Proceedings of the 4th Annual ISC Research Symposium
ISCRS 2010
April 21, 2010, Rolla, Missouri

INTEGRATED CYBER-PHYSICAL FAULT INJECTION FOR RELIABILITY ANALYSIS OF THE SMART GRID

Ayman Faza and Sahra Sedigh
Department of Electrical and Computer Engineering. {azfdmb,sedighs}@mst.edu

Bruce McMillin
Department of Computer Science
ff@mst.edu

ABSTRACT

The term ``Smart Grid" broadly describes emerging power systems whose physical operation is managed by significant intelligence. The cyber infrastructure providing this intelligence is composed of power electronics devices that regulate the flow of power in the physical portion of the grid. Distributed software is used to determine the appropriate settings for these devices. Failures in the operation of the Smart Grid can occur due to malfunctions in physical or cyber (hardware or software) components.

This paper describes the use of fault injection in identifying failure scenarios for the Smart Grid. Software faults are injected to represent failures in the cyber infrastructure. Physical failures are concurrently represented, creating integrated cyber-physical failure scenarios that differentiate this work from related studies. The effect of these failure scenarios is studied in two cases: with and without fault detection in the distributed software. The paper concludes by discussing future research trends for our work.

1. INTRODUCTION

The high complexity of the electric power grid, exacerbated by increased stress on its operation, has motivated the use of cyber infrastructure to fortify the operation of the grid. The intelligence provided by this cyber infrastructure led to the concept of the Smart Grid [1]. Different definitions proposed for the Smart Grid concur that it improves the dependability of its predecessors by using intelligent power electronics devices that communicate with each other to prevent line overloads and cascading failures that can lead to blackouts. The addition of this computing and communication capability creates a cyber-physical system that incorporates both conventional components of the power grid (physical infrastructure), and the computing and communication elements (cyber infrastructure) used for monitoring and control.

Our research considers a Smart Grid where Flexible AC Transmission Systems (FACTS) devices are used to prevent cascading failures by controlling power flow. These devices are deployed on a number of critical transmission lines in the system, and communicate to collectively determine flow values that would prevent overloads from occurring in the physical system, and hence prevent the system from failing, even in the presence of transmission line outages [2], [3]. The settings for the FACTS devices are determined using the Maximum Flow (MaxFlow) algorithm [4], which computes (cyber) the maximum amount of flow that can be carried by each transmission line without violating its capacity constraint (physical).

Incorrect operation of the MaxFlow algorithm can lead to incorrect settings on the FACTS devices, which may or may not lead to errors in the operation of the grid. In this paper, we use fault injection to analyze the effect of errors in the operation of the MaxFlow algorithm. For our analysis, we use an instance of the IEEE118 bus system, shown in Fig. 1 as our case study. In this system, FACTS devices F_1 through F_7 collectively execute the MaxFlow algorithm. A summary of the potential cascade-initiating transmission lines and the placement of the FACTS devices is shown in Table 1.

Table 1 - Locations of FACTS devices required for mitigation of failures

Cascading failure	Initiating line	1st device/line	2nd device/line
1	(4-5)	F_1/(5-11)	F_2(7-12)
2	(37-39)	F_3(37-40)	
3	(89-92)	F_4(91-92)	F_5(82-83)
4	(47-69)	F_6(47-49)	F_7(48-49)

We use simulation to uncover cases where erroneous operation of the FACTS devices can lead to a failure in the operation of the physical portion of the grid. The overarching objective of our work is to develop a quantitative reliability model for the Smart Grid as a cyber-physical system, based on understanding the semantics of the operation of the Smart Grid and the interaction among its components. This model, and the research leading to its development, has been presented in our previous publications [5-7]. Each additional failure scenario identified for the cyber-physical system as a whole refines our model and increases its accuracy. The work presented in this paper aims to discover failure scenarios that would be missed by independent analysis of the cyber and physical infrastructures, respectively.

The remainder of the paper is organized as follows. Section 2 presents a summary of related literature. Section 3 describes the software faults that were injected in the cyber infrastructure, and Section 4 describes the effect of these faults on the physical

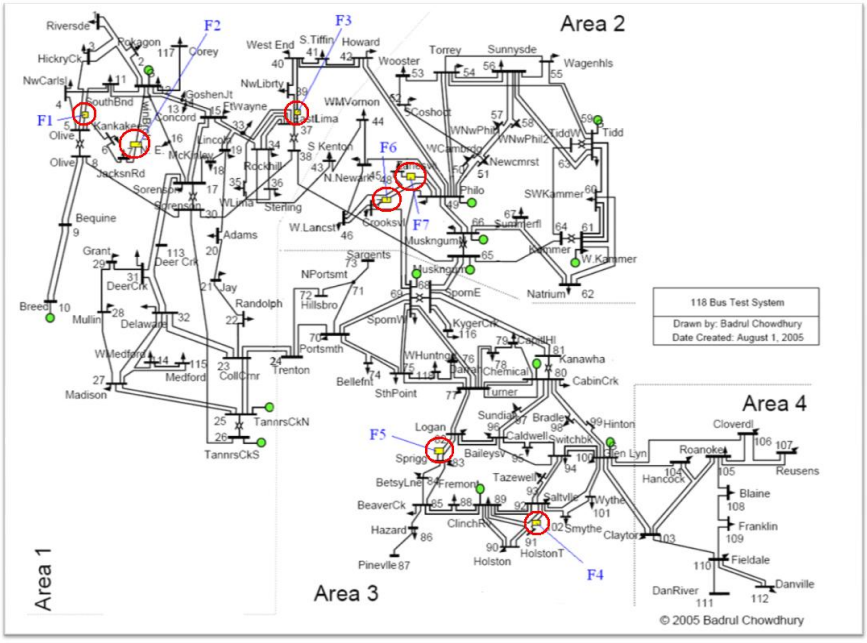

Figure 1-The IEEE118 bus system, with FACTS devices deployed

operation of the grid. Results and analysis are presented in Section 5. Section 6 concludes the paper.

2. LITERATURE REVIEW

The Smart Grid was first mentioned in The Energy Independence and Security Act of 2007 [1], where it was established that the electricity transmission and distribution system should be modernized to maintain a reliable and secure electricity infrastructure that can meet future growth in demand. Since then, several studies have been published [8, 9], which represent efforts in improving the operation of the power grid according to the requirements set by the act or to discuss specific concerns or activities such as security, reliability [10], or smart metering [11].

Our vision is broader and considers a longer-term vision of a Smart Grid transmission system, with emphasis on reliability of such a system. The presence of intelligent equipment in the grid should theoretically help improve the overall system reliability, but it may also cause problems in an otherwise functioning purely physical network. In this paper, we assess the ability of the intelligent devices (FACTS devices in this case) to improve on the reliability of the grid.

Another category of related work is critical infrastructure, the modern version of which is cyber-physical. Protection of the power grid using intelligent equipment has been discussed in [12, 13]. Also relevant are studies such as [14], which models interdependencies among infrastructures that interact with each other. It also presents SimCIP, a simulation environment that captures their interactions.

Our work, while related to the aforementioned studies, is significantly different, as we develop a quantitative model that captures the effect of cyber and physical failures on the operation of the system. The ultimate objective of our work is to identify cases where supplementing the physical infrastructure with cyber computing and communication will be most effective in fortifying the system. The remainder of this paper articulates our approach to system characterization with fault injection, and describes how the failure scenarios identified as a result are used to refine and improve the quantitative reliability model described in our previous work [5-7].

3. FAILURES IN THE CYBER INFRASTRUCTURE

As described in Section 1, our work considers a Smart Grid where power distribution is streamlined and fortified by using FACTS devices that control the flow of power on certain critical transmission lines. The settings for each FACTS device, i.e., the amount of flow on the corresponding line, are determined by the MaxFlow algorithm [4], which uses information about the system topology and line capacities to determine the optimal flow for each line in the grid [15].

Figure 2 below presents an example of what could happen as the result of an error in the software used to implement the MaxFlow algorithm. The resulting software fault could lead to incorrect operation of the MaxFlow algorithm, where the flow in one of the lines could be erroneously increased by 10%. This incorrect increase in the flow of one line can lead to changes in the flow of many other lines, and will eventually cause the MaxFlow algorithm to produce incorrect settings for the FACTS devices. As an example, a FACTS device could erroneously set the flow on a certain transmission line to 80% of the rated value (the typical flow on the line, under normal operating conditions). When such an error occurs, the flow in other transmission lines is forced to increase to satisfy the laws of physics. As a result, overload can occur in a nearby transmission line, causing a line outage that in turn leads to a number of additional overloads, eventually causing a system-level failure.

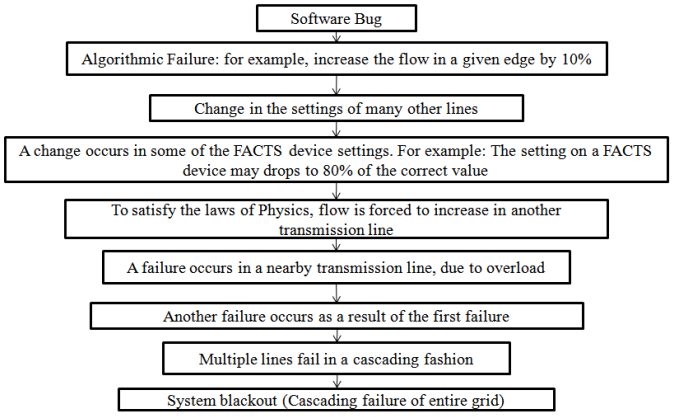

Figure 2-Software errors lead to cascading failures

3.1. Software Faults Injected in the MaxFlow Algorithm

It is clear that any faults in the operation of the MaxFlow algorithm can lead to erroneous settings on the transmission lines. We describe a number of such faults below, and using fault injection, we investigate their effect on the operation of the algorithm. These errors are not comprehensive; their selection is due to the fact that they are among the most typical results of algorithm corruption, and can result from cyber attacks in the form of program modification [16]. Our main goal in this analysis is to identify patterns in how software faults can lead to cyber-physical system failures, and to obtain a better understanding of failure propagation from the cyber infrastructure to the physical infrastructure.

(1) **All-Excess Fault.** During the operation of the MaxFlow algorithm, each vertex in the graph that represents the power grid can hold a certain amount of excess flow. The All-Excess software fault decreases the excess value for each vertex by one unit. This will cause a number of incorrect results in the MaxFlow output, and may lead to erroneous FACTS device settings.

(2) **Excess-Excess Fault.** The Excess-Excess fault increases the excess value of a given vertex by one unit. As opposed to the All-Excess fault, in this case we need to specify a vertex at which the excess value is altered. Since there are 118 vertices in the system (corresponding to the 118 buses of the physical power network), the fault is injected 118 times, each time at a different vertex.

(3) **One-Time-Adjust-Fault.** In this fault, the amount of flow in all edges is increased by 10 units. This fault is applied to all the edges in the network.

(4) **Adjust-Amount Fault.** This fault adjusts the flow in a given edge by increasing the original flow value by 10%. When injecting this fault, we specify a vertex as a parameter, and the fault is applied to all edges connected to that vertex.

3.2. Physical Limitations on the Operation of the FACTS device

The settings determined by MaxFlow for the FACTS devices may change due to the occurrence of any of the software faults mentioned above. The FACTS devices, however, have a certain rating based on their power electronics component ratings, and can only operate between 80% and 120% of their rated value. This imposes a limitation on how severely the fault can affect the operation of the FACTS device. If the erroneous output of the MaxFlow algorithm suggests that the setting on the FACTS device needs to be at a value lower than 80% of the rated value, the FACTS device will simply set itself to exactly 80% of the rated value, due to this physical limitation. Similarly, a FACTS device cannot be set to a value greater than 120% of its rating, and if the MaxFlow setting happens to be higher, the FACTS device will simply limit it to 120% of the rated value.

Furthermore, a FACTS device can be programmed to not allow the flow on a transmission line to go beyond the capacity of the line. If this precautionary measure is not carried out, a FACTS device can allow the flow to become as high as 120% of the rated value of the device, which may be higher than the capacity of the transmission line on which the device is deployed. The result can be overload and subsequent outage of the transmission line.

4. EFFECTS OF CYBER FAILURES ON PHYSICAL OPERATION OF THE SMART GRID

The faults described in the previous section can lead to incorrect operation of a FACTS device. In this section, we describe our fault injection experiments and analyze the effects of the faults injected on the behavior of the FACTS devices and on the operation of the Smart Grid as a whole.

4.1. Fault Injection Experiments

Cyber Failures - No Prior Physical Line Outage. The initial fault injection experiments were performed on a fully-functional physical system; i.e., one with no transmission line outages. The purpose of the experiments was to determine whether any of the cyber faults injected can cause incorrect settings to be determined for the FACTS devices.

Simulation results showed that many of the faults described in Section 3.1 can lead to incorrect MaxFlow settings, but correct settings can still be determined by the algorithm despite the presence of a number of these faults. Table 2 presents a summary of the faults that can lead to a MaxFlow setting less than 80% of the rated value, and ones that can lead to a setting higher than 120%. While all of these values were either less than 80% of the rated value or higher than 120%, constraints on the operation of the FACTS device will only allow the setting to go as low as 80% or as high as 120% of the rated value. A number of cases resulted in values within the range of 80%-120%, but are omitted from the tables for brevity.

Simultaneous Cyber and Physical Failures. To further analyze the system, we performed software fault injection on a system with a pre-existing line outage. We chose three distinct outages, corresponding to lines 4-5, 37-40, and 89-92, respectively. These lines were chosen because in the absence of FACTS devices (a purely physical grid), outage of each of them can cause a cascading failure in the grid (see Table 1 in Section 1). The deployment of FACTS devices and resulting cyber control of the grid prevents these cascading failures. For brevity, we show only the results for software fault injection on a grid with a prior outage of line 4-5. Table 3 summarizes the results. The other two cases (outage of lines 37-40 and 89-92, respectively) provided similar results.

Table 2 - Cyber failure: software fault injection, no prior physical line outage

No physical line contingencies			
Fault type: Excess-Excess			
Parameter(s)	FACTS/ Transmission line	% of rated value	Failure mode
11	F1/5-11	72.3%	Limit to 80%
1-23, 25-34	F3/37-40	0%	Limit to 80%
Fault type: Adjust-Amount			
Parameter(s)	FACTS/ Transmission line	% of rated value	Failure mode
8	F7/48-49	62.8%	Limit to 80%
49	F2/7-12	218%	Limit to 120%

Table 3 - Cyber-physical failure: software fault injection, prior outage of line 4-5

Outage: Line 4-5			
Fault type: Excess-Excess			
Parameter(s)	FACTS/ Transmission line	% of rated value	Failure mode
1-84, 86-118	F3/37-40	0%	Limit to 80%
1-118	F1/5-11	67.9%	Limit to 80%
Fault type: Adjust-Amount			
Parameter(s)	FACTS/ Transmission line	% of rated value	Failure mode
1-84, 86-118	F3/37-40	0%	Limit to 80%
1-52, 54-112, 114-118	F6/47-49	176%	Limit to 120%

4.2 FACTS Device Failures Resulting from Software Fault Injection

Software fault injection on the simulated Smart Grid resulted in three cases: a MaxFlow setting that is 80% of the rated value of the FACTS device, a MaxFlow setting that is 120% of the rated value, and a MaxFlow setting that is somewhere in between these two ranges. The consequences of each of these erroneous settings depend on whether the injected software fault is detected by the algorithm. Two cases are described below, fault detection is enabled for the first and disabled for the second.

Fault Detection Enabled - If we assume that the presence of a software fault can be detected (using executable assertions on the algorithm's correctness [16]), but cannot be corrected, one of the following options can be used as a protective action.

1. *Bypass the FACTS device.* The protective measure taken in this case is to disconnect the FACTS device from the power grid, returning it to the purely physical mode. The advantage of this measure is that it prevents a software- induced error from affecting an otherwise functioning system. The disadvantage is that if a line outage occurs, it might lead to a cascading failure, as cyber control is effectively disabled.
2. *Limit to line capacity.* If a FACTS device cannot determine the actual setting from the MaxFlow algorithm, it can still prevent the transmission line on which it is deployed from overload and subsequent outage. A cascading failure can still occur as a result of outage of a neighboring line, but simulation shows that this protective action prevents cascading failure in some cases.
3. *Use the most recent setting.* FACTS devices can be programmed to revert back to the most recent correct setting if the device is unable to determine the correct setting as the result of a software fault. This is a good option if the system was otherwise functioning properly. The occurrence of a line outage may render this protective action ineffective.

Fault Detection Disabled - Fault detection may not be feasible for all implementations of the MaxFlow algorithm. The three cases below describe the possible scenarios resulting from undetected software faults.

1. *Set flow to 80% of rated value.* If the MaxFlow setting is below 80% of the rated value, the FACTS device will be set to 80%. This will not cause outage of the transmission line on which the FACTS device is deployed, but it may cause changes to occur in the flow values of the remaining lines in the system, which could lead to failures elsewhere in the system.
2. *Set flow to 120% of rated value.* If the MaxFlow setting is above 120% of the rated value, the FACTS device will be set to 120%. If this value is below the line capacity, it will not cause a failure, but it may force the flow values in other transmission lines to change in such a way that could cause the system to fail.
3. *Set flow to the erroneous value obtained from the MaxFlow algorithm*. If the erroneous setting determined by MaxFlow is within 80%-120% of the rated value, it will be used by the FACTS device to set the flow on the corresponding transmission line. Again, depending on the overall system topology and status, this may or may not lead to a failure in the system.

Using power system load flow simulations, we tested all of the aforementioned scenarios, and identified the cases that lead to failures at the system level. The results are presented in the following section.

5. RESULTS AND ANALYSIS

Table 4 summarizes the results obtained from simulating the effects of failures when fault detection is not possible. Each row indicates the system status for a particular pre-existing line outage. Each column corresponds to one failure scenario resulting from software fault injection. An entry labeled as "SAFE" denotes that no cascading failure has occurred in the system. An entry labeled "FAILED" denotes that a cascading failure has occurred as a result of the line outage and/or software fault.

The results show that in the absence of a prior line outage, in no case were software faults and the resulting erroneous FACTS device settings detrimental to the system operation. In other words, a functioning system remained functional despite the software failure. However, in the presence of a line outage, software failure and the resulting malfunction of a FACTS device can be the last straw, causing failure of a system that is highly-stressed, but had been tolerating the initial line outage. An example of this case, where malfunctioning cyber control causes the failure of an otherwise operational physical system, can be seen in Table 4, where prior outage of line 4-5, combined with erroneous FACTS device setting on F_2 (120% of the rated value), leads to cascading failure.

Tables 5 and 6 provide additional insight into the effects of failure in the cyber infrastructure, by identifying interesting operational scenarios for the grid. As opposed to Table 4, the line outages considered in this case are those that would ***not cause*** a cascading failure in a purely physical grid, as shown in the second ("No FACTS") column in Table 5. The addition of FACTS devices, however, introduces cases where a concurrent line outage and malfunction of a FACTS device, or alarmingly, in some cases even correct operation of a FACTS device, will lead to cascading failure. The FACTS devices represented in the columns of Tables 5 and 6, F1/F2, were deployed to prevent the outage of line 4-5 as described in Section 1, specifically in Table 1. In the simulations summarized in Table 4, we investigated the effect of software failures concurrent with the outage of these cascade-triggering lines. In Tables 5 and 6, we investigate scenarios where these lines remain intact, but other lines in their vicinity experience an outage concurrent with the software failure described. Table 5 shows the simulation results with fault detection disabled. Fault detection was enabled for the simulation cases shown in Table 6. The protective action taken is listed next to the fault detected, in the headings of columns 2-4. Two options were considered after fault detection: bypass the FACTS devices, or use the most recent FACTS device setting, both of which were described in Section 4.2.

Table 4 - Simulation results, fault detection disabled

Outage	No FACTS	Perfect FACTS	80% of rated value on $F_1/L_{(5-11)}$	80% of rated value on $F_2/L_{(7-12)}$	120% of rated value on $F_1/L_{(5-11)}$	120% of rated value on $F_2/L_{(7-12)}$
None	Safe	Safe	Safe	Safe	Safe	Safe
$L_{(4-5)}$	Failed	Safe	Failed	Safe	Failed	Failed
			$F_5/L_{(82-83)}$	$F_4/L_{(91-92)}$	$F_5/L_{(82-83)}$	$F_4/L_{(91-92)}$
None	Safe	Safe	Safe	Safe	Safe	Safe
$L_{(89-92)}$	Failed	Safe	Safe	Safe	Safe	Safe
			$F_3/L_{(37-40)}$		$F_3/L_{(37-40)}$	
None	Safe	Safe	Safe		Safe	
$L_{(37-39)}$	Failed	Safe	Failed		Safe	

The simulation results summarized in Tables 5 and 6 show that the deployment of a FACTS device could be detrimental to an otherwise functioning physical system, despite the original intent of their deployment, which is prevention of line outages that lead to cascading failures. As an example, the italicized entry in Table 5 represents a case where the purely physical system was able to withstand the outage of line 8-30, but a malfunctioning FACTS device reduced the fault-tolerance of the system to the point where the same outage causes a cascading failure. This detrimental effect persists even when the software fault leading to malfunction of the FACTS device is detected, and protective action is taken. The italicized entry in Table 6 represents such a case.

Table 5 - Additional simulation results, fault detection disabled

Outage	No FACTS	Perfect FACTS	80% of rated value on $F_1/L_{(5-11)}$	80% of rated value on $F_2/L_{(7-12)}$	120% of rated value on $F_1/L_{(5-11)}$	120% of rated value on $F_2/L_{(7-12)}$
8-30	Safe	Safe	***Failed***	Failed	Safe	Failed
6-7	Safe	Safe	Failed	Failed	Safe	Failed
1-3	Safe	Safe	Safe	Safe	Safe	Safe

Table 6 - Additional simulation results, fault detection enabled

Outage	Use most recent setting on $F_1/L_{(5-11)}$	Use most recent setting on $F_2/L_{(7-12)}$	Bypass FACTS device $F_1/L_{(5-11)}$	Bypass FACTS device $F_2/L_{(7-12)}$
8-30	***Failed***	Failed	Safe	Failed
6-7	Safe	Failed	Safe	Safe
1-3	Safe	Safe	Safe	Safe

An important conclusion of our fault injection experiments is that the net effect of deploying FACTS devices cannot be determined by superficial analysis. Extensive simulation is required to reveal pathological cases that may lead to a negative effect on system reliability. Such extensive simulation can be prohibitively expensive for any non-trivial grid.

6. CONCLUSIONS

Fortification of the physical power infrastructure with cyber control is a costly task, undertaken with the intent of making power distribution more reliable. The research presented in this paper identifies cases where failures in the cyber infrastructure compromise this objective. Several different software faults were injected into the Smart Grid, and their results were studied. The reaction of the FACTS devices was found to vary, based on the type of software fault and the ability of the system to detect the fault. Physical constraints on the operation of FACTS devices limit their settings to between 80% and 120% of the rated value, which in turn limits the potential detrimental effect of failures in cyber control. A number of interesting cases, however, were identified, where a malfunctioning FACTS device caused cascading failure in an otherwise functional physical infrastructure. This discovery reiterates the importance of careful investigation of the effects of cyber control.

In future research, and using the results obtained in the fault injection analysis, we will develop reliability models for the Smart Grid as a cyber-physical system in each one of the failure modes presented above.

Another future goal of our research is to determine the conditions under which FACTS devices improve the overall reliability of the Smart Grid, and to quantify the detrimental effect of failures in the cyber infrastructure when it is not beneficial. The IEEE118 bus system was used as a case study in the work presented in this paper. Our goal is to generalize the work to similar systems, by studying the effects of cyber failure on operation of a cyber-physical system as a whole.

7. ACKNOWLEDGMENTS

The authors would like to thank the Intelligent Systems Center at Missouri S&T for their support of this research.

8. REFERENCES

[1] The United States Congress, 2007 “The Energy Independence and Security Act of 2007”

[2] Chowdhury, B.H., Baravc, S., “Creating cascading failure scenarios in interconnected power systems.” IEEE Power Engineering Society General Meeting

[3] Lininger, A., McMillin, B., Crow, M., Chowdhury, B., 2007, “Use of maxflow on FACTS devices.” North American Power Symposium. pp. 288-294

[4] Armbruster, A., Gosnell, M., McMillin, B., Crow, M., “The Maximum Flow Algorithm Applied to the Placement and Steady State Control of FACTS Devices”, Proc. 2005 North American Power Symposium, pp. 77-83

[5] Faza, A., Sedigh, S., McMillin, B., 2009, “Reliability Analysis for the Advanced Electric Power Grid: From Cyber Control and Communication to Physical Manifestations of Failure”, Proc. Int'l Conf. on Computer Safety, Reliability and Security (SAFECOMP'09), pp. 257-269

[6] Faza, A., Sedigh, S., McMillin, B., 2007, “Reliability Modeling for the Advanced Electric Power Grid”, Proc. Int'l Conf. on Computer Safety, Reliability and Security (SAFECOMP'07), pp. 370-383

[7] Faza, A., Sedigh, S., McMillin, B., 2008, “The Advanced Electric Power Grid: Complexity Reduction Techniques for Reliability Modeling”, Proc. Int'l Conf. on Computer Safety, Reliability and Security (SAFECOMP'08)

[8] Wei, X., Yu-hui, Z., Jie-lin, Z., 2009, “Energy-effcient Distribution in Smart Grid”, Proc. Int'l Conf. on Sustainable Power Generation and Supply, SUPERGEN'09, pp. 1-6

[9] Olofsson, M., 2009, “Power Quality and EMC in Smart Grid”, Proc. 10th Int’l Conf. on Electrical Power Quality and Utilization, pp. 1-6

[10] McDaniel, P., McLaughlin, S., 2009, “Security and Privacy Challenges in the Smart Grid”, IEEE Security and Privacy 7(3) pp. 75-77

[11] Prassana, G., Lakshmi, A., Sumanth, S., Simha, V., Bapat, J., Koomullil, G., 2009, “Data Communication Over the Smart Grid”, Proc. Int'l Symp. on Power Line Communications and its Applications ISPLC'09, pp. 273-279

[12] Chiaradonna, S., Lollini, P., Giandomenico, F.D., 2007, “On a Modelling Framework for the Analysis of Interdependencies in Electtric Power Systems”, Proc. 37th Int'l Conf. on Dependable Systems and Networks DSN'07., pp. 185-195

[13] Luiijf, E., Nieuwenhuijs, A., Klaver, M., Eeten, M., Cruz, E., 2009, “Empirical Findings on Critical Infrastructure Dependencies in Europe”, Third Int'l Workshop on Critical Information Infrastructure Security, CRITIS, pp. 302-310

[14] Klein, R., Rome, E., Beyel, C., Linnemann, R., Reinhardt, W., Usov, A., 2009, “Information Modelling and Simulation in Large Interdependent Critical Infrastructures in IRRIIS”, Third Int'l Workshop on Critical Information Infrastructure Security, CRITIS, pp. 36-47

[15] Kalyani, R., Crow, M., Tauritz, D., 2006 “Optimal placement and control of unified power flow control devices using evolutionary computing and sequential quadratic programming” Power Systems Conf. and Exposition, PSCE '06, pp. 959 -964

[16] Armbruster, A., Gosnell, M., McMillin, B., Crow, M., 2005, “Power Transmission Control Using Distributed Max-Flow”, Proc. 29th Annual Int'l Computer Software and Applications Conf. (COMPSAC'05), pp. 256-263