250	Load 2	250
DG3	250	Load 3	175
DG4	250	–	–

TABLE III. Failure and Repair Rates for Cyber and Power Elements

Elements	λ (failures per year)	μ (occurrences per year)
DG units	0.2	365
Buses	0.4	365
RTAPC units	0.1	73
Servers	0.1	73
Switches	0.1	146

A. Case 1: Failure in Power Network

This case as a base case assumes that the elements of the cyber network do not fail, but elements in the power network are not failure-free.

B. Case 2: Failure in RTAPC Units

In this case, the power network is failure-free, but RTAPC units in the cyber network may fail. The results of this case show the reliability degradation of the microgrid because of DEEI, while the power system is failure-free. For the proposed cyber-power network, the seven cyber-power links in Table I are considered.

C. Case 3: Failure in Entire Cyber Network

If all equipment in the control system, including RTAPC units, switches, and servers, may fail while the microgrid power equipment is failure-free, both DEEI and DNEI exist between the cyber network and power system. The reliability indices in Case 2 and this case are noticeably different, which shows that the impact of DNEI is considerable and that network study is indispensable.

D. Case 4: Failure in Power and Cyber Network

This case calculates the reliability of the cyber-power system when considering the possibility of failures in the entire communications network, including failed switches, servers, and RTAPC units. In addition, the power system is not failure-free.

E. Reliability Evaluation Summary Results

Microgrid reliability results, including LOLE, are presented in Table IV. Case 2 only includes DEEI, while Cases 3 and 4 include both DEEI and DNEI. The reliability indices summarized in Table V show that DNEI in the cyber network is more important than DEEI and must be analyzed and included in the reliability model.

TABLE IV. EQUIPMENT WITH NON-ZERO FAILURE RATE IN FOUR CASES

Case	Power Elements	Cyber Elements
1	Buses	–
2	–	RTAPC units
3	–	RTAPC units, switches, and servers
4	Buses	RTAPC units, switches, and servers

TABLE V. RELIABILITY RESULTS FOR FOUR CASES

Case	Case Summary	LOLE (hours per year)
1	Failure in the power system	57
2	Failure in the controllers	64
3	Failure in the communications network	123
4	Failure in the communications network and power system	166

VI. CONCLUSION

Communications and computer networks are critical for microgrid stability and reliability. A loss-of-control situation is categorized as direct interdependency. This paper quantitatively evaluates the reliability of a microgrid while incorporating the impact of failure in the control system. The reliability model of the cyber-power network is studied and the LOLE index is calculated.

Comparison between the LOLE of Case 2 and Case 3 proves that studying only DEEI is not sufficient enough to evaluate the reliability of an interdependent cyber-power network. Therefore, network study for the cyber network is necessary to find the DNEIs.

VII. REFERENCES

[1] A. Asrari, T. Wu, and S. Lotfifard, "The Impacts of Distributed Energy Sources on Distribution Network Reconfiguration," *IEEE Transactions on Energy Conversion*, Vol. 31, Issue 2, January 2016, pp. 606-613.

[2] Q. Shafiee, J. M. Guerrero, and J. C. Vasquez, "Distributed Secondary Control for Islanded Microgrids—A Novel Approach," *IEEE Transactions on Power Electronics*, Vol. 29, Issue 2, February 2014, pp. 1018-1031.

[3] B. Falahati, A. Kargarian, and Y. Fu, "Impacts of Information and Communication Failures on Optimal Power System Operation," proceedings of the 2013 IEEE PES Innovative Smart Grid Technologies (ISGT) Conference, Washington, DC, February 2013.

[4] R. Majumder, A. Ghosh, G. Ledwich, and F. Zare, "Power Management and Power Flow Control With Back-to-Back Converters in a Utility Connected Microgrid," *IEEE Transactions on Power Systems*, Vol. 25, Issue 2, May 2010, pp. 821-834.

[5] R. Billinton and R. N. Allan, *Reliability Evaluation of Power Systems*. Springer Publishing U.S., New York, 1996.

[6] C. Singh and A. Sprintson, "Reliability Assurance of Cyber-Physical Power Systems," proceedings of the 2010 IEEE Power and Energy Society General Meeting, Minneapolis, MN, July 2010.

[7] B. Falahati, Y. Fu, and W. Lei, "Reliability Assessment of Smart Grid Considering Direct Cyber-Power Interdependencies," *IEEE Transactions on Smart Grid*, Vol. 3, Issue 3, September 2012, pp. 1515–1524.

[8] Q. Wang, M. Pipattanasomporn, M. Kuzlu, Y. Tang, Y. Li, and S. Rahman, "Framework for Vulnerability Assessment of Communication Systems for Electric Power Grids." *IET Generation, Transmission & Distribution*, Vol. 10, Issue 2, February 2016, pp. 477-486.

[9] Y. Wang, W. Li, and J. Lu, "Reliability Analysis of Wide-Area Measurement System," *IEEE Transactions on Power Delivery*, March 2010, Vol. 25, Issue 3, pp. 1483–1491.

[10] Z. Dai, Z. Wang, and Y. Jiao, "Reliability Evaluation of the Communication Network in Wide-Area Protection," *IEEE Transactions on Power Delivery*, Vol. 26, Issue 4, October 2011, pp. 2523–2530.

[11] S.V. Buldyrev, R. Parshani, G. Paul, H. E. Stanley, and S. Havlin, "Catastrophic Cascade of Failures in Interdependent Networks," *Nature*, Vol. 464, February 2010, pp. 1025–1028.

[12] S. Rahman, M. Pipattanasomporn, and Y. Teklu, "Intelligent Distributed Autonomous Power Systems (IDAPS)," proceedings of the 2007 IEEE Power Engineering Society General Meeting, Tampa, FL, June 2007.

[13] M. Shahverdi, M. Mazzola, N. Sockeel, and J. Gafford, "High Bandwidth Energy Storage Devices for HEV/EV Energy Storage System," proceedings of the 2014 IEEE Transportation Electrification Conference and Expo (ITEC), Dearborn, MI, June 2014.

[14] N. Jayawarna, X. Wut, Y. Zhang, N. Jenkins, and M. Barnes, "Stability of a Microgrid," proceedings of the 3rd IET International Conference on Power Electronics, Machines and Drives, Dublin, Ireland, April 2006.

[15] S. R. Bull, "Renewable Energy Today and Tomorrow," *Proceedings of the IEEE*, Vol. 89, Issue 8, August 2001, pp. 1216–1226.

[16] S. Kazemlou and S. Mehraeen, "Novel Decentralized Control of Power Systems With Penetration of Renewable Energy Sources in Small-Scale Power Systems," *IEEE Transactions on Energy Conversion*, Vol. 29, Issue 4, December 2014, pp. 851–861.

[17] X. Liu, P. Wang, and P. C. Loh, "A Hybrid AC/DC Microgrid and Its Coordination Control," *IEEE Transactions on Smart Grid*, Vol. 2, Issue 2, June 2011, pp. 278-286.

[18] B. Falahati, Z. Darabi, Y. Fu, and M. Vakilian, "Quantitative Modeling and Analysis of Substation Automation Systems," proceedings of the 2012 IEEE PES Transmission and Distribution Conference and Exposition (T&D), Orlando, FL, May 2012.

Previously presented at the 2017 IEEE PES General Meeting, Chicago, IL, July 2017.