Carnegie Mellon University

CARNEGIE INSTITUTE OF TECHNOLOGY

THESIS

SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS

FOR THE DEGREE OF Doctor of Philosophy

TITLE **The Emerging Smart Grid: Opportunities for Increased System Reliability and Potential Security Risks**

PRESENTED BY Anu Narayanan

ACCEPTED BY THE DEPARTMENT OF

Engineering and Public Policy

_____ _____

ADVISOR, MAJOR PROFESSOR AND DEPARTMENT HEAD DATE

APPROVED BY THE COLLEGE COUNCIL

_____ _____

DEAN DATE

The Emerging Smart Grid: Opportunities for Increased System Reliability and Potential Security Risks

Submitted in partial fulfillment of the requirements for

the degree of

Doctor of Philosophy

in

Engineering and Public Policy

Anu Narayanan

B.S., Applied Mathematics, The University of Texas at Austin
M.S., Engineering and Public Policy, Carnegie Mellon University

Carnegie Mellon University
Pittsburgh, PA

December 2012

To my parents

“The development of human society is based entirely on people helping each other.”

- The Dalai Lama

Contents

List of Tables ..... **v**

List of Figures ..... **vi**

Acknowledgements ..... **vii**

Abstract ..... **xi**

CHAPTER 1 Introduction **1**

CHAPTER 2 Sustaining Socially Critical Services During Blackouts **9**

2.1. Introduction 10

2.2. The Model System 11

2.3. Operation in an Extended Blackout 14

2.4. Cost Analysis 17

2.5. Costs Not in the Model 28

2.6. Conclusions 31

2.7. Future Work 32

CHAPTER 3 Overview of Smart Meter Features and Hacking Strategies **35**

3.1. Introduction 35

3.2. The Regulatory and Standards Framework for Smart Grid Security 40

3.3. Attack Types 42

3.4. The Oscillatory Attack 44

CHAPTER 4 Simulation of a Large Oscillatory Attack Using Smart Meters **49**

4.1. Introduction 50

4.2. Instability 52

4.3. Model systems and Choice of Troublesome Frequencies 55

4.4. System Loading 58

4.5. Load modeling 60

4.6. Power System Analysis Toolbox (PSAT) 62

4.7. Attack Implementation 63

4.8. Results 67
4.9. Discussion and Conclusions 73
4.10. Future Work 79

CHAPTER 5 Overview of Policy Implications 82

5.1. Smart Grid for Critical Mission Survival: Obstacles to Implementation and Remedies 82
5.2. Implications of Smart Meter Attack Work 85

CHAPTER 6 Conclusions 89

References 93

Appendix A: Sample Data Files 106

List of Tables

Table 1: Schedule of critical social services provided in the example system 17

Table 2: Cost estimates of required components for proposed system 23

List of Figures

Figure 2.1: Load profiles for the critical social services being served in proposed strategy. 19

Figure 2.2: Simplified illustrations of electric power transmission and distribution system under normal operation and under proposed strategy. 24

Figure 2.3: Cost of proposed strategy per meter per month 26

Figure 3.1: A simple schematic of a generic smart metering system 38

Figure 4.1: The 9-bus IEEE test system 56

Figure 4.2: The 39-bus IEEE test system 57

Figure 4.3: Schematic of simulation implementation method 65

Figure 4.4: Voltage profile for sample time domain simulation - stable system 66

Figure 4.5: Voltage profile for sample time domain simulation - unstable system 67

Figure 4.6: Results - 9-bus, constant power loads..... 68

Figure 4.7: Results - 9-bus, constant impedance loads 69

Figure 4.8: Results - 39-bus, constant power loads, low damping..... 70

Figure 4.9: Results - 39-bus, constant impedance loads, low damping 71

Figure 4.10: Results - 39-bus, constant power loads, high damping..... 76

Figure 4.11: Results - 39-bus, constant impedance loads, high damping. 77

Acknowledgements

I could not have been where I am in my life without the help of so many people. This thesis is a sample product of the collective contributions of my family, friends, peers and mentors. I want to acknowledge a few of them here with the full knowledge that this list is incomplete.

I will begin by thanking my parents to whom I dedicate this thesis, and my brother Sriram. My dad is the best teacher I have had. He has taught me to think for myself, to be unafraid of conflict, and to cultivate an open mind. My mom embodies the kind of unconditional love that I continually aspire to give to those close to me, now and always. Her unwavering devotion to our family has, in different ways, kept each of us from becoming entirely lost. Sriram, I am grateful for your affection and for the way in which you have unknowingly pushed me to strive for the best. Your ability to persevere is both an inspiration and a source of pride for me.

Granger Morgan has shaped me as a researcher and as a person. As my thesis advisor he has at times guided me closely and at other times allowed me the freedom to explore and learn from my own mistakes. I'm thankful for his patience and genuine care. Through his own commitment to the cause, Granger has shown me the joys of doing research that truly matters. His highly refined social conscience sets him apart and makes him an inspiration to me.

I'd like to also thank my thesis committee members Paul Hines, Gabriela Hug and Howard Lipson for their varied perspectives on my research, which have continually helped me to refine its scope and intentions. Paul's enthusiasm for research and learning in general is truly infectious. Each of my visits to the University of Vermont (thanks for graciously hosting me!) to work with him has left me wanting to push myself harder, and to enjoy every minute of the process. In addition to providing academic guidance in a friendly way, Gabriela has allowed me to share with her some of my insecurities and doubts regarding graduate school and life in general. I appreciate her patience and cherish the advice she has given me. When I first met Howard I knew close to nothing about cybersecurity, but he never made me feel inadequate. I'm thankful for the way in which he has patiently led me through several aspects of the discipline without overwhelming me.

I am hugely indebted to my friends who have always inspired, encouraged, loved and supported me. Brian, thank you for your tireless support, reassurance, and love. I have learned so much from you about what it means to work hard towards difficult, deeply personal goals through good times and bad. Above all, you have taught me through your effortless compassion how much each of us has to give to the world around us. For this and so much more, I feel extremely fortunate to know you.

Bea, you are like a sister to me. I have confided in you things that I have been afraid to admit even to myself. You have given me great advice in desperate times. And of course, you will always be my favorite 'achiever'! Let's go bowling sometime…

Chris, we are so alike in the ways that we struggle, and over the years, I truly believe that we have grown together. I am thankful for your affection and honesty. I feel certain that we will continue to support and motivate each other for years to come.

Eduardo, I absolutely could not have completed this thesis without your help. It's still a mystery to me how you found the time or energy to answer my miscellaneous questions at all times of day (and night) while trying to concurrently complete a Ph.D. yourself! Thanks also for making UVM seem like a second home to me during my visits. I owe you.

Pete, Jon, Carolyn, Mariam, Dipika, Mike, Beth, Adam, David, Rahul, Hari, and Stefan – each of you has contributed to the completion of this thesis in a unique way. Thank you!

Special thanks to Prof. Suzanne Weekes, Prof. Calvin Lin, and Prof. Benjamin Gregg for believing in me at a time when I had trouble believing in myself. Without your encouragement, I would not have pursued graduate school. Thanks to Dr. Eden Fisher for the many enjoyable philosophical conversations in Hamburg A020 over these past few years. Thanks also for letting me occupy that office for much longer than was probably fair!

I will always look back on my time in EPP and at CMU fondly. EPP is a special department in the already special place that is CMU. Here people passionately work together to solve problems and don't waste time erecting artificial barriers between academic disciplines. EPP is also lucky to have an exceptionally dedicated administrative staff. Special thanks to Vicki for saving me multiple times when I've forgotten to register for classes in a timely fashion!

The research completed in this thesis was made possible by funding from the MacArthur Foundation, the Gordon and Betty Moore Foundation, a Graduate Assistance in Areas of National Need (GAANN) award from the U.S. Department of Education and internal funds from the Department of Engineering and Public Policy. Sincere thanks to these contributors for allowing me the luxury of spending my time thinking about interesting problems these past few years.

Abstract

The drive to make the aging electric grid more efficient, reliable, and clean has been at the heart of the "smart grid" mission. Additionally, provisions of the 2007 Energy Independence and Security Act (EISA) and the 2009 American Recovery and Reinvestment Act (ARRA) have led to smart grid investments in the United States. Smart grid upgrades have included the installation of new technologies at all levels of the electric power delivery system. At the distribution system level modernization has included upgrades to communication systems, distribution automation, local control and protection systems, and advanced metering infrastructure (AMI).

Chapter 2 of this thesis aims to use elements of the emerging smart grid at the distribution system level to alleviate the effects of a widespread and long-duration power blackout. Despite continuing efforts to make the electric grid robust, some risk remains of widespread and extended power outages caused by extreme weather, human error, or premeditated terrorist attack. Chapter 2 applies the concept of survivability to the case of ensuring the continued provision of a subset of socially critical services during such blackouts. A load cycling based methodology is proposed, and an associated economic analysis indicates that the cost of implementing the proposed scheme constitutes less than 1% of median annual household income for a range of assumed outage probabilities, distributed generation resource availabilities, and

financing options. While the technical elements of proposed scheme are largely feasible, a few policy changes are identified as necessary for successful implementation of the scheme.

The latter half of this thesis focuses on one potential security risk posed by the large-scale deployment of smart meters. Smart meters constitute one component of advanced metering infrastructure (AMI), a key element of the smart grid. Chapter 3 describes a few documented smart meter hacking strategies and motivates the following question: What, if any, are the implications of smart meter hacking for the bulk power grid? To help answer this question Chapter 4 focuses on one specific attack type with the potential for causing widespread disruption to electric service – the cycling of a large number of consumer loads using the remote connect/disconnect switch on several smart meters. Results from simulations performed on two IEEE test networks (the 9 and 39-bus dynamic test cases) indicate that it is improbable that the mere toggling of customer loads could destabilize the bulk power grid because the fraction of system load that needs to be cycled to induce instability is likely to be prohibitively large.

CHAPTER 1

Introduction

Continuing efforts to increase the reliability of electric power, incorporate cleaner, distributed renewable energy sources, and provide more consumer choice have driven technological advances in various sectors of the electric power delivery system in the United States and worldwide. Such advances have included increased incorporation of renewable generation, storage technologies, customer participation through demand response programs, and enhanced sensing, control and communications technologies. Together these technical and operational advances are often referred to as the "smart grid" [1].

In addition, several legislative initiatives have contributed to the development of the smart grid in the U.S. These include the Energy Independence and Security Act (EISA) of 2007 and the energy provision of the American Recovery and Reinvestment Act (ARRA) of 2009. The EISA legislated federal policy for the development of the smart grid and thereby sent a clear signal of the commitment of the U.S. federal government to furthering smart grid development and deployment. The act authorized the Federal Energy Regulatory Commission (FERC) to adopt a set of standards that the National Institute of Standards and Technology (NIST) would craft. The act also established the Federal Smart Grid Task Force and the Smart Grid Advisory Committee, further establishing governmental intent in dedicating resources to the smart grid effort. A few years later, with the smart grid movement already gaining momentum, the ARRA

authorized federal investments totaling $4.5 billion to utilities nationwide to further their smart grid projects as part of the Smart Grid Investment Grant (SGIG) program [2]. This investment has spawned smart grid developments nationwide, initiated both by grant recipients as well as by other utilities seeking to remain competitive.

Chapter 2 of this thesis presents one way in which elements of this emerging smart grid could help to alleviate the effects of a wide-spread, long duration power outage in the event that the main grid fails. Despite continuing efforts to make the electric grid robust, some risk remains of widespread and extended power outages caused by extreme weather, human error, or premeditated terrorist attack. While all large blackouts have significant societal effects, the recovery path for each outage typically depends on its cause. For instance, recovering from blackouts caused due to extreme weather such as the 1998 Ontario ice storm often takes longer (millions were without power for weeks in this case) because of the need to work around destroyed physical infrastructure like toppled poles, debris, etc.

Large blackouts could also result from a premeditated cyber attack on the grid or originate with small events (e.g., tree contact) that are exacerbated by the lack of appropriate remedial actions, leading to a cascading failure that spans a large geographic region and lasts a long time. Classic examples of such an outage is the 2003 blackout that disrupted electric service to approximately 50 million people in the northeastern U.S. and Canada [3] and a cascading failure in Europe that affected approximately 57 million customers in Italy, France and

Switzerland in the same year. Some metrics[1] indicate that recent years have seen a slight increase in the annual frequency of this class of blackouts, with the trend holding true even after accounting for increases in population and demand [4].

Retrospective analyses have yielded insight into the causes of such cascading power failures. For instance, the U.S.-Canada Power System Outage Task Force found that a combination of inadequate situational awareness, insufficient understanding of system operations, and malfunctioning alarm systems contributed to the 2003 blackout in the northeastern U.S. and Canada [3]. But irrespective of the causes of such blackouts, the fact remains that they continue to occur, resulting in not just significant financial losses, but also leading to a fundamental disruption of our society that depends so greatly on the reliable supply of electric power. The question that naturally follows and is the motivation for work in Chapter 2 of this thesis is: Concurrently with efforts to make the grid more reliable and to improve our ability to sense the onset of a cascading failure, what can be done regionally to ensure the health and safety of society during large and long duration outages?

The health and safety of society depend on a set of social services that have increasingly come to rely on a reliable supply of electric power. Such services in general include supermarkets to provide food, emergency responders, hospitals, water and sewer service, schools, cellular base towers, and gas stations to ensure mobility, to name a few. This set of socially critical services remains the same during a large blackout, although an abridged level of

[1] E.g., Hines, et. al. showed that there is a statistically significant increase in blackout frequency during peak hours of the day [4].

service at each would likely suffice, as people are naturally conditioned to work with less in emergency situations. So the key to sustaining some level of comfort and safety during a large power blackout is to find the means to sustain at least a subset of socially critical services through the course of the outage, and Chapter 2 of this thesis is devoted to developing an appropriate strategy to do just this.

Several researchers have described a critical mission survival-based approach as being a necessary effort and one that is complementary to reliability enhancements [5, 6, 7, 8]. Talukdar, et. al. argue that, "The survival of essential missions is a more tractable problem than the prevention of all large cascading failures, and its solutions are verifiable." [8]. Extending the views expressed in [5, 6, 7, 8], a first order analysis was performed to assess the incremental costs of using distributed resources and some distribution automation to ensure the provision of a subset of socially critical services in the event that a long duration outage occurs (see Chapter 2). Results show that a load cycling-based method that uses smart grid elements proves to be a cost-effective means to keeping a region safe and relatively comfortable during large blackouts. However, several policy and regulatory impediments stand in the way of successfully implementing the proposed strategy and are also described in Chapter 2.

For any set of technologies that is rapidly evolved and widely adopted, it is difficult if not impossible to foresee all possible risks prior to deployment. Problems are iteratively identified and retrofits are made until a sufficiently stable operating condition is reached. This approach has often been presented as a reasonable one to take with regards to the smart grid [9]. But security experts have argued that what differentiates the smart grid from other systems and necessitates significant *apriori* security testing is that it involves an unprecedented level of

coupling between information and communications technology (IT) and a large engineered system – the electric grid [9]. This coupling, in conjunction with the large scope of smart grid projects, could both significantly increase the potential effects of unexplored security holes as well as lead to the costly process of retrofitting flawed technologies.

Smart meters constitute one component of advanced metering infrastructure (AMI), a key element of the smart grid. In the interest of contributing to a better understanding of smart grid security dimensions and providing usable guidance at this relatively early stage of smart grid deployment, in the latter part of this thesis I analyze the potential cybersecurity threat posed by by smart meters. Smart meters can be used for two-way communication between the customer, the utility and sometimes, third party systems that aggregate and process the data collected by smart meters. Tens of millions of smart meters are projected for deployment in the U.S. in the coming years [10]. Security experts have raised concerns regarding potential cybersecurity breaches associated with this hasty deployment of large numbers of smart meters [11, 12, 13, 14] because in many meter installation projects, cybersecurity is treated as an afterthought instead of a consideration in the initial design phase. Lack of proper planning could result in the resource intensive process of retrofitting millions of meters. Several studies have looked at the privacy concerns associated with smart meter deployments [15, 16]. Others have identified security vulnerabilities in advanced metering systems and demonstrated ways in which meters can be hacked [17, 18, 19].

The risks associated with cyber-attacks on higher-level smart grid components, such as central control systems, have also been identified and discussed. Examples of such studies include the 2009 Department of Homeland Security analysis that revealed inherent

vulnerabilities in the electric grid's SCADA control systems to cyber attacks [20] and a 2008 study by the Idaho National Lab that assessed the cybersecurity vulnerabilities of control systems [21]. The Stuxnet worm, which caused major disruptions in operations at the Natanz nuclear facility in Iran in June 2010, demonstrated that a computer worm could cause significant damage to a physical system [22].

The latter half of this thesis is devoted to: 1) Estimating the effect on the stability of the bulk power grid of an oscillatory attack launched using components of advanced metering infrastructure, and 2) Providing technical as well as policy guidance regarding such an attack.

In summary, this thesis makes the following contributions:

1. Applies the concept of *survivability* to the electric power grid in the event of a large scale and long duration blackout through an illustrative case study that presents a load-cycling scheme to power a subset of socially critical services and estimates associated costs
2. Identifies holes in the policy and regulatory framework that prevent such a scheme from being implemented
3. Formulates a simulation methodology and presents results of analyses conducted to estimate the effects of a large scale cyber-attack on the electric grid using compromised smart meters as the primary attack tool.

This thesis is organized as follows:

Chapter 2 presents a strategy to sustain critical social services during a widespread and long-duration power blackout, and estimates associated costs.

Chapter 3 presents an overview of the security dimensions of smart metering systems and describes regulations, standards and advisory initiatives that are currently relevant to smart grid cybersecurity.

Chapter 4 describes the design of a simulation that is designed to assess the risk associated with an oscillatory attack launched on the grid using smart meters, and presents results.

Chapter 5 presents consolidated policy recommendations stemming from the work completed in this thesis.

Chapter 6 presents conclusions.

CHAPTER 2

Sustaining Socially Critical Services During Blackouts

The objective of this work is to devise a strategy to sustain critical social services during a widespread and long-duration power blackout, and estimate associated costs. The work presented in this chapter was a joint effort with M. Granger Morgan and was published in the journal *Risk Analysis* in December 2011[2,3]. This chapter is organized as follows: Section 2.1. provides an introduction as well as motivation for the work. Section 2.2 describes the model system that was used to perform the analysis. Section 2.3. outlines a scheme for operating critical services during a blackout. Section 2.4. presents results of a cost analysis. Section 2.5. presents an overview of costs not included in the model, and Section 2.6. presents conclusions and policy recommendations.

---

[2] Narayanan, A. and Morgan, M. G. (2012), Sustaining Critical Social Services During Extended Regional Power Blackouts. Risk Analysis, 32: 1183–1193. doi: 10.1111/j.1539-6924.2011.01726.x

[3] Anytime the word "we" is used, it refers to Narayanan and Morgan.

2.1. Introduction

Despite continuing efforts to make the electric power system robust, some risk remains of widespread and extended power outages due to extreme weather or acts of terrorism. One way to alleviate the most serious effects of a prolonged blackout is to find local means to secure the continued provision of critical social services upon which the health and safety of society depend. This paper outlines and estimates the incremental cost of a strategy that uses small, distributed generation, distribution automation, and smart meters, to keep a set of critical social services operational during a prolonged power outage that lasts for days or weeks and extends over hundreds of kilometers.

Engineers have worked hard to make the electric power transmission and distribution system as reliable as possible. However, there are limits to how reliable it is possible to make a system that consists of thousands of critical parts that are spread across the landscape [23]. Widespread and extended power outages can result from human error, intense geomagnetic storms [24], extreme weather such as the 1998 ice storm in Ontario [25] or from terrorist attack [26]. The 1998 Ontario ice storm and the 2003 blackout in the Northeast left millions without power, and in the case of the former, for weeks.

Electricity supports many critical social services. When the power goes out, these services are interrupted or severely curtailed. Most of us have experience with blackouts after storms that last for just a few hours, and are relatively localized. Such blackouts are *not* the focus of this paper. Here we ask, what could be done to make critical social services less

vulnerable to low probability, high-consequence events that cause a blackout lasting for several days or weeks and across hundreds of kilometers.

This work examines four questions:

1. How might “smart grid” additions be made to distribution systems that already contain distribution automation and distributed generation, in order to reduce social vulnerability in the event of large, long-duration blackouts?
2. What would be the incremental cost of such additions?
3. What would the probability of a large, long-duration blackout have to be in order to make deployment of such a system cost-effective?
4. What policy options might be employed to ensure that such a system serves as a sensible social "insurance policy?"

2.2. The Model System

While power systems are interconnected at continental scale, there is great variability in their specific technology and operation at local scales. This makes it impossible to perform a detailed yet general technical design and cost assessment. Accordingly, a simple, hypothetical model is constructed and used to obtain a first-order estimate of costs.

The model system makes use of distributed generation (DG) to serve loads that supply critical social services. Because it would be too expensive to place a DG unit in proximity to all such loads, distribution automation and smart meters are used to create an electrically isolated “island” within which limited amounts of power can be moved to critical loads over existing

distribution circuits, while keeping non-essential loads disconnected. There is already a considerable amount of small-scale distributed generation (DG) installed in some power systems [27], and there is growing interest in micro-grids that serve a number of loads while also maintaining a connection to the distribution system [28]. However, because the necessary DG may not be available in any actual system, in the analysis that follows we also consider alternatives that add DG to the system.

We model an urban/suburban region of approximately 5 km^2 with approximately 5000 households. While the specific services considered to be critical during a large scale blackout would vary seasonally and with local circumstances, here we illustrate the model using grocery stores, gas stations, cell telephone base stations, police stations, and schools. Such a region could be expected to have 5-10 gas stations [29], 2-3 grocery stores [30], 5-10 cell towers [31], 1-2 police stations/zones [32], 2-3 schools [33], and 1200-1500 streetlights [34, 35]. Not all these facilities would need to be powered to meet basic needs[4].

For simplicity in this analysis we assume that the region being impacted is not subject to extremes of heat or cold. If a region did require heat or cooling to protect basic public survival, then arrangements would need to be made to address these needs, probably with centrally located heated or cooled pre-designated shelter facilities such as shopping centers that have their own stand-by generation to power furnace blowers, air conditioning, or heat pumps.

[4] Note that the set of critical services that a region chooses to sustain could include residential loads if the metering infrastructure is equipped to, for instance, limit the amount of power that each home can consume.

A typical distribution feeder moves power from a distribution substation out to customers' loads. Each distribution system includes circuit breakers and reclosers to provide automatic protection in the event of faults (from falling trees or poles, lightning strikes, etc.). The distribution voltage is then stepped down for secondary circuits that supply power to most customers' meters. In our model we assume that a number of small DG units with capacities of 10s to 100s of kW either exist or are added on the customer side of some "smart meters" on one or several of the distribution feeders in the region and that power can be supplied to critical loads by "islanding" and reconfiguring the distribution system if the loads and DG units are not on the same feeders. We assume that the local utility has installed distribution automation and that the smart meters include a remote connect/disconnect feature [36]. A number of utilities, such as Duquesne Light have had distribution automation in place for decades, and most smart meter projects, now being implemented with support from the Department of Energy (DOE) stimulus grants, include automated disconnect [19].

In estimating the cost of the system, we include only the incremental cost of the equipment, controls, and operations required to support the *added* capabilities that we model. During an extended power outage, not all services need to be fully functional at all times. We assume that the limited supply can be cycled among the services based on need and a dynamic load schedule. We assume that prior arrangements have been made so that diesel fuel supply is unaffected by the outage. We also assume that natural gas supply is uninterrupted. If major gas pipelines do not have backup to run electric-powered compressor stations using natural gas, this assumption might become invalid.

There are a number of other critical social services beyond the several we include in our model. Most hospitals, airports and radio and television broadcasting stations already have independent systems for emergency backup power [37]. While a number of other larger critical loads, such as water and sewage treatment plants, or lighting and ventilation in traffic tunnels, often do not have backup, they too are probably best served with their own dedicated standby emergency generators, especially if they are remotely located. Some small, distributed loads, such as traffic signals, are better handled with solar PV trickle charged battery backup [38]. Elevators in high-rise buildings might best be served with hybrid backup systems that use some battery or small generator backup as well as some emergency power supplied via a distribution feeder. Indeed, in many regions, building codes now require limited backup for such purposes in new construction.

2.3. Operation in an Extended Blackout

In the event of an extended outage, events might unfold as follows:

1. The local utility realizes that the outage will continue for an extended period.
2. Smart meters on all relevant feeders are instructed to disconnect (without this feature it would be necessary to send crews to every load on every feeder to manually disconnect).
3. One or a few feeders with distributed units are manually or automatically islanded.
4. Distributed generation units on these feeders are connected sequentially to the islanded system to ensure that they are properly synchronized.

5. Following a previously defined schedule, meters at a select few critical loads are instructed to reconnect, while service to all other loads remains disconnected.
6. Through the course of the outage, based on dynamic needs for power among different critical services, different loads are cycled on and off.
7. Once the extended blackout ends, all meters are once again instructed to disconnect before the islanded feeders are returned to their original configuration and reconnected to the grid, and normal repowering proceeds.

In an emergency some degradation of services should be expected, so it should be sufficient to keep just a large enough fraction of services operational to ensure the safety and wellbeing of those affected. We assume in what follows that in addition to creating the technical capability to serve a subset of critical loads, contractual and other arrangements have been worked out between civic authorities and commercial entities so that there is prior agreement about who will be served and how costs and revenues will be shared.

For instance, fuel pump service and cashiers at two of four gas stations could be kept functional at staggered times. Perishables from grocery stores in the area could be transported to one centrally located store shortly after the outage occurs; refrigeration and essential lighting at this central store could be kept operational throughout the outage. A subset of cell towers in the area could be powered so that essential wireless communication could be sustained, and cell

phones could be charged with solar or hand crank chargers[5]. Assuming that partial lighting is possible, a subset of the region's streetlights could be kept operational at night.

With classes operating in several shifts, one school could temporarily serve as an elementary, middle, and high school during different times of the day. One centrally located police station could run at full capacity during the night and at a lower level of functionality during the day.

For smaller loads like gas stations and cell towers, we set the *critical fraction* of total load equal to the *total power* needed to keep each of these services functional. For the larger loads such as schools, grocery stores and police stations, we use the Energy Information Administration's Commercial Building Energy Consumption Survey (CBECS) data, which breaks down energy consumption by specific functions such as lighting, office equipment, etc., to estimate just the critical fractions of total load [41]. We assume that in the case of these loads, prior arrangements have been made to only power the subset of circuits in the facility that is needed to maintain basic service because otherwise the load would exceed available supply.

Table I describes the level to which each service is maintained during the outage and the accompanying management strategies needed to ensure that limited resources are used most effectively in the scenario we model. Figure 2.1 shows graphical representations of electricity

[5] Hand crank chargers are preferable to solar chargers because they can be used during the night. A wide variety of hand crank cell phone chargers, flashlights, radios and similar products are available [39]. Additionally, solar chargers are now available at affordable prices [40]. Most wire-line telephones are powered from central stations, although increasingly handsets require external power.

load profiles associated with the scenario presented in Table I. The total demand at each moment, D(t), is computed as the sum of individual demand at each of the loads at that time:

$$D(t) = \Sigma P_i(t), \text{ where } P_i(t) = \text{the load at the } i^{th} \text{ service at time t, } i \in \{1,\ldots,6\}. \quad \textbf{(2.1)}$$

Under this scenario the total demand is held constant at 350 kW except for the first few hours of the outage when we assume some backup power is already available (e.g. batteries at cell towers), providing enough time to transition to the network of distributed resources.

2.4. Cost Analysis

Implementing the capability outlined above entails costs in two cost categories: 1. Additional distribution system components, battery installations for existing metering equipment to ensure that they can turn on when instructed during the blackout, and control system upgrades associated with operating the proposed system, and 2. Distributed generation resources if sufficient resources are not already in place to serve the selected group of socially critical services during a large, long-duration blackout. As already noted, we are only considering those costs that result from *additions* to distribution systems that already have a degree of automation and smart meters with auto-disconnect capability. The assumed level of distribution automation includes the ability to reconfigure feeders and the ability to island one or a set of feeders either manually or automatically as needed.

Table 1: Schedule of critical social services provided in the example system

Service	*Points of Service*	*Power Consumed*	*Management Strategy*
Police Stations	1	60 kW to support lighting, office equipment and communications [41, 42]	One station is powered; it runs at full capacity (60 kW) at night and at half capacity (30 kW) during the day.
Grocery Stores	1	200 kW for essential lighting and refrigeration during the day, and 160 kW at night for reduced lighting and essential refrigeration [41, 43]	Under previously agreed upon arrangements, during the first few hours of the outage, perishable foods in stores around the neighborhood are transported to one central store. This store is powered through the course of the entire outage.
Gas Stations	4	5 kW per station for a few dispensers and basic lighting; 10 kW at a time for 2 stations powered at once [44]	Two of four previously designated stations are powered at any given time on an announced rotating schedule (~10 kW).
Schools	1	70 kW for lighting, computers and other office equipment [41, 45, 46]	One school is powered with three groups of students (elementary level, middle-school level and high school level) convening at staggered schedules. For instance, the high school students meet from 7 AM to 10 AM, middle school students from 10 AM to 1 PM, and elementary school students from 1 PM to 4 PM.
Cell Towers	10	5 kW per site for a fully loaded 3G site [47]	Most cell towers require no additional backup power in the first few hours of the outage since they have battery backup power. But after the first few hours, 10 towers are kept operational during the day, and 5 at night.
Streetlights	Variable number	250 W per streetlight [48]	A variable number of lights is kept functional during the course of the outage so that total demand does not exceed 350 kW at any time.

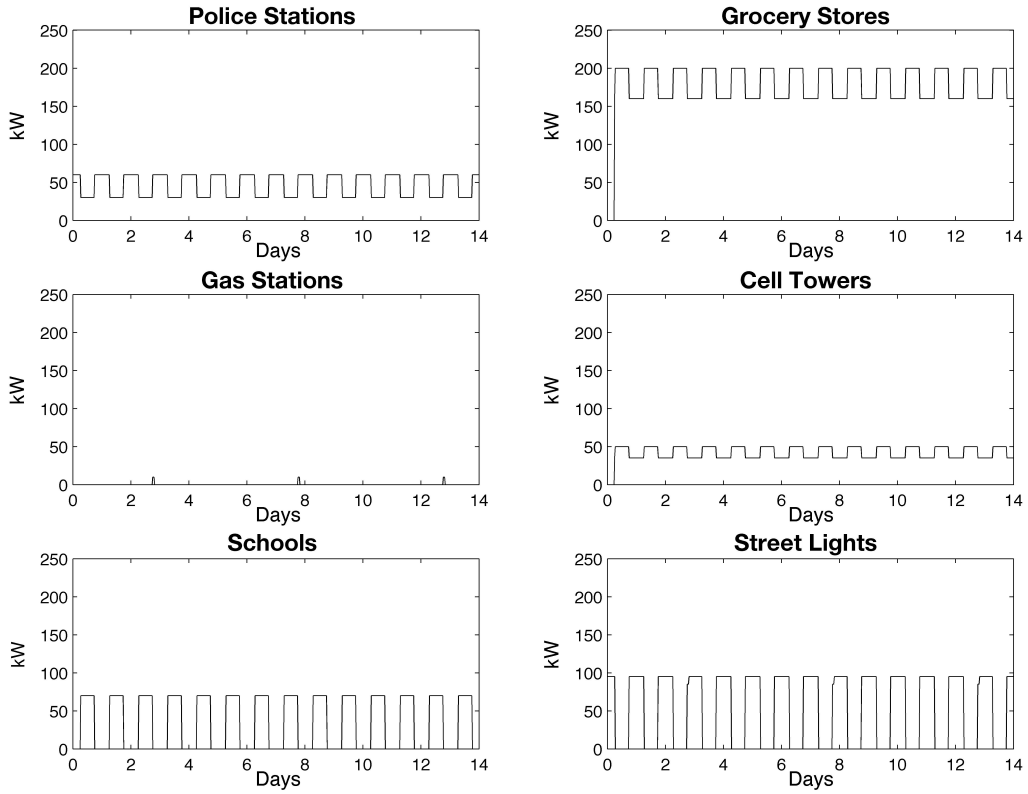

Figure 2.1: Load profiles for the critical social services being served in the sample region reflect the dynamic power allocation strategies presented in Table 1. The x-axis refers to the number of days after the outage occurs, and the y-axis refers to the electricity demand in kW. Peaks and valleys are a function of daytime (0700 to 1800 hours) vs. nighttime.

Additional distribution system components (cost category 1 from above) included in the model are low-power fault handling equipment and necessary controls to operate that equipment. If one or a few feeders are to be disconnected from the main grid and operated as low-power islands during a blackout, existing fault handling equipment will likely need to be augmented [49]. Two main components of fault handling systems are reclosers and sectionalizers [50]. Automatic circuit reclosers are self-contained devices that can sense and interrupt faults, and re-power the line by reclosing automatically. If a fault is permanent, a recloser stays open after a

preset number of operations specified in a built-in counter [50]. Sectionalizers are circuit-opening devices used together with protective devices, such as reclosers and breakers, to automatically isolate faulted sections of electrical distribution systems [50].

Also included in cost category 1 are battery installations for existing metering equipment consisting primarily of smart meters and the control software needed to operate the meters. A "smart meter" is any of a set of different types of meters that can be used for two-way communication between the customer and the utility and sometimes even a third party system [51]. Here we use the term "smart meter" to refer to an individually addressable meter that allows its associated load on a feeder to be connected or disconnected in response to signals from a central control system.

Estimates of the individual components of cost category 1 are summarized in the left hand portion of Table II. Base values were chosen from component cost ranges quoted by a leading distribution automation equipment manufacturer [52]. Sectionalizer and recloser costs include solid dielectric vacuum interrupting components with electronic controls, pole mount frames, cables, internal voltage sensors on the source side, one radio and antenna per control, control programming software, four linemen, two trucks and one technician for installation, programming and testing [52]. The capital and installation cost associated with the additional control software includes two data concentrators for redundancy [52]. Here control system costs refer just to the incremental cost of adding controls for smart-grid style operation of the newly added low-power fault handling equipment and the smart meters in the model. It is likely that if smart meters are present in a region, they already have some battery backup in place [53]. Even if this is not the case, labor costs for battery installation, as opposed to actual battery costs, are

likely to comprise the largest fraction of total costs. For this reason the capital and installation cost for smart meter backup are based on estimates for costs per person-hour for battery installation, and on the assumption that installing a smart meter battery takes one person-hour.

The right hand portion of Table II reports total costs associated with the installation. Component numbers are based the recommendation of engineers responsible for operating a major distribution system [49]. Figure 2.2 presents a simplified diagram of both the normally operating transmission and distribution system (left) and the islanded distribution system serving critical social services (right).

In computing the cost of adding or securing access to DG units (cost category 2) we consider three scenarios: 1) The region has no available DG capacity; 2) The region has some capacity that can be applied to power critical social services, but the available amount is less than 350 kW; 3) The region has 350 kW of capacity available that can be applied to power critical social services in the event of an extended blackout.

Scenario 1: We consider two DG sources, namely, a set of 35 10kW combined heat and power (CHP) natural gas units of the type now being sold for home use in Germany by a consortium of Lichtblick and Volkswagen [54] (capital cost = $740/kW; annual maintenance cost estimated to be $160/unit [49], after adjusting for inflation [55]), and a single 350 kW natural gas fired CHP unit whose cost is estimated by curve fitting to published EPA data [56] and adjusting for inflation [55] (capital cost = $1970/kW; annual maintenance cost estimated to be $160/unit as with the 10 kW engines). Because scenario 1 assumes that the DG units are dedicated for use during a blackout, O&M costs include only the cost of regular maintenance during the year. It is assumed that necessary fuel will be available for use through a previously

negotiated fuel contract. Maintenance costs are dominated by personnel time and are based on two person-hours per visit, two visits per year.

Table 2: Estimates of *incremental* costs of distribution system components required to implement the proposed system

Component	***Capital & Installation per unit***	***Annual O&M per unit***	***Number in model***	***Total Capital and Installation***	***Total Annual O&M***
Low-power sectionalizers and associated control software	$30,000	$200	6	$180,000	$1,200
Low-power reclosers and associated control software	$30,000	$200	6	$180,000	$1,200
Additional software and controls at the substation for smart-grid style operation of meters and low-power fault handing equipment	$100,000	$5,000	1	$100,000	$5,000
Smart meter batteries	$40	$20*	17**	$680	$340
Total				**$460,680**	**$7,740**

*Assuming half a person-hour per year for maintaining one battery installation and $40/person-hour for maintenance costs

** There are 17 individual loads being served in the model (one school, one grocery store, ten cell towers, four gas stations, and one police station) that require individually addressable meters. Since clusters of streetlights are likely controlled from a single point, metering costs are not considered for street lighting.

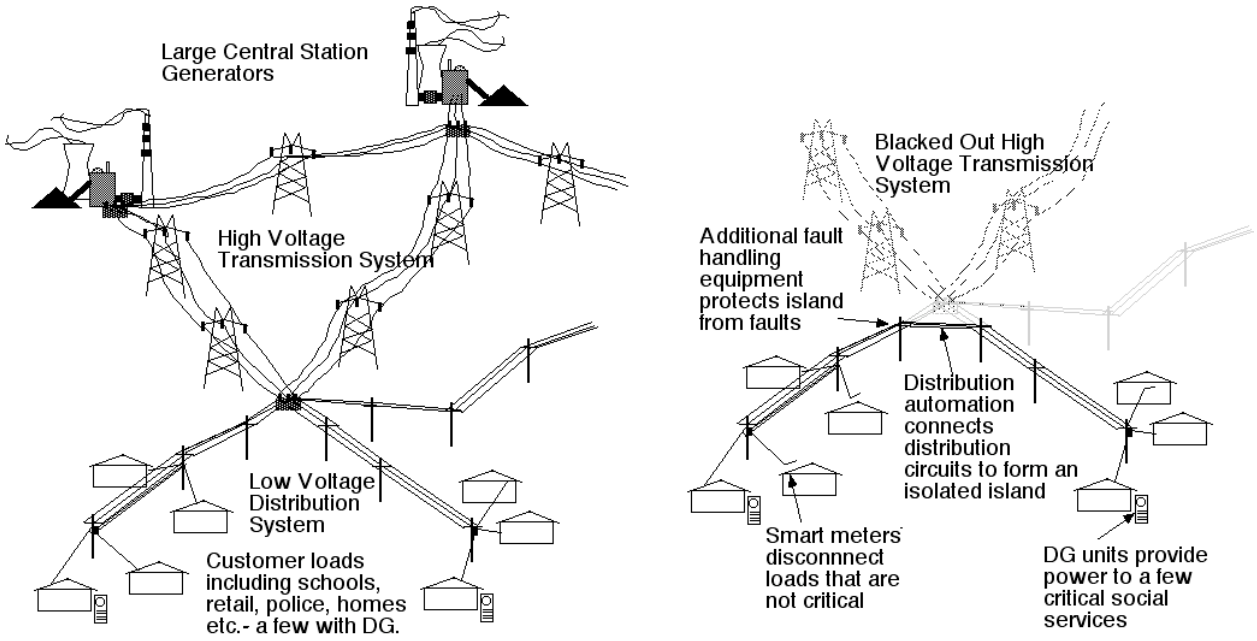

Figure 2.2: Left – simplified illustration of the electric power transmission and distribution system under normal operation. Right – simplified illustration of the islanded distribution system during a large long-duration blackout in which DG units serve local critical social services. Smart meters have disconnected loads that are not critical. Feeders have been reconfigured to form an isolated "island" using distribution automation and added low-power

Scenario 2: Costs in this case include the incremental capital cost of installing enough additional DG to provide sufficient capacity to serve critical social services up to 350 kW as well as the cost of purchasing an option on capacity that is already available.

Again costs are computed for both the case of enough 10 kW Lichtblick/Volkswagen units, or for a single larger unit (again scaling costs from EPA data). The size of the annual fee (R) that must be paid to DG owners to purchase an option to use a portion of their existing capacity will of course depend on local circumstances. For simplicity we estimate an upper bound on R:

$$R = P * A * C * S, \text{ where} \qquad \textbf{(2.2)}$$

P = The annual probability of a large, long-duration outage occurring

A = The quantity of available resources in kW for which owners are willing to sell a use-option

C = The cost per kW of building the same amount of capacity from scratch (again we consider both 10kW units and a large single unit) plus the annualized cost of maintenance

S = A scaling factor ≥ 1 that accounts for the fact that DG owners may require more compensation than the expected value of the new resource before selling an option. The choice of S should be made such that the rent paid to DG owners is sufficiently attractive to induce participation while not being so high that building dedicated DG resources of necessary size proves to be more economical. We compute total system costs for S = 2.

Maintenance costs involved in keeping necessary DG resources in working order are estimated in the same way that they are for Scenario 1

Scenario 3: In this case sufficient capacity is available, and the cost is simply the monthly fee (as calculated in Scenario 2) for purchasing the option to acquire 350 kW in the event of a blackout.

The total cost per customer, assuming 5000 meters**,** can now be computed as the sum of the annualized incremental cost per customer of the additional distribution automation and protection equipment plus the cost of needed DG and option fees. The results are shown in Figure 2.3 for annual outage probabilities of 0.0001, 0.001 and 0.01 for the two types of

generation considered. The costs range from $0.74/meter per month to $1.80/meter per month. A 20-year project lifetime is assumed in annualizing costs. The computation is performed with real interest rates of 3% and 6% in order to examine the implication of securing the needed system upgrades and DG with public (3%) or private (6%) financing.

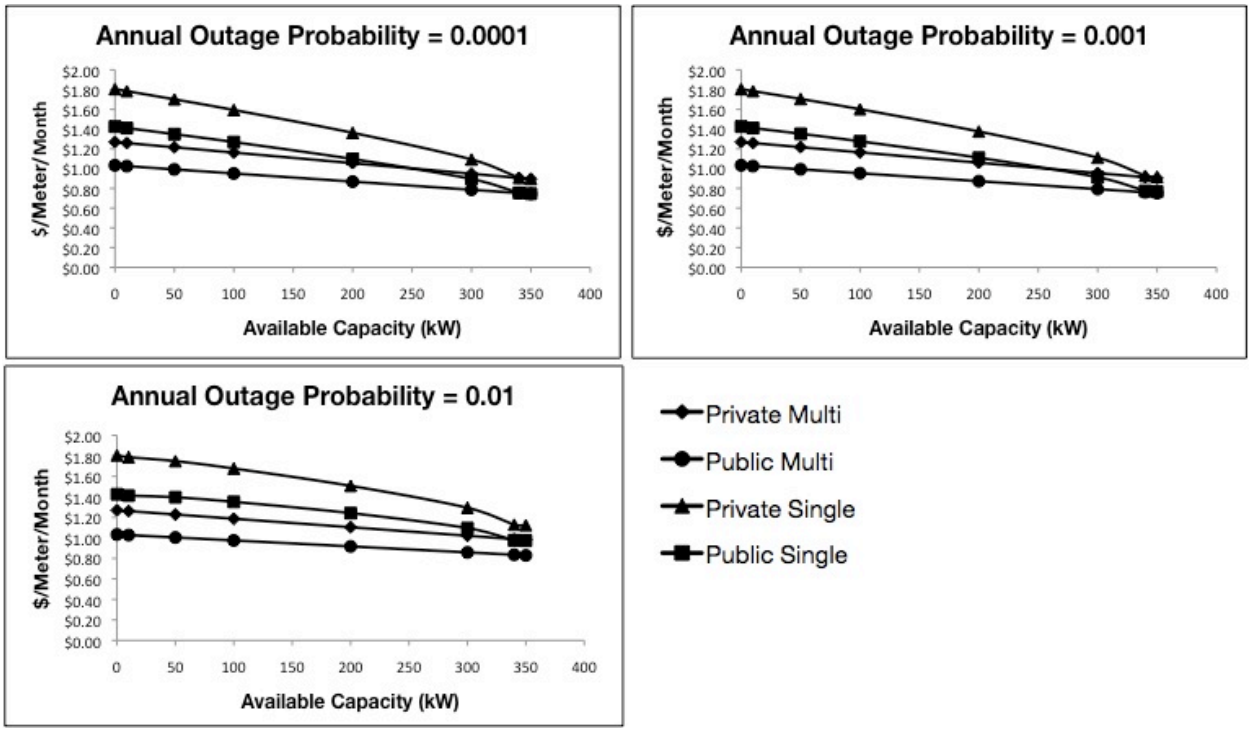

Figure 2.3: Cost (in 2010 dollars) per meter per month as a function of available capacity in the region, of installing sufficient capacity to ensure that 350 kW is available for emergencies for the two DG configurations (single unit, multiple unit) and two financing options (public, private) considered for each of three annual outage probabilities assumed (0.0001, 0.001, 0.01). Here, "Public Multi" refers to the public financing option for the multiple unit configuration, "Private Single" refers to the private financing option for the single unit configuration, and so on. Note that the costs do not vary significantly between the P = 0.0001 and P = 0.001 cases because annual outage probabilities only affect *R* (the annual fee paid to DG owners for use of their resources) in each case, with the capital cost of newly installed DG resources constituting the bulk of total costs.

Whether it is worth making these investments depends upon the probability that such outages will occur and the cost incurred in the event of such an outage. The latter is extremely difficult to estimate. Most available estimates, such as those computed by EPRI, Lawrence Berkeley National Lab and others [57], of the costs of outages are based on lost revenue and earnings from business activity. In an extended outage these values are less relevant than the value to customers of the provision of critical social services. While the value of a few services might be estimated from consumer surplus, others, such as the value of keeping children in school, retaining access to basic food, or maintaining basic policing and emergency communication capabilities, are more difficult to estimate.

For this reason, estimates of the economic losses for past much briefer outages are at best useful only to obtain an order-of-magnitude indication. In its 1990 report the Office of Technology Assessment estimated disruption costs of $1 to $5/kWh for disruptions of relatively modest duration [26]. The blackout that struck the Midwest, the Northeast, and parts of Canada in August 2003 is estimated to have affected more than 50-million people and resulted in costs of between $4.5 and $8.2 billion [58]. North American Reliability Council data indicate that the amount of electrical energy not delivered during that blackout was approximately 920,000 MWh [59]. The last two numbers suggest that the economic cost of the 2003 blackout came to approximately $5 to $9 per forgone kilowatt-hour or between $90 and $160 per capita. The much longer disruption that resulted from the 1998 Ontario ice storm blacked out power to 1,673,000 customers in Quebec, and is reported to have resulted in economic losses of $1.6 billion [60]. This comes to losses of just under $1000 per capita.

One could conduct a survey that asked people's willingness to pay to avoid the loss of critical social services in the event of an extended blackout. However, while some more

sophisticated commercial customers have performed quantitative analyses of the costs of a power outage on business operations, without experiencing an extended outage there is little reason to believe that residential customers could provide an informed, quantitative answer to such a question, even if they generally understand some of the consequences of an extended blackout [61].

Any such estimate will be limited by available income. Let us assume a median income of $50,000 per household [62] for our model community. It is then reasonable to assume that an expenditure of between $500 and $2000, i.e., 1% to 4% of annual household income, to sustain critical services is a reasonable range to consider.

The costs for the system we have outlined range from $9 to $22 per year per household, for annual outage probabilities assumed to be 0.01, 0.001 and 0.0001 for the different scenarios and DG configurations assumed. Even the upper-bound estimate of $22 per year per household comprises less than 1% of median annual household income, making the proposed strategy seem worthwhile. The percentage of annual income that a household is willing to contribute to the cause of sustaining critical services during blackouts could be expected to rise after a surge in terrorist activity, or in the face of evidence that climate change was giving rise to more frequent major ice storms.

2.5. Costs Not in the Model

If a region wanted to make its critical social services truly robust in the face of extended blackouts there are several other investments it should make in addition to the distribution-system modifications that we have modeled. At a minimum, these include backup power for

water and sewage treatment, some limited backup power for traffic signals on key traffic routes, and backup power at the city jail. As noted above, in very hot or cold regions, arrangements would also be needed to provide warmed or cooled shelter space.

A typical water treatment and distribution system includes the following processes: collection from a source, treatment at a water treatment plant, and distribution to end-users [63]. We can estimate just the amount of backup generation capacity needed in the model region to ensure that all 5000 households have access to clean water during an extended blackout. Water consumption per household is around 350 gallons per day [64]. Depending on the topography of the land, the volume of water treated and the distances involved in distribution, the energy intensity of the different processes varies [63]. Assuming an energy intensity of 1.5 kW/1000 gallons for the water use cycle [64] yields an estimate of about 37 MWh of energy, or 109 kW of power, needed to provide clean water to 5000 households over the course of a 2 week outage, assuming 24-hour per day operation. This estimate should serve as an upper bound because it is reasonable to assume that people will consume water frugally during an extended blackout if there are city or region wide ordinances providing specific ways in which water use can be reduced during emergencies [65].

Often electric pumps are used to supply water to the upper stories of high-rise buildings, but the power consumed by such pumps would be small [26]. Further, the burden of ensuring that there is sufficient backup power within buildings should fall on building owners.

Similar to water treatment and distribution, different wastewater treatment and conveyance systems consume varying amounts of power. Assuming an energy intensity of 2.5 kW/1000 gallons for treating and appropriately recycling or discharging wastewater, and

assuming that water consumed is roughly equal to the wastewater produced (i.e., 350 gallons of wastewater produced per household per day), the amount of backup power needed to handle wastewater from 5000 households during an extended power outage would be about 180 kW [63, 64].

For both systems fuel supply and delivery with trucks for diesel and functional pipelines for natural gas are key factors for operation. Often cities or private entities sign priority contracts with fuel suppliers to ensure that necessary is fuel is available in the event of en emergency[6].

Traffic lights were excluded from the model system because we believe they are best handled in a distributed way. Scaling from the city of Pittsburgh we estimate 20-25 intersections with traffic lights in the model region [67]. Assuming signals are converted to LED, and assuming photovoltaic trickle charge batteries are installed at each signal for backup power, the cost of upgrading one traffic signal would be around $9000 [68], making the total cost of upgrading all signals in the model region around $225,000.

Finally, sufficient backup power should be made available at a city or county jail in the region. Jails vary greatly both in capacity and in energy consumption, the latter varying as a function of the extent to which facilities have been modernized to include renewable energy sources and intelligent resource management. As an example, the Santa Rita Jail of Alameda County, CA has a peak electricity demand of around 3 MW and a capacity of 4,500 inmates [69].

---

[6] See [66] for an example.

The facility has a 1.2 MW PV system in addition to a relatively large (4-6 MWh) battery installed onsite. Some correctional facilities such as the Worcester County Jail in Massachusetts are implementing small-scale wind generation to meet the energy demands of the facility as well as to provide power to neighboring loads by selling electricity back to the grid [70]. However, without on-site storage, a wind facility alone would not solve reliably the back-up problem under our scenario.

2.6. Conclusions

Several conclusions follow from the work completed in this chapter. First, a load cycling based method can significantly reduce the amount of power needed to keep a subset of critical services operating in a region during a large blackout. Such a method can be broadly viewed as one component of the larger solution concept of focusing on system *survivability* following disturbance events. Second, this reassessment of the power needed to keep a region healthy and safe during a large blackout can make the use of smaller scale distributed generation a viable option. Third, the completed cost analysis above suggests that the costs involved in implementing a system of the type we have outlined are reasonable for a variety of assumptions regarding the amount of DG resources available to a region. So at least a few regions might find it reasonable to invest in a system of the proposed type. Fourth, as the potential for long duration and large-scale blackouts grows due to climate change or the ever-increasing complexity of the power grid, the value associated with the provision of socially critical services during emergencies is bound to increase, likely increasing consumer willingness to pay for resilience-boosting systems such as the one proposed in this work.

2.7. Future Work

In addition to the recommended policy changes outlined above, a few potential areas for further research on this topic include:

- *Identify specific design constraints that would apply to microgrids that both serve critical loads in islanded mode during emergencies while also operating in conjunction with the main grid to supplement power supply during normal operating conditions.*
- *Survey electric power consumers to: 1) Better understand the types of critical services they consider to be "critical" and would want to have sustained during a blackout, and 2) Estimate consumer willingness to pay (WTP) for system upgrades directed at ensuring the provision of these critical services.* We would argue that to increase the likelihood that people will provide reasonable answers, such an assessment should be completed during or right after blackouts. A preliminary survey was designed to gather information on how consumers perceived the relative value of keeping each of a set of social services during a large, long-duration blackout. Instead of asking responders to directly rank the list of services, the survey presented a budget for total upgrades and asked responders to allocate varying amounts to each social service, with the largest allocation going to the service that they considered to be the most "critical" during a blackout. A few different deficiencies with the survey design, including the lack of complete cost estimates for proposed upgrades at the time, led to the decision to put the effort on hold until a more technical analysis of the costs and feasibility of the upgrades (work presented in this chapter) was completed.

- *Reassess system costs by varying the mix of generation sources to include renewable energy sources with battery storage.*

CHAPTER 3

Overview of Smart Meter Features and Hacking Strategies

This chapter presents an overview of smart metering infrastructure and motivates the research described in Chapter 4. The chapter is organized as follows: Section 3.1. provides background information on the smart grid as a whole and on advanced metering infrastructure. Section 3.2. presents highlights of a few efforts directed at setting security standards for the smart grid and AMI. Section 3.3. describes a few different types of potential attacks on the electric grid that have been shown to be feasible through manipulating metering infrastructure, and Section 3.4. focuses on a specific attack type that is studied in depth in Chapter 4.

3.1. Introduction

Today's electric grid is experiencing several upgrades including more sophisticated sensing technologies, expanded communication networks, and the installation of automation and control equipment at all levels of the electric power delivery system. Such upgrades are intended to increase efficiency (e.g., through better use of the existing high voltage transmission system and through demand side management techniques like load shifting) and reliability (e.g., through the increased use of sensors that enhance situational awareness) of the electric grid. They will

also provide ways to more easily incorporate distributed energy sources and make transactions more transparent to customers [1].

With the growth of such upgrades, the electric grid is increasingly referred to as the "smart grid". As noted in Chapter 1, several governmental initiatives have spurred smart grid investments. First, the Energy Independence and Security Act (EISA) of 2007 legislated federal policy for smart grid advancements, established the Smart Grid Advisory Committee and the Smart Grid Task Force, commissioned the National Institute of Standards and Technology (NIST) to create a framework for smart grid development, and authorized the Federal Energy Regulatory Commission (FERC) to adopt standards developed by NIST. The primary mission of the Task Force was defined as coordinating the efforts of various governmental agencies in the smart grid space. The Advisory Committee was designed provide advice to the Department of Energy (DOE) on various topics related to the changing electric grid.

Second, the Smart Grid Investment Grant (SGIG) program, a part of the American Recovery and Reinvestment Act (ARRA) of 2009, provided more than $3.4 billion for smart grid development in the form of 50/50 matching grants to 100 utilities. Additionally renewable portfolio standards in several states, which require smart grid technologies in order to be implemented, have contributed to the adoption of smart grid technologies.

Smart grid advancements include technologies installed at all levels of the electric power delivery system including the transmission and distribution networks, as well as at the consumer level. At the distribution level smart grid enhancements include upgrades to communication systems, distribution automation (e.g., automatic feeder reconfiguration capability in areas that do not already have it), local control and protection systems, and advanced metering

infrastructure (AMI) [71]. This latter component of the smart distribution system and the potential new cybersecurity risks it introduces to the bulk grid are the focus of the rest of this thesis.

AMI is comprised of several elements including smart meters, communication networks, data management systems, and software and controls needed to integrate new infrastructure into the existing system. AMI acts as a link between customers, distributed generation and storage resources, and the bulk grid, making it an integral part of the emerging smart grid [72].

Smart meters are an indispensible part of AMI because they provide the only direct access points to consumer usage data. Smart meters are also often the first technology that is deployed by utilities in the process of modernizing their systems [71]. Smart metering systems typically use one of two types of communication technologies – radio frequency (RF), and power line career (PLC). In RF mesh network configurations, meters act as repeaters to form a local area network (LAN) from which an aggregator, which can itself be a meter, gathers information to pass on to the utility servers through one of several backhaul methods (e.g., cellular networks, the internet, or the public switched telephone network) [73]. In PLC network configurations, each meter directly transmits data to an aggregator which plays a similar role as it does in the RF network configuration described above. Figure 3.1 presents a simple schematic of a generic smart metering system. Not pictured but a common component of AMI are meter data management systems (MDMS) that process meter data before they are sent to the utility servers.

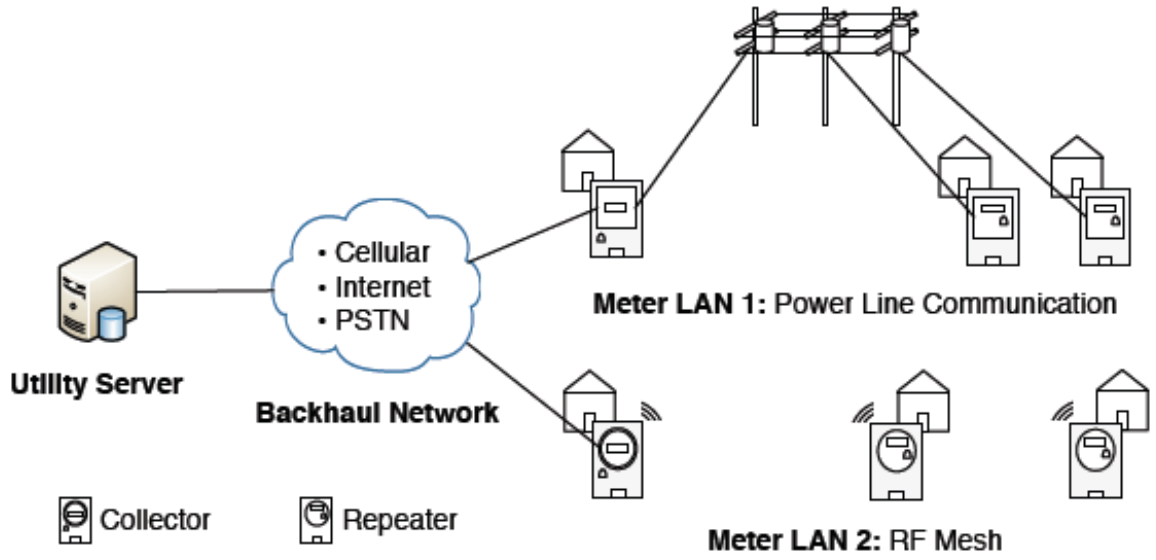

Figure 3.1: A simple schematic of a generic smart metering system, which includes several customer meters configured either as a mesh network or as a power line communication network. The system one or a few collectors, which can act as meters themselves. [19]

The smart meter often includes the following:

- A Microcontroller Unit (MCU)
- Memory
- Network Interface Card (NIC)
- Infrared optical port
- Remote disconnect switch system

The MCU is responsible for retrieving energy usage data and stores it in flash memory. Also stored in memory are logs of various events and operating conditions. The NIC is responsible for coordinating the interface between the meter and the network. In the event that

the meter loses communication with the utility and needs to be repaired or maintained, the optical port provides direct access to meter information like passwords [19]. The access that the optical port provides to such information is at very short range. But if identifying information is shared across several meters in a deployment, then tampering with just one meter could provide an intruder with the information he needs to manipulate several meters at once. Finally, the remote disconnect switch system consists of a physical switch that can break the flow of current to a point of service and the capability of receiving and acting on a set of remote commands sent from the utility [19].

Growing hand in hand with the number of deployed smart meters in the U.S. are concerns regarding the privacy and security implications of metering systems resulting from break-ins at any of the several layers of the advanced metering infrastructure[7]. Smart meter privacy concerns, while clearly an important issue, are not addressed in this thesis. Rather, the focus here is on the security implications of smart metering systems. On this topic there is a large body of work that documents successful efforts directed at hacking smart meters and identifying the sorts of attacks that might subsequently be implemented.

Section 3.2. presents an overview of the standards and regulatory framework for the security dimensions of the smart grid and of AMI. Section 3.3. describes a few different smart meter based attacks that have been demonstrated. Finally Section 3.4. focuses on one of the attack types discussed in Section 3.3. and motivates the work undertaken in Chapter 4.

---

[7] It should be noted that the Federal Opportunity Announcement for the SGIG program did require applicants to submit cybersecurity plans, and annual reviews include assessments of progress with these plans [74].

3.2. The Regulatory and Standards Framework for Smart Grid Security

The power sector is currently in the midst of reconciling existing standards with new ones that are needed to manage the changing needs of the modern grid. Subsequently many standards and regulations pertaining to the security aspects of the smart grid are still evolving as related technologies themselves continue to evolve. It should be noted that many existing standards apply to components of the bulk power grid and not to elements of the distribution system because historically the distribution system has operated in such a way that even significant disturbances to this system would rarely have implications for the bulk power grid. But with the increasing deployment of distributed control technologies, smart meters and sensing equipment, the number of access points to several grid components increases, potentially exposing new vulnerabilities.

An example of standards dedicated to ensuring the security of the bulk power grid is the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection Standards (CIPs). The broad objective of the NERC CIPs is to ensure that the automation, communication and control systems of the electric grid are protected against several threats [75]. NERC CIPs 002-009 provide a cybersecurity framework for identifying and protecting Critical Cyber Assets to support reliable operation of the Bulk Electric System. [75].

Additionally, several volunteer, government, academic, and industry efforts are ongoing to help develop security guidelines pertaining to the smart grid. Key players include NIST, DHS, DOE, volunteer organizations, universities, and security firms. For instance, NIST's

Interagency Report NISTIR 7628 entitled, "Guidelines for Smart Grid Cybersecurity", presents an analytical framework that can be adapted for use as applicable by various organizations embarking on smart grid projects [76]. DHS conducted a workshop in the summer of 2009 called "Future Directions in Cyber-Physical Systems Security" that provided broad recommendations for the development of security standards in the smart grid space. Two key recommendations that grew out of the workshop were to: 1) Organize a coordinated research effort to holistically develop security measures for the modern power delivery system, and 2) Develop techno-economic analyses that reconcile local stability-enhancing mechanisms with global interests [77]. In September of 2011 the Department of Energy published an update to the 2006 version of a roadmap dedicated to ensuring the cybersecurity of energy delivery systems. The updated roadmap presents a strategic framework for achieving system-wide cybersecurity goals while taking into account the changing technological landscape as well needs of the energy sector [78].

One noteworthy effort specific to AMI security was led by the Advanced Metering Infrastructure Security Task Force (AMI-SEC TF) of the Utility Communications Architecture International Users Group (UCAIug) with the help of the Advanced Security Acceleration Project – Smart Grid (ASAP-SG)[8] and produced guidance and security controls to be used by any organization deploying advanced metering systems [14]. The report formally acknowledged the potential risks associated with the remote disconnect switch and recommended a potential

[8] The AMI-SEC TF was established under the UCAIug in 2007 to develop guidelines for AMI. The AMI-SEC TF enlisted the help of the ASAP-SG group (with supporting organizations including DOE, EPRI, and a few electric utilities) to complete the *Security Profile for Advanced Metering Infrastructure* in 2009.

safety feature of implementing a delay in response time, a measure that is not implemented in currently deployed systems [79].

While such efforts are all steps in the right direction, there is concern regarding the lack of evolved standards for smart grid security. In a recent report on the topic of electric grid cyber-security related to the electric grid, the Government Accountability Office (GAO) listed the lack of coordinated effort, jurisdictional issues, a misplaced focus on compliance instead of comprehensive security, the lack of sufficient inbuilt security features, the lack of a proper forum for disseminating knowledge, and the lack of metrics for evaluation as a few key challenges to ensuring the cyber-security of the electric power grid [80].

Chapter 5 describes a few ways in which the work completed in this thesis could contribute to policymaking and the evolution of standards relating to the smart grid.

3.3. Attack Types

There have been many instances of successful smart meter hacks performed by individuals, industry and the academy. This section describes a few different theoretical and practical demonstrations of successful attacks. The purpose of this section is *not* to exhaustively describe all of the different ways in which smart meters have been and could be hacked. Rather the intent is to present a sampling of different attack types and to motivate the research question posed in Chapter 4: What is the *effect* of one type of successful smart meter based attack – the toggling of a large number of system loads – on grid operations?

Different types of attacks are bound to have different implications ranging from annoyance to a few customers or financial losses for the utility to the more serious case of inducing unstable operating conditions in the bulk power grid. Lab work has suggested that a hacker who is relatively knowledgeable about electronics and software engineering might be able to hack into smart meters to commit energy fraud, implement a denial of service attack, or even disrupt electric service to a large number of customers by disconnecting loads via the remote disconnect switch. Researchers at Penn State University demonstrated how smart meters could be hacked to implement the three types of attack [19]. All three attack types broadly require the retrieval of the meter ID and password, and the attacker having knowledge of the communication protocols used and at least cursory knowledge of electronics and software programming. Additionally, the third attack type would exploit the relatively common practice of utilities assigning the same meter passwords to hundreds or even thousands of smart meters in a deployment, making it easy for an attacker to tamper with just one meter physically to retrieve necessary information, and gain an understanding of the meter's programming before proceeding to remotely launch a coordinated attack on several meters using the remote connect/disconnect switch.

The first two attack types involving energy fraud and denial of service are likely to only cause annoyance to customers or result in financial losses for the utility. In a recent alert, the Federal Bureau of Investigation reported that perpetrators with relatively inexpensive tools and access to commercially available software were able to hack into smart meters to commit energy fraud by altering usage data that could have resulted in significant financial losses (estimated to be up to $400 million annually) for a utility company in Puerto Rico [80]. This particular attack required the hackers to have physical access to each of the compromised meters, with the

attackers using an optical converter device to create a communication link between the meter and the attacker's laptop and then altering energy usage data using software downloaded from the internet.

It is possible that if sufficiently large numbers of smart meters were manipulated to report falsified usage data, and if energy usage data were being used to make real-time decisions about dispatch, that the energy fraud attack scenario could have implications for system operations on the whole. But the risk of such a large-scale meter tampering effort, even if successfully implemented, is further diminished by a lack of evidence that suggests that utilities plan to rely solely on current smart meter data aggregation systems to make system-wide decisions.

On the other hand, the third of the three attack types described above – the targeted disconnect attack – if launched remotely to control a large fraction of system load through their smart meter controls, could be more serious if the meters were to respond to spurious commands in ways that directly affect grid operations. Details of this attack type are presented in Section 3.4.

3.4. The Oscillatory Attack

Any of the attack types described in Section 3.2. is sure to have local effects at the distribution system level. But one particular attack type could hold the potential for a larger scale disruption. This is the attack scenario where a hacker breaks into a large number of smart meters and is able to toggle the remote disconnect switch on and off simultaneously on all of the meters at some frequency for a period of time, thereby connecting and disconnecting the entire

electrical load at each of the controlled meters [14, 19]. The oscillatory nature of this type of attack is especially interesting because the simple dropping of even entire distribution feeders (as often happens when lightning strikes) rarely causes any notable reliability problems for the bulk power grid. But it is possible that if the system is already operating at a stressed state and operating and per a contingency plan, then a coordinated, oscillatory attack launched on a large number of smart meters at a frequency that is known to be troublesome, could cause stability issues for the bulk power grid.

Most smart meters in the U.S. include the remote connect/disconnect switch described in Section 3.1. [82, 19, 83]. The switch is designed to allow the utility company to directly control customer load when bills are not paid or when emergency load shedding is needed. But by masquerading as the utility company, researchers have shown that an attacker might be able to activate this switch by sending false connect/disconnect commands [19]. While the switch can theoretically be disabled, it is unclear how many deployed meters actually have the switch disabled. PG&E has reported that as many as 2.2 million of a recent deployment of 2.5 million meters have the switch enabled [82].

A remote connect/disconnect operation does not rely on a central aggregator taking action on false reporting in order to cause a disturbance; it unilaterally cuts off power to several customers, making it a more direct attack strategy. The growing deployment of sensing technologies across various levels of the power delivery system (e.g., phasor measurement units, or PMUs) could enable a determined and resourceful attacker to identify exploitable vulnerabilities such as troublesome frequencies and highly stressed areas within the system [71], potentially exacerbating the effects of such an attack.

IOActive, a security services firm, demonstrated that it is possible to shut off power to thousands of homes within a span of 24 hours, assuming that the attacked meters shared certain attributes [16]. The attack involved first learning about the programming of one meter by accessing its RAM, and then spreading malware through a large deployment of meters with the same passwords and programming as the initially hacked meter, in order to widely issue falsified remote disconnect commands. The reported cost of carrying out such an attack is $500 in equipment and materials, given that the attacker has some knowledge of electronics and software engineering.

In another example Inguardians, a security consulting firm, disclosed in early 2010 that they had found some vulnerabilities within the metering infrastructure that would allow attackers to remotely connect to a number of meters and to intercept commands sent from the utility company [18]. A common problem with such demonstrations and claims performed by private companies is that specific details of the exact steps used to complete the attack are often not disclosed. In addition to the fear that such information would get into the hands of malicious entities seeking to launch similar attacks – a fear that is shared among all entities conducting research in this area – private security firms want to retain proprietary rights to the knowledge they gain. So the public is often made aware of just the results of the analyses and not informed about the methods used.

Of course, even among meters that have all of the features that would be needed for a large-scale attack to be successful (including but not limited to an active remote disconnect switch), there are likely to be inbuilt checks to detect and prevent tampering at various levels of the infrastructure as systems become more sophisticated.

However, assuming that it were possible for a determined, resource-rich adversary to tamper with a large number of smart meters to disrupt electric power service to a large number of customers, it is still unclear whether such a worst-case attack scenario could cause significant disruptions of the bulk electric power system. Specifically, what fraction of system load would need to be compromised before there could be significant effects on grid stability? The answer is likely a function of the nature of the attack itself, and the pre-attack state of the system. Chapter 4 describes the methods and results of a simulation designed to estimate the fraction of system load that would need to be compromised to launch an oscillatory attack on the grid that affects system stability. To be clear, the purpose of the work presented in Chapter 4 is to specifically look at the effects of such an attack on the transmission level grid, and not the distribution system. The analysis that follows in Chapter 4 can be viewed as a worst-case analysis because it assumes that an ideal attack is, in fact, possible.

It should be noted that smart meter-based attacks would have additional effects on the bulk grid depending on whether higher level systems within the advanced metering infrastructure and the smart grid as a whole are concurrently also compromised. In the context of this work, it is assumed that other parts of the system, such as substation automation capabilities, are not compromised in conjunction with attacks on smart meters.

CHAPTER 4

Simulation of a Large Oscillatory Attack Using Smart Meters

Given that, as discussed in Chapter 3, a simultaneous cyber attack on a large number of smart meters might be possible, this chapter describes the steps involved in simulating an oscillatory attack undertaken with the objective of disrupting the bulk power system and presents results obtained by running the simulation for a set of test scenarios. The enabling mechanism for such an attack is the remote disconnect switch that is included in most smart meters. Section 4.1. provides an introduction to the work. Section 4.2. describes the metrics used for "instability" in the context of this work. Section 4.3. describes the model systems used and the choice of troublesome frequencies. Section 4.4. describes the manner in which test cases representing various levels of system stress are created. Section 4.5. describes the two load models used for the simulations. Section 4.6. introduces PSAT, the tool used to perform the simulations. Section 4.7. describes the attack implementation methodology. Section 4.8. presents results, and Section 4.9. presents a discussion of results and conclusions. Finally Section 4.10. identifies areas for future work[9].

[9] Much of the work in this chapter was completed with the help and guidance of Paul Hines and Eduardo Cotilla-Sanchez at the University of Vermont. We intend to jointly publish this work.

4.1. Introduction

Chapter 3 presented an overview of the security dimensions of advanced metering infrastructure and described a few different strategies for hacking smart meters. One specific type of malicious hacking described was the targeted disconnect attack, which researchers have argued might be launched on a large number of smart meters. Through physically tampering with just one meter of the type used in a deployment, a savvy adversary might then be able to extract necessary identifying information that is common to the whole deployment, masquerade as the utility company, and send false connect/disconnect commands to many meters [14, 16, 18, 19]. The remote disconnect switches on all of the compromised meters would then open or close the circuit at a customer load according to directions sent remotely from the adversary. The question that immediately follows is, "So what?" Of course the unintended adding and dropping of loads would cause inconvenience to customers. But aside from annoyance to consumers or disturbances to the local distribution systems, could the effects of a coordinated oscillatory attack launched using smart meters cause any significant instability in the transmission level electric power grid? Further, what would the scale of the attack need to be – in terms of the fraction of system load that is compromised – in order to destabilize the bulk power grid?

The balance of this chapter describes the formulation of results from a simulation designed to help answer these questions. Specifically, the objective of the analysis is to estimate the fraction of system load that needs to be cycled in order to produce any notably detrimental effects on system stability for two test networks, and to estimate this load fraction for each of several loading scenarios and for different attack characteristics. The work broadly aims to place

bounds on the effects on the bulk power grid of implementing an oscillatory attack. The focus is on creating a sample outcome space through a few illustrative cases without making claims about whether and how attack types *not* included in this analysis might affect grid operations.

A few different possible outcomes were considered before designing the simulation. On one end of the spectrum of outcomes would be the case that for all or a majority of combinations of values for the level of system stress and for different parameters that characterize the attack, a very small fraction of system load needs to be oscillated in order to destabilize the system. This result, if extrapolated, would mean that that the remote disconnect switch does, in fact, represent a significant vulnerability. On the other end is the sample outcome that significant stability issues arise only in the event that $\geq$ 30% of the total load is cycled and that too, for a system that is already unrealistically highly stressed. In this case the argument could be made that it is likely impossible that a hacker intending to cause a major disturbance to the bulk power system could control a sufficiently large fraction of the load to accomplish his goal, and hence that the remote disconnect switch does pose a serious risk to the overall security of the power system.

It should be noted that there are bound to be latencies in the system irrespective of the choice of communication network (RF mesh or point-to-point, or PLC), that are likely to make a perfectly coordinated attack difficult [73]. Further, some security experts have suggested that a built-in random delay in response times to commands received by the meter would make the coordinated launch of an attack using the remote disconnect switch difficult, if not impossible [14]. But this is not a feature that is currently included in deployed meters [79]. Further, depending on the purpose for which utilities plan to use the remote disconnect switch, such a delay in response time might limit functionality.

4.2. Instability

A first step before beginning to design the simulation was to define what would constitute an unstable operating condition for the test systems being used. That is, what would signal that the system had become unstable when subjected to the oscillatory attack? There are established mathematical definitions of stability for dynamical systems in general. For instance, the theory of Lyapunov provides the basis for one type of stability metric wherein an equilibrium point, x_e, of a dynamical system is considered Lyapunov stable if all solutions of the system that start out near x_e remain forever in a small neighborhood around it. A stronger stability measure is that of asymptotic stability, which requires that all solutions that start out near x_e *converge* to x_e. [84]

Applying general concepts of stability theory to the specific case of the power system has been a topic of extensive study over the years [85, 86]. Depending on the specific context within which stability is studied, different definitions and classifications of power system stability are used. Further, depending on the analysis tool used to conduct stability studies, there is often the need to translate any purely theoretical or mathematical definition into a form that makes sense when accounting for tool-specific and case-specific parameters. For instance, Kundur et. al. provide the following, widely accepted definition: *"Power system stability is the ability of an electric power system, for a given initial operating condition, to regain a state of operating equilibrium after being subjected to a physical disturbance, with most system variables bounded so that practically the entire system remains intact."* [86]. But the exact meanings of "*a state of operating equilibrium*" or "*with most system variables bounded*" or "*practically the entire system*" vary based on the situation. Drawing from the large body of theoretical as well as empirical work on the topic of power system stability, these terms are typically defined on a

case-by-case basis, ensuring that the right system-specific metrics are used to assess stability.

Often signs of instability can be used as a way to *measure* stability. Signs of instability might be easier to observe, and this approach especially makes sense if the analyst is not as concerned about the specific *way* in which the system becomes unstable, but just that it does. Differences in the manner in which a system returns to steady state could include the speed of return or the degree of perturbations during the return. A prolonged or rocky path to stability could have an impact if other attacks are launched or if other system components fail during the recovery period. But in the analysis that follows, the launched oscillatory attack is considered successful if during the course of a simulation of specified duration, the system becomes unstable per one of two metrics for instability.

The first instability criterion used is that the power flow Jacobian matrix, **J**, becomes singular. **J** is comprised of the first order partial derivatives of the active and reactive components of the power injections at a fraction of system nodes with respect to the voltage magnitudes and voltage angles at those nodes. These derivatives describe the effect that changes in the voltage magnitudes and angles have on the net power injections. The mathematical representation of this instability criterion is as follows:

$$\mathbf{J} = \begin{pmatrix} \frac{dP}{dV} & \frac{dP}{d\theta} \\ \frac{dQ}{dV} & \frac{dQ}{d\theta} \end{pmatrix} \text{ becomes singular,} \qquad \textbf{(4.1)}$$

where **J** is the power flow Jacobian matrix comprised of four sub-matrices, each a Jacobian matrix representing a fraction of nodes in the system. P and Q represent vectors of the active

and reactive power injections at each bus respectively, and V and θ represent vectors of the voltage magnitudes and angles at each bus respectively. This instability metric is commonly used as a signal of voltage collapse resulting from one of several algebraic system constraints not being met [85, 86, 88].

The second instability criterion used is that the voltage phase angle difference between any two adjacent buses in the network is larger than $\pi/2$. Mathematically, this translates to:

$$\max | \theta_j - \theta_k | > \pi/2, \quad \textbf{(4.2)}$$

where θ_j and θ_k are bus voltage phase angles at buses j and k for all adjacent pairs $j, k \in \{1, 2, \ldots, n\}$ in an n-bus network [85]

This second metric follows from the basic AC power flow equations, where the active power transfer from bus j to bus k is proportional to $\sin(\theta_j - \theta_k)$. This limits the amount of power transfer between the buses and results in instability when the voltage phase angle difference exceeds $\pi/2$.

As the dynamic simulations are run, if either of **(4.1)** or **(4.2)** is true, the simulation is stopped, and the instability-inducing attack and system parameters are recorded.

4.3. Model systems and Choice of Troublesome Frequencies

Simulations are run on two test networks – the IEEE 9-bus dynamic test case, and the IEEE 39-bus dynamic test case, which models the New England power system. The base case for the test cases were left unchanged from the standard IEEE cases with the exception of the machine damping coefficients. In both test cases, each load bus can be thought of as representing an entire distribution network. The 39-bus case includes one bus which represents the interconnection of the New England network with the rest of the eastern bulk power grid.

Figure 4.1. is a graphical representation of the IEEE 9-bus dynamic test case, and Figure 4.2. is graphical representation of the IEEE 39-bus dynamic test case[10].

[10] See Appendix A for sample data files used to perform the simulations in PSAT.

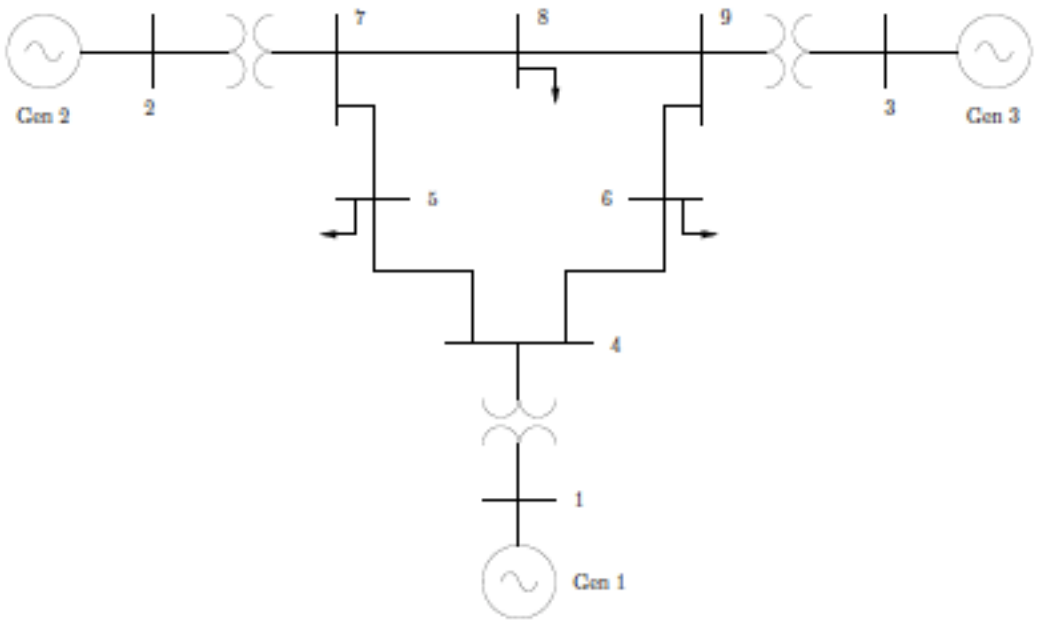

Figure 4.1: The 9-bus IEEE test system contains 3 generators and 3 loads [87].

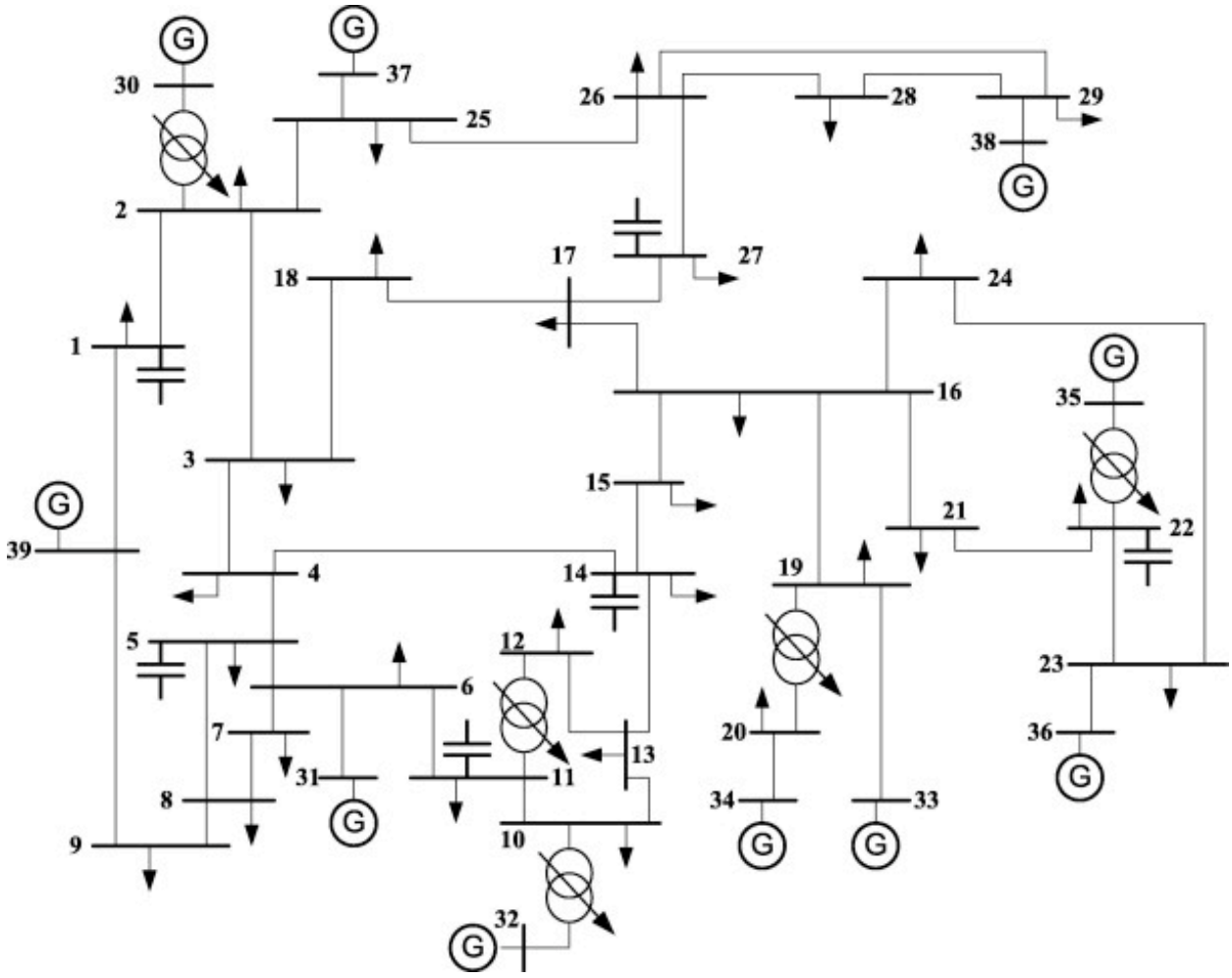

Figure 4.2: The 39-bus IEEE test system contains 10 generators and 30 loads. [89]

For each of the test systems a set of natural frequencies (also referred to as "eigenfrequencies" or "natural modes"), is computed by performing an eigenvalue analysis in PSAT. An eigenvalue analysis provides information about the damped and undamped oscillations inherent to the system being studied, prior to any externally introduced perturbations [85]. Additionally the "damping coefficient", which ranges from -1 to 1, describes the extent to which the natural modes are damped, with positive damping coefficients representing damped

oscillations, and negative damping coefficients representing undamped oscillations. An adversary seeking to exploit system vulnerabilities before launching an oscillatory attack will likely do so at frequencies that are known to be troublesome.

It is, of course, most unlikely that an attacker will have access to the precise eigenfrequencies of a system at each operating condition. So results are obtained for a few different frequencies within this range. The chosen frequencies are those which an intelligent attacker is likely to use when launching an attack.

4.4. System Loading

The effect of an external perturbation introduced to the electric grid, or on any system, is bound to have varying effects depending on the pre-perturbation state of the system. If a system is heavily stressed to begin with, it is likely that even a small disturbance will have notable effects. On the other hand, if the system is functioning well below operational limits, it is unlikely that small disturbances will have a substantial effect on the system. In order to capture this variable effect of external perturbations as a function of the initial stress level of the system, simulations of the oscillatory attack are performed on test cases representing various levels of system stress.

Loading scenarios representing various levels of system stress are created from a base test case by multiplying the active power (P_L) components of system loads by a different base load multiplier, λ, for each case. Additionally, the active power (P_G) output of system generators are multiplied by λ, and the maximum power outputs of system governors (TG) are multiplied by λ*1.1 and the minimum power output is set to 0.

For example, for $\lambda = 1.5$, a test case lambda1pt5 is created, where for each of M loads, N generators, and K governors in the test system,

$$P_{Lm} = 1.5*P_{Lm}^{0}, \ \forall\ m \in \{1,...,M\} \quad \textbf{(4.3)}$$

$$P_{Gn} = 1.5*P_{Gn}^{0}, \ \forall\ n \in \{1,...,N\} \quad \textbf{(4.4)}$$

$$TG_{k} = 1.5*1.1*TG_{k}^{0}, \ \forall\ k \in \{1,...,K\} \quad \textbf{(4.5)}$$

where P_{Lm}^{0} is the base case active power component of the m^{th} load, P_{Gn}^{0} is the base case active power component of the n^{th} generator, and TG_{k}^{0} is the base case maximum active power output limit for the k^{th} governor. The λ-scaled maximum power output for each of the governors is multiplied by 1.1 to capture the flexibility around a dispatch point that a governor typically provides. A set of loading scenarios is created for the 9-bus network and the 39-bus network. These loading scenarios are referenced in Section 4.7., which describes the steps involved in implementing the oscillatory attack.

Generation and turbine governor limits are increased in conjunction with load increases in order to mimic a stressed state that does not place artificial strain on system controls. That is, if only the load were scaled up, then the entire burden of handling the extra system load with all else remaining the same would fall on system controls creating vulnerabilities prior to any sort of attack being launched at all. Hence, in order isolate the effects of the oscillatory attack on the system, generation and governor limits are ramped up as system loads are increased.

Different test networks are likely to have different base case operating points. For instance, the base case 39-bus system represents a higher stress level than the base case 9-bus

system. In order to create a way to compare results across different cases, a normalized measure of system stress, μ, is defined. For each of the 9 and 39-bus test cases, first a λ_{max} is identified, where λ_{max} is found by increasing λ incrementally until a stress level is reached where the static power flow solution cannot be found. The λ corresponding to this system limit is set as λ_{max}. Using this λ_{max}, μ is defined for each loading scenario as:

$$\mu = \lambda / \lambda_{max} \quad \textbf{(4.6)}$$

$\mu = 1$ represents the loading scenario associated with the static power flow limit, i.e., the lowest level of system loading for which a static power flow solution cannot be found. In figures 4.4-4.9 that follow, μ is used as the x-axis variable.

It should be noted, however, that other differences in the fundamental dynamics of these two test systems (other than just the base case stress levels of the two systems) makes any truly comparative study difficult unless great care is taken to normalize all relevant system parameters. The stress measure μ is developed as a first step towards being able to generalize results obtained from a set of test cases, since such generalization is one of the key reasons to perform simulations on multiple test systems in the first place.

4.5. Load modeling

In stability studies the modeling of loads is both a complicated as well as important step. The complexity is due to the fact that it is difficult to accurately characterize aggregated system loads, which can be a mix of different types of lightning, refrigeration, heater and motor loads.

For the purposes of simulation studies loads are broadly classified into two types: static and dynamic loads. Here "static" and "dynamic" do *not* refer to whether the load profile remains the same or changes during the course of a simulation but rather these words are used to describe the *sensitivity* of the load on a bus to variations in the voltage at that bus.

Results are obtained for two types of static load models. The first is a constant power load model, and the second is a constant impedance load model. A "constant power load" refers to a load whose real and reactive components have no relationship to the voltage magnitude, and a "constant impedance load" refers to a load whose real and reactive power components are proportional to the square of the voltage magnitude. A third type of static load model is the "constant current" load model, where the real and reactive components have a linear relationship to the voltage magnitude. This load model is not included in the analysis that follows because its behavior can be bounded between the other two load models in term of severity [85].

All three load models can be described by the following generalized exponential model that describes the load response in terms of the real and reactive power injections:

$$P = P_0 (V/V_0)^{\alpha} \quad \textbf{(4.7)}$$

$$Q = Q_0 (V/V_0)^{\beta} \quad \textbf{(4.8)}$$

P_0, Q_0, and V_0 are obtained through the static power flow analysis, and depending on the values of α and β, the load response is modeled as constant power ($\alpha = \beta = 0$), constant current ($\alpha = \beta = 1$), or constant impedance ($\alpha = \beta = 2$) [85].

Of the three static load models described, the constant power load model is the least forgiving of system stresses because loads modeled as constant power continue to consume the

same amount of power irrespective of voltage fluctuations. Another way to think of this is that constant power loads draw more current during under-voltage situations, thereby further contributing to system stress. On the other hand constant impedance loads smother the effect of voltage fluctuations by drawing less current during under-voltage situations and thereby help to alleviate system stress.

4.6. Power System Analysis Toolbox (PSAT)

All simulations are run using PSAT, an open source tool that operates on the MATLAB platform and can be used to perform static and dynamic power system analyses. PSAT was chosen as the analysis tool for many reasons including transparency and ease of use. But the most attractive feature of PSAT is that its open architecture allows users to create highly customized definitions and implementations of system perturbations by directly changing various system parameters in a MATLAB file. For a thorough description of PSAT see [87, 88].

PSAT contains modules that perform static analyses such as optimal and continuation power flow analyses, and dynamic analyses such as small-signal stability and time-domain simulations which are completed after the basic power flow equations are solved. As do several power system software packages, PSAT uses the Newton-Raphson numerical method to solve the steady state power flow problem. For time domain simulations, PSAT offers two implicit integration methods to update the algebraic and differential variables at each step. The more commonly used Trapezoidal Method is used to perform all simulations in this thesis. For each step of the time domain simulation PSAT accesses a custom perturbation file that describes the oscillatory attack as a function of time, evaluates the disturbance, and updates all system variables. The simulation advances to the next time step until the specified simulation end time

is reached, unless the system becomes unstable per one of the instability metrics described above.

4.7. Attack Implementation

The following two broad steps are involved in implementing the oscillatory attack:

1. A set of test cases representing different loading scenarios is created from the base test case for each of two test networks (described in Section 4.5.). The process of creating these loading scenarios is described in Section 4.6.
2. For each loading scenario, and for each of a few different oscillatory attack frequencies, the fraction of system load that is oscillated is gradually increased and for each increase a time domain simulation is run. This oscillated load fraction is increased until the system becomes unstable according to one of the two instability metrics described in Section 4.2. This instability-inducing load fraction is recorded as the lowest requisite oscillated load fraction that destabilizes the system.

The actual cycling of loads is performed through a custom perturbation file that is accessed at each time step of the time domain simulation, which is run after a static power flow is completed. This perturbation file toggles the P and Q values of system loads between the specified fraction and 100% for the duration of the attack. For instance, if the desired oscillated load fraction is 20% and the oscillatory frequency is 0.2 Hz, then the perturbation file cycles the P and Q values of all system loads between 80% and 100% every 5 seconds.

The base case sets of results for both 9-bus and 39-bus IEEE test systems are obtained by running the time domain simulation for 120 seconds, with an attack duration of 60 seconds. For each time step of the time domain simulation, the perturbation file is accessed, and the disturbance is evaluated. Figure 4.3. shows a schematic of the steps involved in implementing the attack.

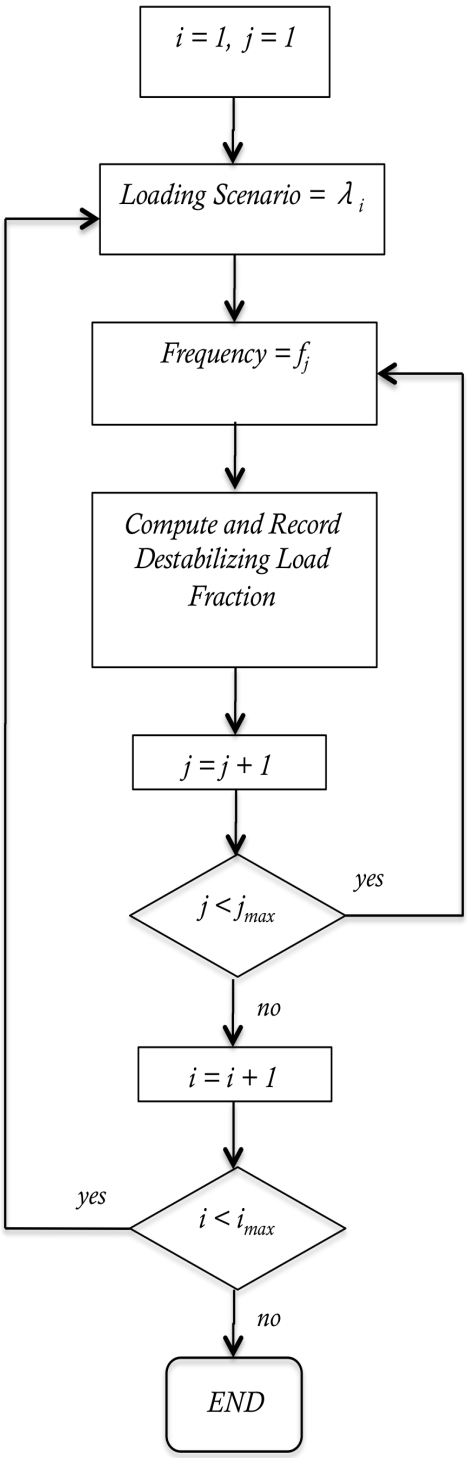

Figure 4.3: After a set of loading scenarios is created with each scenario represented by λ_i for each λ_i and for each of a set of oscillatory frequencies, f_i, the requisite system load fraction that needs to be oscillated in order to make the system unstable is computed as described and recorded. The process is repeated until simulations are run for the complete set of loading scenarios and the set of chosen oscillatory frequencies.

Figures 4.4. and 4.5. show voltage profiles resulting from sample time domain simulations run on the 9-bus test system with Figure 4.4. representing a stable case, and Figure 4.5. representing an unstable case.

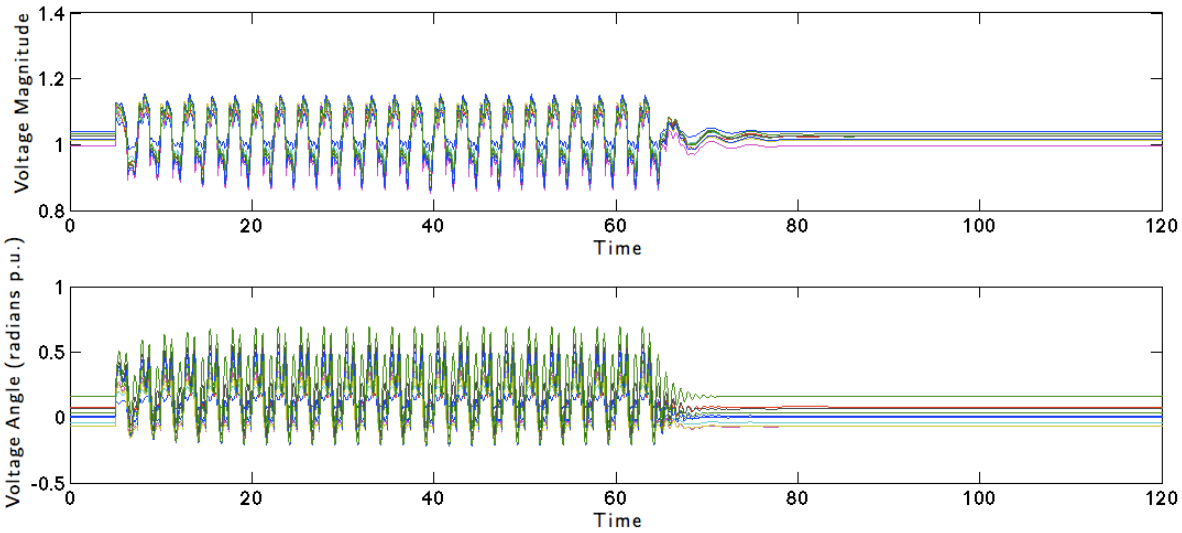

Figure 4.4: Here 95% of system load is oscillated at a frequency of 0.4 Hz for 60 seconds for λ = 1. Once the attack is stopped, the system returns to its pre-disturbance, steady state mode of operation.

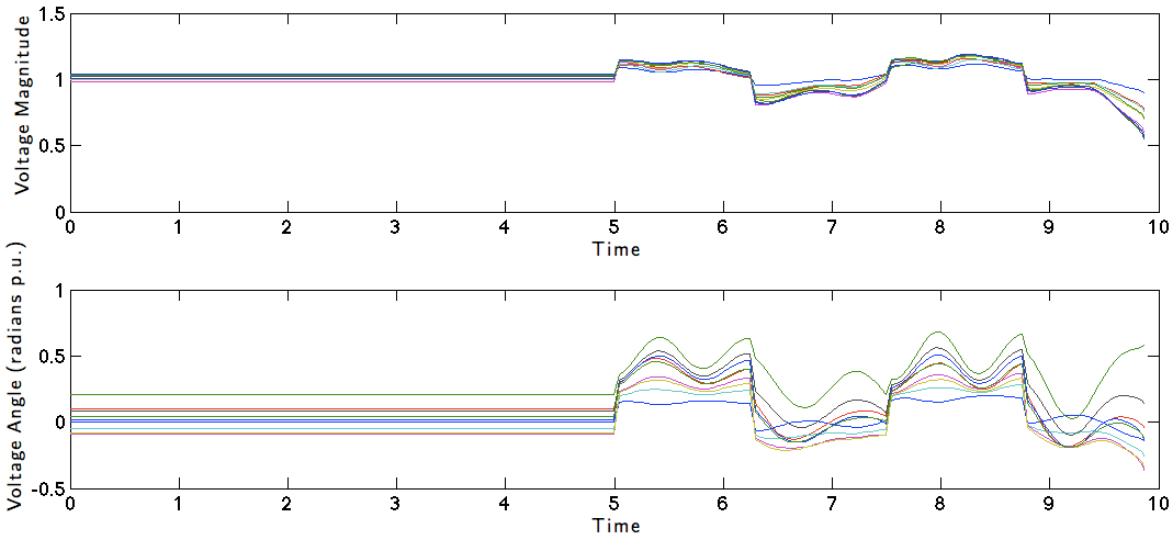

Figure 4.5: Here 95% of system load is oscillated at a frequency of 0.4 Hz for 60 seconds for $\lambda = 1.28$. The attack perturbs the system sufficiently to destabilize it a little before t = 10 seconds.

4.8. Results

Using the method described in Section 4.7. the minimum requisite oscillated fraction of system load that is needed to destabilize each of the two systems (9-bus and 39-bus IEEE dynamic test cases) for each of four different oscillatory frequencies and for each of two load models (constant impedance and constant power) was computed. The results are presented in Figures 4.6-4.9. The x-axis is μ, which is the measure of system stress defined and described in Section 4.4. Each value of μ represents a different system loading scenario. The y-axis represents the requisite oscillated load fraction that induces instability per one of the two instability metrics (see Section 4.1.) for each loading

scenario. $\mu = 1$ represents the loading scenario for which the static power flow equations cannot be solved, i.e., the case where $\lambda = \lambda_{max}$.

For each of Figures 4.6.-4.11. the caption includes the requisite load fraction that induces instability for $\mu \approx 0.6$ to provide a comparative sense of the results for the different test systems and load models.

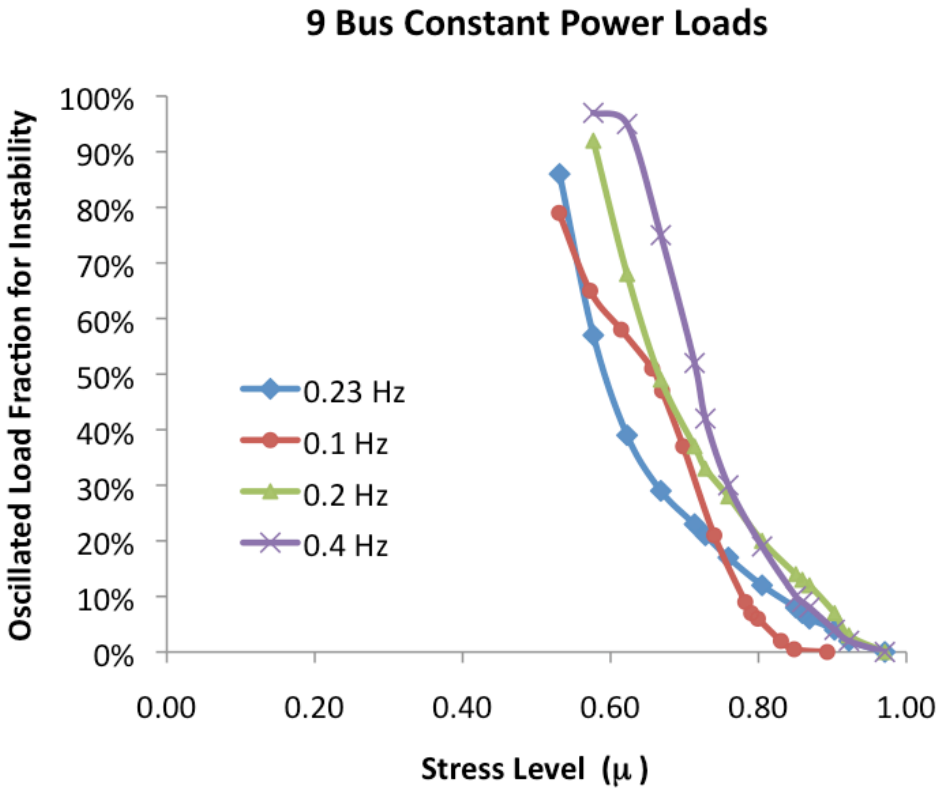

Figure 4.6: Here loads are modeled as constant power loads, meaning that the power consumption at each load bus has no relationship to the voltage magnitude at the bus. The fraction of system load that needs to be oscillated in order to induce instability reduces as a nonlinear function of the system stress level, μ . For $\mu = 0.62$, the lowest destabilizing fraction of oscillated load across the different oscillatory frequencies is 39%, and of the oscillatory frequencies simulated, a frequency of 0.23 Hz consistently requires the least amount of oscillated load to destabilize the system.

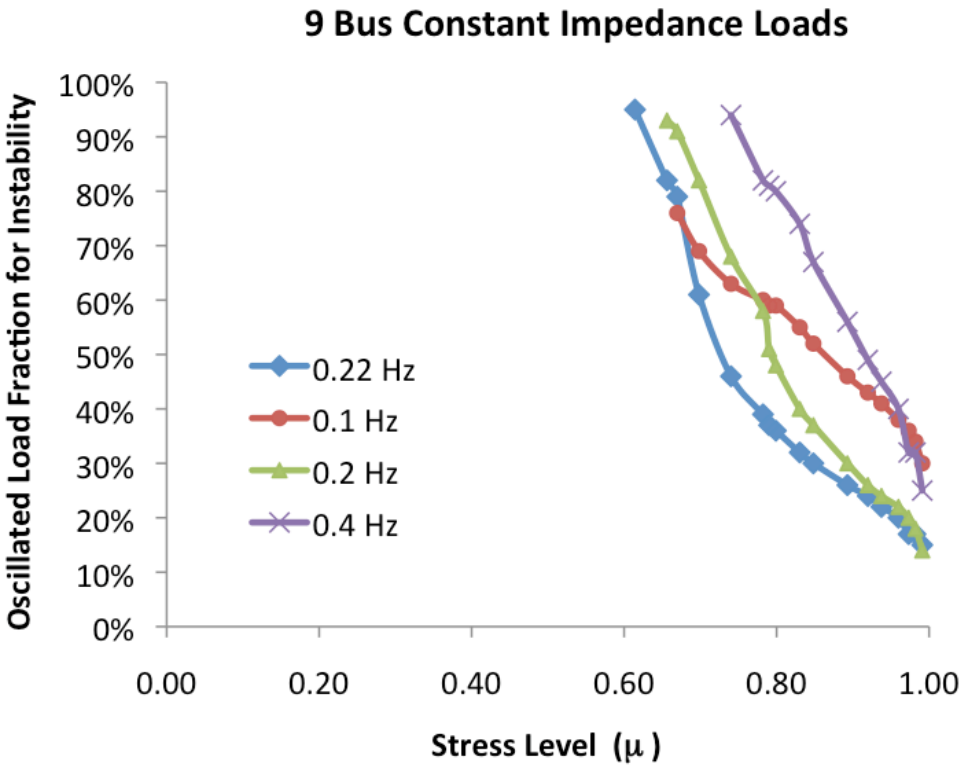

Figure 4.7: Loads are modeled as constant impedance loads, meaning that the power consumed at each load bus is proportional to the square of the voltage magnitude at the bus. For μ = 0.61, the lowest destabilizing fraction of oscillated load across the different oscillatory frequencies is 95%.

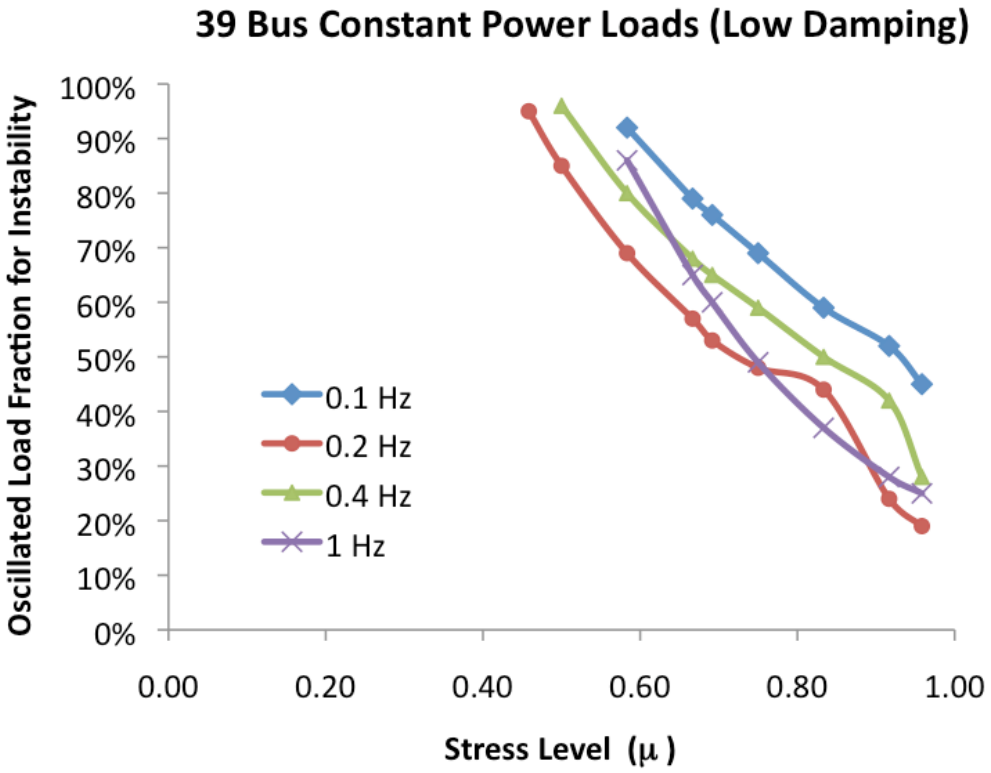

Figure 4.8: Loads are modeled as constant power loads, and the "Low Damping" refers to the machine damping coefficients (D) in the test system. A uniform value of D=0.005, the same value used for the 9-bus system, is assigned to all machines. For μ = 0.58, the lowest destabilizing fraction of oscillated load across the different oscillatory frequencies is 69%.

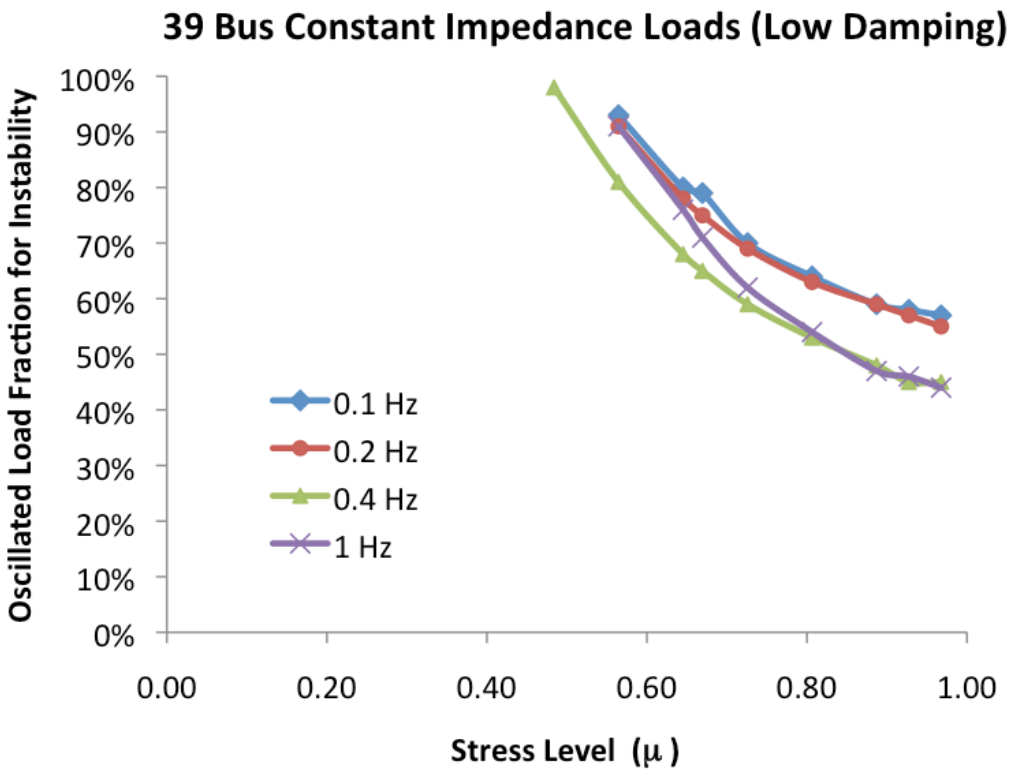

Figure 4.9: Loads are modeled as constant impedance loads, and the "Low Damping" refers to the machine damping coefficients (D) in the test system. A uniform value of D=0.005, the same value used for the 9-bus system, is assigned to all machines. For μ = 0.56, the lowest destabilizing fraction of oscillated load across the different oscillatory frequencies is 81%.

The results presented in Figures 4.6.-4.9. can be interpreted in several ways. First, while it is difficult to estimate the range of 'normal' operating conditions for the electric power system at large, the results indicate that unless the system is operating very close to its steady state stability margin (e.g. $\mu > 0.9$), the fraction of system load that needs to be oscillated to induce instability is larger than 30% except in the 9-bus case with loads modeled as constant power.

Overall the 39-bus test case appears to be more robust when subjected to perturbations spanning the attack parameter space. The 9-bus case proved to be a useful starting point to design and validate the simulation methodology. But since the 39-bus case is more representative of a real power system (it is modeled after the New England power grid and includes a point of interconnection to the main grid) the discussion of results that follows is focused on this test system.

Assuming roughly that each smart meter controls between 2 and 10 kW of load, even the lowest requisite oscillated load fraction that induces instability in the 39-bus case (19% of system load for $\mu = 0.96$ and with a constant power load model) translates to between 130,000 to 660,000 meters. For a less stressed loading scenario represented by, e.g., $\mu = 0.5$, the lowest oscillated load fraction that induces instability is 85%, which translates to between 300,000 to 1.5 million meters[11]. These results indicate that, given the inherent heterogeneity of deployed smart meters across the nation and assuming that the test case is reasonably realistic, it is likely infeasible for even a determined adversary to gain control of a sufficient number of meters to destabilize the bulk power grid. Replicating the type of analysis presented in this chapter for different and larger test systems would help to understand the extent to which these results represent reality.

The results indicate that the choice of load model has a significant effect on how the system responds to a perturbation. Not surprisingly and consistent with equations

[11] The non-linearity in the number of meters needed follows directly from the non-linear system response to perturbations with increasing stress levels.

(4.7) and **(4.8)** that describe the behavior of these load models, the choice of a constant power load model causes the system to respond more severely to perturbations than when a constant impedance load model is chosen. For the purposes of a worst-case analysis and when picking among static load models, it is useful to use the constant power model. Depending on the load model that is used, the attack frequency that has the most destabilizing effect varies. The 0.2 Hz attack frequency proves to be, for a large subset of the attack parameter space, the most troublesome for the constant power load model case, while the 0.4 Hz attack frequency causes the most damage in the constant impedance load model case.

4.9. Discussion and Conclusions

The base set of results spans a relatively diverse set of system states and attack attributes. Though it would be ideal to do so, it is clearly impossible to fully characterize the state of a target system or the nature of the attack that an adversary might launch on that system in order to predict the effects of the attack. So a reasonable approach was used to treat uncertainties parametrically and create a space of possible outcomes based on a set of likely system conditions and attack attributes. Namely, for each loading scenario for a given test network, the oscillated load fraction needed to make the system unstable at the corresponding stress level was calculated for a range of different system and attack parameters.

A few attack attributes that are not varied in the base set of results include the attack *duration* (which is set at 60 seconds), and the *manner* in which the attack is implemented (for e.g., one attack scenario could be where the oscillatory attack is implemented in a staggered way to account for inherent communication and physical latencies in the AMI). Similarly certain parameters that play a role in the dynamics of the test systems, such as the *machine damping coefficients* are not varied. Additionally, *dynamic load models* were not used in any of analyses performed.

A few tests were run to characterize the sensitivity of results to the attack duration. First, with all else remaining the same (an assumption implicit in the rest of this discussion), a longer duration attack (120 seconds instead of 60 seconds) was simulated for a few low and high loading situations to see if the oscillated load fraction needed to destabilize the system reduced in size. This spot-check approach showed that the attack duration did not have an effect on the load fraction required to destabilize the system. Similar tests were not run for mid-loading situations because an examination of the simulation times at which instability occurred for these cases showed that in all cases the system became unstable for $t < 60$ seconds.

The potential effect of staggering the oscillatory attack, i.e., keeping the oscillatory attack frequency the same but cycling subsets of system load in phases, was not studied because it is assumed that any inherent system latencies are more likely to alleviate rather than exacerbate the effects of the attack. That is, it is assumed that a perfectly coordinated attack, which is what is simulated in this analysis, is more likely to represent a worst-case scenario. It is possible that, depending on how system latencies

accumulate over time, that for some attack frequencies and depending on some system dynamics and control mechanisms, latencies might contribute to the system becoming unstable faster. But the design and implementation of a simulation to answer this question is left as future work.

The machine damping coefficients, which are one of a few different mechanisms that work to dampen inherent oscillations in the system as a whole, naturally have an effect on the extent to which external perturbations are able to destabilize the system. The damping coefficients vary across different available dynamic test cases. In an attempt to understand the role of the damping coefficient, in addition to the results presented for the 39-bus network above, an additional set of results (Figures 4.10. and 4.11.) was obtained for the choice of a larger machine-damping coefficient [85]. These results show that the choice of damping coefficient does have a significant effect on results. But since the following results represent a *more* robust system than the one used to obtain results in Figures 4.8. and 4.9., for the purposes of a worst-case analysis, the effect of the larger damping coefficient does not change the implications of the work.

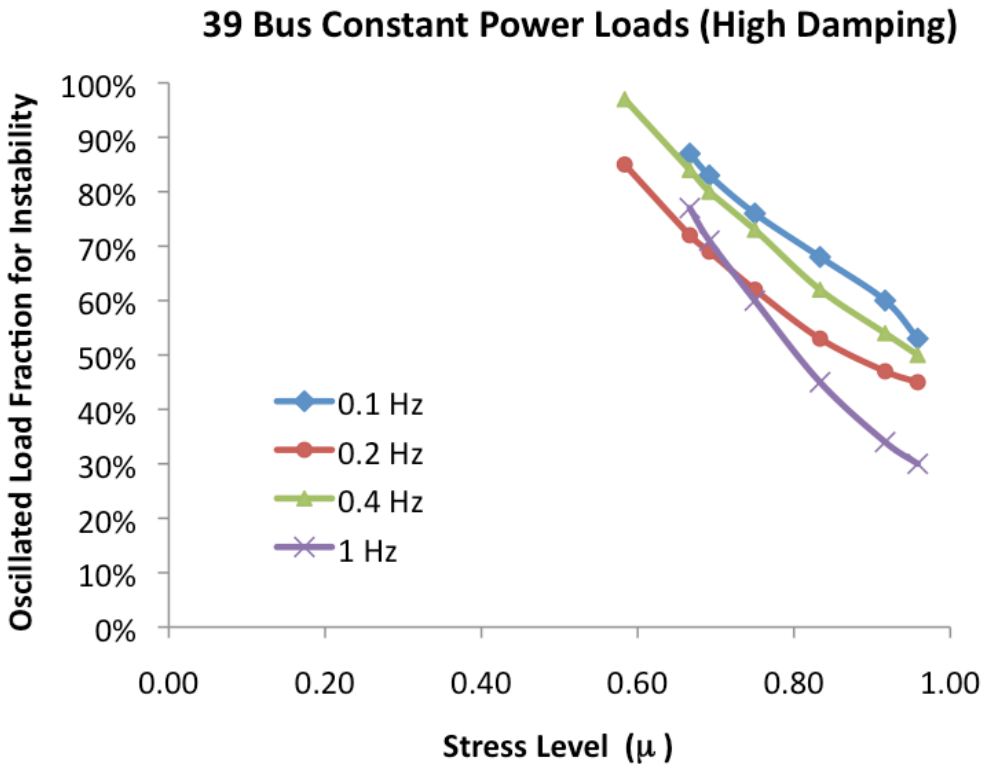

Figure 4.10: Loads are modeled as constant power loads, and the "High Damping" refers to the machine damping coefficients (D) in the test system. A uniform value of D=25 is assigned to all machines. For μ = 0.58, the lowest destabilizing fraction of oscillated load across the different oscillatory frequencies is 85%.

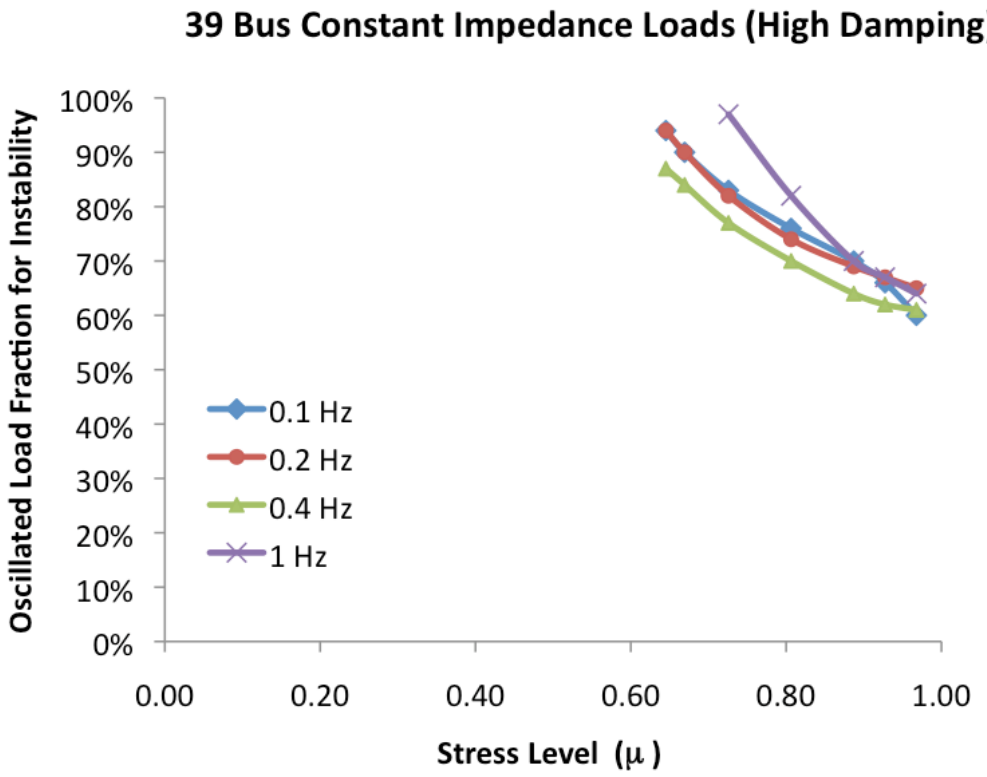

Figure 4.11: Loads are modeled as constant power loads, and the "High Damping" refers to the machine damping coefficients (D) in the test system. A uniform value of D=25 is assigned to all machines. For μ = 0.56, the lowest destabilizing fraction of oscillated load across the different oscillatory frequencies is >100%.

Lastly, dynamic load models are not used in any of the simulations. For instance, loads such as induction motors cannot be sufficiently represented through static load models, and researchers have demonstrated the role that load modeling plays in stability studies [90]. But currently PSAT does not support the implementation of dynamic changes to dynamic loads. So the task of incorporating them is left as future work. As already noted, load modeling is commonly acknowledged as a difficult task in power system modeling and simulation studied. Regardless, the quantitative framework

established in this work and illustrated through the static load model cases should provide a useful starting point for analyses that use more complex representations of the system.

The difference in results between the 9 and 39-bus test systems shows that the way these systems respond to external perturbations is significantly affected by the composition of the systems. Hence it is difficult to make conclusive claims about the effect of the studied attack, or any attack on the electric power grid without replicating results across a sufficiently large set of test cases and attack attributes.

But the completed work provides a good first order bounded estimate of the effects of a large-scale oscillatory attack launched on the bulk power grid using smart meters. Further, this work also provides a systematic quantitative framework for thinking about the problem and can be used as a starting point for further work in the area.

The analysis of the stability of power systems under duress is not a new topic. But the changing landscape of the power delivery system has exposed a new set of vulnerabilities inherent to the electric grid. For instance, an oscillatory attack of the type outlined in this chapter would have been quite difficult if not impossible to launch prior to the existence of remotely addressable meters with disconnect functionality and the necessary accompanying information technology architecture. Analyzing and safeguarding against such new vulnerabilities requires new tools or modifications to existing tools that help to appropriately reframe the stability problem. Through experimentation we established that the current limitation in the PSAT architecture prevents the implementation of the oscillatory attack scenario if system loads are characterized using any of a set of dynamic load models including induction motor

models[12]. A future release of PSAT may fill in some of the holes in the software architecture that make the oscillatory attack implementable for all load characterizations.

4.10. Future Work

Some areas for further research stemming from work presented in this chapter include the following:

- *Incorporate dynamic load models (e.g., induction motor loads) into the analysis to observe how the results change.* As contrasted with a static load model which expresses the characteristics of a load at any instant in time as an algebraic function of the voltage magnitude and angle at that instant, a dynamic load model characterizes the load as a function of the voltage at that instant *as well as* at a past instant in time. Effectively, dynamic load models can be seen as capable of accounting for the inertia of the system.
- *Run simulations on a few test cases that include mixed load models.*
- *Stagger the oscillatory attack across subsets of system loads to mirror inherent latencies in communications and physical relays in a real*

[12] The specific trouble with implementing dynamic load models in PSAT is that these loads can only be individually oscillated though the use of a switch or breaker. But at the point of reconnect, when the switch is closed after having been opened, PSAT does not accurately update all relevant differential and algebraic variables. In a broad sense PSAT is unable to correctly handle islands, which are created when loads are disconnected via a breaker.

network to observe the effects on system stable; does such staggering tend to exacerbate or alleviate frequency deviations?

- *Perform simulations on larger test systems.* Larger systems tend to have higher inertia, potentially reducing the effect of perturbations.

CHAPTER 5

Overview of Policy Implications

This chapter presents consolidated policy implications of the work completed in Chapters 2 and 4. Section 5.1. identifies obstacles to implementing the strategy proposed in Chapter 2 for sustaining socially critical services during blackouts and provides a few recommendations. Section 5.2. discusses some of the policy implications of the work completed in Chapter 4.

5.1. Smart Grid for Critical Mission Survival: Obstacles to Implementation and Remedies

There are currently many obstacles that prevent a scheme such as the one proposed in Chapter 2 from being implemented in the U.S. First, "distributed generation" has been shown to be most economical when allowed to supply power to several customers through a "microgrid." [91]. Here the term microgrid is used to refer to the following, a definition presented by King: "…a small group of customers, interconnected at low voltages on a local power grid with a single point of interconnection with the area electric power system (i.e. utility distribution grid). On-site distributed generation resources are integrated with the HVAC system to allow combined-heat-and-power applications, and the entire system (i.e. electricity and heat supply systems;

interconnection switches) is managed with “smart controls” that ensure reliability and optimize operation to minimize costs.” [92]

The primary deterrent to the proliferation of such microgrid systems in the U.S. is that “exclusive service territory” rights essentially make it illegal to operate microgrids in several states. These rights granted to utilities make it impossible or very difficult for private owners of distributed generation resources to sell power to anyone other than the power company [93].

Second, utilities all across the country have been installing smart meters, but they have no incentive to make the modest investments in the controls and automation equipment needed to implement the strategy proposed in this work. Third, even if a utility wanted to make such investments, currently it has no way to pay for them.

A few regulatory and policy changes could help create a conducive environment for ensuring the provision of critical social services during large blackouts through local means. First, state laws could be modified to allow private owners of distributed generation resources to share their power with a small network of customers.

Second, state PUCs could deem the necessary distribution system upgrades to be a prudent investment, or local, county or state government could choose to fund the project with tax revenue, contracting with the local distribution utility and other parties to implement the changes. Establishing dedicated sources of funding for these upgrades might attract at least a few utilities to invest in them.

Third, in states such as Pennsylvania that incentivize CHP distributed generation sources, the enabling legislation could be modified to incentivize DG owners to install additional capacity that they would contract to share during emergencies. The Pennsylvania Alternative Energy Portfolio Standards Act allows net metering[13] for private owners of 3-5 MW generators on the condition that they serve the primary or secondary purpose of maintaining critical infrastructure. Owners of units that are smaller than 3 MW can participate in net metering irrespective of whether they share any of their electricity with critical infrastructures in times of need [95]. The law could be amended to allow participation in net metering only if owners of units smaller than 3 MW also agree to share power during emergencies. A DG owner for whom net metering is sufficiently beneficial [92] might agree to bear the entire cost of installing necessary distribution automation equipment.

Fourth, agencies such as the U.S. Department of Energy, could fund projects that further the work presented in Chapter 2. For instance, there are many unanswered questions related to the technical design and operation of microgrid systems that can operate in conjunction with the main grid while being also being optimized for providing power to critical missions during emergencies. Another area of research is in the design of fair incentives for DG owners who are willing to share their power during

[13] The Energy Policy Act of 2005 defines net metering as "…service to an electric consumer under which electric energy generated by that electric consumer from an eligible on-site generating facility and delivered to the local distribution facilities may be used to offset electric energy provided by the electric utility to the electric consumer during the applicable billing period." [94]

emergencies. The rental cost proposed in Chapter 2 can be seen as a rough starting point with much room for refinement.

There are a few concerns that parties undertaking the implementation of the proposed strategy should bear in mind. For instance, if a region does choose to invest in a system of the type we have outlined, then it will face the task of negotiating a set of contractual and other agreements with private firms such as gas stations and food stores, as well as service providers such as police and school systems to determine which will be powered in an emergency. These agreements should specify how cost and revenues are allocated.

Further, if upgrades are not geographically widespread, then in the event of a major disruption regions that have secured their social services could find themselves inundated by people from neighboring regions to use services during blackouts. This potential predicament argues for implementation at a state level, or perhaps even national level, with support from the Department of Homeland Security.

5.2. Implications of Smart Meter Attack Work

Chapter 4 presented results of a simulation that was designed to estimate the effects of an attack launched on the electric grid through the manipulation of a large number of smart meters. This section describes a few implications stemming from and related to the work completed in Chapter 4.

First, the completed work provides a quantitative framework that can be used to conduct simulation studies spanning different smart grid elements and attack types. The designed simulation is inherently adaptable through small modifications to the attack driver file because the specific smart grid elements – smart meters in this case – are treated as black boxes and can be replaced with any other element of interest whose vulnerabilities are known. For instance, the same simulation setup could be used with a minor adjustment to the attack algorithm to mimic fluctuations in demand resulting from the broadcast of spurious price signals. The use of a quantitative framework such as the one presented can help to systematically identify and rank smart grid security risks.

Second, the completed work highlights a fundamental need in the smart grid space to let objectives guide functionality instead of the other way around. For example, regardless of whether the remote disconnect switch could be used to launch a malicious attack (results from the analysis performed in Chapter 4 suggest that it likely could not), would the inclusion of a built-in random delay in smart meter response times hinder the intended objectives of the remote disconnect functionality? If not, such a measure, depending on its cost, could be a worthy safeguard. In addition to such *component-level* assessments of objectives and effectiveness, a *systemic* assessment approach that pays special attention to the interactions between various parts of the smart grid could help to strike an overall balance between increased functionality and reduced vulnerabilities. Such a consolidated approach is in line with recommendations made in the 2010 DHS report on cyber-physical system security [76].

Third, the simulation designed in Chapter 4 identified limitations of the PSAT software with regards to using dynamic load models for the purposes of simulating an oscillatory attack of the studied type. Such limitations could well exist in other, similar dynamic power system analysis tools. Publishing this work could bring attention to current deficiencies in modeling software packages that serve the specific need of performing dynamic simulations of power systems – a need that is likely to grow with the increasing complexity of the smart grid and the accompanying set of unknowns.

Lastly, in studying the current environment for the evolution of smart grid standards and regulations, it is clear that there is a need to consolidate efforts and share knowledge when possible. Some effort has already been directed towards this objective. For example, in 2010 the DOE established the National Electric Sector Cybersecurity Organization (NESCO) to coordinate cybersecurity efforts. NESCO operates under the wing of EnergySec, a non-profit organization dedicated to "strengthening the cybersecurity posture of critical energy infrastructures", and in conjunction with the Electric Power Research Institute (EPRI) as the research arm [96]. Other such collaborations are necessary and critical, especially among universities, the utility sector, governmental agencies and regulators.

CHAPTER 6

Conclusions

This dissertation accomplished the following:

1. Devised a strategy to sustain socially critical services during widespread and extended power blackouts and estimated associated costs.
2. Identified holes in the policy and regulatory framework that prevent such a scheme from being implemented.
3. Designed and presented results of a simulation that was formulated to estimate the size of a smart-meter based attack that is capable of destabilizing the bulk power grid.

In Chapter 2 a load cycling based method that employs individually addressable smart meters and distributed automation and controls to selectively serve a subset of socially critical loads during long-duration and widespread power outages was developed. Additionally, the incremental costs associated with implementing such a method were estimated. The proposed strategy can be seen as an application of the broad concept of survivability engineering to the provision of critical services during large-scale grid failures. The performed analysis indicates that the costs involved in implementing the outlined system constitute less than 1% of median annual household income in the United States for a variety of assumptions regarding the amount of DG

resources available to a region. A few areas for further work stemming from the completed work include: 1) Identifying technical constraints specific to microgrids that are designed for the dual purpose of providing power during blackouts and otherwise, 2) Conducting a survey to estimate consumer willingness to pay for a scheme that would allow for a subset of critical social services to continue being powered during a blackout, and 3) Varying the mix of generation sources and reassessing associated costs.

Chapter 3 provided an overview of advanced metering infrastructure and described a few different feasible smart meter based attacks on the electric power grid such as energy fraud, denial of service and the targeted disconnect attack. One specific application of the targeted disconnect attack type was brought into focus – the cycling of a large number of customer loads using the remote disconnect switch functionality in smart metering systems. This chapter also included a brief summary of the standards and regulatory environment for the emerging smart grid and metering systems.

In Chapter 4 a simulation was designed to estimate the effect that the large-scale cycling of customer loads might have on the stability of the bulk power grid. Specifically, the simulation was designed to estimate the fraction of system load that would need to be cycled in order to produce any notably detrimental effects on system stability. Simulations were run on two IEEE dynamic test networks – the 9-bus and 39-bus systems – for a range of different system loading scenarios and attack attributes. Results for the more realistic 39-bus test system indicate that unless the system is operating very close to its steady state stability margin the fraction of system load that needs to be oscillated to induce instability is larger than 30%, making the successful implementation of such an attack extremely unlikely. A few potential ways in which the

work completed in Chapter 4 could be extended include: 1) Incorporating mixed and dynamic load models into the simulation to assess the effect of such variations on results, 2) Staggering the oscillatory attack across subsets of system loads to observe the manner in which system latencies, which were not simulated, exacerbate or alleviate the effects of the attack, and 3) Performing simulations on larger test systems to test the hypothesis that the higher inertia associated with larger systems is likely to further diminish the effect of external perturbations.

Policy implications of the work completed in this dissertation were presented in Chapter 5. In summary, while the technical elements of the scheme proposed in Chapter 2 are largely feasible, a few policy changes are necessary for successful implementation of the scheme. These include: 1) New or improved legislation that would legalize the operation of microgrids, which have been shown to be the most cost-effective configuration for CHP DG units, 2) Incentives (e.g., in the form of PUC provisions for investment) for power companies to invest in the types of upgrades to distribution automation that are needed to implement the proposed strategy, and 3) Investments in research and development (e.g., through DOE grants) pertaining to the design and operation of microgrids that are built with the intention of serving critical loads during grid emergencies.

The work completed in Chapter 4 could inform policymaking by: 1) Providing an adaptable quantitative framework for conducting similar simulation studies in the smart grid space, and 2) Helping to prioritize smart grid security efforts by providing a means for quantifying and ranking the risks associated with different smart grid elements.

References

1. Understanding the Benefits of the Smart Grid. National Energy Technology Laboratory (NETL) Report DOE/NETL-2010/1413. Available at: http://www.netl.doe.gov/smartgrid/referenceshelf/whitepapers/06.18.2010_Understanding%20Smart%20Grid%20Benefits.pdf
2. Recovery Act Selections for Smart Grid Investment Grant Awards – By Category Updated July 10. Department of Energy. Available at: http://energy.gov/downloads/recovery-act-selections-smart-grid-investment-grant-awards-category-updated-july-2010
3. U.S.-Canada Power System Outage Task Force. (2004) Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations. [Online]. Available at: http://www.nerc.com
4. Hines, P.; Apt, J.; Talukdar, S.; , "Trends in the history of large blackouts in the United States," Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century, 2008 IEEE , vol., no., pp.1-8, 20-24 July 2008
5. J. Apt, L. B. Lave, S. Talukdar, M. G. Morgan, and M. Ilic (2004). "Electrical Blackouts: A Systemic Problem." Issues in Science & Technology 20(4):

6. 55–61.Ellison, R.J.; Fisher, D.A.; Linger, R.C.; Lipson, H.F.; Longstaff, T.A.; Mead, N.R.; , "Survivability: protecting your critical systems," *Internet Computing, IEEE* , vol.3, no.6, pp.55-63, Nov/Dec 1999
7. Howard F. Lipson and David A. Fisher. 1999. Survivability\—a new technical and usiness perspective on security. In *Proceedings of the 1999 workshop on New security paradigms* (NSPW '99). ACM, New York, NY, USA, 33-39.
8. Talukdar, Apt, Ilic, Lave, Morgan. (2006) Cascading Failures: Survival versus Prevention. The Electricity Journal, 16(9), 25-31.
9. Perrig - Yilin Mo; Kim, T.H.-J.; Brancik, K.; Dickinson, D.; Heejo Lee; Perrig, A.; Sinopoli, B.; , "Cyber–Physical Security of a Smart Grid Infrastructure," Proceedings of the IEEE , vol.100, no.1, pp.195-209, Jan. 2012
10. Smart Grid Deployment Tracker 3Q10. Pike Research. Available at: http://www.pikeresearch.com/research/smart-grid-deployment-tracker-3q10
11. Cleveland, F.M.; , "Cybersecurity issues for Advanced Metering Infrastructure (AMI)," Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century, 2008 IEEE , vol., no., pp.1-5, 20-24 July 2008
12. Security Pros Question Deployment of Smart Meters. (2010) Wired. Available at: http://www.wired.com/threatlevel/2010/03/smart-grids-done-smartly/
13. Smart Meter Worm Could Spread Like a Virus. (2009) Gigaom. Available at: http://gigaom.com/cleantech/smart-meter-worm-could-spread-like-a-virus/
14. Security Profile for Advanced Metering Infrastructure. (2009). Report prepared by the Advanced Security Acceleration Project (ASAP-WG) for NIST

Cybersecurity Coordination Task Force and the UCAIug. Available at: http://osgug.ucaiug.org/utilisec/amisec/Shared%20Documents/AMI%20Security%20Profile%20(ASAP-SG)/AMI%20Security%20Profile%20-%20v1_0.pdf

15. McDaniel et. al. : McDaniel, P.; McLaughlin, S.; , "Security and Privacy Challenges in the Smart Grid," Security & Privacy, IEEE , vol.7, no.3, pp.75-77, May-June 2009
16. Khurana, H.; Hadley, M.; Ning Lu; Frincke, D.A., "Smart-grid security issues," *Security & Privacy, IEEE* , vol.8, no.1, pp.81-85, Jan.-Feb. 2010
17. Smart Meters Not Ready for Primetime. (2009). Technology Review. Available at: http://www.technologyreview.com/view/414563/smart-meters-not-ready-for-primetime/
18. Hacking the Smart Grid. (2010). Technology Review. Availble at: http://www.technologyreview.com/news/418320/hacking-the-smart-grid/
19. Stephen McLaughlin, Dmitry Podkuiko, Adam Delozier, Sergei Miadzvezhanka, and Patrick McDaniel. Multi-vendor Penetration Testing in the Advanced Metering Infrastructure. 26th Annual Computer Security Applications Conference (ACSAC 2010), Austin, TX, USA. December, 2010.
20. High-Impact, Low-Frequency Event Risk to the North American Bulk Power System. Department of Energy and North American Electric Reliability Corporation joint report. June 2010. Available at: www.nerc.com/files/HILF.pdf
21. Common Cybersecurity Vulnerabilities Observed in Control System Assessments by the INL NSTB Program. (2008). Report prepared by the Idaho National

Laboratory for the U.S. Department of Energy. Available at: http://www.inl.gov/scada/publications/d/inl_nstb_common_vulnerabilities.pdf

22. James P. Farwell & Rafal Rohozinski (2011): Stuxnet and the Future of Cyber War, Survival, 53:1, 23-40
23. Fairley, P. The unruly power grid. IEEE Spectrum, 2004; 41(8):22- 27.
24. National Research Council of the National Academies. Severe Space Weather Events: Understanding Societal and Economic Impacts Workshop Report. Washington, DC: National Academies Press, 2008.
25. Klaassen J, Cheng S, Auld H, Li Q, Ros E, Geast M, Li G, Lee R. Estimation of Severe Ice Storms Risks for South-Central Canada. Ottawa (ON): MSC-Ontario Region for the Office of Critical Infrastructure Protection and Emergency Preparedness (Canada); c2003.
26. US Congress Office of Technology Assessment. Physical Vulnerability of Electric System to Natural Disasters and Sabotage. Washington, DC: U.S. Government Printing Office; 1990 Jun. OTA-E-453.
27. Combined Heat and Power Installation Database [Internet]. Washington, DC: Energy and Environmental Analysis, Inc. 2010 – [cited 2010 Jun 10]. Available at: http://www.eea-inc.com/chpdata/index.html
28. King D, Morgan MG. Customer-focused Assessment of Electric Power Microgrids. Journal of Energy Engineering, 2007; 133(3): 150-164.
29. Newsroom: County Business Patterns: A Gas Station for Every 2,500 People [Internet]. Washington, DC: U.S. Census Bureau; 2008 Jun 27 [cited 2010 Apr 15]. Available at:

http://www.census.gov/newsroom/releases/archives/county_business_patterns/cb08-96.html

30. Giant Eagle – Store Locator [Internet]. [place unknown]: Giant Eagle, Inc.; [cited 2009 Sep 1]. Available at: http://www.gianteagle.com/storelocator/default.aspx
31. U.S. Wireless Quick Facts [Internet]. [place unknown]: CTIA – The Wireless Association; [cited 2009 Aug 25]. Available at: http://www.ctia.org/media/industry_info/index.cfm/AID/10323
32. Police Zones Map [Internet]. Pittsburgh: City of Pittsburgh; [cited 2009 Aug 15]. Available at: http://www.city.pittsburgh.pa.us/police/html/police_zones_map.html
33. District Info Source [Internet]. Pittsburgh: Pittsburgh Public Schools; [cited 2009 Aug 15]. Available at: http://www.pps.k12.pa.us/pps/lib/pps/_shared/1340_DistrictGuide_v08.pdf
34. Pittsburgh discussing process to replace 40,000 streetlights. Pittsburgh Post-Gazette [Internet]. 2009 Feb 9 [cited 2009 Jul 13]; News:[about 1 screen]. Available at: http://www.post-gazette.com/pg/09040/947927-100.stm
35. Population Estimates [Internet]. [place unknown]: U.S. Census Bureau; [cited 2009 July 13]. Available at: http://www.census.gov/popest/estimates.html
36. DUQUESNE LIGHT feeder reconf. ref (FOOTNOTE 2)
37. Farrell AE, Lave L, Morgan MG. Bolstering the Security of the Electric Power System. Issues in Science and Technology, 2007 Spring: 49-56.
38. Stauffer RF. Renewable Energy Systems as Emergency Power Sources [Internet]. Washington, DC: US Department of Energy; 1995 Oct [cited 2010 Jun 15]. Available at: http://www.freshstart.ncat.org/articles/enrgsyst.htm#resilient

39. Krikke J. Sunrise for Energy Harvesting Products. IEEE Pervasive Computing, 2005; 4(1): 4-8.

40. SOLAR CHARGER REF (FOOTNOTE 3): http://reviews.cnet.com/4520-11288_7-6427792-3.html)

41. Energy Information Administration - Commercial Energy Consumption Survey [Internet]. [Washington, DC]: U.S. Energy Information Administration; 2008 Sep [cited 2009 Jul 13]. Available at: http://www.eia.doe.gov/emeu/cbecs

42. Regional Municipality of Waterloo – Division 1 Police Station [Internet]. Toronto (ON): Local Authorities Services Ltd.; [cited 2009 Aug 24]. Available at: http://www.amo.on.ca/AM/Template.cfm?Section=Audit_Binder1&Template=/CM/ContentDisplay.cfm&ContentID=154700

43. Timko, Cliff (Engineer, Giant Eagle, Inc., PA). Conversation with: Anu Narayanan (Department of Engineering and Public Policy, Carnegie Mellon University, Pittsburgh, PA). 2009 Jul 31.

44. Commercial and Fleet Dispensers [Internet]. [place unknown]: Gasboy Inc.; 2009 [cited 2009 Aug 5]. Available at: http://www.gasboy.com/page/fleet_commercial_gas_pump_dispensers

45. KWH Consumption and Cost per Square Foot [Internet]. Low Moor (VA): Alleghany County School Board Office; [cited 2009 Aug 25]. Available at: http://www.alleghany.k12.va.us/x_upload/files/Energy_3.pdf

46. Frazier, Ken (Energy Management Coordinator, Pittsburgh School District, PA). Email correspondence with: Anu Narayanan (Department of Engineering and Public Policy, Carnegie Mellon University, Pittsburgh, PA). 2009 Jul 29.

47. Green Issues Challenge Basestation Power [Internet]. Bruxelles, Belgium: EETimes Europe; 2007 Sep 9 [cited 2009 Aug 4]. Available at: http://eetimes.eu/showArticle.jhtml?articleID=201807401

48. Azevedo IL, Morgan MG, Morgan F. The Transition to Solid-State Lighting. Proceedings of the IEEE, 2009; 97(3): 481-510.

49. Anonymous engineers (Unnamed, major electric utility). Personal interview with: Anu Narayanan (Department of Engineering and Public Policy, Carnegie Mellon University, Pittsburgh, PA). 2009 Sep 18.

50. Cooper Power Systems Products [Internet]. [place unknown]: Cooper Industries, Inc.; [cited 2009 Oct 15]. Available at: http://www.cooperpower.com/Products

51. Collier SE. Ten Steps to a Smarter Grid. Industry Applications Magazine, IEEE. 2010; 16(2): 62-68.

52. Anonymous sales representative (Unnamed distribution automation equipment manufacturing company). Email correspondence with: Anu Narayanan (Department of Engineering and Public Policy, Carnegie Mellon University, Pittsburgh, PA). 2009 Nov 13.

53. Conner M. Tamper-resistant smart power meters rely on isolated sensors [Internet]. [place unknown]: UBM Electronics; [cited 2009 Nov 10]. Available at: http://www.ednasia.com/article-23996-tamperresistantsmart powermeters relyonisolatedsensors-asia.html

54. Volkswagen and LichtBlick Partner on Home Combined Heat and Power Systems [Internet]. [place unknown]: Green Car Congress; 2009 Sep 9 [cited 2009 Nov 28]. Available at: http://www.greencarcongress.com/2009/09/volkswagen-

lichtblick-20090909.html

55. CPI Inflation Calculator [Internet]. [place unknown]: Bureau of Labor Statistics; [cited 2010 Apr 15]. Available at: http://data.bls.gov/cgi-bin/cpicalc.pl

56. Catalog of CHP Technologies [Internet]. [Washington, DC]: U.S. Environmental Protection Agency; [cited 2009 Sep 4]. Available at: http://www.epa.gov/chp/basic/catalog.html

57. LaCommare KH, Eto JH. Cost of power interruptions to electricity consumers in the United States (U.S.). Energy, 2006; 31(12):1845–1855.

58. The Economic Impacts of the August 2003 [Internet]. Washington, DC: Electricity Consumers Resource Council (ELCON); 2004 Feb 9 [cited 2010 Apr 21]. Available at: http://www.elcon.org/Documents/EconomicImpactsOfAugust2003Blackout.pdf

59. Morgan G, Apt J, Lave L. The U.S. Electric Power Sector and Climate Change Mitigation. Arlington (VA): Pew Center on Global Climate Change; 2005 86 p.

60. Lecomte EL, Pang AW, Russell JW. Ice Storm '98 [Internet]. Toronto (ON): Institute for Catastrophic Loss Reduction (Canada); 1998 [cited 2009 Oct 18]. 37 p. ICLR Research Paper Series No. 1. Available at: http://www.iclr.org/images/icestorm98_english.pdf

61. Fischhoff, B. Value Elicitation: Is there anything in there? American Psychologist, 1991; 46: 835-847.

62. Webster BH, Alemayehu B, U.S. Census Bureau, American Community Survey Reports, ACS-02. Income, Earnings, and Poverty Data From the 2005 American

Community Survey [Internet]. Washington DC: U.S. Government Printing Office; 2006 22 p. Available at: http://www.census.gov/prod/2006pubs/acs-02.pdf

63. Klein G, Krebs M, Hall V, O'Brien T, Blevins BB. California's Water-Energy Relationship [Internet]. San Francisco: California Energy Commission; 2005 Nov. Available at: http://www.energy.ca.gov/2005publications/CEC-700-2005-011/CEC-700-2005-011-SF.PDF
64. Vickers A. Handbook of Water Use and Conservation. Amherst: Waterplow Press; 2001.
65. Emergency Water Conservation Ordinance [Internet]. Tucson: City of Tucson; 2011 [cited 2011 Jan 20]. Available at: http://cms3.tucsonaz.gov/water/emergency_ord
66. Welcome to Foster Fuels [Internet]. [place unknown]: Foster Fuels; 2010 [cited Jul 10 2010]. Available at: http://www.fosterfuels.com/pages/foster_fuels_company_info.html
67. Engineer (Pittsburgh Public Works Department, Pittsburgh, PA). Phone conversation with: Anu Narayanan (Department of Engineering and Public Policy, Carnegie Mellon University, Pittsburgh, PA). 2008 Sep 18.
68. Energy Efficient Traffic Signals – LED Traffic Signal Retrofits [Internet]. [place unknown]: Metropolitan Washington Council of Governments; [cited 2010 Apr 12]. Available at: http://www.mwcog.org/uploads/committee-documents/oVtfW1k20050523143436.pdf

69. Marnay C et. al. Applications of Optimal Building Energy System Selection. Paper presented at Microgen' II: Second International Conference on Microgeneration and Related Technologies; April 4-6, 2011; Glasgow, Scotland.
70. Worcester County Jail Planning Wind Turbine Installation. Clean Technica, 2009. Available at: http://cleantechnica.com/2009/02/03/worcester-county-jail-planning-windturbine-installation/, Accessed on August 23, 2011.
71. Estimating the Costs and Benefits of the Smart Grid. (2011). Electric Power Research Institute (EPRI) Technical Report. Available at: http://www.energycentral.com/download/products/EPRI%20Smart%20Grid%20Report.pdf
72. Advanced Metering Infrastructure. National Energy Technology Laboratory (NETL) report. February 2008. Available at: http://www.netl.doe.gov/smartgrid/referenceshelf/whitepapers/AMI%20White%20paper%20final%20021108%20(2)%20APPROVED_2008_02_12.pdf
73. Smart Meters and Smart Meter Systems: A Metering Industry Perspective. (2011). Available at: http://www.dteenergy.com/pdfs/smartMeterWhitePaper.pdf
74. Opportunity: Recovery Act – Smart Grid Investment Grant. (2009). Available at: https://www.fedconnect.net/FedConnect/?doc=DE-FOA-0000058&agency=DOE
75. Reliability Standards. North American Electric Reliability Corporation (NERC). Available under the "CIP" tab at: http://www.nerc.com/page.php?cid=2%7C20
76. Guidelines for Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements. (2010). NIST Interagency Report 7628. Prepared by the Smart Grid Interoperability Panel – Cybersecurity Working Group of the National

Institute of Standards and Technology (NIST). Volume 1 available at: http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf (Vol. 2 and Vol. 3 available at: http://csrc.nist.gov/publications/PubsNISTIRs.html)

77. Workshop on Future Direction in Cyber-Physical Systems Security – The Final Report. (2010). The U.S. Department of Homeland Security.
78. Roadmap to Achieve Energy Delivery Systems Cybersecurity. (2011). The U.S. Department of Energy. Available at: http://energy.gov/sites/prod/files/Energy%20Delivery%20Systems%20Cybersecurity%20Roadmap_finalweb.pdf
79. Personal conversation with Howard Lipson. September 11, 2012.
80. Cybersecurity: Challenges in Securing the Modernized Electricity Grid, GAO-12-507T. Washington, D.C.: February 28, 2012. Available at: http://www.gao.gov/assets/590/588913.pdf
81. FBI: Smart Meter Hacks Likely to Spread. (2012). KrebsonSecurity. Available at: http://krebsonsecurity.com/2012/04/fbi-smart-meter-hacks-likely-to-spread/
82. Security Pros Question Deployment of Smart Meters. (2010) Wired. Available at: http://www.wired.com/threatlevel/2010/03/smart-grids-done-smartly/
83. Remote Connect/Disconnect for Utilities. (2005). Chartwell Inc. Available at: http://www.lebed.biz/nihk.pdf
84. Lin, C.C. and Segel, L.A. Mathematics Applied to Deterministic Problems in the Natural Sciences. SIAM Edition. (1988). New York: Macmillan Publishing Co.
85. Kundur, P. (1994). Power system control and stability. New York: McGraw-Hill, Inc.

86. Kundur, P.; Paserba, J.; Ajjarapu, V.; Andersson, G.; Bose, A.; Canizares, C.; Hatziargyriou, N.; Hill, D.; Stankovic, A.; Taylor, C.; Van Cutsem, T.; Vittal, V.; "Definition and classification of power system stability IEEE/CIGRE joint task force on stability terms and definitions," *Power Systems, IEEE Transactions on* , vol.19, no.3, pp. 1387- 1401, Aug. 2004

87. Milano, F.; , "An Open Source Power System Analysis Toolbox," *Power Systems, IEEE Transactions on* , vol.20, no.3, pp. 1199- 1206, Aug. 2005

88. Documentation for Power System Analysis Toolbox Version 2.1.6. (2010)

89. Abbas Rabiee, Maziar Vanouni, Mostafa Parniani. Optimal reactive power dispatch for improving voltage stability margin using a local voltage stability index. Energy Conversion and Management, Volume 59, July 2012, Pages 66–73

90. Lof, P.-A.; Andersson, G.; Hill, D.J.; , "Voltage stability indices for stressed power systems," *Power Systems, IEEE Transactions on* , vol.8, no.1, pp.326-335, Feb 1993

91. King, D. and Morgan M. (2007). ”Customer-Focused Assessment of Electric Power Microgrids.” J. Energy Eng. 133, SPECIAL ISSUE: Distributed Energy Resources-Potentials for the Electric Power Industry, 150–164.

92. King, D. E. (2006). Electric power micro-grids: Opportunities and challenges for an emerging distributed energy architecture. Carnegie Mellon University). ProQuest Dissertations and Theses. 181 p.

93. King, D., and Morgan, G. 2003. “Guidance for drafting state legislation to facilitate the growth of independent electric power microgrids.” Rep. CEIC-03-

17, Carnegie Mellon Electricity Industries Center, Carnegie Mellon Univ., Pittsburgh, Pa

94. Energy Policy Act of 2005, Pub. L. 109–58, 119 Stat. 594 (Aug. 8, 2005).
95. Alternative Energy Portfolio Standards. Commonwealth of Pennsylvania, 2009. Available at: http://www.pacode.com/secure/data/052/chapter75/052 0075.pdf, Accessed on April 12, 2010.
96. Electric Power Research Institute Smart Grid Resource Center – NESCOR. http://www.smartgrid.epri.com/NESCOR.aspx
97. Cybersecurity: Challenges in Securing the Electricity Grid, GAO-12-926T. Washington, D.C.: July 17, 2012. Available at: http://www.gao.gov/assets/600/592508.pdf

Appendix A: Sample Data Files

9-BUS DATA

Buses

```
Bus.con = [ ...
1   16.5     1     0     4     1;
2  18   1   0   5   1;
3   13.8     1     0     3     1;
4  230   1   0   2   1;
5  230   1   0   2   1;
6  230   1   0   2   1;
7  230   1   0   2   1;
8  230   1   0   2   1;
9  230   1   0   2   1 ];
```

Lines

```
Line.con = [ ...
9      8     100     230     60      0      0   0.0119   0.1008    0.209       0       0       0       0       0;
7      8     100     230     60      0      0   0.0085    0.072    0.149       0       0       0       0       0;
9      6     100     230     60      0      0    0.039     0.17    0.358       0       0       0       0       0;
7      5     100     230     60      0      0    0.032    0.161    0.306       0       0       0       0       0;
5      4     100     230     60      0      0     0.01    0.085    0.176       0       0       0       0       0;
6      4     100     230     60      0      0    0.017    0.092    0.158       0       0       0       0       0;
2      7    100     18     60      0    0.0782609      0  0.0625      0      0      0      0      0      0;
3      9    100    13.8     60      0    0.06      0  0.0586      0      0      0      0      0      0;
1      4    100    16.5     60      0    0.0717391      0  0.0576      0      0      0      0      0      0 ];
```

Swing Bus

```
SW.con = [ ...
1    100    16.5    1.04      0     99    -99     1.1     0.9     0.8      1 ];
```

Generators

```
Syn.con = [ ...
2    100     18     60      4      0      0  0.8958  0.1198      0      6      0  0.8645  0.1969      0   0.535      0
12.8      0.005      0      0      1      1   0.002;
3    100    13.8     60      4      0      0  1.3125  0.1813      0    5.89      0  1.2578    0.25      0    0.6      0   6.02
0.005      0      0      1      1   0.002;
1    100    16.5     60      4      0      0   0.146  0.0608      0    8.96      0  0.0969  0.0969      0    0.31      0
47.28      0.005      0      0      1      1   0.002 ];
```

Generator Data

```
PV.con = [ ...
2    100     18     1.63    1.025     99    -99     1.1     0.9      1;
3    100    13.8     0.85    1.025     99    -99     1.1     0.9      1 ];
```

Loads

```
PQ.con = [ ...
6    100    230    0.9    0.3    1.2    0.8      0;
8    100    230    1   0.35    1.2    0.8      0;
5    100    230    1.25   0.5    1.2    0.8      0 ];
```

Governors

```
Tg.con = [ ...
2    2    1    0.05   1.1    0   0.1    0.3;
3    2    1    0.05   1.1    0   0.1    0.3];
```

Exciters

```
Exc.con = [ ...
2    2    5    -5    20    0.2  0.063   0.35   0.01  0.314  0.001  0.0039   1.555;
1    2    5    -5    20    0.2  0.063   0.35   0.01  0.314  0.001  0.0039   1.555;
3    2    5    -5    20    0.2  0.063   0.35   0.01  0.314  0.001  0.0039   1.555 ];
```

39-BUS DATA

Buses

```
Bus.con = [ ...
  1  1.00  1.048   -0.1646   1 1;
  2  1.00  1.0505  -0.1203   1 1;
  3  1.00  1.0341  -0.1698   1 1;
  4  1.00  1.0116  -0.1838   1 1;
  5  1.00  1.0165  -0.1637   1 1;
  6  1.00  1.0172  -0.1515   1 1;
  7  1.00  1.0067  -0.1892   1 1;
  8  1.00  1.0057  -0.1979   1 1;
  9  1.00  1.0322  -0.1946   1 1;
 10  1.00  1.0235  -0.1101   1 1;
 11  1.00  1.0201  -0.1243   1 1;
 12  1.00  1.0072  -0.1246   2 1;
 13  1.00  1.0207  -0.1225   3 1;
 14  1.00  1.0181  -0.1511   4 1;
 15  1.00  1.0194  -0.1581   5 1;
 16  1.00  1.0346  -0.1337   6 1;
 17  1.00  1.0365  -0.1510   7 1;
 18  1.00  1.0343  -0.1656   8 1;
 19  1.00  1.0509  -0.0531   9 1;
 20  1.00  0.9914  -0.0777   1 1;
 21  1.00  1.0337  -0.0918   1 1;
 22  1.00  1.0509  -0.0143   2 1;
 23  1.00  1.0459  -0.0178   3 1;
 24  1.00  1.0399  -0.1316   4 1;
 25  1.00  1.0587  -0.0962   5 1;
 26  1.00  1.0536  -0.1182   6 1;
 27  1.00  1.0399  -0.1532   7 1;
 28  1.00  1.0509  -0.0571   8 1;
 29  1.00  1.0505  -0.0089   9 1;
 30  1.00  1.0475  -0.0780   1 1;
```

```
 31   1.00  0.9820       0   1 1;
 32   1.00  0.9831   0.0284   2 1;
 33   1.00  0.9972   0.0380   3 1;
 34   1.00  1.0123   0.0129   4 1;
 35   1.00  1.0493   0.0723   5 1;
 36   1.00  1.0635   0.1192   6 1;
 37   1.00  1.0278   0.0220   7 1;
 38   1.00  1.0265   0.1143   8 1;
 39   1.00  1.0300  -0.1913   9 1];
```

Swing Bus

```
SW.con = [ ...
 31 100.0   1.00  0.98200   0    8.00000  -5.0000 1.1 0.9  2 1];
```

Lines

```
Line.con = [ ...
  1    2   100.00   1.00 60 0  0.00  0.00350  0.04110  0.69870  1.00000  0.00000 0    0.000    0.000;
  1   39   100.00   1.00 60 0  0.00  0.00100  0.02500  0.75000  1.00000  0.00000 0    0.000    0.000;
  2    3   100.00   1.00 60 0  0.00  0.00130  0.01510  0.25720  1.00000  0.00000 0    0.000    0.000;
  2   25   100.00   1.00 60 0  0.00  0.00700  0.00860  0.14600  1.00000  0.00000 0    0.000    0.000;
  2   30   100.00   1.00 60 0  1.025 0.00000  0.01810  0.00000  1.02500  0.00000 0    0.000    0.000;
  3    4   100.00   1.00 60 0  0.00  0.00130  0.02130  0.22140  1.00000  0.00000 0    0.000    0.000;
  3   18   100.00   1.00 60 0  0.00  0.00110  0.01330  0.21380  1.00000  0.00000 0    0.000    0.000;
  4    5   100.00   1.00 60 0  0.00  0.00080  0.01280  0.13420  1.00000  0.00000 0    0.000    0.000;
  4   14   100.00   1.00 60 0  0.00  0.00080  0.01290  0.13820  1.00000  0.00000 0    0.000    0.000;
  5    8   100.00   1.00 60 0  0.00  0.00080  0.01120  0.14760  1.00000  0.00000 0    0.000    0.000;
  6    5   100.00   1.00 60 0  0.00  0.00020  0.00260  0.04340  1.00000  0.00000 0    0.000    0.000;
  6    7   100.00   1.00 60 0  0.00  0.00060  0.00920  0.11300  1.00000  0.00000 0    0.000    0.000;
  6   11   100.00   1.00 60 0  0.00  0.00070  0.00820  0.13890  1.00000  0.00000 0    0.000    0.000;
  7    8   100.00   1.00 60 0  0.00  0.00040  0.00460  0.07800  1.00000  0.00000 0    0.000    0.000;
  8    9   100.00   1.00 60 0  0.00  0.00230  0.03630  0.38040  1.00000  0.00000 0    0.000    0.000;
  9   39   100.00   1.00 60 0  0.00  0.00100  0.02500  1.20000  1.00000  0.00000 0    0.000    0.000;
 10   11   100.00   1.00 60 0  0.00  0.00040  0.00430  0.07290  1.00000  0.00000 0    0.000    0.000;
 10   13   100.00   1.00 60 0  0.00  0.00040  0.00430  0.07290  1.00000  0.00000 0    0.000    0.000;
 10   32   100.00   1.00 60 0  1.07  0.00000  0.02000  0.00000  1.07000  0.00000 0    0.000    0.000;
 12   11   100.00   1.00 60 0  1.006 0.00160  0.04350  0.00000  1.00600  0.00000 0    0.000    0.000;
 12   13   100.00   1.00 60 0  1.006 0.00160  0.04350  0.00000  1.00600  0.00000 0    0.000    0.000;
 13   14   100.00   1.00 60 0  0.00  0.00090  0.01010  0.17230  1.00000  0.00000 0    0.000    0.000;
 14   15   100.00   1.00 60 0  0.00  0.00180  0.02170  0.36600  1.00000  0.00000 0    0.000    0.000;
 15   16   100.00   1.00 60 0  0.00  0.00090  0.00940  0.17100  1.00000  0.00000 0    0.000    0.000;
 16   17   100.00   1.00 60 0  0.00  0.00070  0.00890  0.13420  1.00000  0.00000 0    0.000    0.000;
 16   19   100.00   1.00 60 0  0.00  0.00160  0.01950  0.30400  1.00000  0.00000 0    0.000    0.000;
 16   21   100.00   1.00 60 0  0.00  0.00080  0.01350  0.25480  1.00000  0.00000 0    0.000    0.000;
 16   24   100.00   1.00 60 0  0.00  0.00030  0.00590  0.06800  1.00000  0.00000 0    0.000    0.000;
 17   18   100.00   1.00 60 0  0.00  0.00070  0.00820  0.13190  1.00000  0.00000 0    0.000    0.000;
 17   27   100.00   1.00 60 0  0.00  0.00130  0.01730  0.32160  1.00000  0.00000 0    0.000    0.000;
 19   33   100.00   1.00 60 0  1.07  0.00070  0.01420  0.00000  1.07000  0.00000 0    0.000    0.000;
 19   20   100.00   1.00 60 0  1.06  0.00070  0.01380  0.00000  1.06000  0.00000 0    0.000    0.000;
 20   34   100.00   1.00 60 0  1.009 0.00090  0.01800  0.00000  1.00900  0.00000 0    0.000    0.000;
 21   22   100.00   1.00 60 0  0.00  0.00080  0.01400  0.25650  1.00000  0.00000 0    0.000    0.000;
 22   23   100.00   1.00 60 0  0.00  0.00060  0.00960  0.18460  1.00000  0.00000 0    0.000    0.000;
 22   35   100.00   1.00 60 0  1.025 0.00000  0.01430  0.00000  1.02500  0.00000 0    0.000    0.000;
```

```
 23   24   100.00   1.00 60 0  0.00  0.00220  0.03500  0.36100  1.00000  0.00000 0    0.000    0.000;
 23   36   100.00   1.00 60 0  1.00  0.00050  0.02720  0.00000  1.00000  0.00000 0    0.000    0.000;
 25   26   100.00   1.00 60 0  0.00  0.00320  0.03230  0.51300  1.00000  0.00000 0    0.000    0.000;
 25   37   100.00   1.00 60 0  1.025 0.00060  0.02320  0.00000  1.02500  0.00000 0    0.000    0.000;
 26   27   100.00   1.00 60 0  0.00  0.00140  0.01470  0.23960  1.00000  0.00000 0    0.000    0.000;
 26   28   100.00   1.00 60 0  0.00  0.00430  0.04740  0.78020  1.00000  0.00000 0    0.000    0.000;
 26   29   100.00   1.00 60 0  0.00  0.00570  0.06250  1.02900  1.00000  0.00000 0    0.000    0.000;
 28   29   100.00   1.00 60 0  0.00  0.00140  0.01510  0.24900  1.00000  0.00000 0    0.000    0.000;
 29   38   100.00   1.00 60 0  1.025 0.00080  0.01560  0.00000  1.02500  0.00000 0    0.000    0.000;
  6   31   100.00   1.00 60 0  1.07  0.00000  0.02500  0.00000  1.07000  0.00000 0    0.000    0.000];
```

Generators

```
Syn.con = [ ...
 39  100.0  1.0  60  3  0.0030  0.00010  0.0200  0.0060  0  7.000  0  0.019  0.008    0  0.700  0 1000.0  0.005
0.00  0  1  1  0.002;
 31  100.0  1.0  60  4  0.035   0.00270  0.2950  0.0697  0  6.560  0  0.2820  0.170   0  1.500  0 60.600  0.005
0.00  0  1  1  0.002;
 32  100.0  1.0  60  4  0.0304  0.000386 0.2495  0.0531  0  5.700  0  0.2370  0.0531  0  1.500  0 70.600
0.005  0.00  0  1  1  0.002;
 33  100.0  1.0  60  4  0.0295  0.000222 0.2620  0.0436  0  5.690  0  0.2580  0.0436  0  1.500  0 57.200
0.005  0.00  0  1  1  0.002;
 34  100.0  1.0  60  4  0.0540  0.00014  0.6700  0.1320  0  5.400  0  0.6200  0.1320  0  0.440  0 52.000
0.005  0.00  0  1  1  0.002;
 35  100.0  1.0  60  4  0.0224  0.00615  0.2540  0.0500  0  7.300  0  0.2410  0.0500  0  0.400  0 69.600
0.005  0.00  0  1  1  0.002;
 36  100.0  1.0  60  4  0.0322  0.000268 0.2950  0.0490  0  5.660  0  0.2920  0.0490  0  1.500  0 52.800
0.005  0.00  0  1  1  0.002;
 37  100.0  1.0  60  4  0.0280  0.000686 0.2900  0.0570  0  6.700  0  0.2800  0.0570  0  0.410  0 48.600
0.005  0.00  0  1  1  0.002;
 38  100.0  1.0  60  4  0.0298  0.00030  0.2106  0.0570  0  4.790  0  0.2050  0.0570  0  1.960  0 69.000
0.005  0.00  0  1  1  0.002;
 30  100.0  1.0  60  4  0.0125  0.00014  0.1000  0.0310  0  10.20  0  0.0690  0.0310  0  1.500  0 84.000
0.005  0.00  0  1  1  0.002];
```

Generator Data

```
PV.con = [ ...
30 100.0   1.00  2.5   1.0475  8      -5     1.1 0.9 1;
32 100.0   1.00  6.5   0.9831  8      -5     1.1 0.9 1;
33 100.0   1.00  6.32   0.9972  8      -5     1.1 0.9 1;
34 100.0   1.00  5.08   1.0123  4      -3     1.1 0.9 1;
35 100.0   1.00  6.5   1.0493  8      -5     1.1 0.9 1;
36 100.0   1.00  5.6   1.0635  8      -5     1.1 0.9 1;
37 100.0   1.00  5.4   1.0278  8      -5     1.1 0.9 1;
38 100.0   1.00  8.3   1.0265  8      -5     1.1 0.9 1;
39 100.0   1.00  10   1.0300  15    -10     1.1 0.9 1];
```

Exciters

```
Exc.con = [ ...  %Gen.no Type Max.limit
 1   2   10.5 -10.5  40.00 0.020    0.03  0.1000  1  1.400  0.001  0.0039   1.555;
 2   2   5    -5     6.20 0.050    0.06  0.0500  1  0.410  0.001  0.0039   1.555;
 3   2   5    -5     5.00 0.060    0.08  0.1000  1  0.500  0.001  0.0039   1.555;
 4   2   5    -5     5.00 0.060    0.08  0.1000  1  0.500  0.001  0.0039   1.555;
 5   2   30   -10    40.00 0.020    0.03  0.1000  1  0.785  0.001  0.0039   1.555;
```

```
 6   2   5    -5      5.00 0.020    0.08  0.125   1  0.471  0.001  0.0039   1.555;
 7   2   6.5  -6.5   40.00 0.020    0.03  0.1000  1  0.730  0.001  0.0039   1.555;
 8   2   5    -5      5.00 0.020    0.09  0.1260  1  0.528  0.001  0.0039   1.555;
 9   2   10.5 -10.5   5.00 0.020    0.03  0.1000  1  0.500  0.001  0.0039   1.555;
10   2   5    -5      5.00 0.060    0.04  0.1000  1  0.25   0.001  0.0039   1.555];
```

Loads

```
PQ.con = [ ...
1 100.0   1.00  0   0.0000  1.1 0.9 0;
2 100.0   1.00  0   0.0000  1.1 0.9 0;
3 100.0   1.00  3.22   0.0240  1.1 0.9 0;
4 100.0   1.00  5   1.8400  1.1 0.9 0;
5 100.0   1.00  0   0.0000  1.1 0.9 0;
6 100.0   1.00  0   0.0000  1.1 0.9 0;
7 100.0   1.00  2.338   0.8400  1.1 0.9 0;
8 100.0   1.00  5.22   1.7600  1.1 0.9 0;
9 100.0   1.00  0   0.0000  1.1 0.9 0;
10 100.0   1.00  0   0.0000  1.1 0.9 0;
11 100.0   1.00  0   0.0000  1.1 0.9 0;
12 100.0   1.00  0.085   0.8800  1.1 0.9 0;
13 100.0   1.00  0   0.0000  1.1 0.9 0;
14 100.0   1.00  0   0.0000  1.1 0.9 0;
15 100.0   1.00  3.2   1.5300  1.1 0.9 0;
16 100.0   1.00  3.29   0.3230  1.1 0.9 0;
17 100.0   1.00  0   0.0000  1.1 0.9 0;
18 100.0   1.00  1.58   0.3000  1.1 0.9 0;
19 100.0   1.00  0   0.0000  1.1 0.9 0;
20 100.0   1.00  6.28   1.0300  1.1 0.9 0;
21 100.0   1.00  2.74   1.1500  1.1 0.9 0;
22 100.0   1.00  0   0.0000  1.1 0.9 0;
23 100.0   1.00  2.475   0.8460  1.1 0.9 0;
24 100.0   1.00  3.086   -0.922  1.1 0.9 0;
25 100.0   1.00  2.24   0.4720  1.1 0.9 0;
26 100.0   1.00  1.39   0.1700  1.1 0.9 0;
27 100.0   1.00  2.81   0.7550  1.1 0.9 0;
28 100.0   1.00  2.06   0.2760  1.1 0.9 0;
29 100.0   1.00  2.835   0.2690  1.1 0.9 0;
39 100.0   1.00  11.04   2.5000  1.1 0.9 0];
```

Governors

```
Tg.con = [ ...
1   1   1   0.02   13.2    0    0.1   0.45   0.00   12.0   50.0;
2   1   1   0.02   17.864    0    0.1   0.45   0.00   12.0   50.0;
3   1   1   0.02   8.58    0  0.1   0.45   0.00   12.0   50.0;
4   1   1   0.02   8.316    0   0.1   0.45   0.00   12.0   50.0;
5   1   1   0.02   6.732    0  0.1   0.45   0.00   12.0   50.0;
6   1   1   0.02   8.932    0  0.1   0.45   0.00   12.0   50.0;
7   1   1   0.02   7.392    0  0.1   0.45   0.00   12.0   50.0;
8   1   1   0.02   7.15    0  0.1   0.45   0.00   12.0   50.0;
9   1   1   0.02   10.978    0   0.1   0.45   0.00   12.0   50.0;
10   1   1   0.02   3.3  0  0.1   0.45   0.00   12.0   50.0];
```