Impact Analysis of Transient Stability Due to Cyber Attack on FACTS Devices

Bo Chen, Karen L. Butler-Purry
Electrical and Computer Engineering Department
Texas A&M University
College Station, TX, USA
{bchen, klbutler}@tamu.edu

Deepa Kundur
Electrical and Computer Engineering Department
University of Toronto
Toronto, ON, Canada
dkundur@comm.utoronto.ca

***Abstract*—The innovations in information and communication technologies (ICT) and digital computer controllers are increasingly integrated into the smart grid. This introduces cybersecurity vulnerabilities which may cause system stability problems. In this paper, the modification attack on SVC and STATCOM in IEEE 39 bus system is simulated with DSATools™. Then the impact on the system transient stability is studied. The results show that some modification cyber attacks can make the system angle or voltage unstable under the proposed attack scenarios.**

***Index Terms*—cyber attack, cyber security, smart grids, SVC, STATCOM, FACTS, transient stability, voltage support device**

I. INTRODUCTION

The innovations in information and communication technologies (ICT) and digital computer controllers are increasingly integrated into the smart grid. Some emerging smart grid applications such as Advanced Metering Infrastructure (AMI), Distribution management System (DMS), Wide Area Measurement System (WAMS), and Home Area Network (HAN) will be widely deployed to facilitate smart grid applications in monitoring, control, data analysis, and resource optimization [1]. On the other hand, these technologies greatly increase the dependency of smart grid applications on ICT. Considering the current power grids are not designed to be adequately protected from cyber attack, these applications introduce numerous cyber security vulnerabilities that threaten the security of cyber-physical power system span across generation, transmission and distribution systems [2]. Therefore, cyber security is becoming an important R&D concern for smart grid.

Many efforts have been made on developing cyber resilient smart grid. Guidelines and frameworks for Industrial Control Systems (ICS) security have been presented by the National Institute of Standards and Technology (NIST) [3-5] and other organizations and agencies [6],[7]. However, key challenges still remain to be addressed. Numerous vulnerabilities of a cyber-physical smart grid have been identified in [8],[9], in terms of SCADA systems, digital computer controllers and programmable logic controllers (PLC). The cyber vulnerabilities can be used for performing cyber attacks by corrupted personnel, unauthorized parties and terrorists [10],[11].

The amount of cyber attacks on the U.S. power grid infrastructure has increased 17-fold from 2009 to 2011 [12]. And the resulting losses have been reported in [13]. It can be expected that the losses caused by cyber attack on power grid infrastructure will increase significantly, if no proper protections are applied.

Several types of cyber attacks and their impacts have been studied. Recent research on cyber attack modeling focuses on compromising the state estimator by injecting bad data [14],[15]. The impacts on state estimation and power market are studied. The attackers with knowledge of both communication and power can make profit from power market, or make the system operating under suboptimal conditions, without being detected by current configuration of state estimation. Data integrity attacks were also launched on a load management system in [11], in which a graph based dynamic system model was used to analyze the impact of the cyber attack. The impact of cyber attacks on the automatic generation control loop was studied in [16], in which the integrity of information security was compromised. An increase in system frequency and tie-line flow was observed. A coordinated switching attack was studied in [17]. The results showed how switching a load in and out along a certain sliding mode could lead to system instability. Two data attack strategies on smart meters were studied in [18]. The results showed that the network state became unobservable when a certain set of meters were hacked.

Voltage support devices, e.g. SVC and STATCOM, are used for VAR compensation to improve voltage profile, and identified as one of the critical components of smart grid. The communication routes between control center, measurement unit, and field operation are vulnerable to types of cyber attacks. Therefore, it is necessary to study the impact of compromised voltage support devices on system stability.

In this paper, section II briefly summarizes the vulnerabilities of smart grid sensor network, and three possible attack scenarios. Section III discusses the stability indices to quantify the impacts. Then section VI introduces the test system.

This work was supported in part by Norman Hackerman Advanced Research Program Project 000512-0111-2009 and NSF grants EECS-1028246 and EEC-1062603.

978-1-4799-1255-1/13/$31.00 ©2013 IEEE

Section V reports the cyber attack simulation results from several cases. Finally, this paper is concluded in section VI.

II. Cyber Attack on FACTS Devices

A. Cyber Vulnerabilities of Smart Grid Infrastructure

The cyber vulnerabilities of smart grid infrastructure can be categorized as multiple levels of cyber-physical system, e.g. information level, information and communication technologies (ICT) infrastructure level, and smart grid application level [1]. The security analysis for the information level and ICT infrastructure level is continuously studied for the past years. But the vulnerabilities within application level still remain to be investigated. Since the legacy power grid was not designed to be cyber attack resilient, numerous vulnerabilities have been identified span across generation, transmission and distribution systems [8].

In addition to SCADA networks, the typical control loops, such as AVR, AGC, EMS, VAR Compensation, WAMS, state estimation, are all considered vulnerable to cyber attacks. Reference [1] generalized the forms of cyber attacks, including protocol attack, routing attack, intrusion, malware, denial of service (DoS) attack, and insider threats. The network protocols used in smart grid applications, e.g. IEC 61850, DNP3, can be potentially compromised. With the access to the network, the attackers can be able to intercept, modify, and fabricate the system states and control [19].

B. Modification Attack

The network protocol of VAR compensation system is assumed to be compromised by attackers who can get access to the communication network of smart grid. Then the protocol attack is launched, this paper assumes that the measurement values are modified by the attackers for certain reasons (financial, political, or personal challenge for fun). Specifically, the attacker can add a bias to the measurements that represents the remote bus voltage at any time. This kind of attack, we call it modification attack, can also be categorized into integrity attack. Because it violates the information integrity of the cyber-physical system [19].

C. Cyber Attack Scenarios

The cyber attacks can be launched anytime, no matter the system is operating in normal state, alert state, emergency state, or restorative state. Therefore, to assess the impact of modification attack on system stability, three scenarios were considered based on the timing that the modification attack was launched.

1) Scenario A: Bias is added under normal condition

This is the most common scenario when the cyber attack is launched. The bias is added when the system is operating at normal state, in which all the system states are operating within the security constraints. In addition, because the system is designed for N-1 redundancy [20], the stability of the system can be maintained under any one of the most severe contingencies or loss of any one of the generators. For most of the time the system is operating at normal state.

2) Scenario B: Bias is added before the fault occurs

As the name implies, in this scenario, the bias is added prior to when the contingency occurs. This situation can happen when the modification attack is applied and keeps being undetected, until the contingency occurs somewhere in the system. This scenario also happens under a cyber-physical coordinated attack (launch modification attack first, then launch physical contingency attack at somewhere of the system). Due to the widely geographical dispersion of the power infrastructure without the proper physical protection, it is easy to apply a physical contingency. Since the system will operate in a suboptimal state, when subjected to the modification attack, this will deteriorate the transient stability when the system encounters a contingency afterwards.

3) Scenario C: Bias is added simultaneously with the fault

This scenario is similar to the previous one. The difference is that the bias is added simultaneously with the contingency occurrence. This scenario could occur when a coordinated attack is launched. Here are two possible ways to perform a coordinated attack in this scenario. First, the attacker launches interception attack to monitor the system operation states, and then launch modification attack as long as the system is in alert state or emergency state because of contingency [20]. Second, the cyber attack and physical attack is coordinated and launched at the same time. It can be categorized as "low frequency high impact event" based on the definition given in [21]. The stability margin shrinks as some constraints are violated in alert or emergency state. So this scenario will threaten the system stability.

III. Power System Transient Stability

Power system stability is the ability of an interconnected system to regain a state of operating equilibrium after being subjected to a physical disturbance [22]. Power system stability is always a great concern for secure system operation. It can be classified based on the time span (long term, short term), size of disturbance (large disturbance, small disturbance), and system variables in which instability can be observed (rotor angle, voltage, frequency). To assess the impact of cyber attacks on transient stability in smart grids, the angle stability index (ASI) and voltage stability index (VSI) were used in impact analysis.

A. Angle Stability and Angle Stability Index

Angle stability refers to the ability of an interconnected power system to maintain synchronism when subjected to a disturbance [22]. It depends on the ability of the system to maintain or restore the equilibrium between the mechanical and the electromagnetic torque. The angle stability index used in this paper is defined in [23] as:

$$\eta = \frac{360^\circ - \delta_{max}}{360^\circ + \delta_{max}} \times 100\% \quad (1)$$

Where $\delta_{\max}$ is the maximum angle separation of any two generators in the same island in the post-contingency system. This index varies between -100% and 100%. $\eta > 0$ and $\eta \leq 0$ denote stable and unstable conditions, respectively. Also, a bigger η corresponds to a more stable system.

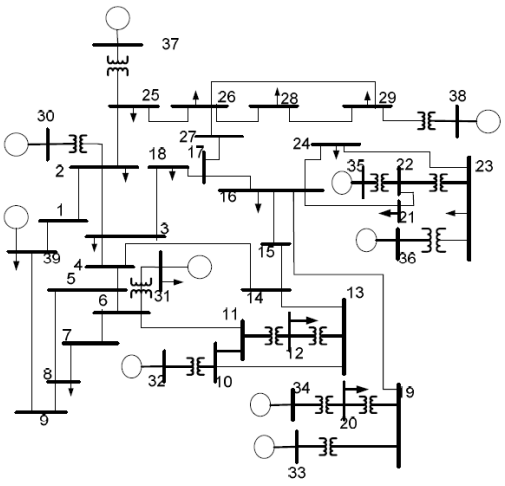
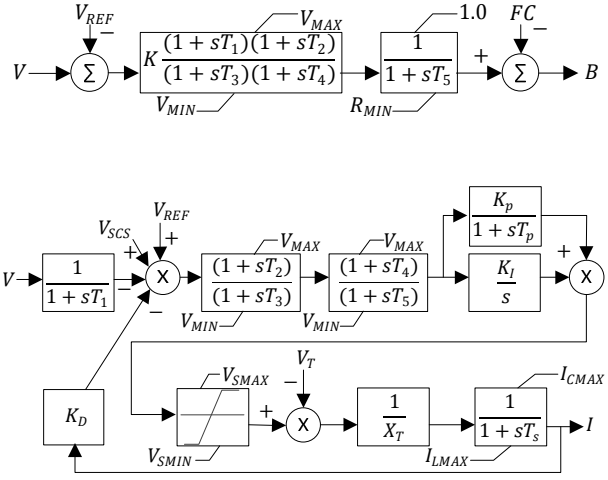


Figure 1. Test system: 39 bus system



B. Voltage Stability and Voltage Stability Index

Voltage stability refers to the ability of an interconnected system to maintain the voltage at all buses within a certain level, when subjected to a disturbance [22]. It depends on the ability of the system to maintain or restore the equilibrium of supply and demand at load buses. Voltage instability may cause tripping of system elements (loads or lines), due to operation of protective devices. In a worse scenario, voltage stability may trigger a progressive fall or rise of voltages at some buses and lead to a cascading outage.

According to the Western Electricity Coordinating Council (WECC) standards, after an event or fault leading to the loss of a single power system element, load bus voltages must satisfy the following two constraints [24]. Firstly, the voltage dip/sag should not exceed 25%. Secondly, the voltage dip/sag must not exceed 20% for more than 20 cycles (330 milli-seconds in 60 Hz systems).

Based on these requirements and since all the cases in this paper study contingencies which lead to voltage drops, the voltage stability index for the studies conducted in this paper is defined to be the maximum time a load bus voltage remains below 0.8pu, among all system load buses. For instance, consider a fault which causes the bus voltages at buses 2, 5, and 7 to stay below 0.8pu for 400ms, 500ms, and 350ms, respectively. In this case, the defined voltage stability index would be 500ms, which is the maximum time among all load buses. This index, i.e. 500ms, denotes an unacceptable voltage behavior, since it is greater than 330ms.

IV. Simulation Setup

A. Test System

New England 39 bus system was used in this paper to analyze the impact of cyber attacks on the smart grid. The single line diagram shown in Fig. 1 was comprised of 10 generators, 16 loads, 13 transformers and 34 lines. The system parameters can be found in [25]. The static VAR compensator (SVC) and the static synchronous compensator (STATCOM) are considered as the voltage support systems.

B. System Modelling

This system was modeled in Transient Security Assessment Tool (TSAT) of DSA*Tools*™ package. TSAT is a time-domain simulation tool designed for power system dynamic behavior assessment. Each generator is modeled as a round rotor synchronous generator (GENROU) with an exciter and a Power System Stabilizer (PSS). The loads in the system were modeled as constant PQ loads. Also, pi models were used for transformers and transmission lines.

SVC and STATCOM are assumed to be allocated at bus 20, according to the optimized allocation given in [26]. The capacity ranges -400 MVAr to 400 MVAr with fixed capacitor 100 MVar. So the adjustable capacity rangs -300 MVAr to 500 MVAr. Given any contingency on transmission line, the transient voltage profile can be assured to satisfy the criteria, with the support of SVC or STATCOM. The control blocks for the SVC and the STATCOM are plotted in Fig. 2 and Fig. 3. Note that due to the space limit, the characteristics of SVC and STATCOM are not fully included in Fig. 2 and Fig.3. The controllers of SVC and STATCOM will be blocked when the sensed voltage is below 0.7 pu, according to their V-I characteristics [20]. Then they will become a fixed capacitors. For STATCOM, it will be isolated when the sensed voltage is below 0.3 pu.

C. Impact of Voltage Support Devices

To demonstrate the effect of voltage support devices on improving voltage profile, three case studies were performed. Case A includes no voltage support devices. In cases B and C, the system is equipped with a SVC and a STATCOM, respectively. The contingency on line 16-17 was chosen because it was considered as the most severe contingency among all the contingencies on transmission lines [26]. A 3-phase bolted fault was applied for each case on bus 16 at 0.1 second, and was cleared after 100 ms by opening line 16-17 at 0.2 second. The voltage profiles at bus 20 and reactive power output for each case are shown in Fig. 4. And the angle stability indices and the voltage stability indices are listed in Table I.

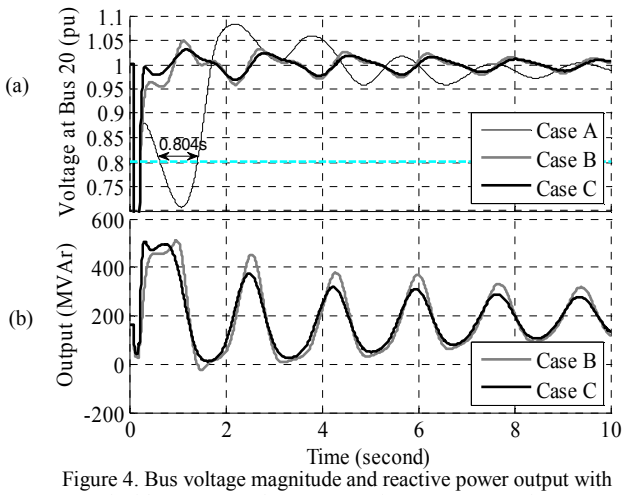


Figure 4. Bus voltage magnitude and reactive power output with and without SVC and STATCOM in cases A, B, and C

TABLE I. TRANSIENT STABILITY INDICES FOR CASE A, B, AND C

Case No	Case Description	Stability Index	
		Angle	*Voltage*
A	Without SVC or STATCOM	36.57%	0.804s
B	With SVC	45.19%	0.024s
C	With STATCOM	47.15%	0.020s

Fig. 4(a) compares the voltage profiles at bus 20 with the reference value and Fig. 4(b) compares the reactive power contribution of SVC and STATCOM in cases B and C respectively. For case A, the voltage of bus 20 drops below 0.8 pu for 0.804 second. Thus the system will violate the voltage criteria due to the contingency applied to the system. For cases B and C, the reactive power output of SVC and STATCOM reaches the peak value when the bus voltage is the lowest. Therefore the voltage profile is improved. Table I shows that in case A, although the system is angle stable, but the voltage criteria is violated, which is more than the threshold (330ms). But with the voltage support devices, the voltage indices are very small. In conclusion, voltage support devices can improve the voltage profile and transient stability. In the following case studies, it will be shown that the modification attack on voltage support devices can deteriorate the transient stability or even make the system unstable.

V. CYBER ATTACK CASE STUDIES

This section presents the results of the case studies for the three scenarios explained in section II. For each scenario, the attacker was assumed to be able to perform the modification attack by gaining the access to the protocols of the network. A bias was added to the original measurement value. The modification attack can be defined as shown in (2).

$$v'_{20}(t) = \begin{cases} v_{20}(t) & t < T \\ v_{20}(t) + \Delta v & t \geq T \end{cases} \quad (2)$$

where $v_{20}(t)$ is the original measurement value, Δv is the bias that the attacker added, $v'_{20}(t)$ is the modified voltage value that is supposed to be sent to control systems, T is the moment when the bias is added according to different scenarios.

The impact analysis was performed by investigating the stability indices for each scenario. The magnitude of the bias ranged from -1.0 pu to +1.0 pu with 0.1 pu per step. For each case in each scenario, one bias for SVC and STATOM was studied. So there is a total of 63 cases that with different biases in different scenarios. For scenario A, no contingency was considered. For scenario B and C, the 3 phase bolted contingency was applied to the 30 transmission lines of the system in each case. Due to the space limit, this paper just shows the representative cases, instead of showing the results of all the cases.

A. Impact of Modification Attack in Scenario A

In scenario A, the biases are added at 0.2 second under normal state, and no contingencies are applied. The angle stability indices for each case are plotted in Fig. 5. The voltage stability indices were all zeros. The reactive power output of SVC and STATCOM is show in Fig. 6.

For the positive biases, the controller sensed a higher voltage magnitude than the reference voltage. This makes the SVC and the STATCOM reduce the reactive output, or even absorb the reactive power from the grid. From Fig. 5, the indices keep the same when the bias is positive and the magnitude is larger than 0.3 for both SVC and STATCOM. This is because the output of control blocks already hits the limit, when the voltage difference proceeded to the voltage regulators in both SVC and STATCOM controllers. So the reactive output corresponding to these cases are the same, as shown in Fig. 6.

For the negative biases, the controller sensed a lower voltage magnitude than the reference voltage, which makes the SVC and the STATCOM output more reactive power. In Fig. 5, the angle stability indices are almost the same for all the negative biases. In Fig. 6, the reactive output of SVC and

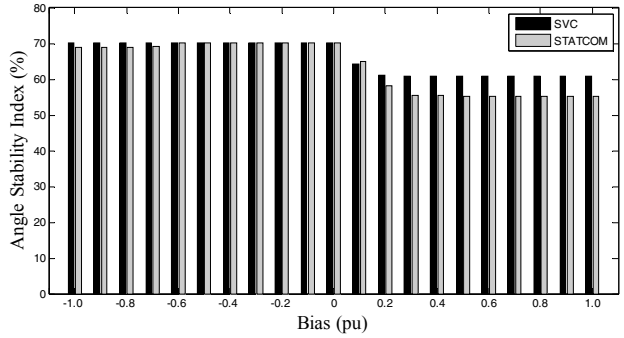


Figure 5. Angle stability indices for scenario A

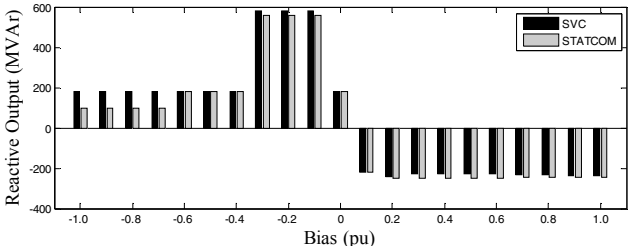


Figure 6. Reactive output for scenario A

STATCOM reduced when the bias was negative and the magnitude was smaller than 0.4 pu. This is because according to the characteristics of SVC and STATCOM, controller will be blocked when the sensed voltage is below the threshold (0.7 pu), therefore SVC or STATCOM will become a fixed capacitor. Also the STATCOM will be isolated when the sensed voltage is below 0.3 pu, leaving the fixed capacitor connected to the grid.

B. Impact of Modification Attack in Scenario B

In this scenario, the biases are added at 0.2 second under normal state, and then the contingencies are applied to the assumed transmission lines at 10.0 second, cleared at 10.1 second. Fig. 7 shows the voltage profiles on bus 20, corresponding to the selected biases. Table II summarizes the angle and voltage stability indices corresponding to each bias, with respect to the contingency 16-17. In this paper, only one contingency on line 16-17 was analyzed due to the space limit. Table II also summarizes the total number of cases that violate the ASI and VSI for each bias for all the 30 contingencies.

From Fig. 7, the system can maintain stable when the magnitude of the bias is smaller than 0.1. There are a small range of negative biases that will make the system unstable: -0.2, -0.3 for SVC and -0.6 for STATCOM. Other biases make the steady state voltage a little bit higher than the reference value. For positive biases, they make the system unstable as long as the magnitude is bigger than a certain value (refer to Table II). Because before the contingency occurs, the devices both absorb reactive power from grid, thus deteriorate the voltage profiles until the voltage collapse occurs.

In Table II, all the cases with non-zero bias violate the VSI criteria. It also can be observed that STATCOM is more sensitive to the bias, since all the VSIs are bigger than that of SVC. For all the 30 contingencies, only one contingency on 16-17can make the system with SVC unstable, while 2 contingencies will make the system with STATCOM unstable. Note that with STATCOM, all the contingencies will make the system violate VSI criteria.

C. Impact of Modification Attack in Scenario C

In this scenario, the biases are injected when the contingency is applied at 0.1 second. Table III and Fig. 8 show the stability indices for each bias and voltage profiles for selected biases. Note the contingency used in this scenario is also 16-17.

Fig. 8 shows the voltage profiles when the modification attack and contingency occur simultaneously. System will go unstable when the bias is positive and bigger than certain values. In addition, the small negative biases can result a higher bus voltage, while the positive biases can make the bus voltage lower than the original value.

From Table III, the most obvious difference between scenario B and scenario C is the total number of contingencies that can make the system unstable, with the corresponding biases. With STATCOM, 27 out of 30 contingencies can make the system unstable, if the modification attack is launched with a positive bias bigger than 0.4. This means the positive biases deteriorate the stability margin greatly in this

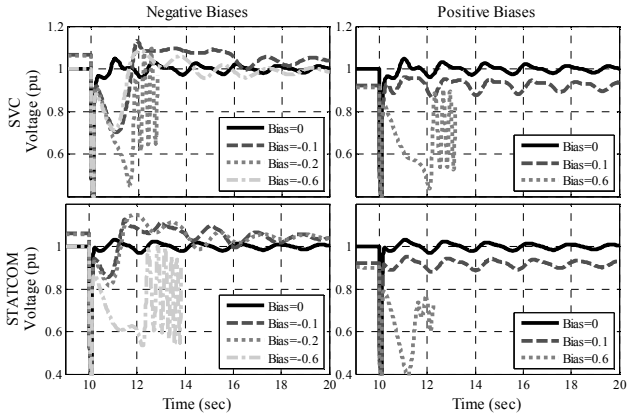


Figure 7. Scenario B: Voltage profile on bus 20 due to selected biases and contingency 16-17

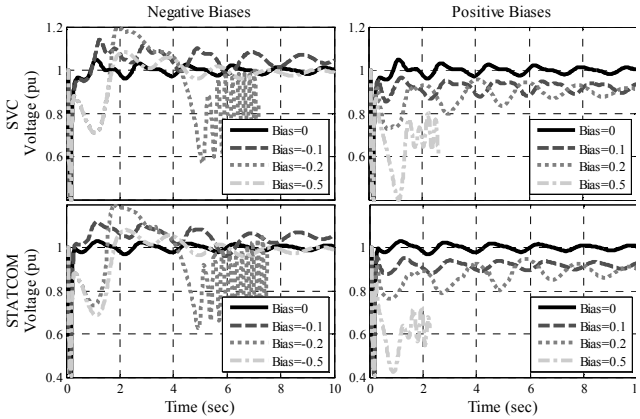


Figure 8. Scenario C: Voltage profile on bus 20 due to selected biases and contingency 16-17

scenario. Negative bias can also make the system unstable when the contingencies are applied.

To summarize, the above case studies show that the modification attack may cause severe consequences when followed by a contingency. The system is more vulnerable when installed a STATCOM than SVC. Also, the positive biases make the devices absorb reactive power, thus deteriorate the voltage profile and threaten the system stability. Although the negative biases have minor impact on stability indices in scenario A, the system can be driven unstable when certain contingencies occur.

VI. CONCLUSIONS AND FUTURE WORK

This paper discussed the cyber security issues for smart grid. The modification attack was proposed as a type of cyber attack, and then the impact of the modification attack on the system stability was studied. The case studies carried out on 39 bus system show that the cyber attack on measurements of SVC or STATCOM system can cause a deterioration of the stability margin, or even make the system unstable when contingencies applied. Future work includes mathematically modeling the impact of cyber attacks, investigation of mitigation strategies, and development of frameworks to identify cyber physical system vulnerabilities.

TABLE II. STABILITY INDICES FOR SCENARIO B

Bias (pu)	Contingency 16-17				Total No. of Contingencies Violate the Indices			
	SVC		*STATCOM*		*SVC*		*STATCOM*	
	ASI(%)	*VSI(s)*	*ASI(%)*	*VSI(s)*	*ASI*	*VSI*	*ASI*	*VSI*
0.0	45.19	0.02	47.15	0.02	0	0	0	0
-0.1	34.44	0.98	39.47	0.17	0	2	0	1
-0.2	-90.37	1.33	37.31	0.48	1	3	0	2
-0.3	-90.37	1.33	36.74	0.54	1	3	0	2
-0.4	36.47	0.79	36.81	0.75	0	2	0	2
-0.5	36.47	0.79	35.98	0.92	0	2	0	2
-0.6	36.47	0.79	-79.31	1.91	0	2	1	3
-0.7	36.47	0.79	36.33	0.84	0	2	0	2
-0.8	36.47	0.79	36.28	0.84	0	2	0	2
-0.9	36.47	0.79	36.28	0.84	0	2	0	2
-1.0	36.47	0.79	36.28	0.84	0	2	0	2
+0.1	44.63	0.04	44.25	0.03	0	0	0	0
+0.2	38.70	0.54	38.16	0.59	0	2	0	2
+0.3	40.64	0.85	29.08	1.49	0	2	0	30
+0.4	36.22	1.28	-61.64	1.90	0	3	2	30
+0.5	-71.26	1.93	-71.73	1.92	1	4	2	30
+0.6	-65.73	2.48	-67.48	2.20	1	4	2	30
+0.7	-65.49	2.47	-67.33	2.19	1	4	2	30
+0.8	-64.41	2.44	-67.33	2.19	1	4	2	30
+0.9	-64.24	2.44	-67.33	2.19	1	4	2	30
+1.0	-63.09	2.43	-67.33	2.19	1	4	2	30

TABLE III. STABILITY INDICES FOR SCENARIO C

Bias (pu)	Contingency 16-17				Total No. of Contingencies Violate the Indices			
	SVC		*STATCOM*		*SVC*		*STATCOM*	
	ASI(%)	*VSI(s)*	*ASI(%)*	*VSI(s)*	*ASI*	*VSI*	*ASI*	*VSI*
0.0	45.19	0.02	47.15	0.02	0	0	0	0
-0.1	44.72	0.02	48.18	0.02	0	2	0	0
-0.2	-85.00	0.80	-87.14	0.70	1	3	1	1
-0.3	-85.40	0.80	-86.8	0.93	1	3	1	1
-0.4	36.57	0.80	37.29	0.70	0	2	0	1
-0.5	36.57	0.80	36.58	0.88	0	2	0	1
-0.6	36.57	0.80	-88.65	1.92	0	2	1	3
-0.7	36.57	0.80	-88.65	1.92	0	2	8	10
-0.8	36.57	0.80	-88.65	1.92	0	2	1	3
-0.9	36.57	0.80	-88.65	1.92	0	2	1	3
-1.0	36.57	0.80	-88.65	1.92	0	2	1	3
+0.1	42.30	0.02	42.6	0.02	0	0	0	1
+0.2	33.58	0.82	34.68	0.74	0	2	0	17
+0.3	-88.30	1.84	-87.26	2.13	2	2	4	24
+0.4	-89.80	1.96	-90.14	2.00	4	3	27	30
+0.5	-89.20	1.83	-90.14	2.00	4	4	27	30
+0.6	-88.60	2.03	-89.93	1.85	4	4	27	30
+0.7	-88.60	2.02	-91.05	1.95	4	4	27	30
+0.8	-88.60	1.94	-91.09	2.00	4	4	27	30
+0.9	-88.60	1.93	-91.12	2.00	4	4	27	30
+1.0	-88.60	1.82	-91.16	2.01	4	4	27	30

REFERENCES

[1] M. Govindarasu, A. Hahn, and P. Sauer, "Cyber-Physical Systems Security for Smart Grid," 2012. [Online]. Available: http://www.pserc.wisc.edu

[2] "Common Cybersecurity Vulnerabilities in Industrial Control Systems," Idaho Ntional Laboratory May 2010. [Online]. Available: http://ics-cert.us-cert.gov

[3] "NISTIR 7628: Guidelines for Smart Grid Cyber Security," National Institute for Standards and Technology (NIST) 2010. [Online]. Available: www.nist.gov

[4] "NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0," National Institute of Standards and Technology (NIST) 2010. [Online]. Available: www.nist.gov

[5] "Guide to Industrial Control Systems (ICS) Security," National Institute of Standards and Technology (NIST) 2011. [Online]. Available: http://csrc.nist.gov/

[6] "Roadmap to Achieve Energy Delivery Systems Cybersecurity," Energy Sector Control Systems Working Group September 2011. [Online]. Available: http://www.cyber.st.dhs.gov/

[7] "Electricity Grid Modernization: Progress Being Made on Cybersecurity Guidelines, but Key Challenges Remain to be Addressed," United States Government Accountability Office (GAO) January 2011. [Online]. Available: www.gao.gov

[8] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber Physical System Security for the Electric Power Grid," Proceedings of the IEEE, vol. 100, pp. 210-224, 2012.

[9] M. Yilin, T. H. J. Kim, K. Brancik, D. Dickinson, L. Heejo, A. Perrig, and B. Sinopoli, "Cyber Physical Security of a Smart Grid Infrastructure," Proceedings of the IEEE, vol. 100, pp. 195-209, 2012.

[10] N. R. Council, Terrorism and the Electric Power Delivery System. The National Academies Press, 2012.

[11] D. Kundur, F. Xianyong, L. Shan, T. Zourntos, and K. L. Butler-Purry, "Towards a Framework for Cyber Attack Impact Analysis of the Electric Smart Grid," in Proc. 2010 Smart Grid Communications (SmartGridComm), First IEEE International Conference on, Gaithersburg, MD, pp. 244-249, 4-6 Oct. 2010.

[12] "Cyber attacks against infrastructure jump 17-fold warns National Security Agency," 2012. [Online]. Available: http://www.smartgridnews.com

[13] S. Baker, S. Waterman, and G. Ivanov, "In the Crossfire: Critical Infrastructure in the Age of Cyber War," McAfee 2009. [Online]. Available: www.mcafee.com

[14] X. Le, M. Yilin, and B. Sinopoli, "Integrity Data Attacks in Power Market Operations," IEEE Transactions on Smart Grid, vol. 2, pp. 659-666, 2011.

[15] Y. Liu, P. Ning, and M. K. Reiter, "False Data Injection Attacks Against State Estimation in Electric Power Grids," ACM Transactions on Information and System Security, vol. 14, pp. 1-33, 2011.

[16] S. Sridhar and G. Manimaran, "Data Integrity Attacks and Their Impacts on SCADA Control System," in Proc. 2010 Power and Energy Society General Meeting, 2010 IEEE, pp. 1-6, 25-29 July 2010, 2010.

[17] L. Shan, F. Xianyong, D. Kundur, T. Zourntos, and K. L. Butler-Purry, "Switched System Models for Coordinated Cyber-physical Attack Construction and Simulation," in Proc. 2011 Smart Grid Modeling and Simulation (SGMS), IEEE First International Workshop on, Brussels, Belgium, pp. 49-54, 17-17 Oct. 2011.

[18] O. Kosut, J. Liyan, R. J. Thomas, and T. Lang, "Malicious Data Attacks on the Smart Grid," IEEE Transactions on Smart Grid, vol. 2, pp. 645-658, 2011.

[19] D. Kundur, "Cyber Security of the Smart Grid handouts," Texas A&M University 2012.

[20] P. Kundur, Power System Stability And Control. New York: McGraw-Hill, 1994.

[21] "High-Impact, Low-Frequency Event Risk to the North American Bulk Power System," North American Electric Reliability Corporation (NERC) and the U.S. Department of Energy (DoE) June 2010. [Online]. Available: http://www.nerc.com

[22] P. Kundur, J. Paserba, V. Ajjarapu, G. Andersson, A. Bose, C. Canizares, N. Hatziargyriou, D. Hill, A. Stankovic, C. Taylor, T. Van Cutsem, and V. Vittal, "Definition and Classification of Power System Stability," IEEE Transactions on Power Systems, vol. 19, pp. 1387-1401, 2004.

[23] "TSAT User Manual," Powertech Labs Inc., Canada, 2012.

[24] WECC WECC-NERC Planning Standards, WECC Standard, 2007.

[25] A. Pai, Energy Function Analysis for Power System Stability. Springer, 1989.

[26] L. Xijuan and B. Jeyasurya, "Static VAR Compensator Allocation by Simplified Sensitivity Analysis and Its Influence on Transient Voltage Performance Improvement," in Proc. 2012 North American Power Symposium (NAPS), Champaign, IL, pp. 1-6, 9-11 Sept. 2012.