RELIABILITY ANALYSIS FOR THE ADVANCED ELECTRIC POWER GRID: FROM CYBER CONTROL AND COMMUNICATION TO PHYSICAL MANIFESTATIONS OF FAILURE

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

Bruce McMillin/Department of Computer Science/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. We investigate a number of software failure modes in the FACTS devices, and evaluate their effect on the operation 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 cascading failures.

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. In this paper, 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 Fig. 1. The left portion of the figure shows a typical physical network comprised of a few generators, transmission lines and loads. Superimposed on this physical infrastructure is the cyber network, which consists of a number of interconnected computers that control the operation of the physical components. On the right side, a graph theoretic version of the same figure is shown, which separates the two layers into two parallel planes. In the lower plane, the physical layer is represented as a number of nodes connected by edges in which electric power flows in one direction, while the upper plane represents the cyber network components, which communicate over bidirectional channels.

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 a device 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 the 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 Fig. 2. By doing so, the power grid is protected against potential cascading failures that could cause the entire grid to fail.

Through simulation, we examine the effect of faulty behavior of a 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 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 models. We define “safe” states as the states where the system as a whole is functional even if it includes failed components. We define “failed” states as the states in which the 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 model. 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 the
IEEE118 bus system with FACTS devices deployed, 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 the future work, and conclude the paper.

2. RELATED WORK
Estimating the reliability of cyber-physical systems is made more challenging by the fact that such systems are composed of two layers; the cyber and the physical. In particular, the difficulty arises from the interdependencies between the cyber and physical components, as a failure in the physical portion of the network could lead to a failure in the cyber network, and vice versa. A number of studies have been presented in the literature, which describe efforts to capture such 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

Ayman Faza, Sahra Sedigh, and Bruce McMillin
© ISC Research Symposium Missouri S&T 2009
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 the 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 [7] 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 [8] 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 Infrastructure 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.

A related study presents 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.

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 software failures in the cyber network, and their effect on the physical portion of the power grid. The work in [3] and [4] focuses on developing a reliability model for the power grid based on the documented cascading failures, without considering the original causes of faults in the system. In this paper, we take a step forward by analyzing the effect of failures in the cyber network on the system operation.

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 these failures could be mitigated by prudent deployment of FACTS devices. Specifically, it was found that four cascading scenarios could be mitigated by proper FACTS placement [2].

The IEEE118 bus system, which we used as a case study 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. Safe states are defined as states where the system has remained functional despite the failure of one of these 143 lines. Simultaneous failure of two or more lines is considered to place the system in a “failed” state. With these definitions in mind, direct application of the MIS technique [15] yields the following equation for system reliability, when no FACTS devices are included.

\[
R_{sys} = p^{210}_L + 143p^{209}_L q_L
\]  \hspace{1cm} (1)

where,

\[
p_L \text{ and } q_L = 1 - p_L \text{ are the reliability and unreliability of the transmission line, respectively.}
\]

Adding FACTS devices to the system is expected to increase the reliability of the system. This is reflected mathematically in Eq. (1) by an overall increase in the number of “safe” states, which will subsequently increase the reliability.

In analyzing the consequences of the failure of FACTS devices, we begin with a trivial case, where it is assumed that the system simply bypasses a failed FACTS device, and operates as if the device was never installed. We call this the fail-bypass failure mode.

In this mode of operation, correct operation of FACTS devices can only add safe states to the system, i.e., they can never be detrimental to the overall reliability. The added safe states correspond to the cascading scenarios that were prevented by introducing the FACTS devices. Adding those safe states to the reliability model will modify it as follows.

\[
R_{sys} = p^{210}_L + 143p^{209}_L q_L + p^{209}_L q_{L(4-5)} P_{F1} P_{F2}
+ p^{209}_L q_{L(37-39)} P_{F3} + p^{209}_L q_{L(89-92)} P_{F4} P_{F5}
+ p^{209}_L q_{L(47-69)} P_{F6} P_{F7}
\]  \hspace{1cm} (2)

Ayman Faza, Sahra Sedigh, and Bruce McMillin
ISC Research Symposium Missouri S&T 2009
where, 

\[ p_F \text{ and } q_F = 1 - p_F \text{ are the reliability and unreliability of FACTS device } j, \text{ respectively.} \]

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

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

(3)

Comparing Eq. (1) and Eq. (3) we can see an obvious increase in the system reliability. Figure 3 below confirms this assertion. Note that while the increase in reliability may appear to be relatively minor, prevention of cascading failures can lead to significant cost savings.

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

![Figure 3 - System Reliability with and without FACTS devices](image)

4. FAILURE MODES OF FACTS DEVICES

Faults in the software running on the FACTS devices can lead to failures 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 models for the system in each 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 determine 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 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.

4.2. Malicious operation of FACTS devices

Diametrically opposed to the fail-bypass mode are cases where FACTS devices induce a failure in a system that would have been functional in their absence. We present two such cases in the subsections below.

4.2.1 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, as 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 failure-free operation for the rest of the system, and as determined by simulation, could even cause cascading failures. 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 networks, in the form of FACTS devices, was the sole cause of failure. It should be stressed at this point that adding cyber control to the system is only beneficial if the cyber components are highly reliable. We verify that unreliable FACTS devices can result in a cyber-physical system less reliable than its purely physical counterpart.

Using simulation, we develop the following model for system reliability in this failure mode.

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

(5)

4.2.2 Failure mode 3: Maliciously set to 80% of correct value

This case is similar to that of the previous section. However, the flow here is being set to 80% of the correct value, rather than to line capacity, which was the previous case.

This fault could occur due to a malfunction in the operation of the algorithm used to calculate appropriate settings on the...
FACTS devices [16]. 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 it may cause overloads and subsequent cascades elsewhere in the system. Simulation results yield the following model for the reliability of the system.

\[ R_{sys} = p_L^{210} p_F + p_L^{209} q_L (141 p_F + 3 p_F^2 + p_F^3 + 1) \]  

(6)

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 in terms of system reliability, while failure mode 1 is the best. Since the system reliability in modes 2 and 3 is always less than the reliability in mode 1, we can see that malicious operation of a FACTS device, where line settings are inappropriately changed, 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 increase in the overall system reliability. It can be seen from Figs. 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 significant damage to the system, even when all other system components are working properly.

5. CONCLUSIONS AND FUTURE WORK

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.

In the advanced electric power grid, where the physical infrastructure is enhanced by cyber control, the goal is to adjust power flow at specified locations in order to maintain reliable operation in the grid. The cyber network runs a distributed algorithm [16] to determine appropriate settings for power flow on the transmission lines. In the immediate future, it is our objective to inject several types of faults; such as vertex, edge, and message faults in the cyber network, while it is running the distributed 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 one of the three failure modes discussed in Section 4, or introduce previously undiscovered failure modes. This will help complete our reliability model, and will give a much more clear idea of how to improve the cyber control of the grid, with the ultimate goal of fortifying the power distribution infrastructure.

![System Reliability - Fail limit to line capacity](image1)

**Figure 4 - System reliability in the different software failure modes**

![System Reliability - Fail limit to line capacity](image2)

**Figure 5 - System reliability - Fail limit to line capacity**

Analyzing the frequency of occurrence of software faults in the system can give us a more accurate projection of how frequently to expect the cyber network to fail in a particular failure mode, which can lead to more precise estimation of the system reliability. It is our ultimate objective to have a complete model of the reliability of the advanced electric power grid, which will help identify reliability bottlenecks in the system and guide efforts in maintenance and fortification.

6. ACKNOWLEDGMENTS

The authors of this paper would like to thank the Intelligent Systems Center and the Missouri University of Science and Technology for their support of this research.

Ayman Faza, Sahra Sedigh, and Bruce McMillin
© ISC Research Symposium Missouri S&T 2009
7. REFERENCES


Ayman Faza, Sahra Sedigh, and Bruce McMillin
© ISC Research Symposium Missouri S&T 2009