MISSOURI S&T

CENTER FOR TRANSPORTATION INFRASTRUCTURE AND SAFETY

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

by

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

A National University Transportation Center at Missouri University of Science and Technology

Disclaimer

The contents of this report reflect the views of the author(s), who are responsible for the facts and the accuracy of information presented herein. This document is disseminated under the sponsorship of the Department of Transportation, University Transportation Centers Program and the Center for Transportation Infrastructure and Safety NUTC program at the Missouri University of Science and Technology, in the interest of information exchange. The U.S. Government and Center for Transportation Infrastructure and Safety assumes no liability for the contents or use thereof.

Technical Report Documentation Page

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.
NUTC R203		

4. Title and Subtitle	5. Report Date
Reliability Analysis for the Smart Grid: From Cyber Control and Communication to Physical Manifestations of Failure	January 2010
	6. Performing Organization Code

7. Author/s	8. Performing Organization Report No.
Ayman Z. Faza, Sahra Sedigh and Bruce M. McMillin	00016751

9. Performing Organization Name and Address	10. Work Unit No. (TRAIS)
Center for Transportation Infrastructure and Safety/NUTC program Missouri University of Science and Technology 220 Engineering Research Lab Rolla, MO 65409	11. Contract or Grant No. DTRT06-G-0014

12. Sponsoring Organization Name and Address	13. Type of Report and Period Covered
U.S. Department of Transportation Research and Innovative Technology Administration 1200 New Jersey Avenue, SE Washington, DC 20590	Final
	14. Sponsoring Agency Code

15. Supplementary Notes

16. Abstract

The Smart 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. Our objective 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.

17. Key Words	18. Distribution Statement
Reliability Analysis, Smart Grid, Communications	No restrictions. This document is available to the public through the National Technical Information Service, Springfield, Virginia 22161.

19. Security Classification (of this report)	20. Security Classification (of this page)	21. No. Of Pages	22. Price
unclassified	unclassified	10	

Form DOT F 1700.7 (8-72)

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

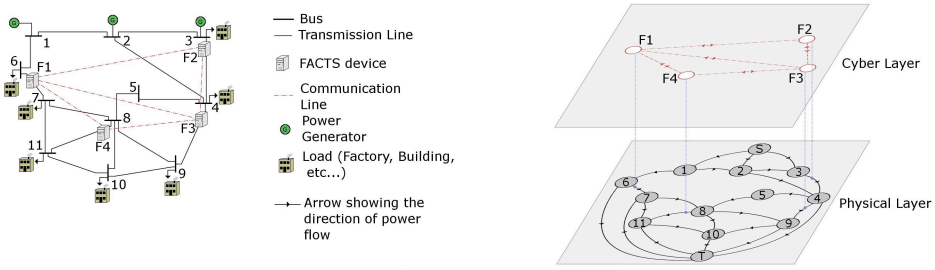
Ayman Z. Faza and Sahra Sedigh and Bruce M. McMillin

Abstract

The Smart 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. Our objective 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.

1 Introduction

The Smart 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 fashion that can prevent failures from occurring in the system. In this report, a transmission line failure is defined as the unanticipated outage of that line due to protective device actions. A typical cyber-physical system is shown in Figure 1 below. Figure 1(a) shows a typical physical network comprised of a number of generators, transmission lines and loads. Overlaid on this physical network is the cyber network, which includes interconnected computers that control the operation of the physical network. Figure 1(b) depicts a graph-theoretic version of Figure 1(a), where these two networks are shown as parallel planes. In the lower plane, the physical layer is represented as a number of nodes connected with edges (transmission lines) in which electric power flows in one direction, while the upper plane represents the cyber components, which communicate information over bidirectional channels.



(a) Interconnected cyber and physical components

(b) Graph-theoretic view

Figure 1: Depiction of the electric power grid as a cyber-physical system.

While adding cyber control to the power grid aims at improving the system's performance and increasing its overall reliability, the addition of requisite cyber components to an already complex system will further increase its complexity and will introduce new vulnerabilities. In fact, we will show in Section 4.4 that there

exist cases where the deployment of a failure-prone FACTS device is detrimental to the overall reliability of the grid.

FACTS devices can fail in a number of ways, including software and hardware failures. In this report, our main focus is on software failures of the FACTS devices, and their manifestations at the physical portion of the power grid. We use the IEEE118 bus system as our case study, and based on the results shown in [1] and [2], we simulate the deployment of FACTS devices at the locations shown in Figure 2. The goal of this deployment is to protect the power grid against potential cascading failures.

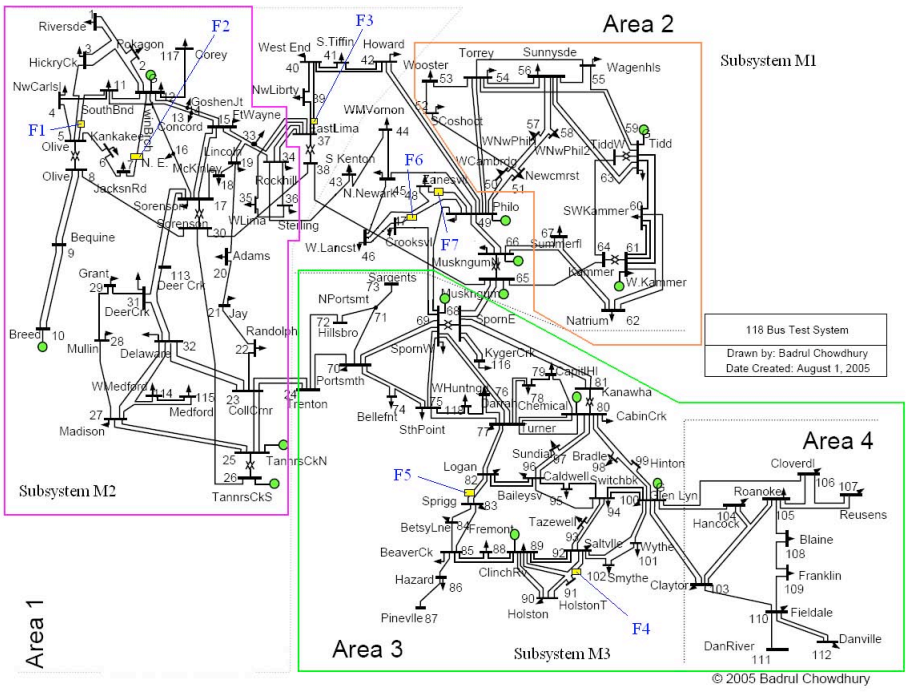


Figure 2: The IEEE118 bus system, with FACTS devices deployed.

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

As presented in [3] and [4], we use the Markov chain Imbeddable Structures (MIS) technique as the basis for our reliability model. This technique requires enumeration of "safe" and "unsafe" states of the system being analyzed. System reliability is defined as the probability that the system will stay in a safe state for a given amount of time."Safe" states are defined as the states where the system as a whole is considered functional, despite the possible failure of a number of components. "Failed" states are defined as the states where the system as a whole is considered to have failed, due to the failure of one or more components.

The main contribution in this research is in relating the software failure modes of FACTS devices to their manifestations in the combined cyber-physical power grid, and quantification of this interdependency through the development of reliability models for the grid. While the focus of this report is on the Smart Grid as a cyber-physical system, the work presented in this report can be extended to many other similar infrastructure systems, such as the the ground transportation system, the air traffic control system.

The remainder of the report is organized as follows. Section 2 provides a summary of related literature. Section 3 describes the system used as a case study, and presents the problem in more detail, while Section 4 specifically targets the failure modes of the FACTS devices. In Section 5, we discuss fault injection as a means of refining our reliability model. Section 6 concludes the paper.

2 Related Work

Estimating the reliability of a cyber-physical system is significantly complicated by interdependencies among its cyber and physical components, as a failure in the physical network could cause a subsequent cyber failure, and vice versa. A number of studies related to this paper describe efforts to capture these interdependencies.

One such study is [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 network, such as the power grid, can cause disruptions in other networks, 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 that identifies vulnerabilities in the design of infrastructure systems by observing the interdependencies among them [6]. 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 alternative 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 alternative sources. 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 report, 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, 11], all of which provide a qualitative analysis of security aspects in the power grid infrastructure. In [10], 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 [10] 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 [11].

The work presented in this report is part of an ongoing research project, and a continuation of the

work presented in [3] and [4] and [12].

3 Effects of Cyber Control on Grid Reliability

In the absence of cyber control of the physical network, the power grid is vulnerable to cascading failures. A number of these failures can be mitigated through prudent deployment of FACTS devices, the form of cyber control investigated in this report. In the IEEE118 bus system used as our case study, four cascading scenarios were found to be mitigated by proper FACTS placement [2]. Table 1 summarizes the cascading failures, and Table 2 shows the locations where FACTS devices can be deployed to prevent each cascading failure. These locations are also depicted in Figure 2.

Table 1: Preventable Cascading Failures in the IEEE118 Bus System

Cascading Failure	**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: Locations of FACTS Devices Required for Mitigation of Failures

Cascading Failure	Initiating Line	1^{st} Device/Line	2^{nd} Device/Line
1	(4-5)	F1/(5-11)	F2/(7-12)
2	(37-39)	F3/(37-40)	
3	(89-92)	F4/(91-92)	F5/(82-83)
4	(47-69)	F6/(47-49)	F7/(48-49)

The IEEE118 bus system includes 210 transmission lines, out of which only 143 can fail without causing the system to fail, according to our simulation. Any state where the only failed component of the physical network is one of these 143 lines is classified as a "safe" state for the grid. Any state where two or more lines have failed is considered a "failed" state. In our work, we focus on the failures of transmission lines, since the other physical components of the grid usually have sufficient backup to compensate for their failures. With those arguments in mind, application of the MIS technique yields the following model for system reliability, when no FACTS devices are included, i.e., system reliability of the purely physical grid.

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

where p_L is the reliability of the transmission line, and $q_L = 1 - p_L$ is the unreliability of the transmission line. For tractability, all transmission lines have been assumed to be equally reliable.

Adding FACTS devices to the system is expected to increase the reliability of the system, as the purpose of their deployment is mitigation of failure. This is reflected in the MIS model by an overall increase in the number of "safe" states, which yields higher reliability.

For example, consider the simple case where a FACTS device can never do any harm to the network, i.e., if the device fails, the system simply bypasses it and continues to operate. This is denoted as the the "fail-bypass" failure mode. In this failure mode, correct operation of the FACTS devices adds safe states to the system, and failure of these devices has no effect on system operation, as a failed device is bypassed. The additional safe states correspond to the cascading failures prevented by introducing the FACTS devices (see Table 2). The resulting reliability model is given by Equation 2.

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

where p_{F_i} and $q_{F_i} = 1 - p_{F_i}$ are the reliability and unreliability of FACTS device i, respectively. If we assume that all FACTS devices are equally reliable, the model reduces to the following:

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

An increase in system reliability is evident from comparing Equations 1 and 3. Figure 3, which depicts the system reliability with and without FACTS devices, confirms this assertion. The average increase in reliability was found to be about 0.18%. The financial savings that result from the prevention of cascading failures magnify the impact of even the smallest improvements to grid reliability.

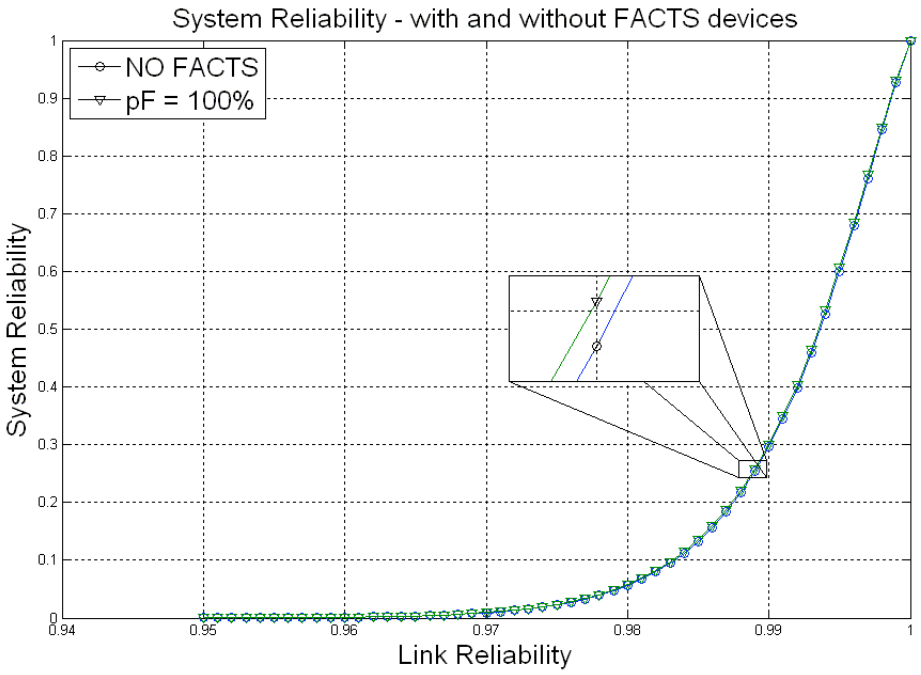


Figure 3: System reliability, with and without FACTS devices

In the following section, we investigate more sophisticated failure modes of the FACTS devices and evaluate their effect on system reliability.

4 Software-Induced Failures in Cyber Control

Faults in the software executed by the FACTS devices can lead to failures that can affect the performance of the power grid. Here, we focus on failures in software, rather than hardware, since hardware reliability is a well studied area and hardware failures can be mitigated by redundancy. This section extends the analysis of the previous section to three non-trivial failure modes of FACTS devices. A system reliability model is developed for each failure mode.

4.1 Failure mode 1: Fail-limit to line capacity

This mode 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 other FACTS devices in the

system. In such a case, if the flow in the line carrying the FACTS device is already within the line capacity, the FACTS device leaves it as is, but if the flow begins to exceed the line capacity, the FACTS device will limit it to the line capacity. The latter will only be necessary if a line fails elsewhere in the system.

This is a localized approach that prevents failure of the line carrying the FACTS device, but could lead to overloads in other parts of the grid, and even cascading failure. Due to lack of communication capability, a FACTS device that has failed in this mode can monitor only the line on which it is deployed, and has no information about the consequences of its actions for other lines in the grid.

This situation was investigated for the IEEE118 bus system, and using simulation, we verified that cascading failure is a possible result of FACTS device failure in mode 1. The results of this simulation were used to identify the "safe" and "failed" states of the grid, leading to the reliability model of Equation 4.

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

Assuming all transmission lines and all FACTS devices are equally reliable, respectively, the model reduces to that of Equation 5.

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

4.2 Failure mode 2: Erroneously set flow to line capacity

In this failure mode, the FACTS device will push the flow on its corresponding transmission line to the line's capacity. This will happen even in the absence of failures elsewhere in the system, unlike mode 1, where the failure of the FACTS device only manifested when failure of a different transmission line is about to cause overload in the line bearing the device.

As in mode 1, this erroneous operation will not cause failure on the line bearing the device, but it may have consequences for other lines in the system. Simulation of this failure mode confirmed that cascading failures could occur as a result of failures in mode 2. This mode is an example of a situation where cyber control is actually detrimental to a functional physical system. This underscores the fact that only highly reliable cyber control will only improve a physical system.

Using simulation, the reliability model of Equation 6 for the grid, assuming failure mode 2 for the FACTS devices.

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

4.3 Failure mode 3: Erroneously set flow to 80% of correct value

This case is similar to failure mode 2, in that failure of the FACTS device can cause the grid to fail, even when all physical components are functioning correctly. However, instead of pushing the flow in the transmission line bearing the FACTS device to its capacity, as in mode 2, the failure results in the flow being set to 80% of what would have been the correct value. This fault could occur due to malfunction of the maximum flow algorithm used to calculate the appropriate settings for the FACTS devices [13].

As in the failure modes 1 and 2, this incorrect operation of the FACT device will not cause an overload in the line bearing the device, but it may cause overloads elsewhere in the grid. Simulation was used to verify that FACTS device failure in mode 3 could lead to cascading failures. Results of the simulation were used to develop the reliability model of Equation 7, which assumes that the FACTS devices fail in mode 3.

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

4.4 Comparison of failure modes

Figure 4 compares system reliability for the three aforementioned failure modes, using the reliability models of Equations 5 through 7. The figure shows that failure mode 2, where the flow of the line bearing the FACTS device is erroneously set to line capacity, is most detrimental to system reliability, while failure mode 1, which only limits the flow to capacity in case of an overload, is least detrimental. The figure illustrates that needlessly changing the flow on a line, as in modes 2 and 3, generally has worse consequences than carrying out an incorrect operation when action is required, as happens in mode 1.

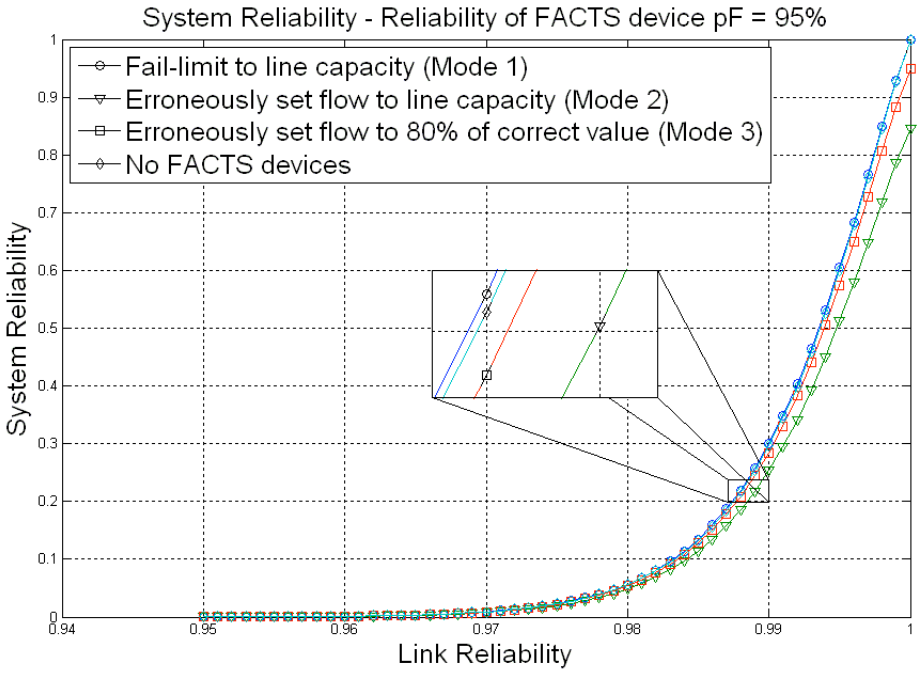


Figure 4: System reliability in different software failure modes

5 Fault Injection in the Cyber Network

The three failure modes described above represent several ways in which the FACTS devices can behave at the occurrence of a fault. In this section, we investigate in more detail the last two failure modes; namely, "Erroneously set flow to line capacity", and "Erroneously set flow to 80% of correct value". Specifically, we attempt to answer the following question: why would a FACTS device set the flow to a value other that its correct value, given that the physical system is functioning properly?

The answer to that question is related to the way FACTS devices react to errors in the software running in the cyber network, and has also a lot to do with the physical limitations of the FACTS device itself.

As mentioned earlier, the network of FACTS devices collectively decides on the appropriate flow values in the transmission lines on which they are deployed. Information about the system, such as the capacities of the transmission lines in the grid, the loading condition on each bus, and the locations and capabilities of the power generating units are fed into the algorithm that runs on the cyber network; the Maximum Flow (MaxFlow) algorithm. This algorithm uses all that information and computes the amount of flow that should ideally go through each transmission line in the network to achieve a maximum amount of power

flow in the system, in such a way that no capacity constraints are violated in the transmission lines. The results of the MaxFlow algorithm are then fed to the FACTS devices in the system, and each one of the devices sets the flow in the line on which it is deployed to the value received from the algorithm. Ideally, the flow would be enforced using the MaxFlow settings on all the transmission lines in the system; this however is impractical, as it would be impossible to place a FACTS device on each and every transmission line in the grid. Instead, only a few FACTS devices are used in a network, and their placement is determined based on factors such as line capacity, location, expected power flow, and previous knowledge of potential cascading scenarios. In other words, the FACTS devices are placed at locations where they would be most effective in preventing the system from failing.

It is clear that any faults in the operation of the MaxFlow algorithm can lead to an erroneous settings on the transmission lines. Below we describe a number of such faults, and investigate their effect on the operation of the algorithm, which will lead to their overall effect on the operation of the grid. Our main goal from this analysis is to identify patterns in which software faults can lead to system failures, and obtain a better understanding of how a cyber fault can cause a failure in the physical system.

5.1 The 'All Excess' fault

During the operation of the MaxFlow algorithm, each vertex can have a certain amount of excess flow in it. This software fault decreases the excess value for each vertex by one unit. This will cause a number of incorrect results in the overall MaxFlow settings, and may lead to erroneous FACTS device settings. This fault does not take any parameters, and the decrease in the excess value is applied to all the vertices in the network.

5.2 The '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 needs to be injected for 118 times, each time at a different vertex.

5.3 The 'One Time Adjust' fault

In this fault, the amount of flow in all edges is increased by 10 units exactly once. This fault requires no additional parameters, and it applied to all the edges in the network.

5.4 The 'Adjust Amount' fault

This fault adjusts the flow in a given edge by adding 10% of the flow to the original flow value. In other words, the new amount of flow it 110% of the original value. This fault takes a given vertex as its parameter, and applies the fault to all the edges connected to that vertex.

Physical limitations on the operation of the FACTS device

Due to the occurrence of one of the software faults mentioned above, the MaxFlow settings on the FACTS devices might change. This change may be small or large. The FACTS devices, however, have a certain rating, and can only change within a range between 80% and 120% of its rated value. This imposes a limitation on how badly the fault can affect the settings on the FACTS device. If the erroneous operation of the MaxFlow 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 it to exactly 80% of the correct value due to its physical limitations. Similarly, a setting on the FACTS device cannot go to a value larger 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 setting on a transmission line to go beyond its capacity. While a FACTS device can allow the flow to go as high as 120% of its rated value, this value might be well higher than the capacity of the transmission line, which can cause the transmission line to fail. Therefore, FACTS devices are normally programmed to only allow the settings to go up to the capacity of the line, to prevent the line from failing due to an erroneous MaxFlow setting.

Fault injection simulation results

Simulation results showed that a number of those faults will lead to incorrect MaxFlow settings, while many of the settings will stay correct. Table 3 presents a summary of the faults that can lead to a MaxFlow setting that is less than 80% of the correct value (the rated value). While all these values were less than 80% of the correct setting, the limitations in the operation of the FACTS device will only allow the setting to go as low as 80% of the correct value, and fix it at that point. This is an example of how a software fault can lead to failure mode 5, in which the FACTS device erroneously sets the flow to 80% of the correct value even though there are no contingencies in the physical network. Furthermore, we showed earlier that in several cases, failure mode 5 can lead to a cascading failure in the physical network, which will cause a system blackout.

Table 3: Summary of cases where fault injection revealed a potential occurrence of a software failure mode under no contingencies

No Contingencies			
Fault Type: Excess Excess			
Parameter(s)	FACTS/Transmission line	% of correct value	Failure mode
11	F1/5-11	72.3%	5
13	F1/5-11	75.1%	5
1-23,25-34	F3/37-40	0%	5
Fault Type: Adjust Amount			
Parameter(s)	FACTS/Transmission line	% of correct value	Failure mode
8	F7/48-49	62.8%	5
46	F6/47-49	18.3%	5
47	F6/47-49	2%	5

6 Conclusions

In this paper, we presented a reliability model for the advanced electric power grid, as a cyber-physical system, with a focus on software faults. FACTS devices, which control the flow of power in the physical infrastructure, were the tools of choice in carrying out cyber control. The effect of this form of cyber control on the overall reliability of the grid was quantitatively investigated using simulation, for different failure modes of the FACTS devices.

We also investigated the effects of several software faults on the operation of the FACTS device. Using fault injection techniques we were able to see how the MaxFlow algorithm can sometimes produce incorrect settings on the FACTS devices, which can lead to one of the software failure modes described earlier. The results obtained from the fault injection analysis will be used to further refine and improve our model.

Future extensions to this project include refining the current reliability model for the Smart Grid by performing statistical analysis and developing confidence levels for our reliability model, and extending the model to other similar critical infrastructures.

References

[1] B. H. Chowdhury and S. Baravc, "Creating cascading failure scenarios in interconnected power systems," in *IEEE Power Engineering Society General Meeting*, June 2006.

[2] A. Lininger, B. McMillin, M. Crow, and B. Chowdhury, "Use of max-flow on FACTS devices," in *North American Power Symposium*, 2007.

[3] A. Faza, S. Sedigh, and B. McMillin, "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, pp. 370–383.

[4] ——, "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, pp. 429–439.

[5] S. Rinaldi, J. Peerenboom, and T. Kelly, "Identifying, understanding, and analyzing critical infrastructure interdependencies," *IEEE Control Systems Magazine*, vol. 11, no. 6, pp. 11–25, Dec. 2001.

[6] I. Lee, E.E., J. Mitchell, and W. Wallace, "Assessing vulnerability of proposed designs for interdependent infrastructure systems," in *Proceedings of the 37th Annual Hawaii International Conference on System Sciences.*, Jan. 2004.

[7] C. Singh and A. Lago-Gonzalez, "Reliability Modeling of Generation Systems Including Unconventional Energy Sources," *IEEE Transactiosn on Power Apparatus and Systems*, vol. PAS-104, no. 5, pp. 1049–1056, May 1985.

[8] J. Endrenyi, M. Bhavaraju, K. Clements, K. Dhir, M. McCoy, K. Medicherla, N. Reppen, L. Salvaderi, S. Shahidehpour, C. Singh, and J. Stratton, "Bulk Power System Reliability Concepts and Applications," *IEEE Transactions on Power Systems*, vol. 3, no. 1, pp. 109–117, February 1988.

[9] J.-C. Laprie, K. Kanoun, and M. Kaaniche, "Modelling interdependencies between the electricity and information infrastructures," in *Proc. of the Int'l Conf. on Computer Safety, Reliability and Security (SAFECOMP)*, September 2007, pp. 54–67.

[10] D. Geer, "Security of Critical Control Systems Sparks Concern," *Computer*, vol. 39, no. 1, pp. 20–23, January 2006.

[11] T. Rigole, K. Vanthournout, and G. Deconinck, "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, pp. 428–440.

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

[13] A. Armbruster, M. Gosnell, B. McMillin, and M. L. Crow, "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, pp. 256–263.