01 Sep 2009

Reliability Analysis for the Advanced Electric Power Grid: From Cyber Control and Communication to Physical Manifestations of Failure

Ayman Z. Faza

Sahra Sedigh
Missouri University of Science and Technology, sedighs@mst.edu

Bruce M. McMillin
Missouri University of Science and Technology, ff@mst.edu

Reliability analysis for the advanced electric power grid: from cyber control and communication to physical manifestations of failure

Ayman Z. Faza, Sahra Sedigh, and Bruce M. McMillin

Missouri University of Science and Technology, Rolla, MO, 65409-0040, USA
Phone: +1(573)341-7505 Fax: +1(573)341-4532
{azfdmb,sedighs,ff}@mst.edu

Abstract. The advanced electric power grid is a cyber-physical system comprised of physical components such as transmission lines and generators and a network of embedded systems deployed for their cyber control. The objective of this paper is to qualitatively and quantitatively analyze the reliability of this cyber-physical system. The original contribution of the approach lies in the scope of failures analyzed, which crosses the cyber-physical boundary by investigating physical manifestations of failures in cyber control. As an example of power electronics deployed to enhance and control the operation of the grid, we study Flexible AC Transmission System (FACTS) devices, which are used to alter the flow of power on specific transmission lines. Through prudent fault injection, we enumerate the failure modes of FACTS devices, as triggered by their embedded software, and evaluate their effect on the reliability of the device and the reliability of the power grid on which they are deployed. The IEEE118 bus system is used as our case study, where the physical infrastructure is supplemented with seven FACTS devices to prevent the occurrence of four previously documented potential cascading failures.

Key words: reliability analysis, failure propagation, cyber-physical, power grid, FACTS devices

1 Introduction

The advanced electric power grid is a cyber-physical system comprised of physical components such as transmission lines and generators and a network of embedded systems deployed for their cyber control. This cyber control is achieved by using Flexible AC Transmission System (FACTS) devices. These devices can alter the flow in the transmission lines in a way that can prevent failures from occurring in the system. A typical cyber-physical system is shown in Figure 1 below. The left portion of the figure shows a typical physical network comprised of a few generators, transmission lines and loads. On top of that, there is another network; the cyber network, made up of a number of computers connected with

each other, which control the operation of the physical network. On the right side, a graph theoretic version of the same figure is shown, which separates the two layers, in two parallel planes. In the lower plane, the physical layer is represented as a number of nodes connected with edges in which electric power flows in one direction, while the upper plane represents the cyber network components, which communicate over bidirectional channels.

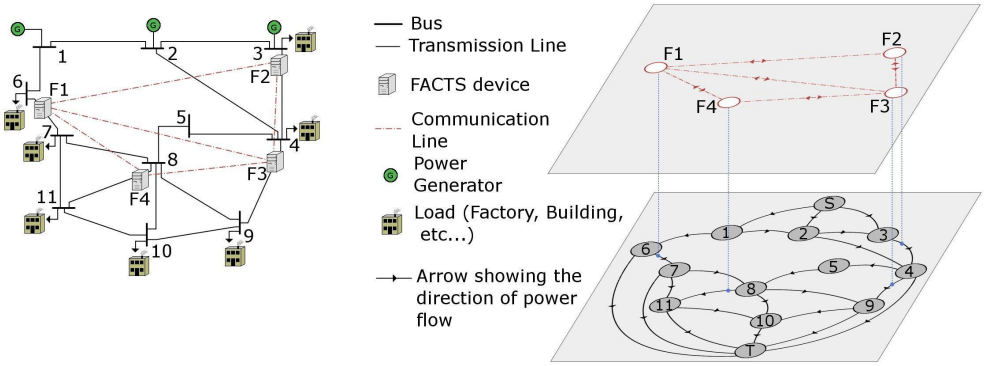

Fig. 1. Cyber-Physical Systems

While adding cyber control to the power grid aims at improving the system's performance and increasing its overall reliability, its presence in an already complex system will increase its complexity and will introduce new sources of failure. In fact, we will show later in this paper that there are some cases in which a failure in the operation of a FACTS device can be more harmful than having no FACTS devices deployed at all.

FACTS devices can fail in a number of ways. Failures could occur in the hardware part of it or in the software. In this paper, we will focus more on the software failures of the FACTS devices, and their manifestations at the physical portion of power grid. We use the IEEE118 bus system as our case study, and based on the results shown in [1] and [2], we deploy FACTS devices in the system at specified locations as shown in Figure 2. By doing so, the power grid is protected against potential cascading failures that could cause the whole grid to fail.

Through simulation, we examine the effect of a faulty behavior of a FACTS device on the operation of the IEEE118 bus system. The results of this simulation are then used to develop equations for system reliability that correspond to the different failure modes of FACTS devices.

As per our discussions in [3] and [4], we use the Markov chain Imbeddable Structures (MIS) technique to develop our reliability equations. We define "safe" states as the states at which the system as a whole is functional even if it has failed components in it, and define "failed" states as the states in which the

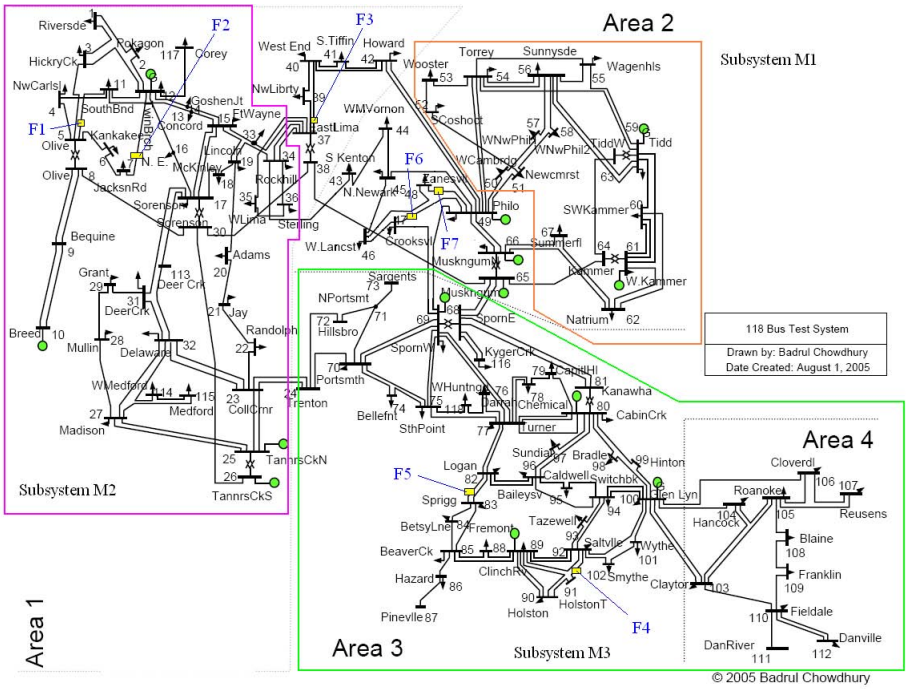

Fig. 2. The IEEE118 bus system with FACTS devices deployed

system as a whole has failed due to the failure of one or more components. With this reasoning, we enumerate the safe states in the system in order to construct its reliability equation. System reliability can simply be defined as the probability that the system stays in a safe state for a certain amount of time.

The main contribution in this paper relates software failure modes of FACTS devices to their manifestations in the combined cyber-physical system and the development of reliability equations for the system in those failure modes.

The rest of the paper is organized as follows. Section 2 provides a summary of related literature. Section 3 describes our system, and presents the problem in more detail, while Section 4 specifically targets the failure modes of the FACTS devices. In Section 5, we talk about fault injection as a method to improve our reliability model, and Section 6 concludes the paper.

2 Related Work

Estimating the reliability of cyber-physical systems is made more challenging by the fact that it is made up of two layers; the cyber and the physical. In particular, the difficulty arises from the interdependencies between its cyber and physical components, as a failure in the physical portion of the network could lead to a

failure in the cyber one, and vice versa. A number of studies were presented in the literature that describe efforts to capture those interdependencies.

One such study is presented in [5], where the authors provide a qualitative analysis of interdependencies among the electric, water, gas, oil, and telecommunication networks. The paper describes how a failure in one of the systems, such as the power grid, can cause disruptions in the rest of the systems, such as curtailment in the production of natural gas, or disruptions in irrigation pumps in the water distribution system. Second- and third-order effects are also investigated, highlighting the importance of studying interdependencies among the systems.

In another study, Lee et al. present an algorithm in [6] that identifies vulnerabilities in the design of infrastructure systems by observing the interdependencies among them. They also present an example that illustrates interdependencies between the power and telecommunication systems.

It is important to stress that in the two aforementioned studies, the analysis of interdependencies is of a qualitative nature. Our model, however, proceeds to quantitatively capture such interdependencies through semantic understanding of a specific system as an example, the physical power distribution system and the power electronics used for its cyber control.

Reliability of the physical infrastructure of the power grid has been the topic of decades of research. These studies are vital to analysis of modern power distribution systems, however, they give no consideration to cyber control, computation, or communication issues, and as such, their application to intelligent networks is limited. Notable examples of reliability analysis of physical components of the power grid include [7] and [8].

The study presented in [8] sheds light on the main challenges in modeling the reliability of the power grid. Factors cited include conceptual difficulties in defining appropriate metrics for the evaluation, challenges in choosing appropriate models, and computational limitations. Alleviating computational limitations on reliability analysis is one objective of our work.

The study in [7] presents a method for evaluating the reliability of an electric power generation system with unconventional energy sources, such as solar panels and wind turbines. The model presented attempts to capture the effects of primary energy fluctuations, in addition to failure and repair characteristics of the unconventional units. The focus of this study is on the generation aspect of the power grid, and its results do not extend to the remainder of the grid, in particular the transmission lines, whose failures can cause cascading power outages.

In this paper, we go beyond the physical infrastructure to explore interdependencies among the cyber and physical components of the power grid with regard to their semantics. Our goal is the development of a quantitative reliability model that captures such interdependencies. A number of related studies take a qualitative approach to the same problem, including [9], which analyzes interdependencies among the electric power infrastructure and the information infrastructures supporting its management, control and maintenance.

The EU Critical Utility Infrastructural Analysis initiative (CRUTIAL) also aims to understand interdependencies among the power and information infrastructures. Results published thus far include [10–13], all of which provide a qualitative analysis of security aspects in the power grid infrastructure. In [11], the authors present a detailed analysis of several potential intrusion scenarios in the power grid infrastructure in an attempt to raise the issue of security in the system and help develop methods to defend against such intrusions. The author of [11] tries to motivate the research towards increasing the security of the control systems that manage critical infrastructures. The paper presents reasons for enforcing increased security based on past attacks or potential security breaches, and provides general ideas for improving the security of those systems, in addition to identifying potential challenges. Recommendations for improvements to the reliability and robustness of intelligent power grids are made in [12].

In another study, vulnerability assessment of cyber security in a SCADA system used to control the operation of the power grid is presented in [14]. Two submodels are used for the system; a firewall model that regulates the packets flowing between the networks, and a password model, which is used to monitor penetration attempts. Petri nets are used to model the system, and simulation is used to provide an estimate of the vulnerability of the system to security attacks launched against it. This work is similar to our work in the sense that it is related to providing control over the power grid; however, their focus is on security aspects in the system, rather than reliability.

On the topic of fault injection for dependability analysis a number of interesting studies were found such as [15], [16]. In [16], the authors define a methodology for dependability assessment of a hardware/software system by using fault injection tools. They explain the use of the "Messaline" fault injection tool and provide examples and experimental results of how their tool was used. While the paper presents a fault injection framework with a higher focus on the hardware part than the software, the methodology provided will be useful in our efforts towards improving our model by implementing software fault injection schemes.

The study presented in [15] provides an analysis more similar to what we are looking for, as it injects software faults in a high-speed network system and assesses the effect of those faults on the network dependability. The types of faults analyzed in this paper include message corruption, message drop and computer hanging, which are similar to the types of software faults that can occur in the cyber portion of our systems, and while the results found in this paper might be useful for us, we will still need to assess the effect of such faults on the physical portion of the grid.

The work presented in this paper is part of an ongoing research project, and a continuation of the work presented in [3] and [4]. It is significantly different from those papers as it focuses on the software failures in the cyber network, and their effect on the physical portion of the power grid. It also leads to the introduction of fault injection as the tool to our next step towards continuing our development of the reliability model for our cyber-physical system.

3 System reliability, the effect of adding FACTS devices

Before adding any cyber control to the physical network, the system is vulnerable to several cascading failures. Some of those failures could be mitigated by deploying FACTS devices in certain locations. Specifically, four cascading scenarios were discovered to be mitigated by proper FACTS placement [2]. Table 1 summarizes the cascading failures, and Table 2 shows where the FACTS devices need to be placed in order to prevent those cascading failures from occurring. Those placements can also be seen in Figure 2.

Table 1. Cascading Failures that can be Mitigated

	Stage 1	**Stage 2**	**Stage 3**	**Stage 4**	**Stage 5**	**Stage 6**	**Stage 7**	**Stage 8**
1	4-5	5-11	7-12	3-5	16-17	14-15	failure	
2	37-39	37-40	40-42	40-41	failure			
3	47-69	47-49	46-48	45-49	failure			
4	89-92	82-83	91-92	100-101	94-100	95-96	94-96	failure

Table 2. Successful Mitigation of Cascading Failure Scenarios

Line causing cascade	1^{st} FACTS/Transmission Line	2^{nd} FACTS/Transmission Line
(4-5)	F1/(5-11)	F2/(7-12)
(37-39)	F3/(37-40)	
(89-92)	F4/(91-92)	F5/(82-83)
(47-69)	F6/(47-49)	F7/(48-49)

A more detailed look at the IEEE118 bus system will reveal that it consists of 210 transmission lines. According to our simulation results, out of those 210 lines, only 143 can fail without causing the system to fail. The states representing the failure of these 143 lines while all other lines are functional represent safe states. We will consider the failure of two or more transmission lines as an unacceptable scenario, and will consider any states in which two or more lines have failed as a "failed" state. With those arguments in mind the direct application of the MIS technique should yield the following equation for system reliability when no FACTS devices are included.

$$R_{sys} = p_L^{210} + 143 p_L^{209} q_L \tag{1}$$

where,

p_L: is the reliability of the transmission line.

q_L: is the unreliability of the transmission line and is equal to 1-p_L

Adding FACTS devices to the system, should theoretically increase the reliability of the system. This is reflected mathematically in the Equation 1 above

by an overall increase in the number of "safe" states, which will subsequently increase the reliability value.

For example, lets take the simple case where a FACTS device can never do any harm to the network, and if it fails, the system simply bypasses the device, and it behaves as if it does not exist any more. We call this the fail-bypass failure mode.

In this mode of operation, safe states can only be added to the system by the proper behavior of the FACTS devices, and no negative impact can occur on the system. The safe states here correspond to the cascading scenarios that were prevented by introducing the FACTS devices (See Table 2). Adding those safe states to the reliability equation will modify it as follows.

$$R_{sys} = p_L^{210} + 143p_L^{209}q_L + p_L^{209}q_{L_{(4-5)}}p_{F_1}p_{F_2} + p_L^{209}q_{L_{(37-39)}}p_{F_3} + p_L^{209}q_{L_{(89-92)}}p_{F_4}p_{F_5} + p_L^{209}q_{L_{(47-69)}}p_{F_6}p_{F_7} \quad (2)$$

where,

p_F: is the reliability of the FACTS device.

q_F: is the unreliability of the FACTS device and is equal to 1-p_F

If we assume all FACTS devices have equal reliabilities, the equation reduces to the following.

$$R_{sys} = p_L^{210} + p_L^{209}q_L(143 + 3p_F^2 + p_F) \quad (3)$$

Comparing Equations 1 and 3 we can see an obvious increase in the system reliability. Figure 3 below confirms this. Note that while the increase in reliability is relatively small, the significance of this is much bigger if we consider the amount financial losses that can be saved by preventing the cascading failures from happening.

In the following section, we take a look at some of the more interesting failure modes in the FACTS devices, and evaluate their effect on system reliability.

4 Software failure modes in FACTS devices

Due to faults in the software running on the FACTS devices, failures can occur that can affect the performance of the power grid. Below, we discuss three of the most common failure modes in the FACTS devices, and develop reliability equations for the system in each one of those failure modes.

4.1 Failure mode 1: Fail-limit to line capacity

This mode of operation occurs when a FACTS device has lost its ability to decide on an appropriate setting for the line on which it is deployed. This could be due to loss of communication with the other FACTS devices in the system. In such a case, one way the FACTS device could behave is to limit the amount of flow

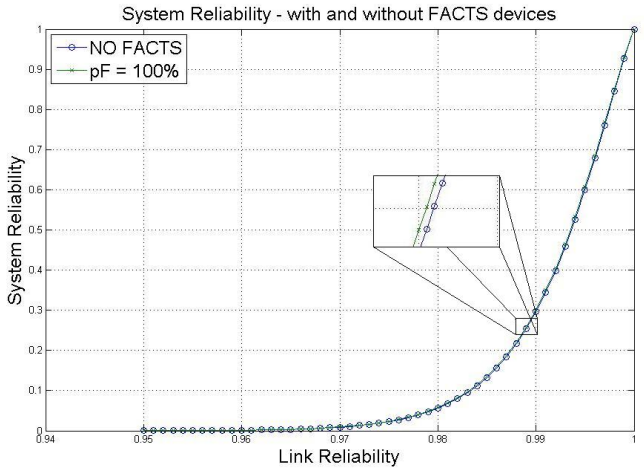

Fig. 3. System Reliability with and without FACTS devices

in the line to the capacity of that line; that is, if the flow in the line is already within the line capacity, the FACTS device leaves it so, but if the flow attempts to increase beyond the line capacity, the FACTS device will simply stop it from doing that and keep the flow equal to the line capacity.

While this might be considered a safe way of dealing with the situation, it is possible that somewhere else in the network an overload occurs. Since the FACTS device in this case can only monitor the line on which it is deployed, the overload occurring in the other line will cause it to fail. This in turn can cause other lines to fail in result, and eventually a blackout occurs.

We investigated that situation in the IEEE118 bus system, and using simulation we determined that in some cases such a failure mode will not cause any problems, but in other cases a cascading failure occurs. The results of this simulation determine which states are "safe" and which are "failed", and based on these results, we develop equation 4 below, which represents the reliability of the system in this failure mode.

$$\begin{aligned} R_{sys} = p_L^{210} + p_L^{209} q_{L_{(4-5)}} q_{F_1} p_{F_2} p_F^5 + p_L^{209} q_{L_{(4-5)}} p_{F_1} p_{F_2} p_F^5 \\ + p_L^{209} q_{L_{(37-39)}} q_{F_3} p_F^6 + p_L^{209} q_{L_{(37-39)}} p_{F_3} p_F^6 + p_L^{209} q_{L_{(89-92)}} q_{F_4} p_{F_5} p_F^5 \\ + p_L^{209} q_{L_{(89-92)}} p_{F_4} p_{F_5} p_F^5 + p_L^{209} q_{L_{(47-69)}} q_{F_6} p_{F_7} p_F^5 \\ + p_L^{209} q_{L_{(47-69)}} p_{F_6} p_{F_7} p_F^5 + 143 p_L^{209} q_L \end{aligned} \tag{4}$$

Assuming all transmisison lines have equal reliabilities, and all FACTS devices have equal reliabilities, the equation reduces to,

$$R_{sys} = p_L^{210} + 143 p_L^{209} q_L + 4 p_L^{209} q_L p_F^6 \tag{5}$$

4.2 Malicious behavior of FACTS devices

In some cases, a software failure in the FACTS device can introduce an error that might affect the operation of the system even without the occurrence of any transmission line failures. In the two subsections below, we present two such cases.

Failure mode 2: Maliciously set flow to line capacity In this failure mode, a failure in the operation of a FACTS device will push the flow in the corresponding transmission line to the line's capacity. Again, like in the case of the previous failure mode, this will cause no problems in the line on which the device is deployed. This, however, does not guarantee a failure-free operation for the rest of the system. Simulation using this failure mode shows that in some cases this would not cause problems in the rest of the system, but in other cases, it might cause failures elsewhere, which would lead to a cascading failure and a system blackout. This case is an example of a situation where there was originally no problem in the physical part of the system. The introduction of the cyber part in the form of FACTS devices provided the opportunity for such a fault to occur and cause the blackout in the system. It should be stressed at this point that adding cyber control to the system can only increase its reliability if the cyber parts were highly reliable. We will show that an unreliable operation of the FACTS devices will result in a system with a less overall reliability than the reliability of the physical portion by itself without including the cyber control.

Using the simulation results for this part, we develop the following equation for system reliability in this failure mode.

$$R_{sys} = p_L^{210}(p_F^7 + 4p_F^6 q_F) + 143p_L^{209}q_L(p_F^7 + 4p_F^6 q_F) + 4p_L^{209}q_L p_F^6 \tag{6}$$

Failure mode 3: Maliciously set to 80% of desired setting This case is similar to the one in the previous section. However, instead of pushing the flow in the transmission line to its capacity, the flow here is being set to 80% of its desired setting. This fault could occur due to a malfunction in the operation of the maximum flow algorithm used to calculate the appropriate settings on the FACTS devices [17]. An incorrect operation of this algorithm can, in this case, result in the FACTS device setting the flow in the transmission line to just 80% of the actual value that needs to flow in the line. As in the past two cases, this will not cause any problems in the transmission line itself, as the new setting will still be below the line capacity, but maintaining that setting on the transmission line might force the flow to increase at different locations in the system, causing other lines to fail and cause a cascade. Again, using simulation we figured that in some of the cases, this will not lead to a failure, but in other cases it will. The results of this simulation yield the following equation for the reliability of the system.

$$R_{sys} = p_L^{210}p_F + p_L^{209}q_L(141p_F + 3p_F^2 + p_F^3 + 1) \tag{7}$$

4.3 Results and analysis

Figure 4 shows a comparison of the failure modes discussed above. It can be seen from the diagram that failure mode 2 is the worst one in terms of system reliability, while failure mode 1 is the best. The diagram confirms that a malicious operation of a FACTS device in which the settings on transmission lines are changed when they do not need to is generally worse than a device making a mistake when required to take some action.

Figures 5 through 7 show the system reliability in each of the three failure modes discussed in Section 4. For failure mode 1, the reliability of a system with FACTS devices added can only increase the system reliability, and a failed FACTS device is only as bad as no FACTS devices at all. In the other two modes, however, FACTS devices have to be extremely reliable in order to provide an increased overall system reliability. It can be seen from Figures 6 and 7 that system reliability decreases drastically when the reliability of FACTS device decreases. This shows that an unreliable FACTS device can do a lot of damage to the system, even with all the other system components working properly.

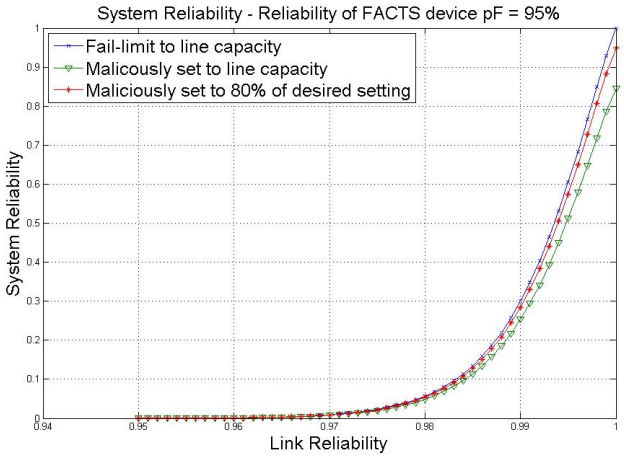

Fig. 4. System Reliability in the different software failure modes

5 Software fault injection in the cyber network

The analysis presented so far describes how does a faulty FACTS device impacts the operation of the physical part of the power grid. We have analyzed three failure modes in which the FACTS devices behaved in such ways that could potentially cause catastrophic failures in the physical part of the power grid. A

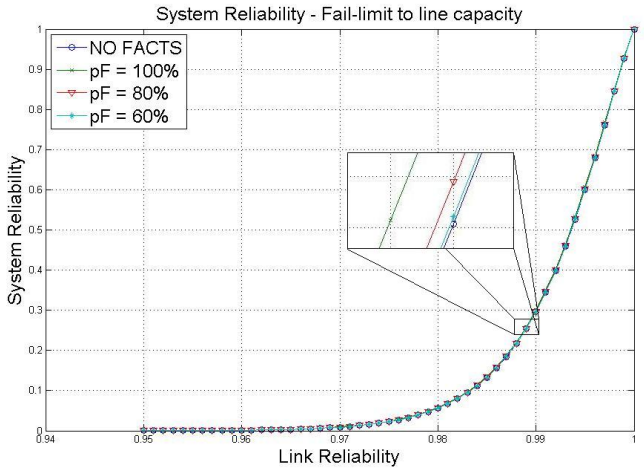

Fig. 5. System Reliability - Fail limit to line capacity

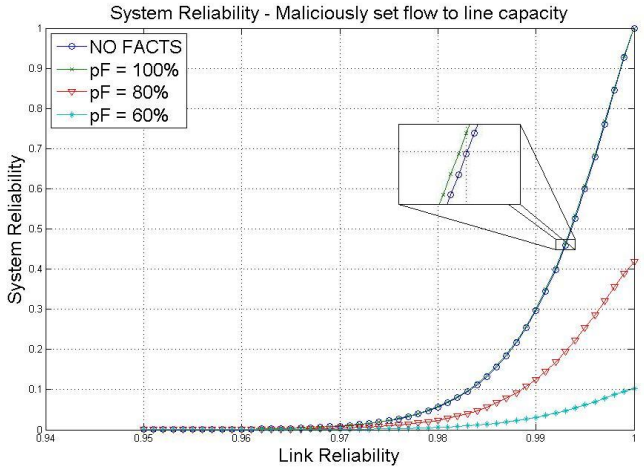

Fig. 6. System Reliability - Maliciously set flow to line capacity

deeper look into the operation of the FACTS device can help identify the causes of such behavior.

In the advanced electric power grid presented in this paper, the cyber control is intended to set the right amount of power flow in the network at specified locations in order to maintain a reliable operation in the grid. Namely, the cyber network runs a distributed version of the maximum flow algorithm [17], and based on that algorithm it can determine the appropriate settings in the transmission lines in the network that would keep it in a stable working condition.

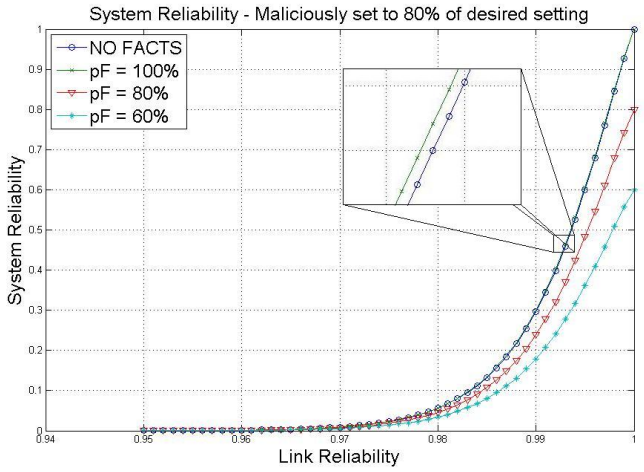

Fig. 7. System Reliability - Maliciously set to 80% of desired setting value

The main job of the FACTS device is to set the power flow in a transmission line to some predetermined value, but another very important job that it does is to help determine that value by participating in running of the distributed maximum flow algorithm in the system. The FACTS devices with the communication links between them collectively perform that task. Three types of faults can contribute to a failure in the operation of a FACTS device;

- A vertex fault
- An edge fault
- A message fault

It is our next objective in this research to inject several types of faults in the cyber network while it is running the maximum flow algorithm, and determine the effect of such faults on the operation of the FACTS device. It is likely that faults injected into the system will cause the FACTS device to behave in of the three failure modes discussed in Section 4, or introduce some new failure modes that we are not familiar with. It is the goal of this research to discover such failure modes, and trace down the ones that we know into their original causes. Doing so will help complete our reliability model, and will give a much more clear idea of how to improve the cyber control of the grid, and reduce the probability of faults.

Analyzing the frequency of occurrence of the software faults in the system can give us a more accurate measure of how frequently to expect the cyber network to fail in a particular failure mode, which can help get to a more precise estimation of how much the actual reliability of the system is. It is our ultimate goal to have a complete model of the reliability of our advanced electric power grid, which will help identify the reliability bottlenecks in the system. Identifying

the locations of those bottlenecks will be critical in finding the solution towards increasing the overall system reliability.

6 Conclusion

In this paper, we present a reliability model for the advanced electric power grid as a cyber-physical system, with a focus on software faults in the cyber part of the network. We use FACTS devices as the cyber components that control the flow of power in the physical part of the system, and discuss three failure modes for those FACTS devices. We analyze the effect of these failure modes on the operation of the FACTS and investigate its impact on the physical part of the system. We use simulation to evaluate the effect of the FACTS failure modes, and use the results of the simulation to develop reliability equations for the system in each one of those modes.

This paper laid the groundwork for the next step of cyber-physical system analysis; software fault injection. Software fault injection will be used to determine the faults in the software that would lead to the failure modes of the FACTS devices. By doing this step, we will be able to describe more completely how and why do FACTS devices behave in certain ways. In addition, knowing the rates of occurrences of such software faults will help develop a better idea of how frequently do we expect the FACTS device to fail in one particular mode. Eventually, this will lead to a more complete model of the reliability of our cyber-physical system.

References

1. Chowdhury, B.H., Baravc, S.: Creating cascading failure scenarios in interconnected power systems. In: IEEE Power Engineering Society General Meeting. (June 2006)
2. Lininger, A., McMillin, B., Crow, M., Chowdhury, B.: Use of max-flow on FACTS devices. In: North American Power Symposium. (2007)
3. Faza, A., Sedigh, S., McMillin, B.: Reliability Modeling for the Advanced Electric Power Grid. In: Proc. of the Int'l Conf. on Computer Safety, Reliability and Security (SAFECOMP'07). (September 2007) 370–383
4. Faza, A., Sedigh, S., McMillin, B.: The Advanced Electric Power Grid: Complexity Reduction Techniques for Reliability Modeling. In: Proc. of the Int'l Conf. on Computer Safety, Reliability and Security (SAFECOMP'08). (September 2008) 429–439
5. Rinaldi, S., Peerenboom, J., Kelly, T.: Identifying, understanding, and analyzing critical infrastructure interdependencies. IEEE Control Systems Magazine **11**(6) (Dec. 2001) 11–25
6. Lee, E.E., I., Mitchell, J., Wallace, W.: Assessing vulnerability of proposed designs for interdependent infrastructure systems. In: Proceedings of the 37th Annual Hawaii International Conference on System Sciences. (Jan. 2004)
7. Singh, C., Lago-Gonzalez, A.: Reliability Modeling of Generation Systems Including Unconventional Energy Sources. IEEE Transactiosn on Power Apparatus and Systems **PAS-104**(5) (May 1985) 1049–1056

8. Endrenyi, J., Bhavaraju, M., Clements, K., Dhir, K., McCoy, M., Medicherla, K., Reppen, N., Salvaderi, L., Shahidehpour, S., Singh, C., Stratton, J.: Bulk Power System Reliability Concepts and Applications. IEEE Transactions on Power Systems **3**(1) (February 1988) 109–117
9. Laprie, J.C., Kanoun, K., Kaaniche, M.: Modelling interdependencies between the electricity and information infrastructures. In: Proc. of the Int'l Conf. on Computer Safety, Reliability and Security (SAFECOMP). (September 2007) 54–67
10. Dondossola, G., Garrone, F., Szanto, J., Fiorenza, G.: Emerging Information Technology Scenarios for the Control and Management of the Distribution Grid. In: Proc. of the 19th Int'l Conf. on Electricity Distribution. (2007)
11. Geer, D.: Security of Critical Control Systems Sparks Concern. Computer **39**(1) (January 2006) 20–23
12. Rigole, T., Vanthournout, K., Deconinck, G.: Interdependencies Between an Electric Power Infrastructure with Distributed Control, and the Underlying ICT Infrastructure. In: Proc. of Int' Workshop on Complex Network and Infrastructure Protection (CNIP-2006), Rome, Italy. (March 2006) 428–440
13. Deconinck, G., Belmans, R., Driesem, J., Nauwelaers, B., Lil, E.V.: Reaching for 100% Reliable Electricity Services: Multi-system Interactions and Fundamental Solutions. In: Proc. of the DIGESEC-CRIS Workshop 2006 Influence of Distributed Generation and Renewable Generation on Power Systemm Security, Magdeburg, Germany. (December 2006)
14. Ten, C.W., Liu, C.C., Govindarasu, M.: Vulnerability Assessment of Cybersecurity for SCADA Systems. to appear in IEEE Transactions on Power Systems (2009)
15. Stott, D.T., Ries, G., Hsueh, M.C., Iyer, R.K.: Dependability Analysis of a High-Speed Network Using Software-Implemented Fault Injection and Simulated Fault Injection. IEEE Transactions on Computers **47**(1) (January 1998) 108–119
16. Arlat, J., Aguera, M., Amat, L., Crouzet, Y., Martins, E., Powell, D.: Fault Injection for Dependability Validation: A Methodology and Some Applications. IEEE Transactions on Software Engineering **16**(2) (Fabruary 1990) 166–182
17. Armbruster, A., Gosnell, M., McMillin, B., Crow, M.L.: Power transmission control using distributed max flow. In: Proc. of the 29th Annual Int'l Computer Software and Applications Conf. (COMPSAC'05), Washington, DC, USA, IEEE Computer Society (2005) 256–263