Control and Communication for a Secure and Reconfigurable Power Distribution System

A DISSERTATION
SUBMITTED TO THE FACULTY OF THE GRADUATE SCHOOL
OF THE UNIVERSITY OF MINNESOTA
BY

Anthony Michael Giacomoni

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF
DOCTOR OF PHILOSOPHY

S. Massoud Amin, Bruce F. Wollenberg

November 2011

Acknowledgements

I would like to acknowledge the National Science Foundation (grant number 0831059) for financial support of my doctoral research at the University of Minnesota, and Dr. Sara Mullen who provided a piece of software code that played a critical role in the simulations I developed as part of this dissertation.

I would like to thank my parents who never questioned my decision to pursue a Ph.D., and my friends and lab-mates who made my four and a half years in graduate school much more enjoyable. I would also like to thank Professor Ned Mohan of the Electrical and Computer Engineering Department for serving as chair of my final oral examination committee, and Professor Elizabeth Wilson of the Humphrey Institute of Public Affairs for reviewing my dissertation and serving on my final oral examination committee.

Finally, I am extremely grateful to my co-advisers Professors Massoud Amin and Bruce Wollenberg for supporting me throughout my entire graduate career. They were always available to discuss ideas or work through problems, and provided encouragement and guidance every step of the way.

Abstract

A major transformation is taking place throughout the electric power industry to overlay existing electric infrastructure with advanced sensing, communications, and control system technologies. This transformation to a smart grid promises to enhance system efficiency, increase system reliability, support the electrification of transportation, and provide customers with greater control over their electricity consumption. Upgrading control and communication systems for the end-to-end electric power grid, however, will present many new security challenges that must be dealt with before extensive deployment and implementation of these technologies can begin.

In this dissertation, a comprehensive systems approach is taken to minimize and prevent cyber-physical disturbances to electric power distribution systems using sensing, communications, and control system technologies. To accomplish this task, an intelligent distributed secure control (IDSC) architecture is presented and validated *in silico* for distribution systems to provide greater adaptive protection, with the ability to proactively reconfigure, and rapidly respond to disturbances. Detailed descriptions of functionalities at each layer of the architecture as well as the whole system are provided.

To compare the performance of the IDSC architecture with that of other control architectures, an original simulation methodology is developed. The simulation model integrates aspects of cyber-physical security, dynamic price and demand response, sensing, communications, intermittent distributed energy resources (DERs), and dynamic optimization and reconfiguration. Applying this comprehensive systems approach,

performance results for the IEEE 123 node test feeder are simulated and analyzed. The results show the trade-offs between system reliability, operational constraints, and costs for several control architectures and optimization algorithms. Additional simulation results are also provided. In particular, the advantages of an IDSC architecture are highlighted when an intermittent DER is present on the system.

Table of Contents

List of Tables

List of Tables

List of Figures

List of Abbreviations

AC	Alternating current
ALS	Annealed local search
AMI	Advanced metering infrastructure
AMM	Automatic meter management
AMR	Automated meter reading
ARRA	American Recovery and Reinvestment Act
ASAI	Average service availability index
BAU	Business as usual
BMS	Building management system
CAIDI	Customer average interruption duration index
CC	Centralized control
CIGRÈ	The International Council on Large Electric Systems
CIN/SI	Complex Interactive Networks/Systems Initiative
CMU	Carnegie Mellon University
CPS	Cyber protection system
DAS	Distribution automation systems
DC	Decentralized control
DCS	Distributed control system
DER	Distributed energy resource
DOD	United States Department of Defense

DOE	United States Department of Energy
DR	Demand response
EEI	The Edison Electric Institute
EISA	Energy Independence and Security Act
EMS	Energy management system
EPRI	The Electric Power Research Institute
ESPP	Energy Smart Pricing Plan
FERC	Federal Energy Regulatory Commission
GDP	Gross domestic product
HAN	Home area network
IDSC	Intelligent distributed secure control
IEEE	The Institute of Electrical and Electronics Engineers
IP	Internet protocol
ISAC	Information Sharing and Analysis Center
IT	Information technology
LOEE	Loss of energy expectation
M&V	Measurement & verification
MCP	Market clearing price
MDMS	Meter data management system
MISO	Midwest Independent Transmission System Operator
NDB	Neighborhood database
NERC	North American Electric Reliability Corporation

NPS	The Naval Postgraduate School
OTPC	Otter Tail Power Company
PKI	Public key infrastructure
PUC	Public Utilities Commission
RMS	Root mean square
RPS	Renewable portfolio standard
RTU	Remote terminal unit
SAIDI	System average interruption duration index
SAIFI	System average interruption frequency index
SARFI	System average RMS (variation) frequency index
SCADA	Supervisory control and data acquisition
SGIG	Smart Grid Investment Grant
SPID	Strategic power infrastructure defense
SQRA	Security, quality, reliability, and availability
SSO	Sequential switch opening
UML	Unified modeling language
UMM	The University of Minnesota Morris
UTA	The University of Texas at Austin
WTP	Willingness to pay

1 Introduction

Planning has already begun to replace control and communication systems of the existing power-delivery system with digital systems to provide the grid with the capability to reconfigure itself and prevent widespread outages. Often, this collection of digital overlaid systems is referred to as 'smart grid'. Attributes of a smart grid include advanced sensing, communications, and control capabilities that provide increased system reliability, engage consumers, allow for increased integration of renewable distributed energy resources (DERs), and support the electrification of transportation. Additional characteristics are presented in [1], [2], and [3]. Such capabilities will transform the existing electric industry operating model, marking the first major architectural change to the grid since AC become the dominant system after the Chicago World's Fair in 1893 [4].

While this transformation of the electrical grid has gained much momentum over the last several years, the ideas are not new. The necessary control systems were first described by Fred Schweppe in 1978, although he predicted, a bit too optimistically, that they would be implemented by the year 2000. His rationalization for this prediction was that "the need exists, the technology is available, and the dividends for its use will justify the expense" [5], which remains just as true today as it was then.

Currently, it is estimated that disruptions in the electricity supply cost consumers over $150 billion a year [6]. It is expected that the increase in efficiency and reliability

from smart grid will reduce the cost of power disturbances by $49 billion per year [7], and add nearly $1.8 trillion in annual revenue to the U.S. economy by 2020 [8]. Consumer load management could add another $5-$7 billion per year by 2015, and $15-$20 billion per year by 2020. Assuming a 10% penetration, distributed generation and smart, interactive storage capacity for residential and small commercial applications could further augment this amount by $10 billion per year by 2020 [7]. In addition, the resulting increases in efficiency and reliability to the existing grid will decrease the need for major infrastructure investments in the future. Over the next 20 years, this is expected to reduce infrastructure investment costs by $46-$117 billion [7].

The benefits from smart grid, however, go well beyond just increasing the reliability and security of the nation's electricity supply. It provides a means to reach national energy independence, control emissions, and combat global warming [9]. Increased efficiency will result in decreased fuel consumption and thus, lower fuel prices for all consumers. The increased demand for smart gird technologies will also spur the development of new markets and job growth as private industry develops advanced technologies such as smart meters, energy-efficient and intelligent appliances, and advanced sensing and communications capabilities [10].

Several of these potential benefits are summarized in Table 1.1, and the potential reductions in energy and carbon dioxide emissions attributable to various smart grid technologies are listed in Table 1.2. In Table 1.2, direct reductions were calculated from the mechanisms that directly affected energy and carbon dioxide emissions, while indirect reductions were calculated by translating the estimated cost savings in energy

and/or capacity into their energy or carbon equivalents through the purchase of additional cost-effective energy efficiency. While a smart grid is "not the central means of providing the savings that energy efficiency and renewables represent," the tables show that it "appears to have a significant role in enhancing those savings and achieving them at less cost" [11].

Table 1.1: Potential Smart Grid Economic and Environmental Benefits [8]

	2000	2025		
Parameter	**Baseline**	**Business as Usual (BAU)**	**Enhanced Electric Power System**	**Improvement of Enhanced Productivity Over BAU**
Electricity Consumption (billion kilowatt-hours [kWh])	3,800	5,800	4,900-5,200	10% - 15% reduction
Delivered Electricity Intensity (kWh/$GDP)	0.41	0.28	0.20	29% reduction
% Demand Reduction at Peak	6%	15%	25%	66% increase
% Load Requiring Digital Quality Power	<10%	30%	50%	66% increase
Carbon Dioxide Emissions (million metric tons of carbon)	590	900	720	20% reduction
Productivity Growth Rate ($/year)	2.9	2.5	3.2	28% increase
Real GDP (billions of dollars, 1996)	9,200	20,700	24,300	17% increase
Cost of Power Disturbances to Businesses (billions of dollars, 1996)	100	200	20	90% reduction

Initial demonstrations of smart grid technologies have already shown much promise. While "the value of Smart Grid technologies has been difficult to quantify in a simple cost-benefit analysis due to the multi-tiered benefits they provide to the utility, the consumer, and society" [10], studies and experience from the utility Hydro One in Ontario, Canada [12] have revealed that the incremental benefits from smart grid applications significantly outweigh their costs. Their findings are beginning to be leveraged and adopted by others across the industry. A recent report published by the Electric Power Research Institute (EPRI) has come to a similar conclusion, estimating

Table 1.2: Potential Reductions in Energy and CO_2 Emissions in 2030 Attributable to Smart Grid Technologies [11]

Mechanism	Reductions in Electricity Sector Energy and CO_2 Emissions[(a)]	
	Direct (%)	Indirect (%)
Conservation Effect of Consumer Information and Feedback Systems	3	-
Joint Marketing of Energy Efficiency and Demand Response Programs	-	0
Deployment of Diagnostics in Residential and Small/Medium Commercial Buildings	3	-
Measurement & Verification (M&V) for Energy Efficiency Programs	1	0.5
Shifting Load to More Efficient Generation	<0.1	-
Support Additional Electric Vehicles and Plug-In Hybrid Electric Vehicles	3	-
Conservation Voltage Reduction and Advanced Voltage Control	2	-
Support Penetration of Renewable Wind and Solar Generation (25% renewable portfolio standard [RPS])	<0.1	5
Total Reduction	12	6

(a) Assume 100% penetration of smart grid technologies.

that the benefits from smart grid will outweigh the costs by approximately 2.8 - 6.0 times [13].

Although the business case for the smart grid transformation is sound, and analyses, such as the Smart Grid Implementation Plan developed for the state of West Virginia [14], clearly illustrate this fact, the question that remains is "who pays for the investments?" Since the majority of benefits accrue to consumers and society, utilities have little incentive to invest in such technologies. Therefore, consumers need to understand that they are the ones who will benefit from the transformation, and they must be willing to compensate utilities for its implementation. However, utilities also have the responsibility to extensively test out the technologies before widespread deployment and implementation begins. Thus, smart grid risks need to be shared between utilities and consumers. It is therefore imperative to educate all stakeholders about the costs and

benefits of smart grid technologies in order to gain public support for future projects. The preceding clearly did not happen in Xcel Energy's SmartGridCity project in Boulder, CO, where ratepayers were saddled with a $27.9 million bill to cover triple cost overruns [15].

1.1 Motivation

Upgrading control and communication systems for the power grid, however, will present many new security challenges that must be dealt with before extensive deployment and implementation of smart grid technologies can begin. The digitalization of electric grid control and communication systems may enable remote attacks to grow rapidly, potentially spanning countries or even continents [9]. Moreover, it is rapidly becoming easier to compromise computer systems due to the increased availability of hacker tools on the Internet and the decrease in technical knowledge required to use them to impose significant damage [16]. As a result, electric infrastructure must be adequately defended from both malicious attacks and natural disasters.

1.1.1 Types of Vulnerabilities

In order to defend electric infrastructure against such threats, three types of vulnerabilities must be considered – physical, cyber, and open-source information.

1.1.1.1 Physical

The size and complexity of the North American electric power grid makes it impossible both financially and logistically to physically protect the entire infrastructure.

There currently exist over 215,000 miles of $230kV$ or higher transmission lines, and many more thousands of miles of lower-voltage lines [17]. As an increasing amount of electricity is generated from renewable DERs, the problem will only be exacerbated as the U.S. Department of Energy (DOE) has concluded that generating 20% of electricity with land-based wind installations will require at least 20,000 square miles [18] resulting in an even greater dispersal of assets. Thus, it is probable that a well-organized and determined group of terrorists could take out portions of the grid as they have previously done in the United States, Colombia, and other locations around the globe. Colombia, for example, has faced up to 200 terrorist attacks per year on its transmission infrastructure over the last 11 years [19].

The small silver lining, however, is that such attacks, although troublesome and costly to the local region, affect only a small portion of the overall grid. To cause physical damage equivalent to that from a small to moderate-size tornado would be extremely difficult, even for a large, well-organized group of terrorists [17].

Data on terrorist attacks on the world's electricity sector from 1994-2004 from the National Memorial Institute for the Prevention of Terrorism shows that transmission systems are by far the most common target in terms of the total number of physical attacks [18]. Figure 1.1 shows the percentage of terrorist attacks aimed at each of the major grid components.

One possible solution to increase the physical security of power lines is to bury them. However, a 2006 study by the Edison Electric Institute (EEI) calculated that putting power lines underground would cost approximately $1 million a mile compared

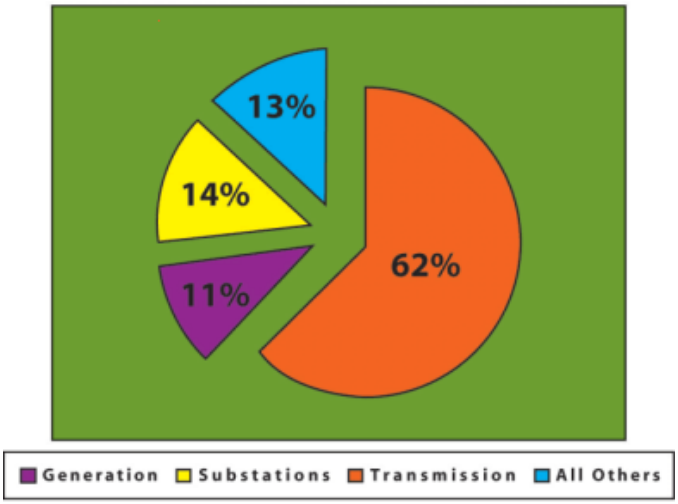

Figure 1.1: Electric Terrorism: Grid Component Targets (1994-2004) [18]

with $100,000 for overhead lines, thus making it financially infeasible [18].

1.1.1.2 *Cyber*

While physical attacks – facility break-ins, weapon attacks, or explosives – are real and frightening possibilities, cyber attacks have the potential to be just as destructive and carry the added threats of stealth and long-distance control [17]. Adversaries have the potential to initiate attacks from nearly any location in the world. "One senior American military source has said that if any country were found to be planting logic bombs on the grid, it would provoke the equivalent of the Cuban missile crisis" [20]. Furthermore, currently more than 90% of successful cyber attacks take advantage of known vulnerabilities and misconfigured operating systems, servers, and network devices [21]. As a result, possible cyber threats that have been envisioned include [22]:

1. Cutting electricity to all homes and businesses

2. Overburdening the grid
3. Causing brown-outs
4. Having the smart-grid devices attack the grid itself
5. Getting free service
6. Undermining confidence

In part, the problem stems from the fact that existing control systems, which were originally designed for use with proprietary, stand-alone communications networks, were later connected to the Internet to increase productivity and lower costs, but without ever adding the technology required to make them secure [23]. In addition, numerous types of communication media and protocols are used in the communication and control of power systems. Within a substation control network, it is common to find commercial telephone lines along with wireless, microwave, optical fiber, and Internet connections. The diversity and lack of interoperability between the communication protocols causes problems for anyone who tries to establish secure communication to and from a substation (or among substations in a network of heterogeneous protocols and devices) [24].

As a result, cyber security is just as important if not more so than physical security. Due to the gravity of these threats, the Federal Energy Regulatory Commission (FERC) policy statement on smart grid has stated that cyber security is essential to the operation of the smart grid and that the development of cyber security standards is a key priority [25]. The U.S. DOE [18] has also stated that the ability to resist attack – by identifying and responding to disruptions caused by sabotage – is one of smart grid's seven crucial functions.

Nevertheless, many obstacles currently exist to securing electric power control systems from cyber attacks. One is that current practices have to be a synthesis of the original 1970's practices and today's standards due to the expected life of various supervisory control and data acquisition (SCADA) devices. Since a device has to operate for 15-20 years, a wide variety of devices based on different technologies may end up in the field [26]. Significant work must also be done to create standards that if implemented will adequately protect the grid from cyber attacks. Emerging standards fall well short of achieving this ultimate purpose [27].

Furthermore, there is the insider threat from internal employees or other individuals with intimate knowledge of system operations. A 2008 survey by the Computer Security Institute/Federal Bureau of Investigation reported data compiled from 522 computer security practitioners and senior executives from U.S. corporations, government agencies, financial and medical institutions, and universities. The survey reported that within a 12-month period, 59% of the respondents experienced an attack from a virus, 29% reported unauthorized use of computer services, and 44% reported insider abuse [28].

1.1.1.3 Open-Source Information

Some analysts have estimated that public sources could be used to gain at least 80% of the information needed to plot an attack on the smart grid. Widely popular and accessible programs, such as Google Earth, routinely provide digital satellite images of critical installations, which in the past would have only been available to government

agencies [18]. In the future, the accessibility of such information is likely to become even more prevalent.

1.2 Recent Work

Over the last decade and since the terrorist attacks of September 11, 2001, several steps have been taken, initiatives completed, and research programs commenced to enhance the security and reliability of the nation's electric infrastructure. Several of these developments are briefly highlighted below.

- The Complex Interactive Networks/Systems Initiative (CIN/SI), a joint program sponsored by EPRI and the U.S. Department of Defense (DOD), developed a mathematical basis along with several practical tools for improving the security, performance, and robustness of critical energy, transportation, financial, and communications infrastructure [29].
- The North American Electric Reliability Corporation (NERC) completed initiatives such as the Information Sharing and Analysis Centers (ISACs), public key infrastructure (PKI), and spare equipment database [21].
- In response to the August 14, 2003 blackout that affected most of the Northeastern United States and parts of Canada, several electric utility responses were undertaken as outlined in [30].
- CIGRÈ, the International Council on Large Electric Systems, developed information security frameworks for electric power utilities [31]. A security framework is considered as the skeleton upon which various elements are integrated for the appropriate management of security risk. The different elements considered include security domains, baseline controls, and security processes.

- Researchers at the University of Texas at Austin (UTA) and the Naval Postgraduate School (NPS) developed an analytic technique to prevent disruptions to the grid from physical terrorist attacks [32]. Their approach identifies critical sets of a power grid's components, which a terrorist group might target to inflict maximum damage.
- Finally, a new distributed model predictive control theory is under development at Carnegie Mellon University (CMU) to better model large-scale infrastructure systems [33]. For these systems, such as power, water, and traffic, it is useful and often necessary to have distributed or decentralized control schemes, where local control inputs are computed using local measurements and reduced-order models of the local dynamics. Models under investigation include those where distributed controllers, or agents, are able to exchange information. Such models are especially useful in applications where a centralized controller is not appropriate or feasible because although some degree of coordination is desired, the agents cannot divulge all the information about their local models and objectives. Examples of such applications include the recently deregulated power markets in the United States.

1.3 Security Needs

While significant steps have been made toward improving the security and reliability of the nation's electric infrastructure, considerable work remains to be done. Two essential components of a comprehensive security approach as well as additional issues for electric infrastructure that must be considered are described in this section.

1.3.1 Layered Security

In order to protect electric infrastructure from the threats outlined in Section 1.1.1, several layers of security are needed to minimize disruptions to system operations. Layered security (or defense-in-depth) involves strategically combining multiple security technologies at each layer of a computing system in order to reduce the risk of unauthorized access due to the failure of any single security technology. It exponentially increases the cost and difficulty for an attacker to compromise a system by creating a much stronger defense than the use of any individual component alone, thus, reducing the likelihood of an attack [34], [35].

Furthermore, the trend of connecting electrical control systems to the Internet exposes all layers of each system to possible attack. Computing layers that must be considered include [34]:

- Personnel
- Networks
- Operating Systems
- Applications
- Databases

Security features to be employed at each layer include examination, detection, prevention, and encryption in addition to other well-established information security practices [27]. Additional methods to improve the security of control systems based on a layered security approach are described in [36].

1.3.2 Deception

An additional defense mechanism is the use of deception. Deception consists of two possible techniques, dissimulation, hiding the real, and simulation, showing the false. In [37], several potential dissimulation and simulation techniques that can be used for control systems are described. Three potential dissimulation techniques include:

1) **Masking** the real by making a relevant object undetectable or blend into background irrelevance
2) **Repackaging** which hides the real by making a relevant object appear to be something it isn't
3) **Dazzling** which hides the real by making a relevant object's identification less certain by confusing the adversary about its true nature.

Likewise, three potential simulation techniques include:

1) **Inventing** the false by creating a perception that a relevant object exists when it doesn't
2) **Mimicking** which invents the false by presenting characteristics of an actual, and relevant object
3) **Decoying** which displays the false by attracting attention away from more relevant objects.

Deception will need to play a key role in smart grid defense mechanisms. With the digitalization of electric infrastructure, immense amounts of data will be transmitted across communication networks. Ramifications from penetrated systems could be devastating, possibly leading to large-scale blackouts or major electricity market failures. Furthermore, the strength of potential adversaries is amplified since existing control system architectures are not random, and therefore response characteristics are

reproducible [38]. Deception defense mechanisms can greatly increase the difficulty of planning and conducting successful attacks upon a system by portraying control system response characteristics as random to attackers. They can also alert operators to possible threats before any systems are harmed.

1.3.3 Additional Issues

An additional industry need is the development of new technologies with built-in inherent security, and tools to enable better management of security postures throughout the technology lifecycle [27]. Most systems currently in use lack any security features, and the majority that have any are grossly inadequate since most systems were designed for use on proprietary, stand-alone platforms and control networks. Furthermore, special consideration must be given to the impact of cyber security controls on electric power utility operation data networks. Often these networks are more sensitive to reliability and latency factors than typical IT data networks [31], meaning that the loss or delay of information on a utility data network often has much greater consequences than on a typical IT data network.

Finally, rapid containment, restoration, and recovery strategies will be needed when systems are inevitably compromised. Either software patching or the ability to rapidly identify and isolate the exploited systems must be enabled [9] in order to minimize downtime since the consequences of an attack are directly proportional to the length of time that the service is disrupted [27]. A plan for how an electric utility can coordinate a program for security response is presented in [39].

1.4 Objectives and Key Contributions

In order to enhance the reliability, robustness, efficiency, and security of the electric power grid to meet the needs of today's digital society and those of the future, the end-to-end electric infrastructure must effectively use sensing, communications, and control system technologies to continually assess and optimize system performance. Such technologies will provide the grid with the flexibility needed to prevent and withstand potential threats, both traditional and those ensuing from the digitalization of the grid's control and communications systems.

In this dissertation, a comprehensive systems approach is taken to minimize and prevent cyber-physical disturbances to electric power distribution systems using sensing, communications, and control system technologies, and the concepts of adaptive and self-healing protection. This research aspires to provide insight to the questions of how such technologies can and should be used to optimize system performance in such an uncertain environment. In particular, this research achieves each of the following:

1) The development of a control architecture for distribution systems to provide greater adaptive and self-healing protection, with the ability to proactively reconfigure, and rapidly respond to disturbances.
2) The development of an analytical and multi-domain methodology to assess the effects of smart grid technologies on distribution system operations and performance.
3) The integration of aspects of cyber-physical security, dynamic price and demand response, sensing, communications, intermittent DERs, and dynamic optimization and reconfiguration into one all-inclusive model.

4) An analysis of the trade-offs between system reliability, operational constraints, and costs for different control architectures and optimization algorithms.

1.5 Dissertation Structure

The remainder of this dissertation is organized as follows. Chapter 2 provides a review of methodologies found in the literature that have been used to model and evaluate cyber security defense systems for electric power and other critical infrastructure. Chapter 3 presents a description of the capabilities, vulnerabilities, security needs, and recent advances for advanced metering infrastructure (AMI), which represents one of the first steps in the digitalization of electric grid control systems. Chapter 4 provides a description of distribution automation systems (DAS), which use AMI, followed by the development of an intelligent distributed secure control (IDSC) architecture that uses DAS for more robust distribution system operations. Chapter 5 explores the distribution system reconfiguration problem, one of the most important tasks of DAS, and presents a method of solution called annealed local search (ALS). Chapter 6 develops several simulations to compare the performance of the IDSC architecture with other control architectures, and provides some simulation results using the IEEE 123 node test feeder. Chapter 7 discusses the simulation results presented in Chapter 6, and Chapter 8 analyzes the potential benefits from smart grid technologies using the University of Minnesota Morris (UMM) campus as a case study. Finally, Chapter 9 states some conclusions and describes areas for future research.

In addition, Appendix A lists the cyber security threat categories described in Section 2.5, Appendix B lists some typical distribution system parameters, and Appendix C provides the data for the IEEE 123 node test feeder used in the simulations presented in Chapter 6.

2 Cyber Security Modeling, Simulation, and Evaluation

Due to the human element of a malicious actor, traditional reliability methods cannot be used for cyber defense systems. The reason for this is that "dynamic mechanisms of probabilistic risk analysis that can link human reliability with the system state are still maturing. The intellectual level and background of the adversary makes stochastic methods unusable due to the variability of both the objective and the motives" [38]. Furthermore, simulating the effects of cyber defense systems is severely limited by the following aspects [40]:

1) The accuracy of the models.
2) The accuracy of the data upon which the simulations are based.
3) The ability to explore the simulation space using multiple runs of the simulator through the space.

Unlike in other fields, in information protection there are no widely published or accepted information physics from which to develop an accurate model. Instead, researchers are left with the overwhelming task of modeling extremely complex phenomena, involving mixes of human behavior and interactions of complex interdependent systems with time bases ranging from nanoseconds to years. This task is further complicated by the fact that the sizes of the networks and systems being modeled are so large and complex that they cannot be described with any degree of accuracy [40].

Therefore, in order to assess the effectiveness of existing cyber security defense systems and to help decide where additional investments need to be made, several cyber security modeling methodologies have been developed. This chapter presents several of these methodologies found in the literature that have been used to model and evaluate cyber security defense systems for electric power and other critical infrastructure. However, it must be noted that, as one would expect, no method fully describes how to identify a vulnerability, threat, or risk. If this were possible, then it would be possible to identify all of them, which is not possible. This can be proven by the simple argument that a presumed complete list of vulnerabilities could be used to show that it is not complete since knowledge of the complete list is itself a vulnerability and is not on the list [41].

2.1 Attack Trees

A common method used to determine the vulnerability of a system to cyber threats is the use of attack trees. Attack trees model specific attack paths that an adversary can take to compromise a system [26], [42]. The root node of the tree is the desired goal of the adversary, while the intermediate nodes specify the steps that must be taken to achieve the desired goal and are labeled as sub-goals. Each node can have multiple branches, which are related through the logical operators "AND" and "OR" to allow for different attack scenarios. Often, adversaries have multiple attack goals resulting in a forest of attack trees. An example of two attack trees for a power system utilizing advanced metering infrastructure (AMI) is shown in Figure 2.1.

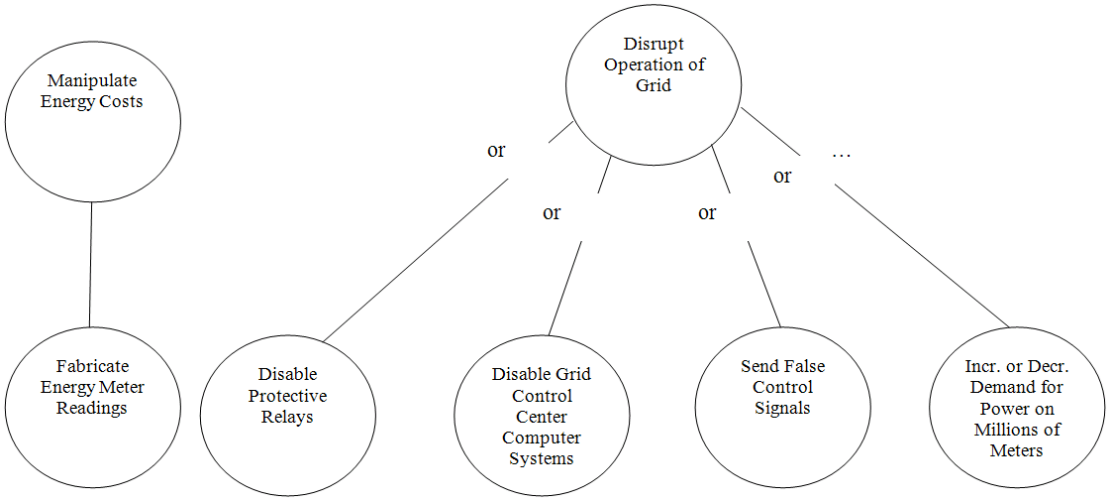

Figure 2.1: Attack Trees

An approach to evaluate the vulnerability indices for an attack tree in a systematic manner is described in [26]. The concept of an attack tree can also be extended to include controllable countermeasures resulting in the creation of a defense tree [42]. In addition, a way to enhance the capabilities of attack trees based on Petri nets, called PENET, is described in [26].

2.2 Bayesian Defense Graphs and Architectural Models

Bayesian defense graphs are used in [42] to quantify expected losses before and after potential investments in cyber security systems are made in order to aide decision makers. Such graphs use Bayesian statistic based extended influence diagrams, which can be derived from defense trees. Once a defense tree has been constructed, an extended influence diagram can be created by adding the abilities of the adversary to the model

using deterministic definitional relations and conditional probability tables as described in [42]. An abstract model can then be derived from the extended influence diagrams and defense trees using Unified Modeling Language (UML). Finally, the abstract model can be instantiated to generate a concrete model from which a value for security and expected losses can be obtained.

It must be noted, however, that the above method also has significant drawbacks. The actual loss from an attack often cannot be computed even after the loss has occurred, and the range of expected losses can vary by several orders of magnitude depending on the specifics of what has taken place. It has been described as "an estimate multiplied by a guess computed to three digits of accuracy, and used to make multi-million dollar decisions" [40].

2.3 Attack Detection

In order to warn system operators whenever computer activity is outside its normal operating range, on-line, real-time surveillance capabilities are needed. Normal operating ranges can be determined based on historical usage patterns. A method of intrusion detection that uses stochastic processes to determine when computer systems have been compromised, such as from unauthorized access, changes to and destruction of files, and denial of service attacks, is discussed in [43]. Bounds for detection performance, as well as an analysis of optimal intrusion detection are also provided.

While pattern-recognition techniques can be used to identify patterns of attacks that have historically occurred they are unable to recognize novel or atypical attacks with

unique signature patterns. Databases of attack patterns must also be continually updated to remain valid. Anomaly-detection techniques, on the other hand, create a normal activity profile for the system, and signal attacks when observed activities differ considerably from the normal profile. Thus, they are able to detect both known and unknown attacks if they result in observed activities with irregular profiles. In [44], a method of anomaly detection is presented, which uses a Markov-chain model to determine the normal activity profile of a computer and network system.

2.4 Multi-agent Modeling

In [45], several requirements for effective cyber-defense systems are provided. These include the ability to be adaptive and evolve dynamically with changing network conditions. Moreover, a system must provide three levels of cyber-security. The first level includes "traditional" static cyber-defense mechanisms, such as identification, authentication, and cryptographic protections. The second level includes proactive cyber-defense mechanisms that provide, for example, information collection, security assessment, and attack detection and counteraction. The third level includes cyber-defense management such as evaluation of the network state, and the choice of adequate or optimal defense mechanisms and their adaptation.

In order to design defense mechanisms that meet the above requirements, a multi-agent-based approach is also proposed to examine distributed cooperative cyber-defense strategies against network attacks utilizing discrete-event simulations, and packet-level simulations of network protocols. To perform the simulations, a multi-level software

environment was developed using the OMNeT++ INET Framework. It must be cautioned, however, that cooperative decision-making strategies provide users with the following unique challenges [46]:

- Malicious users: dishonest ("Byzantine") participants (*Byzantine* refers to the Byzantine Generals' Problem, an agreement problem, where generals of the Byzantine army must decide unanimously whether to attack an enemy army. The problem is complicated by the fact that the generals are geographically separated, and thus they can only communicate by sending messengers, and the existence of traitors amongst the generals who are trying to doom any resulting attack.)
- Distinguishing tastes: the advice of one honest agent may not be helpful to others
- Temporal fluctuations: the quality of resources varies over time so that past experience is not necessarily predictive of future performance.

2.5 Evidence-Based Techniques

A technique to assess the effectiveness of cyber protection systems for critical infrastructure is presented in [47]. The technique focuses on three security primitives for cyber protection systems; authentication, network access control, and user access control, although others could easily be incorporated. For each security primitive, several categories of protection are described with each category providing a different level of security depending on the goals, skills, resources, and intent of the adversary based on Belief Theory. A method is also presented to calculate the effectiveness of the entire cyber protection system from which comparisons can then be made.

An example of the technique performed on a simple distribution system utilizing AMI is shown in Figure 2.2.

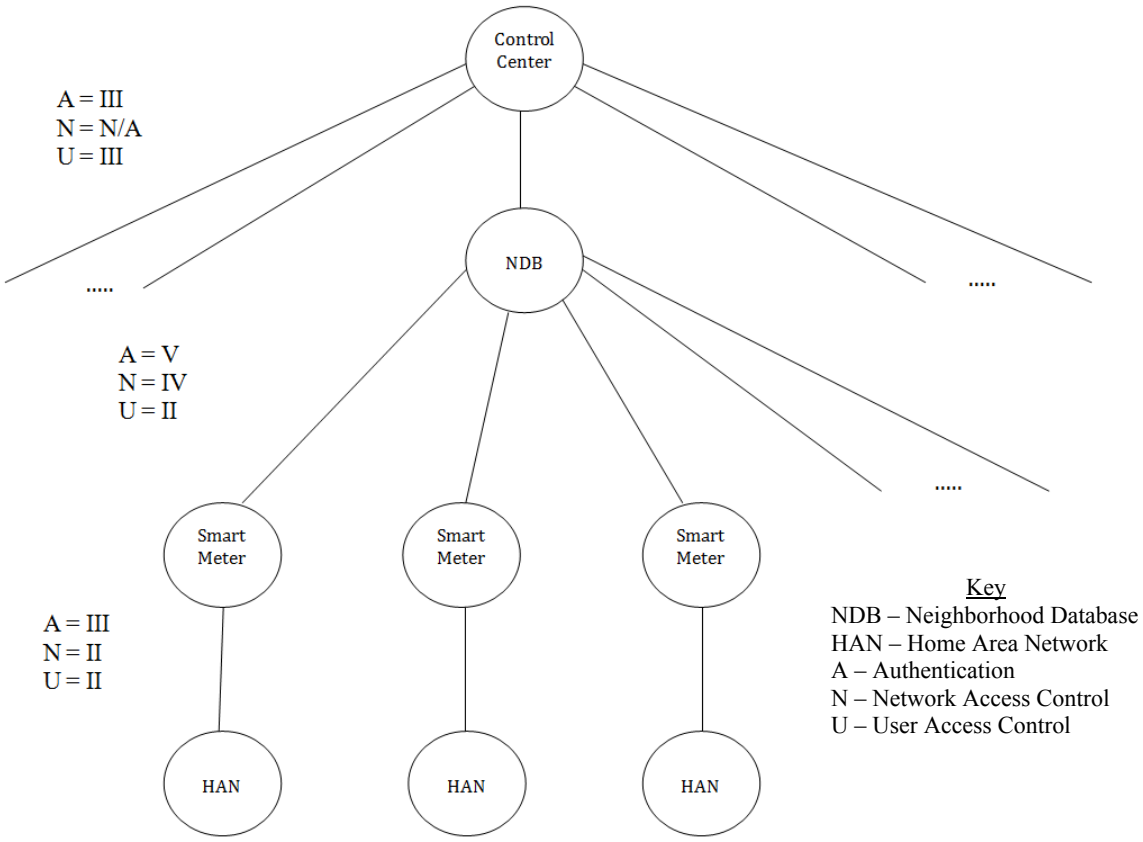

Figure 2.2: Example Distribution System Utilizing AMI

The system is composed of a control center connected to several neighborhood databases (NDB) that aggregate the information received from customer smart meters. Each smart meter is also connected to a home area network (HAN) located within each customer's residence. The three security primitives used for each network connection are authentication (A), network access control (N), and user access control (U). For each security primitive, a level of security is chosen with higher numbers representing greater security. For the system shown in Figure 2.2, typical security levels for such a system

were used. A description of each security level for each security primitive is provided in Table A.1, Table A.2, and Table A.3 in Appendix A.

The effectiveness of the system shown in Figure 2.2 to various threat categories is shown in Table 2.1.

Table 2.1: Cyber Protection System (CPS) Effectiveness

Cyber Threat Category	CPS Effectiveness
I	[0]
II	[0.34, 0.94]
III	[0.92, 1]
IV	[1]
V	[1]
VI	[1]

The greater the number of the threat category the weaker the threat. A description of the threat categories is provided in Table A.4 in Appendix A. The results show that the cyber protection system prevents threats from categories IV-VI with probability 1, but only protects against threats from categories II and III for a range of probabilities. The protection system is completely ineffective against threats from category I.

2.6 SCADA Systems

In the operation of an electric power system, a supervisory control and data acquisition (SCADA) system provides three critical functions: data acquisition, supervisory control, and alarm display and control. It consists of one or more computers with appropriate application software connected by a communications system to a number of remote terminal units (RTUs) placed at various locations to collect data, perform intelligent control of electrical system devices, and report results back to an

energy management system (EMS). A SCADA system can have real-time communication links with one or more EMSs and hundreds of substations [48].

A framework for a vulnerability assessment of cyber security for supervisory control and data acquisition (SCADA) systems is presented in [49]. The methodology integrates both a cyber-net model, used to define various intrusion scenarios and system status, and power flow simulations in order to quantify the effects of a potential cyber attack. In addition, security needs and solutions for SCADA systems are discussed in [26], and a broad overview of cyber security and risk assessment for SCADA systems and distributed control systems (DCSs) is presented in [50].

2.7 Summary

In this chapter, several methodologies found in the literature to model and evaluate cyber security defense systems for electric power and other critical infrastructure are presented. These included in the use of attack trees, Bayesian defense graphs, pattern recognition and anomaly-detection techniques, multi-agent based modeling approaches, evidence-based techniques, and methodologies for SCADA systems.

The next chapter provides a description of the capabilities, vulnerabilities, security needs, and recent advances for AMI. The implementation of AMI represents one of the first steps in the digitalization of control systems for the electric grid.

3 Advanced Metering Infrastructure

Presently, many utilities and other stakeholders are becoming increasingly interested in deployment of smart grid technologies such as advanced metering infrastructure (AMI). The installation of AMI provides two-way communication between customers and utilities, and it represents one of the first steps in the digitalization of control systems for the electric grid. Several countries including Italy, the Netherlands, Denmark, Sweden, and the United States have already taken initial steps toward the deployment of AMI by installing automated meter reading (AMR) systems, which can read measurement registers remotely. Sweden, for example, had nearly 100% utilization of AMR systems as of July 1, 2009 in order to meet legislation requiring that all electricity consumers with a main fuse of 63*A* or smaller have monthly energy meter readings [51].

AMI is widely considered to consist of the following components [52]:

- Smart Meter
- Customer Gateway
- AMI Communication Network
- AMI Headend

The smart meter is the source of all energy data and energy-related information. The customer gateway provides an interface between the AMI communication network and customer systems such as a home area network (HAN) or building management system

(BMS), which may or may not be built into the smart meter. The AMI communication network provides a communication link from the smart meter to the AMI headend, and the AMI headend handles the informational exchange between external systems such as a meter data management system (MDMS). A diagram of the relationship between the AMI system components is shown in Figure 3.1.

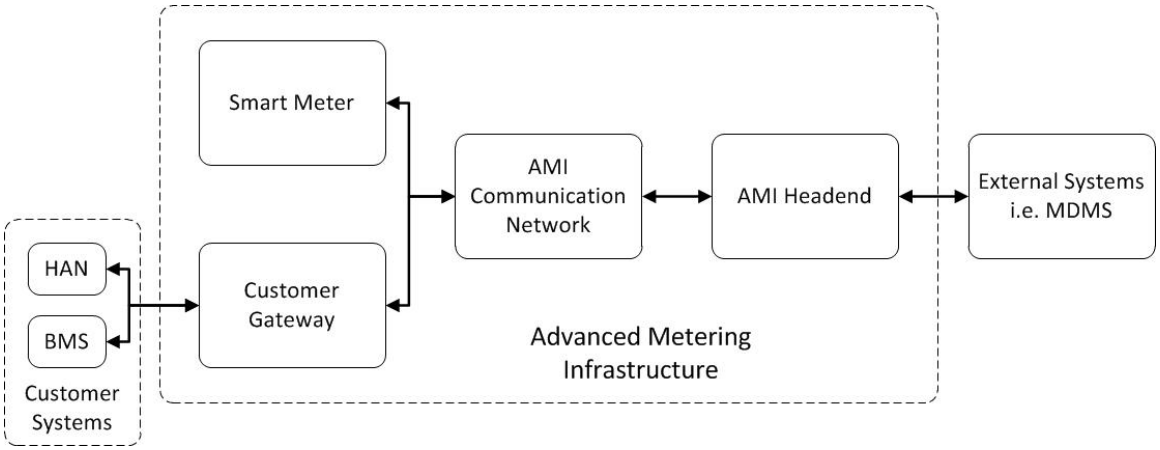

Figure 3.1: AMI System Components

Lesser versions of AMI include AMR systems, and automatic meter management (AMM) systems, which augment the capability of AMR systems with the ability to manage meters remotely [53].

3.1 Capabilities

AMI allows for numerous advanced capabilities in comparison to traditional electromechanical meters. Such capabilities include the following:

- Track customer usage such as total energy consumption
- Remotely connect and disconnect customers
- Send out alarms in case of problems

- Provide real-time pricing
- Remotely read measurement registers
- Send power quality data
- Reduce customer usage for non-paying customers
- Remotely receive firmware upgrades in order to update software and incorporate new functionality.

The flow of information through a typical AMI system is shown in Figure 3.2.

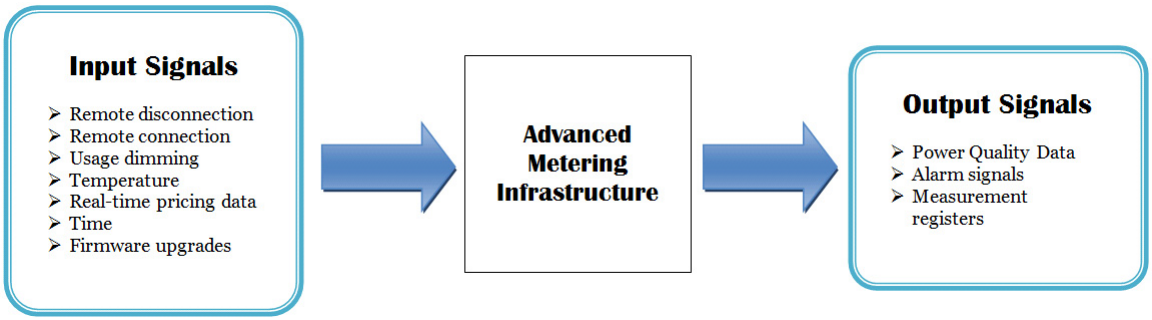

Figure 3.2: Typical AMI Information Flow

If measurements are made and transferred between customers and utilities at high frequency intervals, then large amounts of data will need to be transmitted requiring broadband connections. A discussion of specific communication requirements for AMI is presented in [53].

AMI will provide grid operators with increased control over gird operations by improving their ability to manage demand. For example, several customers could be simultaneously turned off on short notice in an emergency in order to balance the grid. Small amounts of load could also be curtailed during peak demand times in order to reduce significantly the need for expensive peaking generation. Often, curtailing as little as 5% of load can reduce the need for such generation by half [54].

Additionally, AMI can be integrated into home automation systems or HANs for automatic responses to varying real-time prices [53]. Consumer surveys indicate that many consumers are interested in real-time pricing, and results from Ameren's Energy Smart Pricing Plan (ESPP) pilot in Illinois and its ensuing Power Smart Pricing program have provided proof that consumers can and will respond to price signals [55]. Studies have also shown that significant benefits can be achieved from such programs even at modest penetration levels. Research performed by Carnegie Mellon's Electricity Industry Center has shown that in many cases only about 20% of the larger and more flexible customers need to adopt real-time pricing in order to get nearly 80% of the benefits that would be achieved if all customers participated in such a program [54].

3.2 Vulnerabilities

Despite the increased interest in the utilization of AMI, there has been very little assessment or research and development effort to identify the security needs for such devices. However, as more utilities move toward using Internet protocol (IP)-based systems for wide area communications and the trend of using standardized protocols continues throughout the industry [49], maintaining the security of such devices will be critical.

For example, smart meters are extremely attractive targets for exploitation since vulnerabilities can be easily monetized through manipulated energy costs and measurement readings. Currently, in the U.S. alone, it is estimated that $6 billion is lost by electricity providers to consumer fraud in the electric grid [9]. Given the immense

amount of data and energy-related information that is planned to be stored in smart meters, this amount could increase significantly.

The availability of such data also introduces earnest privacy concerns. Breaches into the data could expose customer habits and behaviors [9], [52]. Such arguments have led to the recent moratoriums on AMI installations in numerous Northern California communities and other areas throughout the country [56]. As a result, several key privacy concerns need to be addressed [35], [57], which include:

- Personal Profiling – using personal energy data to determine consumer energy behavioral patterns for commercial purposes
- Real-time Remote Surveillance – using live energy data to determine whether people are in a specific facility or residence and what they are doing
- Identity Theft and Home Invasions – protecting personal energy data from criminals who could use it to harm consumers
- Activity Censorship – preventing the use of energy for certain activities or taxing those activities at a higher rate
- Decisions Based on Inaccurate Data – shutting off power to life-sustaining electrical devices or providing inaccurate information to government and credit-reporting agencies.

Additional threats to the electrical grid introduced by the use of AMI include:

- Disrupting the load balance of local systems by suddenly increasing or decreasing the demand for power
- Gaining control of possibly millions of meters and simultaneously shutting them down
- Sending false control signals

- Disabling grid control center computer systems and monitors
- Disabling protective relays.

3.3 Security Needs

In order to defend against the vulnerabilities described in Section 3.2, several security features need to be incorporated into the development of AMI, along with new privacy laws to protect consumers. Current privacy laws in the United States are fragmented and vague, and do not specifically address consumer energy usage [9]. In [52], the generic security requirements for managing data are listed as follows:

- Confidentiality – Requirement that data is accessible only to authorized entities, and that intentional or unintentional disclosures of the data do not occur.
- Integrity – Requirement that data is authentic, correctly reflecting the source data, and complete, without unauthorized modifications, deletions, or additions. (This does not imply the data is valid, only that it is the same as the source.)
- Availability – Requirement that data is accessible by authorized entities whenever they need it.
- Non-Repudiation – Requirement that the entities receiving the data do not subsequently deny receiving it. The reverse is also true: that if the entities do not receive the data, then they cannot subsequently state that they did receive it.

The relationships between these security requirements and possible security threats are shown in Figure 3.3.

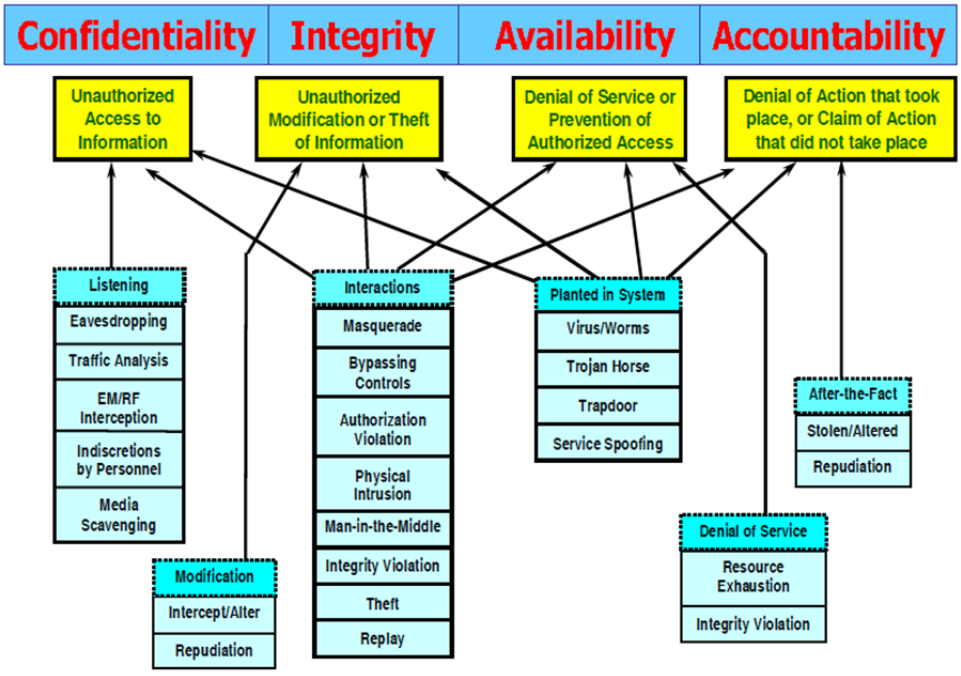

Figure 3.3: Security Requirements Undermined by Security Threats [52]

One security feature alone, such as encryption, will not be able to cover all possible security threats [52]. Since it will be imperative that the industry maintain 100 percent uptime, both physical security of the AMI system hardware, and multiple standard IT security features such as encryption and authentication will be needed [58], [59]. AMI systems will need to be defended against traditional cyber threats such as mobile/malicious code, denial-of-service attacks, misuse and malicious insider threats, accidental faults introduced by human error, and the problems associated with software and hardware aging [24]. Furthermore, since it will be impossible to protect against all threats, smart meters must be able to detect even the most subtle unauthorized changes [52] and precursors to tampering or intrusion.

To achieve these goals, timestamp information and continuous time synchronization across all AMI system components will be imperative. Additional consideration must also be given to the cost and impact that the security features will have on AMI system operations. Smart meters will still need to be cost-effective, since millions will need to be purchased and installed to replace antiquated analog devices, and they must also be robust, as they will be deployed in very insecure locations.

3.4 Demand Side Energy Management

An example of a recent advance in demand side energy management is the development and deployment of "smart" power cables produced by Packet Power [60]. Smart power cables allow users to digitally record the electrical energy consumption and other desired energy use information of electrical appliances wirelessly to an Internet database. Online software then analyzes the data to generate energy management reports for the user according to his or her specifications. Such features will soon become standard for major electrical household appliances. Whirlpool, for example, has recently announced that by 2015 all its appliances will be smart grid compatible [4], and will thus be able to interface with consumer's HANs and/or smart meters.

Sample results utilizing the smart power cables are shown in Figure 3.4 and Figure 3.5. Figure 3.4 depicts the electrical energy consumption for several rooms of a small two-bedroom apartment over a 24-hour period. The electrical energy consumption for each of the rooms along with the cumulative consumption for the entire apartment is shown. Figure 3.5 provides the corresponding average temperature at each of the smart

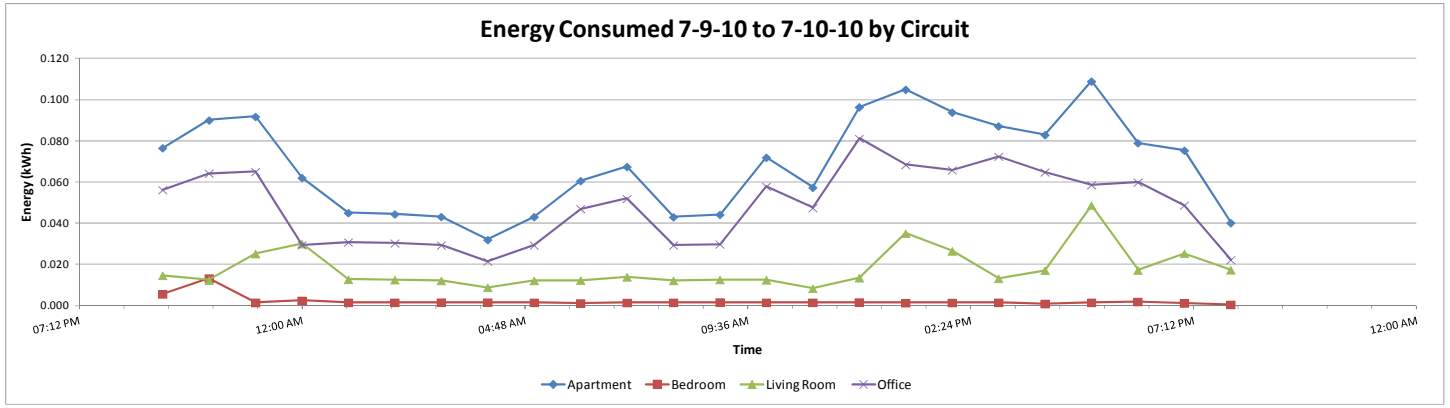

Figure 3.4: Energy Consumption by Room Over a 24-hour Period

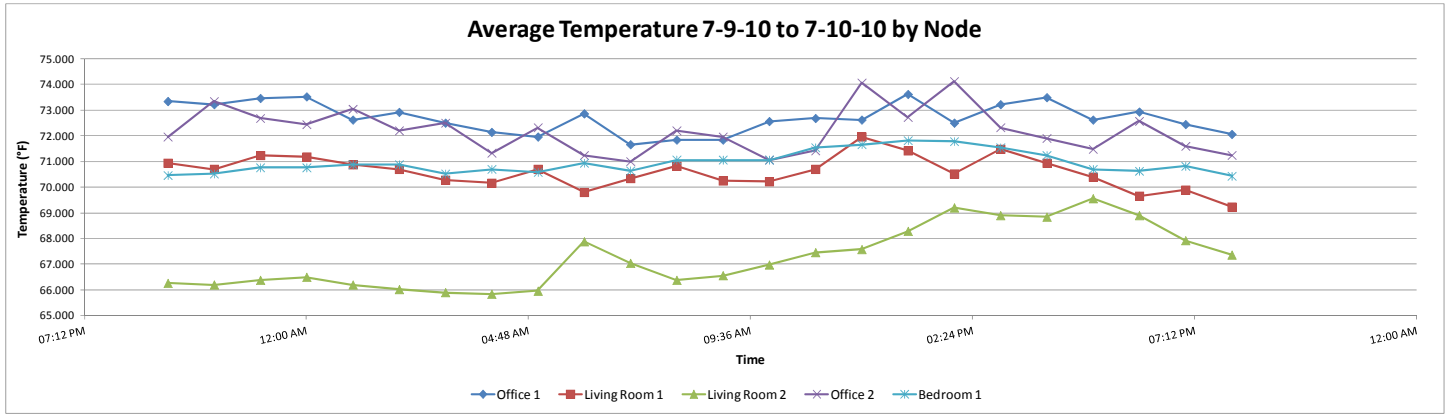

Figure 3.5: Average Temperature for each Smart Power Cable Over a 24-hour Period

power cables used to record the data, which were located throughout the apartment.

3.5 Summary

In this chapter, an overview of AMI and its proposed capabilities are presented. Despite the critical role that AMI will play in managing energy data, there has been very little work done to identify its security needs. To adequately protect such systems, several security features to be incorporated into the development of AMI are also described.

The next chapter provides a description of distribution automation systems (DAS), which use AMI. The development and wide-scale deployment of DAS represents one of the first steps in the smart grid transformation. In addition, an intelligent distributed secure control (IDSC) architecture that uses DAS is presented for distribution systems to provide greater adaptive protection, with the ability to proactively reconfigure, and rapidly respond to disturbances.

4 Distribution System Control

Due to its size, complexity, and cost, the transformation of the existing electrical grid to a smart self-healing system will need to occur in several stages over time with equipment being gradually replaced as it reaches the end of its operating life. Estimates by the U.S. DOE assess the value of the nation's electricity infrastructure to exceed $800 billion. Power plants comprise approximately 60% of this value, distribution facilities 30%, and transmission facilities 10%. Thus, the grid itself represents a total investment of approximately $320 billion [61].

Since almost 90% of all power outages and disturbances have their roots in the distribution network, the transformation should begin at the distribution level [62] where customers will see the greatest increase in performance. In the United States, initial investments in smart grid technologies have highlighted this fact. Of the $3.4 billion awarded by the American Recovery and Reinvestment Act (ARRA) Smart Grid Investment Grants (SGIGs), announced in October 2009, only $148 million (less than 5%) went to transmission related projects [63]. Nearly all the rest went to distribution related projects.

In particular, distribution systems are responsible for transferring electricity from the high-voltage 100-800kV power grid to commercial, industrial, and residential customers. Currently, distribution systems serve approximately 138 million customers by supplying 3.66 trillion kWh of electricity [64]. Primary distribution lines consist of

medium-voltage circuits that range from 600V- 35kV, while secondary distribution lines consist of low-voltage circuits often either 120V or 240V. Although system shapes and sizes vary widely depending on their location and the population being served, on average they provide a peak load of 7MVA, cover 25 square miles, and serve 400 customers. A list of typical distribution system circuit parameters is provided in Appendix B.

The various operating states of a distribution system are shown in Figure 4.1.

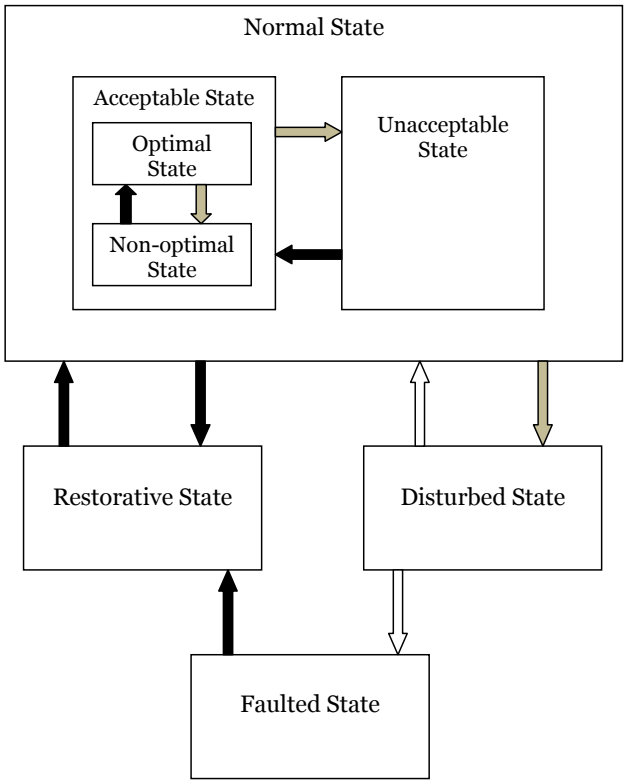

Figure 4.1: Distribution System Operating States and State Transitions [65]

The normal state functions commonly consist of planning tasks, while those outside it tend to be operational problems. The normal state is divided into two sections, an acceptable state, and an unacceptable state. The acceptable state includes both optimal

and non-optimal states. The unacceptable state comprises constraint violations that must be detected by network analysis, but does not include disturbed states, which are events that are detected and alarmed by SCADA functions. When a disturbance is detected, such as a faulted feeder, an alarm is signaled and the system enters the faulted state where it is removed from service. Once corrective action has been taken to compensate for the faulted event, such as opening switches to return the faulted feeder to service, the system enters the restorative state. In addition, a feeder that has been faulted or switched open for maintenance purposes, and is now being returned back to service, would also be considered as being in the restorative state.

Transitions between states are also depicted in the diagram. They can be caused by either automatic operation (white arrow), operator action (black arrow), or external factors (grey arrow). Automatic operations include the opening or closing of protective relays or breakers, and external factors include those that cause state changes independent of the operator, such as faults or load changes.

4.1 Distribution Automation Systems

A first step in the smart grid transformation will be in the development and wide-scale deployment of distribution automation systems (DAS). DAS allow long-duration interruptions to be reduced to momentary interruptions by allowing the rapid isolation of faults and restoration of the network [66]. Currently, only a small minority of distribution systems worldwide are equipped with such capabilities. Even in North America, home of one of the world's most advanced power systems, less than a quarter

of the distribution system is equipped with information and communications systems, and only about 15% to 20% of the system at the feeder level. As a result, many utilities believe that initially investing in DAS will provide them with increasing capabilities over time, as shown in Figure 4.2.

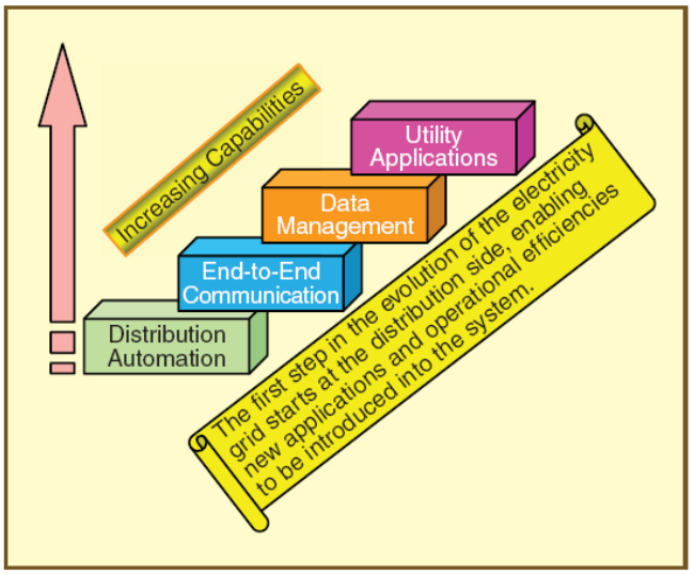

Figure 4.2: Utility-desired Capabilities [62]

DAS are equipped with information and communications systems to provide system dispatchers with support for day-to-day operations. Common functions include [67]:

- Automatic bus sectionalizing: the ability to rapidly isolate one section of a bus from the others if a bus fault were to occur on that section.
- Feeder deployment switching and automatic sectionalizing: the ability to control feeder switches remotely, and to rapidly isolate a feeder section due to a fault or other disturbance.
- Integrated volt/var control: the ability to keep feeder voltages within prescribed limits through the control of a combination of transformers

with load tap changers, voltage regulators, and switched capacitors, and the ability to control the flow of reactive power.

- Substation transformer load balancing: the ability to monitor the loading of transformers to prevent overloads, burnouts, or abnormal operations by timely reinforcement, replacement, or reconfiguration.
- Feeder load balancing: the ability to monitor feeder loads and line sections, and reconfigure feeders as necessary to prevent overloads or abnormal operations.
- Remote metering: the ability to manage meters remotely.
- Load control: the ability to directly control customer appliances such as water heaters, air conditioners, and other major loads.

In addition, they provide the dispatcher with emergency control of: voltages, reactive power, load shedding of preplanned feeders, general feeder load pickups after major outages, and control of dispersed generation located anywhere on the distribution network [67].

4.2 Intelligent Distributed Secure Control

The control of DAS can be either centralized or decentralized. In centralized control, all computing and control functions are based in one centralized location, while in decentralized control computing and control functions may be dispersed in many different locations. Arguments in favor of centralized control include reduced generator fuel costs due to more coordinated operation, improved dynamic control and security because more of the system is being controlled from one point, and easier implementation. Arguments in favor of decentralized control include the insignificance

of economic-dynamic improvements obtainable from centralization, the fear of major catastrophes from the failure of centralized control, existing institutional constraints (different utilities in different states, etc.), and the ability to respond quicker to local adverse events [5]. However, the lack of information exchange may lead to unreliable or biased decision making.

Thus, an intelligent form of decentralized control is needed to respond quickly to adverse events, and make reliable and unbiased decisions. Reference [68] states that for deeper and layered protection, an intelligent distributed secure control (IDSC) is required, which would enable parts of the network to remain operational and even automatically reconfigure in the event of local failures or threats of failure. With distributed intelligence and components acting as independent agents, those in each isolated area would have the ability to reorganize themselves and make efficient use of whatever local resources remain to them in ways consonant with established global goals to minimize adverse impacts on the overall network. Local controllers would then be able to guide the isolated areas to operate independently while preparing them to rejoin the network, without creating unacceptable local conditions either during or after the transition.

Numerous sources in the literature proclaim how future distribution systems will employ control and communications technologies to achieve such goals. They discuss numerous operating capabilities such as how "the switches will communicate with each other and, using preset conditions, or even artificial intelligence, will operate without human intervention" [64]. The literature, however, provides few descriptions or models

of how such objectives will be achieved and no analysis of the effects such technology will have on system operations.

4.2.1 Architecture

To achieve the desired goals stated above, an IDSC architecture for distribution systems was developed. The model is based upon the Strategic Power Infrastructure Defense (SPID) system control architecture produced by the CIN/SI for systems with intelligent wide-area sensing, protection, and reconfiguration capabilities [29], [69], and uses the concepts of adaptive and self-healing protection central to the SPID system. Specifically, adaptive and self-healing control strategies are used to steer power systems to more secure, less vulnerable operating conditions [69]. A diagram of the resulting control architecture is shown in Figure 4.3.

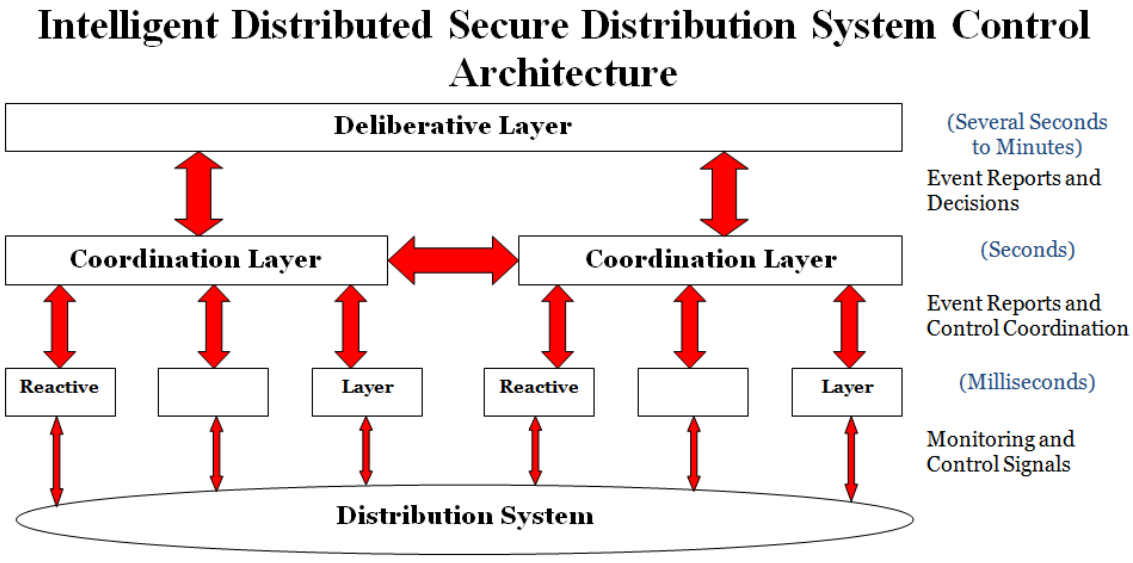

Figure 4.3: Intelligent Distributed Secure Distribution System Control Architecture (Adapted from [29])

The architecture uses three layers composed of numerous independent, intelligent agents. A thorough description of what intelligent agents are and how they operate is provided in [70]. In general, an intelligent agent is a controller that is able to take automatic action and make decisions based on whatever local information is available to it, but still provides system operators with the ability override such decisions when necessary. In the architecture, the agents gather and exchange information with each other in real-time or near real-time in order to provide coordinated protection and to optimize system performance. Some possible locations for different agents at each layer of the control architecture and their corresponding control functions are listed in Table 4.1.

Table 4.1: Distribution System Intelligent Agents and Functionalities

Layer	Agent Locations	Control Functions
Reactive	-Smart Meters -Substations -DERs	- Demand response - Load management - Connect/disconnect load - Send alarm signals
Coordination	-Switches	- Connect islands - Connect substations - Disconnect compromised sections - Send alarm signals
Deliberative	-Microgrids -Feeder Systems	- Determine system objectives - Optimal radial reconfiguration for each island (e.g. min. losses) - Determine electricity price - Calculate power flows - Send alarm signals

In addition, a diagram of example control functions and signals being sent between different agents at each layer of the control architecture is shown in Figure 4.4. In the diagram, each block represents the control functions for the agents at that layer,

with the bottom block representing the reactive layer, the middle block representing the coordination layer, and the top block representing the deliberative layer.

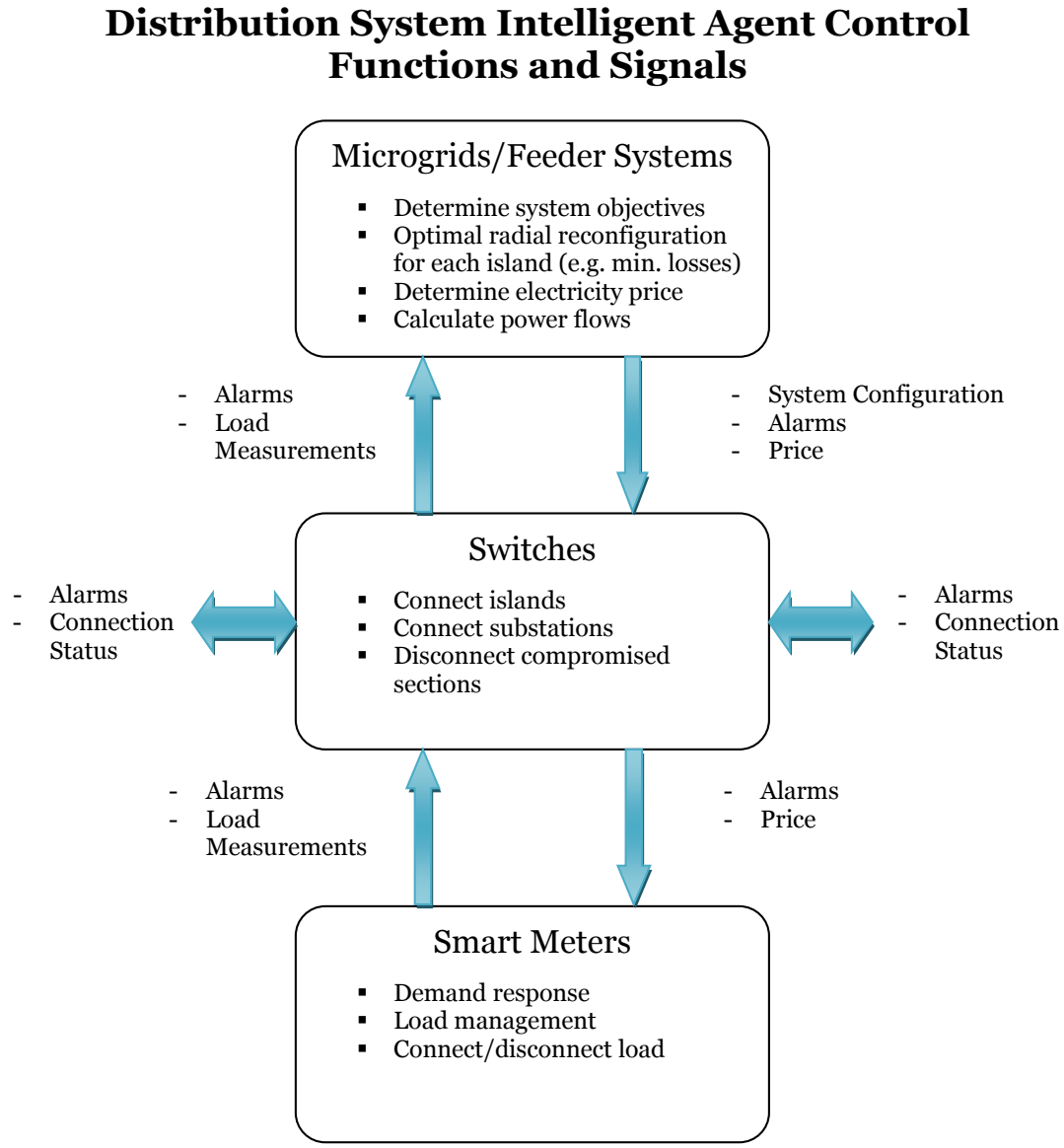

Figure 4.4: Distribution System Intelligent Agent Control Functions and Signals

The control architecture can then be implemented in conjunction with a multiagent-based intrusion prevention system, such as the one described in [71], in order

to detect and prevent cyber attacks over the network. A multiagent cyber security approach has several advantages for network and distributed systems, including reduced network load, overcoming network latency, platform independency, and fault tolerance.

4.2.1.1 Reactive Layer

At the lowest control level, the reactive layer is composed of agents located at each smart meter, substation, and distributed energy resource (DER) in the system. The agents gather and exchange information with adjacent coordination level agents. They respond to incoming price signals and alarms by performing demand response and load management functions, such as shedding load or shifting load to lower price times, and by connecting or disconnecting load from the distribution system. In return, load measurement data and alarm signals are sent back up to the coordination layer.

4.2.1.2 Coordination Layer

The coordination layer is composed of agents located at each switch in the system. The agents exchange information with each other as well as forward signals sent by the reactive and deliberative layer agents to their appropriate destinations. They make decisions regarding their connection status, and take swift action if faults or attacks are detected. They have the ability to recognize if they are islanded from the rest of the system and to utilize whatever local resources are available to them. In addition, they implement optimal system configurations as determined by the deliberative layer agents.

4.2.1.3 Deliberative Layer

Finally, the deliberative layer is composed of agents located at the microgrid or feeder system level. The agents gather and exchange information with adjacent coordination layer agents, and determine the overall system objectives such as increased network reliability or minimized line losses. They also determine the optimal system configuration for each island in their system based on the chosen system objectives and send these control signals down to the coordination layer agents for implementation. Furthermore, they perform analysis on their systems to determine if all operating constraints have been met and aggregate system load in order to submit bids into real-time electricity markets at the transmission system level.

4.3 Decentralized and Centralized Control

Conversely, more decentralized or centralized control architectures can be used as shown in Figure 4.5 and Figure 4.6 respectively. Numerous simulations comparing the performance of these control architectures with the IDSC architecture are described in Chapter 6. The decentralized control architecture does not use deliberative layer agents for centralized decision-making. Thus, coordination and reactive layer agents use only local information, and reconfiguration is performed using preprogrammed switching priorities. For the simulations performed in Chapter 6, switches were prioritized by 1) being in the minimum loss configuration and 2) being connected to the lowest numbered adjacent node. In contrast, the centralized control architecture does not use coordination layer agents for distributed decision-making. Thus, it is assumed that reconfiguration

capabilities are not available in real-time, and can only be implemented with advanced planning, such as for maintenance or planned outages.

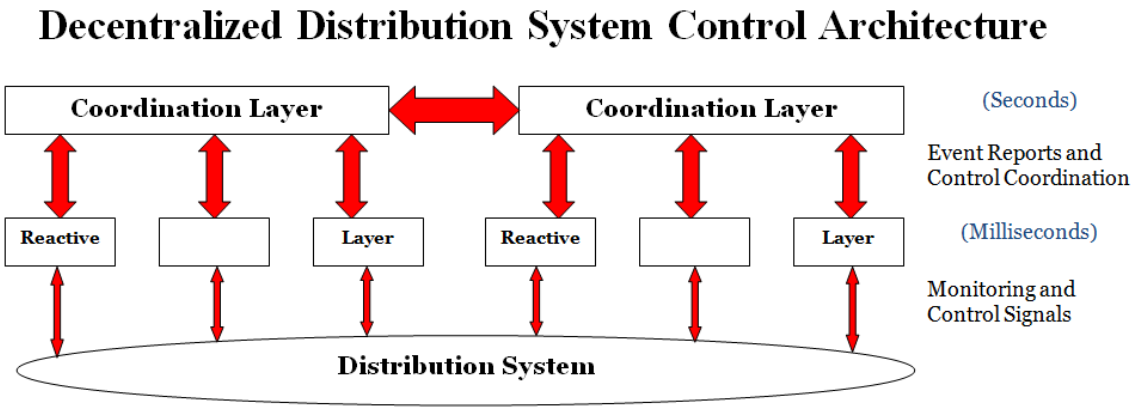

Figure 4.5: Decentralized Distribution System Control Architecture

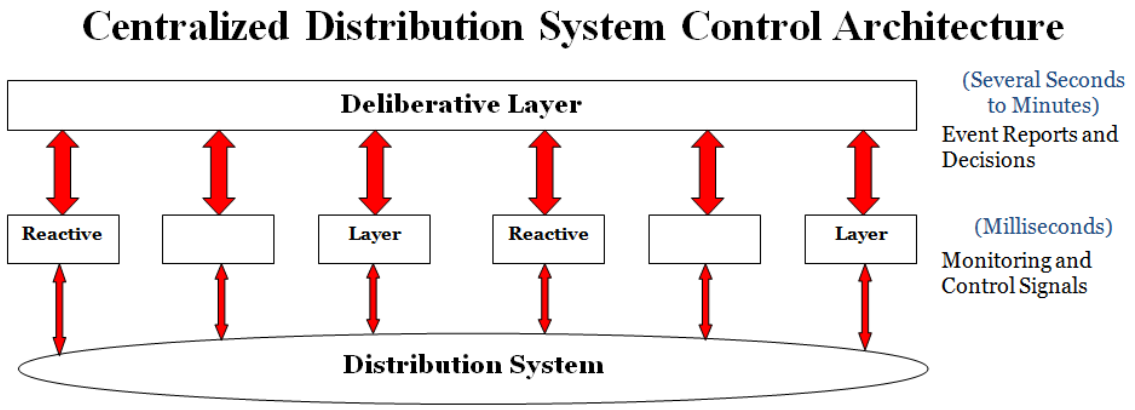

Figure 4.6: Centralized Distribution System Control Architecture

4.4 Summary

In this chapter, several functions of DAS are described, which provide system dispatchers with support for day-to-day operations. Utilizing DAS, an IDSC architecture is also presented for more robust distribution system operations. Detailed descriptions of functionalities at each layer of the architecture as well as the whole system are provided.

The next chapter explores the distribution system reconfiguration problem, one of the most important tasks of DAS. To solve this problem, a solution approach called annealed local search (ALS) is presented. ALS is specifically designed to handle the radial structure of distribution systems, and overcomes many of the shortcomings encountered by other proposed solution methods.

5 Dynamic Reconfiguration

In 2007, the United States Congress passed the Energy Independence and Security Act (EISA) outlining specific goals for the development of the nation's smart grid. Section 1301 of the act states that, "It is the policy of the United States to support the modernization of the Nation's electricity transmission and distribution system to maintain a reliable and secure electricity infrastructure that can meet future demand growth and to achieve each of the following, which together characterize a Smart Grid:

1) Increased use of digital information and controls technology to improve reliability, security, and efficiency of the electric grid.
2) Dynamic optimization of grid operations and resources, with full cyber-security…" [35].

In order to meet the above objectives for power distribution systems (≤ 35kV), an IDSC architecture was developed as described in Section 4.2 along with a method to dynamically optimize its configuration, which is described in this chapter. The control architecture provides deeper and layered protection against threats and the ability to respond quickly to attacks and disturbances by taking advantage of digital information and controls technology. Dynamic optimization allows the system to continually reconfigure itself to maximize system performance and minimize or prevent disturbances.

5.1 Distribution System Reconfiguration

Distribution system reconfiguration is one of the most important tasks of DAS. The objective is to determine the status of switches in the network in order to optimize system performance. The types of switches include both sectionalizing switches (normally closed) and tie-switches (normally open), and large feeder systems can contain several hundred switches. Normally, distribution system reconfiguration is performed for the following reasons [72], [73], [74], [75]:

1) To reduce line losses
2) To alleviate network overloads
3) To restore service to as many customers as possible following a fault on the system
4) To increase network reliability.

The majority of past work has focused on minimizing line losses. IDSC, however, provides the grid with the ability to dynamically optimize its configuration in the event of local failures or the threat of failures. Thus, new objectives can be developed for distribution system reconfiguration to take into account current system operating conditions.

5.1.1 Performance Metrics

Reference [48] specifies the four key performance metrics used to assess electric power systems. These include security, quality, reliability, and availability (SQRA).

5.1.1.1 Security

Traditionally, the security of a power system is defined as the capability of a system "to experience contingencies (outages) and maintain service to all customers and respect all equipment limits" [48]. However, specific standards or indices for measuring security performance do not currently exist. Moreover, for traditional distribution systems such a definition is not meaningful. For example, in a single source radial feeder, any outage will result in customer interruptions, and thus, by definition, the system is insecure.

5.1.1.2 Quality

Power quality refers to the set of parameters that enables electrical equipment to function properly with minimum or no harmonics. Several metrics have been developed to quantify power quality issues such as voltage sag, acceptable harmonic distortion, flicker, and unbalance levels. One of the most common power quality issues and often the most controversial between customers and utilities is voltage sag. *Voltage sag* is defined in [66] as "an rms reduction in the ac voltage, at the power frequency, for durations from a half cycle to a few seconds." Often, voltage sag problems are initiated by transmission and distribution system faults.

The most widely used power quality index is the System Average RMS (Variation) Frequency Index (SARFI). SARFI, as defined in [66], is shown in (5.1).

$SARFI_X$, System Average RMS (Variation) Frequency Index: represents the average number of specified rms variation measurement events that occurred over the assessment period per customer served, where the

specified disturbances are those with a magnitude less than X for sags or a magnitude greater than X for swells.

$$SARFI_X = \frac{\sum_{\forall i} N_i}{N_T} \tag{5.1}$$

Where:

X - rms voltage threshold; possible values are 140, 120, 110, 90, 80, 70, 50, and 10

N_i - number of customers experiencing short-duration voltage deviations with magnitudes above $X\%$ for $X > 100$ or below $X\%$ for $X < 100$ due to measurement event i

N_T - number of customers served from the section of the system to be assessed.

5.1.1.3 Reliability

Reliability metrics are used to measure the performance of a given transmission or distribution system. Numerous indices have been developed for this purpose. Often, these include some variation of the frequency of interruptions, time between interruptions, total duration or restoration time, number of end users affected, or the number, duration, or severity of outage events. Three of the most commonly used reliability indices are the System Average Interruption Frequency Index (SAIFI), the System Average Interruption Duration Index (SAIDI), and the Customer Average Interruption Duration Index (CAIDI), which are used to measure the system frequency, system duration, and customer duration of interruptions respectively over a given time period, often several years. These indices, as defined in [66], are shown in (5.2), (5.3), and (5.4).

SAIFI - System Average Interruption Frequency Index

$$SAIFI = \frac{Total\ \#\ of\ customer\ interruptions}{Total\ \#\ of\ customers\ served} \tag{5.2}$$

SAIDI - System Average Interruption Duration Index

$$SAIDI = \frac{Sum\ of\ all\ customer\ interruption\ durations}{Total\ \#\ of\ customers\ served} \tag{5.3}$$

CAIDI - Customer Average Interruption Duration Index

$$CAIDI = \frac{SAIDI}{SAIFI} = \frac{Sum\ of\ all\ customer\ interruption\ durations}{Total\ \#\ of\ customer\ interruptions} \tag{5.4}$$

Using the reliability indices in (5.2)-(5.4), studies performed by the IEEE Working Group on Distribution Reliability have concluded that distribution system reliability is deteriorating across the country [64]. A graph of the indices recorded from 2000-2005 is shown in Figure 5.1.

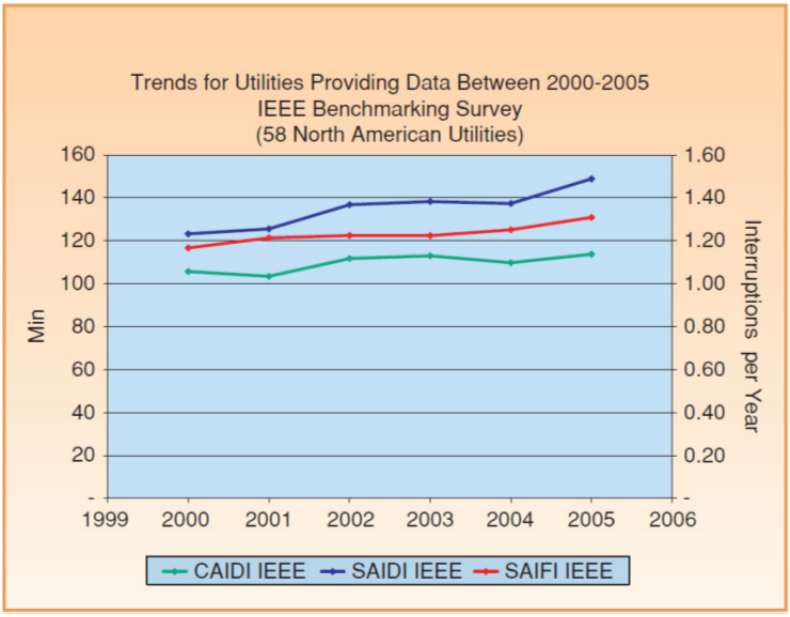

Figure 5.1: National Distribution System Reliability Performance (2000-2005) [64]

Furthermore, customer electricity service issues have also been increasing. A graph of the number of customer complaints for Xcel Energy, the state of Minnesota's largest electricity provider, for 2009-2010 is shown in Figure 5.2 broken down by complaint type. A list of the specific complaints included in each complaint type is provided in Table 5.1. The data was provided by the Minnesota Public Utilities Commission (PUC), and it is representative of all investor owned utilities throughout the state.

5.1.1.4 Availability

Availability refers to the operating time, or up time, of a system stated as a percent of the total time of interest. It can be calculated using the reliability indices (5.2) and (5.3) as specified in [66], and is shown in (5.5).

ASAI - Average Service Availability Index

$$ASAI = \frac{SAIDI}{SAIFI} = \frac{Customer\ hours\ service\ availability}{Customer\ hours\ service\ demanded} \tag{5.5}$$

5.1.2 Objective Function

An objective function is proposed in this dissertation in order to optimize the performance metrics described above in Section 5.1.1. The objective aims to minimize the expected impact of cyber and physical disturbances on a system by taking into account its reliability, and the availability of its sensing, communications, and control systems. The latter is accounted for using the availability of each intelligent agent, which is continually changing due to the effects of cyber and physical disturbances. The availability of each intelligent agent is calculated by finding the percentage of time it is

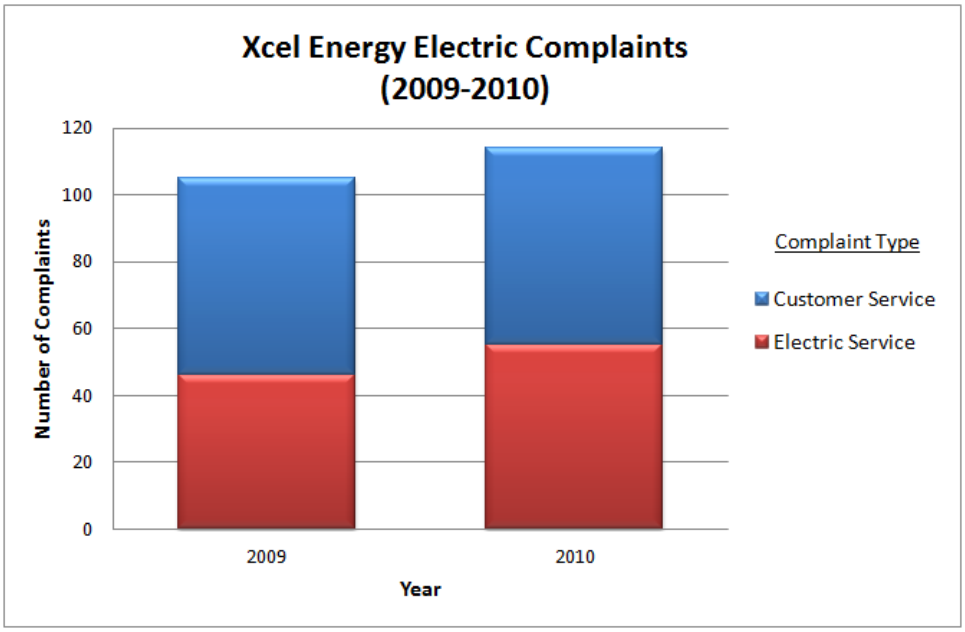

Figure 5.2: Xcel Energy Electric Complaints (2009-2010) (Minnesota PUC)

Table 5.1: Electric Complaint Types

Customer Service	Electric Service
Billing Dispute	Company Equipment Failure
Cold Weather Rule Miscellaneous	Gas Leak
Disconnect w/o Notice	Lines Equipment
Disconnect/Reconnect	Meter Malfunction
Disconnection by Company Error	Miscellaneous Meter Issues
Discourteous Company Representative	Miscellaneous Service Issues
Department of Commerce Issues/Referrals	Service Area
Install Delay/Held Order	Service Interruptions
Medical Emergency Statement	Stray Voltage
Miscellaneous Billing Issues	Voltage/Low Pressure Variation
Miscellaneous Customer Service	
Miscellaneous Disconnection/Refusal of Service	
Payment Arrangement	
Repair Delay	

operating in the up state over the total time being measured as shown in (5.6). Such values can be determined from operating records for each individual agent.

$$Agent\ Availability = \frac{Up\ time}{Total\ time\ period\ measured} \tag{5.6}$$

The expected impact of disturbances on a system is measured by computing the loss of energy expectation (LOEE) for a given configuration. The LOEE is calculated by finding the sum of the probabilities that the path from each load to its source is unavailable weighted by its load. The probability of each path being unavailable is one minus the product of the reliabilities and availabilities of each line and intelligent agent respectively encountered in the path. The LOEE and the path availability calculations are shown in (5.7) and (5.8) respectively.

$$LOEE = F(N, P_{load}, T) = \sum_{\forall i \in B, i \neq s} (1 - N_{is}) \times P_{load_i} \times T \tag{5.7}$$

$$N_{is} = \prod_{\forall j,k \in L_{is}} R_{jk} \times \prod_{\forall l \in D_{is}} A_l \tag{5.8}$$

Where:

F - system LOEE

B - set of all buses

P_{load} - set of all real power loads

P_{load_i} - real power load at bus i

N - set of all path availability probabilities

N_{is} - path availability probability of path from bus i to source bus s

T - length of time period being measured

L_{is} - set of all lines in the path from bus i to source bus s

R_{jk} - reliability of the line from bus j to bus k

D_{is} - set of all intelligent agents encountered in the path from bus i to source bus s

A_l - availability of intelligent agent l

For example, a 4-bus system is shown in Figure 5.3, with the intelligent agents as described in Section 4.2.

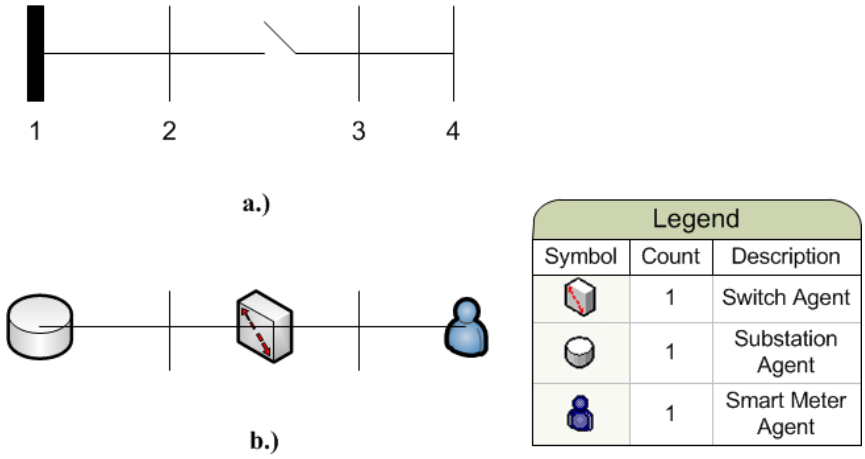

Figure 5.3: a.) 4-Bus One-Line Diagram b.) 4-Bus Diagram with Intelligent Agents

The path availability probability for a load at bus 4 to reach the substation at bus 1 is the product of the availability of the smart meter agent at bus 4, the reliability of line 3-4, the availability of the switching agent located between buses 2 and 3, the reliability of line 1-2, and the availability of the substation agent at bus 1.

5.1.3 Problem Formulation

Constraints are added to the problem to ensure that all operating conditions are met. To maintain standard utility operating practices, the system is required to remain radially connected, and all scheduled loads must be served, if possible. Radial system configurations are characterized by having a set of series components between a substation and each load point. Such configurations account for over 99% of all

distribution systems in North America [76]. They are widely used because they provide numerous advantages. These include [66], [76]:

- Easier fault current protection
- Lower fault currents over most of the circuit
- Easier voltage control
- Easier prediction and control of power flows
- Lower cost

Furthermore, since power can only flow one way in a radial system, its analysis and predictability of performance is greatly simplified. While radial systems are less reliable than more complex configurations, "the additional cost of an inherently more reliable configuration … cannot possibly be justified for the slight improvement that is gained over a well-designed radial system" [76]. Moreover, feeder systems are almost never connected between substations since this puts the feeder network path in parallel with the transmission path between substations and results in unacceptable loop and circular flows, and large dynamic shifts in load on the distribution system [76].

The resulting formulation for the distribution system reconfiguration problem is shown in (5.9)-(5.17).

$$\min \; F(x) \tag{5.9}$$

$s.t.$

$$\left(P_{gen_i} - P_{load_i}\right) - \text{Real}\left\{V_i \left(\sum_{k=1}^{|B|} Y_{ik}\, V_k\right)^*\right\} = 0 \quad \forall i \in B \tag{5.10}$$

$$\left(Q_{gen_i} - Q_{load_i}\right) - \text{Imag}\left\{V_i \left(\sum_{k=1}^{|B|} Y_{ik}\, V_k\right)^*\right\} = 0 \quad \forall i \in B \tag{5.11}$$

$$|V_i|^{min} \leq |V_i| \quad \forall i \in B \tag{5.12}$$

$$S_{ij} \leq S_{ij}^{max} \quad \forall i, j \in L \tag{5.13}$$

$$\sum_{i,j \in L} x_{ij} = |B| - 1 \tag{5.14}$$

$$\sum_{i,j \in (W,W)} x_{ij} \leq |W| - 1 \quad \forall W \subseteq B \tag{5.15}$$

$$x_{ij} = 1 \quad \forall i, j \in L_P \tag{5.16}$$

$$x_{ij} \in \{0,1\} \quad \forall i, j \in L_T \tag{5.17}$$

Where:

P_{gen_i} - real power generation at bus i

Q_{gen_i} - reactive power generation at bus i

Q_{load_i} - reactive power load at bus i

Y_{ik} - i, k term of the bus admittance matrix

V_i - complex voltage at bus i

$|V_i|$ - voltage magnitude at bus i

$|V_i|^{min}$ - minimum voltage magnitude limit at bus i

S_{ij} - complex power flow on line from bus i to bus j

S_{ij}^{max} - maximum complex power flow limit on line from bus i to bus j

L - set of all lines

L_p - set of all permanent lines in L

L_T - set of all switches in L

x_{ij} - decision variable for the line from bus i to bus j (1 if in configuration, 0 otherwise)

(W, W) - denotes all lines that go from a bus in the set W to another bus in the set W

Constraint (5.10) represents the real power equality constraints, (5.11) the reactive power equality constraints, (5.12) the bus voltage magnitude limits, (5.13) the line complex power flow limits, (5.14) and (5.15) the condition that the system be radially connected, and (5.16) the condition that all permanent lines be included in the configuration. To implement constraints (5.12) and (5.13), they are added as penalty factors to the objective function. The penalty factor formulations used for the bus voltage magnitude limits and the line complex power flow limits are shown in (5.18) and (5.19) respectively.

$$voltage\ mag.limits\ penalty\ factor = \sum_{\forall i \in B} \max\left[\frac{|V_i|^{min} - |V_i|}{|V_i|^{min}}, 0\right] \qquad (5.18)$$

$$line\ flow\ limits\ penalty\ factor = \sum_{\forall i,j \in L} \max\left[\frac{S_{ij} - S_{ij}^{max}}{S_{ij}^{max}}, 0\right] \qquad (5.19)$$

5.2 Annealed Local Search

Distribution system reconfiguration represents a discrete optimization problem. Since typical distribution systems can include hundreds of switches, exhaustive enumeration of all possible combinations (2^n) would quickly become computationally infeasible. This problem is further complicated by the addition of constraints such as those listed in (5.10)-(5.15). Nevertheless, the performance of the optimization, and ultimately the potential cost savings, increases dramatically as the number of switches increases [77]. Thus, the analysis technique must be able to handle large systems.

Both genetic algorithms [73] and simulated annealing [78] have been applied to similar discrete optimization problems, but they encounter difficulty with the radial structure of distribution systems. Reference [79] states two reasons for this being that:

1) Most of the generated switch position combinations will not represent feasible solutions.
2) Generating a new radial tree structure for each combination of switch positions is computationally intensive.

In addition, branch-and-bound methods have been attempted, but they provide no assurance that convergence will be reached, and for the cases where convergence is reached, the computational burden to solve them is extremely high [75].

To determine the optimal radial configuration for the problem formulation described in Section 5.1.3, annealed local search (ALS) is used. ALS takes advantage of the radial structure of distribution systems and overcomes the shortcomings encountered by genetic algorithms and simulated annealing. The algorithm is based on the one described in [79] for distribution system reliability optimization problems, which has been successfully applied to topologically diverse systems with up to 345 switches.

To adapt the algorithm for the current problem, a few modifications were implemented. The original algorithm made use of the *tie switch shift*, where a normally open switch is closed and a nearby upstream switch is opened, to make incremental changes to the radial system structure. However, to ensure that all feasible switch combinations were searched utilizing IDSC, search tables comprising the switches currently in the closed position, and those available in the opened position were

generated. Each of the feasible switch combinations was then searched. The resulting method was found to be both efficient, and straightforward to implement.

Specifically, the algorithm works by searching the possible switch combinations and it makes small changes to the system via opening a closed switch and closing an available opened switch. At the beginning of each iteration loop, two tables are generated, one comprising the switches currently in the closed position and the other comprising the available switches in the opened position. The available opened switches include those whose switching agents are available during the period of interest and are not connected to any sections that have been compromised. The algorithm then checks each of the switching combinations to ensure that the resulting configuration is feasible by being both radial and spanning all of the previously connected buses. If the new configuration meets this criteria and the objective function value improves, then the configuration is saved, and the process continues until a local optimal solution is reached.

In order to overcome the problem of identifying solutions that differ significantly from the initial configuration, [79] describes a method that allows "a greater search area to be explored by probabilistically accepting certain solutions with worse objective functions" to increase the "likelihood of a near-optimal solution being discovered." The method uses a temperature, $\tau \in [0,1]$, that determines whether a solution with a worse objective function value is accepted, and an annealing rate, $\rho \in [0,1)$, that determines the rate at which the temperature is decreased during each iteration loop. The initial temperature, τ_o, controls how much of the search area is initially explored. Following each iteration loop, the temperature continues to decrease until the solution ceases to

change, at which point the algorithm terminates. Furthermore, the algorithm ensures local optimality since it reduces to integer programming at a temperature of zero. A flow chart depicting the algorithm is provided in Figure 5.4.

5.3 Summary

In this chapter, the distribution system reconfiguration problem, one of the most important tasks of DAS is presented. In addition, an objective function is proposed for the reconfiguration problem that optimizes several of the key performance metrics for power systems. To solve this problem, a solution approach called ALS is described, which is specifically designed to handle the radial structure of distribution systems.

The next chapter develops several simulation models to compare the performance of the IDSC architecture and ALS with other control architectures and optimization algorithms. Results for the IEEE 123 node test feeder are presented and show the trade-offs between system reliability, operational constraints, and costs for the different control architectures and optimization algorithms.

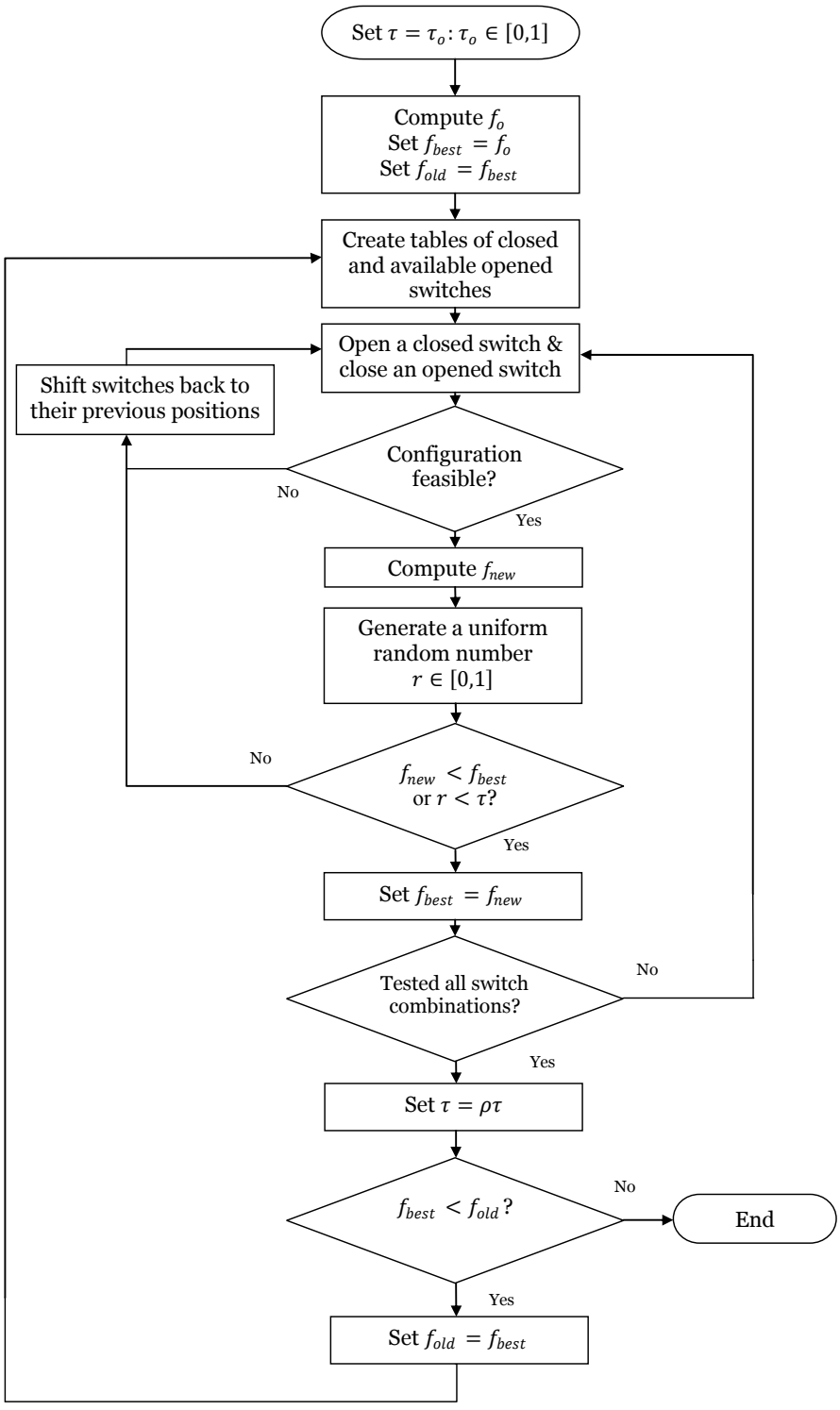

Figure 5.4: Annealed Local Search (ALS) Method

6 Simulations and Results

To investigate the performance of the IDSC architecture presented in Section 4.2 with ALS described in Section 5.2, the IEEE 123 node test feeder was simulated using MATLAB. Results were compared to those obtained using the sequential switch opening (SSO) method, a widely used minimum loss reconfiguration algorithm for normal operating conditions, and decentralized and centralized control architectures as described in Section 4.3.

6.1 Test Case

A one-line diagram of the IEEE 123 node test feeder is shown in Figure 6.1, and a diagram of the sensing, communications, and control system for the feeder utilizing an IDSC architecture is shown in Figure 6.2. The feeder is of modest complexity with 4 substations and 12 switches, and key system characteristics are listed in Table 6.1. Data for the IEEE 123 node test feeder used in the simulations is provided in Appendix C. In addition, data for the IEEE 123 node test feeder and other feeder test cases are available from [80].

It was assumed that all elements were balanced in both impedances and loadings, which has traditionally been chosen as the best compromise between available resources and required results for such an analysis [76]. Each line was set to have a reliability of 97%, each tie-line/switch was set to have a reliability of 100%, and the initial availability

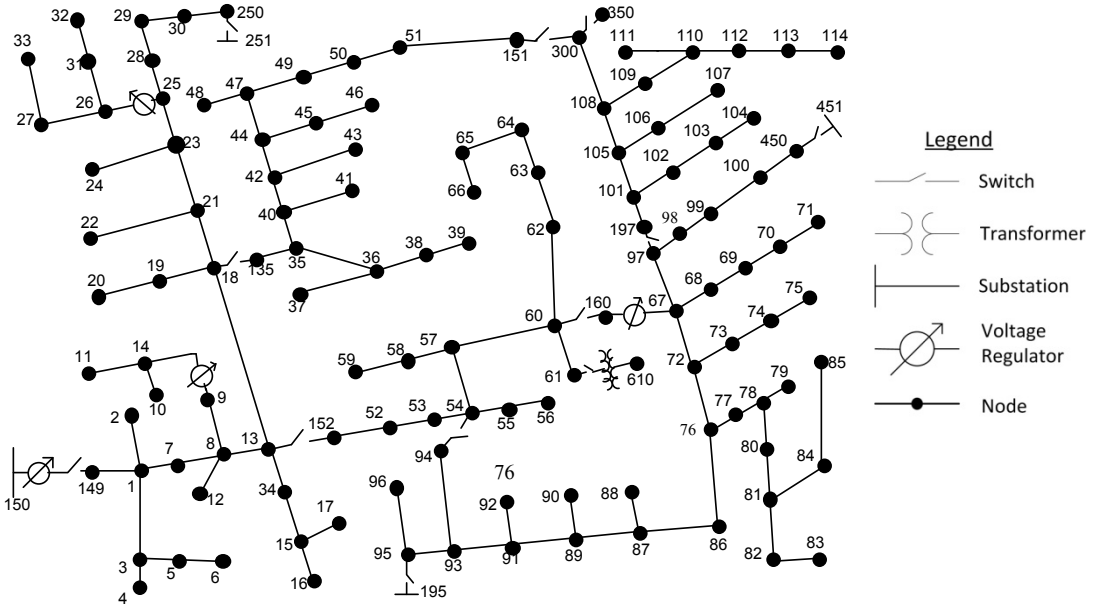

Figure 6.1: IEEE 123 Node Test Feeder One-line Diagram [80]

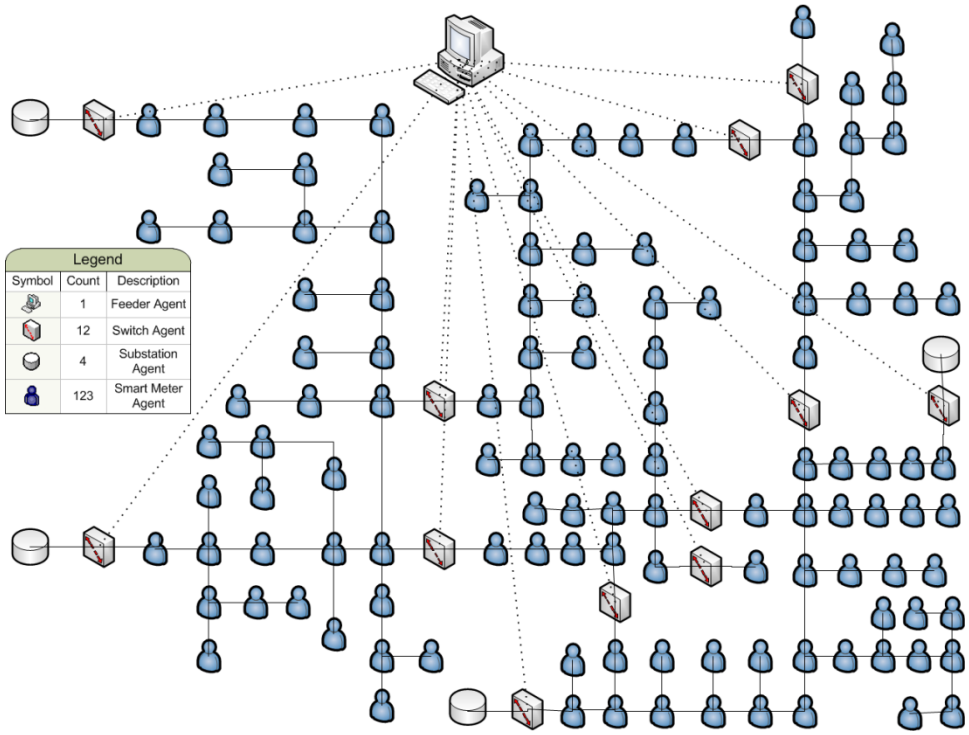

Figure 6.2: Sensing, Communications, and Control System Diagram for IEEE 123 Node Test Feeder

Table 6.1: IEEE 123 Node Test Feeder Key System Characteristics

	Value
Substations	4
Switches	12
Lines	118
Load (kW)	761.25
Base Voltage (kV)	4.16
Base Complex Power (MVA)	10

of each intelligent agent was set to 100%. The minimum bus voltage magnitude for each bus was set to $0.94pu$, and the maximum complex power flow for each line was set to $2{,}496kVA$ based on the standard practice by electric utilities of designing main feeder lines with an emergency rating of $600A$ [66].

6.2 Customer Load Model

Each node on the system was modeled as a customer with the relative load demand curve shown in Figure 6.3, which is divided into three levels. The lowest level represents load that a customer absolutely requires in order to maintain basic living functions or critical business operations. It is assumed that this type of load comprises one-tenth of a customer's total electricity demand, and it is served regardless of electricity price.

The next level represents nondiscretionary load. It includes load that is necessary for a customer to maintain his or her basic quality of life or normal business operations, but he or she can do without it for short periods of time or in the event of an emergency. It is assumed that this type of load comprises four-tenths of a customer's electricity demand, and it is served as long as the electricity price is below some upper price limit,

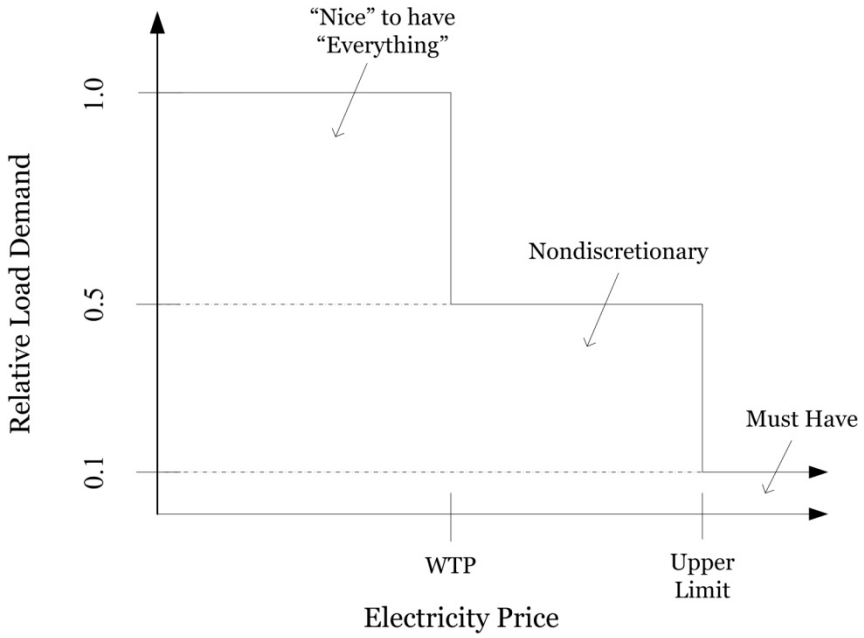

Figure 6.3: Customer Load Demand Curve

which is the same for all customers.

The last level represents discretionary or supplemental types of load that can be scheduled in advance or are unnecessary to maintain one's basic quality of life or normal business operations. This type of load is assumed to comprise one-half of a customer's electricity demand and it is served only if the electricity price is below one's willingness to pay (WTP). The WTP for each customer was randomly generated from a uniform probability distribution in the range $[0,100]$ $\$/MWh$ and remained constant throughout the simulations.

6.3 Smart Meter Agents

Each smart meter agent was designed with demand response capabilities to shift discretionary and supplemental load from periods when the electricity price is above its

owner's WTP or service is unavailable to periods when the electricity price is below its owner's WTP and service is available. For example, during each period, the amount of discretionary load not served due to price or disturbances on the system is calculated and then shifted to the next available period that meets its owner's WTP.

Furthermore, several protective measures were built into each smart meter agent to combat key threats to the smart grid as described in [22]. To prevent abnormal loads from overburdening the system, each smart meter agent caps its owner's load demand during any period to a specified multiple of its average peak load based on historical data. If an owner's initial load demand for a period is below this limit, then additional load may be shifted to that period until the limit is reached, as long as the price of electricity is below his or her WTP.

To prevent brownouts from occurring, each agent is programmed to serve only necessary or "Must Have" load when the price of electricity rises above some predefined abnormally high upper limit set by the local electric utility or PUC as shown in Figure 6.3. The above actions help prevent adversaries from compromising the system and ultimately undermining consumer confidence.

6.4 Sequential Switch Opening Method

Recent work in distribution system reconfiguration has focused on the use of heuristics, such as the SSO method to minimize line losses under normal operating conditions. The main advantages of the SSO method are that the final system configuration is independent of the initial status of the switches, and the solution process

leads to an optimal or near-optimal solution. The main drawbacks are that system operating constraints, such as voltage magnitude limits and line flow limits, are ignored, and alternative objective functions cannot be employed [81].

The SSO method begins with all switches closed, representing a weakly meshed state. A load flow of the resulting meshed system then produces a minimum-loss solution. Next, the switch carrying the least amount of current is opened in order to minimize the disturbance to the optimum flow pattern on the system. The load flow is then recalculated, and the process continues until a radial configuration is achieved [75], [77]. A flow chart depicting the algorithm is shown in Figure 6.4.

6.5 Annealed Local Search Parameter Analysis

An analysis was first performed to determine appropriate parameter values for the ALS method's initial temperature, τ_o, and annealing rate, ρ, as described in Section 5.2. The IEEE 123 node test feeder described in Section 6.1 was used for this purpose with no line outages or failures enabled, and the electricity price was set to $50\ \$/MWh$. The initial radial configuration for the system was found via the SSO method using the default substation at bus 150.

6.5.1 Annealing Rate

Ten trials were performed for various annealing rates, ρ, in the range $[0,1)$ for one period in length, with each period representing one hour. The initial temperature, τ_o, was set equal to the annealing rate for each trial so that a larger search area would be explored

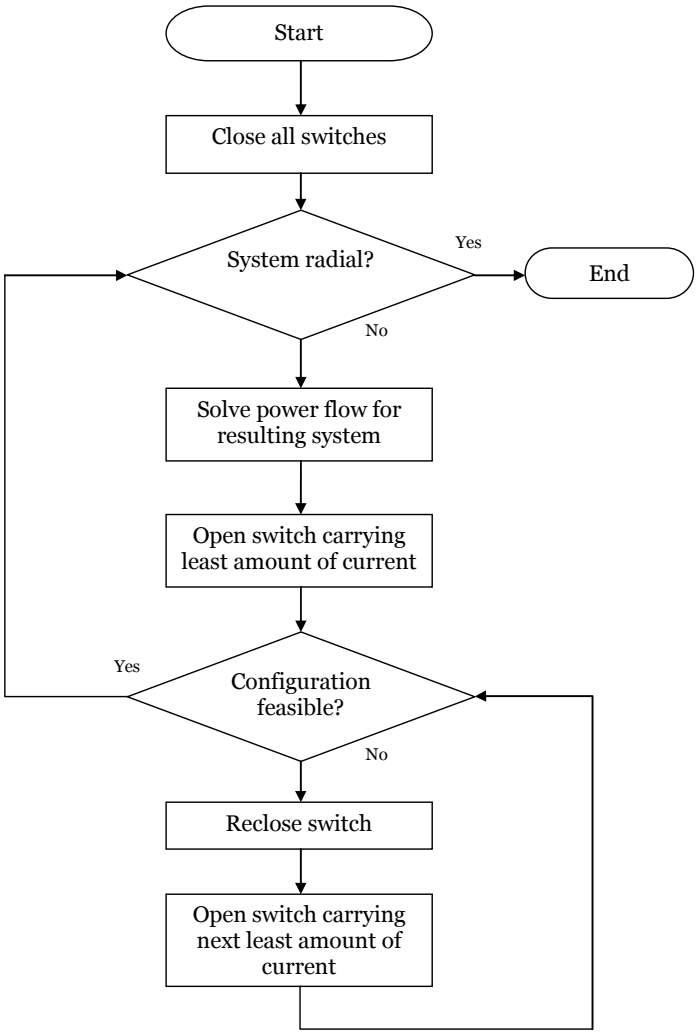

Figure 6.4: Sequential Switch Opening (SSO) Method

for slower annealing rates. For each trial, the LOEE and the execution time were recorded, and plots of the average LOEE and the average normalized execution time for each annealing rate tested are shown in Figure 6.5 and Figure 6.6 respectively. The normalized execution times were found by dividing each average execution time by the average execution time for an annealing rate of zero.

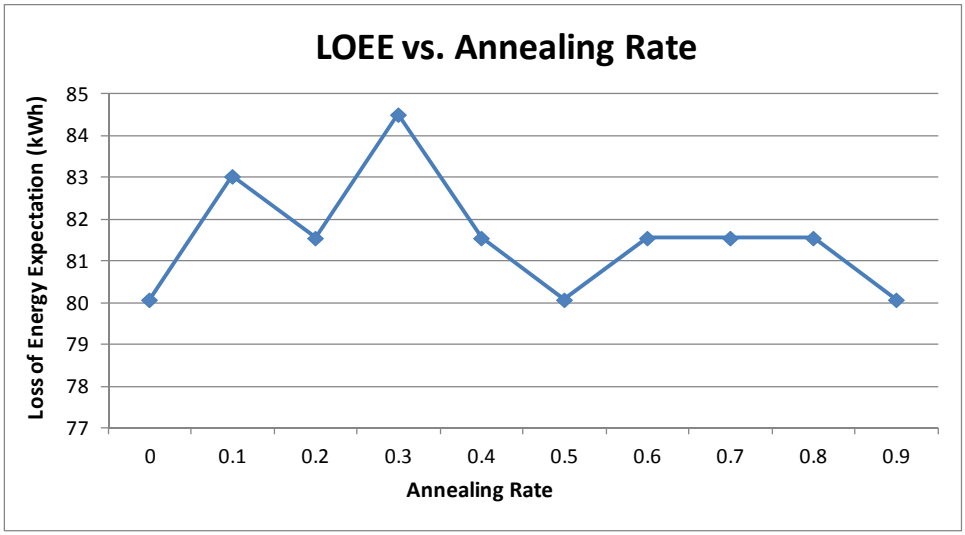

Figure 6.5: Loss of Energy Expectation (LOEE) vs. Annealing Rate

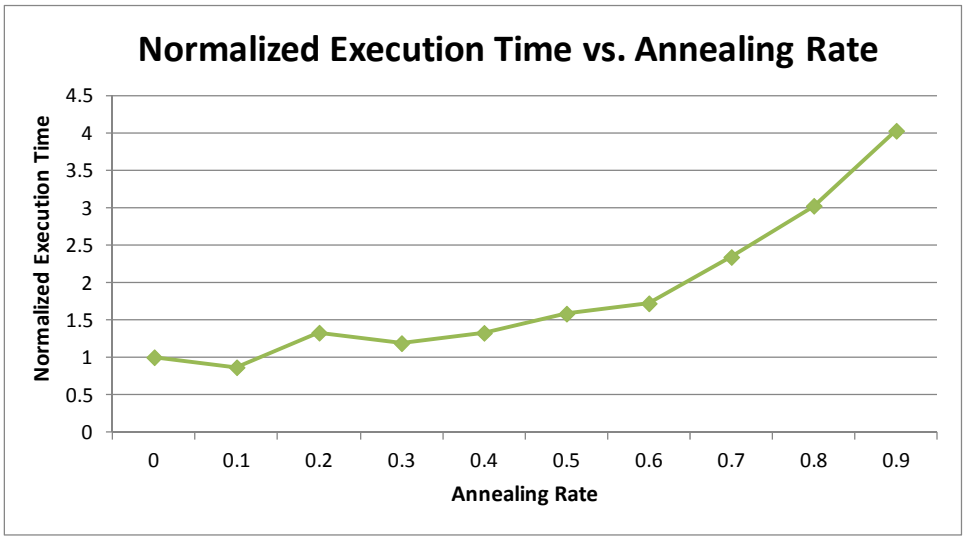

Figure 6.6: Normalized Execution Time vs. Annealing Rate

Figure 6.5 shows that slower annealing rates produce better quality solutions, and Figure 6.6 shows that the execution time increases exponentially for slower annealing rates. It was desired to obtain a high quality solution while also minimizing the execution time. As a result, an annealing rate of 0.5 was selected since it was found to produce

high quality solutions with only a small increase in execution time. An annealing rate of zero was also found to produce high quality solutions, but it must be noted that this result is due to the initial configuration of the system since the algorithm reduces to integer programming at an initial temperature of zero.

6.5.2 Initial Temperature

A similar analysis was performed for various initial temperatures, τ_o, in the range [0,1]. An annealing rate of 0.5 was used based on the results of Section 6.5.1. Again, for each trial, the LOEE and the execution time were recorded, and plots of the average LOEE and the average normalized execution time for each initial temperature tested are shown in Figure 6.7 and Figure 6.8 respectively. The normalized execution times were found by dividing each average execution time by the average execution time for an initial temperature of zero.

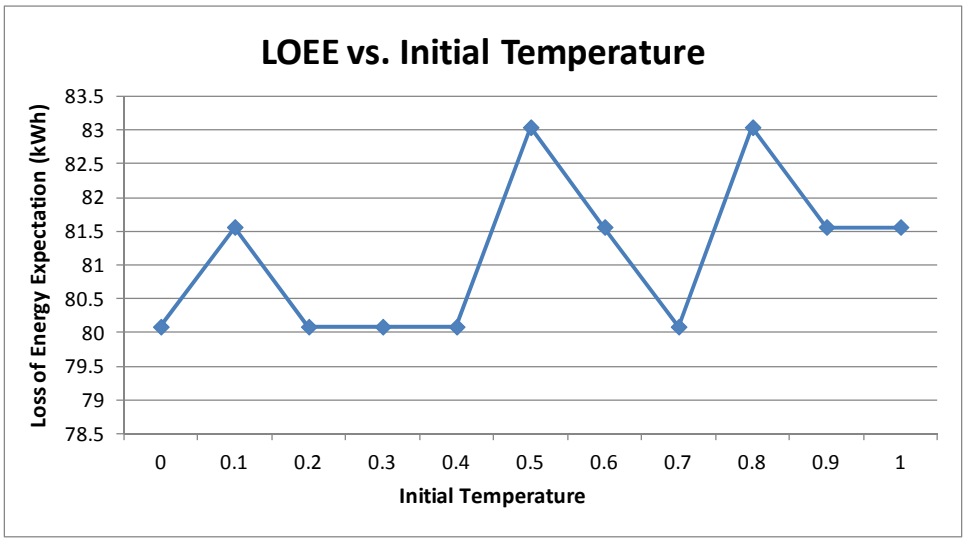

Figure 6.7: Loss of Energy Expectation (LOEE) vs. Initial Temperature with $\rho = 0.5$

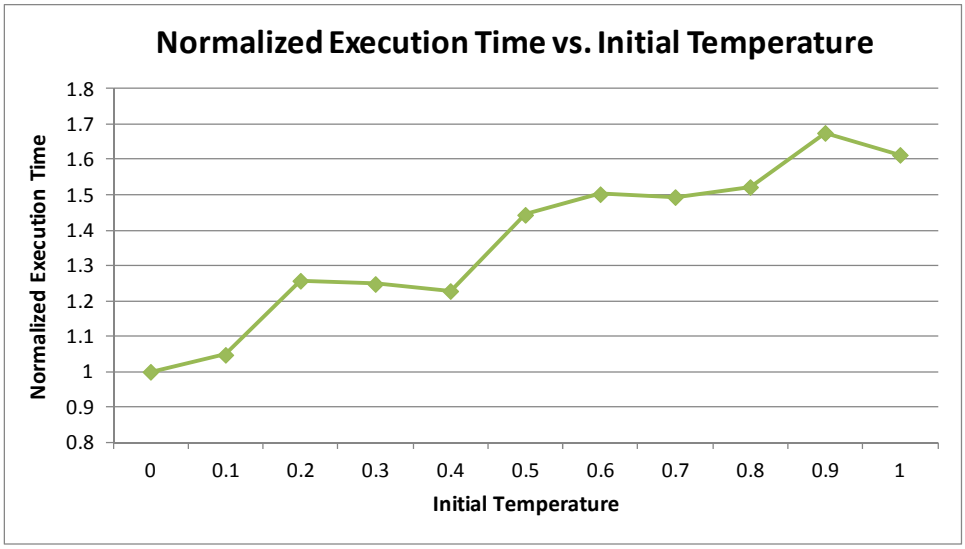

Figure 6.8: Normalized Execution Time vs. Initial Temperature with $\rho = 0.5$

Figure 6.7 shows that higher initial temperatures produce more variable results, and Figure 6.8 shows that the execution time increases almost linearly for higher initial temperatures. Once more, it was desired to obtain a high quality solution while minimizing the execution time. Thus, an initial temperature of 0.4 was selected since it was found to produce high quality solutions with only a small increase in execution time. An initial temperature of zero was found to produce high quality solutions with the least execution time, but it must be noted that this result is due to the initial configuration of the system since the algorithm reduces to integer programming at a temperature of zero. For other initial configurations, this would not be the case.

Based on the above results, an initial temperature, τ_o, of 0.4 and an annealing rate, ρ, of 0.5 were chosen for use in the ALS algorithm for the following simulations.

6.6 Dynamic Simulations

6.6.1 Simulation Parameters

Simulations were executed for a length of 1,368 hours with each discrete period representing one hour in length. The electricity price and load demand curve data were obtained from the Midwest Independent Transmission System Operator (MISO) [82]. The electricity prices used were the real-time market clearing prices (MCPs) for each hour during the period from July 6, 2009 - August 31, 2009, and ranged from 1.79 $\$/MWh$ to 78.85 $\$/MWh$. An electricity price of 75 $\$/MWh$ was set as the upper price limit as shown in Figure 6.3. The load demand curve for each customer was generated using the MISO actual load curve from July 6, 2009 - August 31, 2009 scaled to the value of each customer's peak load. Plots of the real-time MCPs and the normalized actual load curve for MISO from July 6, 2009 - Aug. 31, 2009 are shown in Figure 6.9 and Figure 6.10 respectively.

The smart meters agents were programmed to cap their owner's load demand during each period to three times his or her average peak load. In addition, they were enabled to shift discretionary or supplemental load as described in Section 6.3, and to serve all discretionary load in the first available period regardless of price, as is the case in conventional distribution system operations.

Random cyber attacks were enabled to occur during each hour with each reactive layer agent having a failure rate of 20%, and each coordination layer agent having a failure rate of 10%. The failure rate for a reactive layer agent was set to be greater than that for a coordination layer agent because of their larger numbers and their tendency to

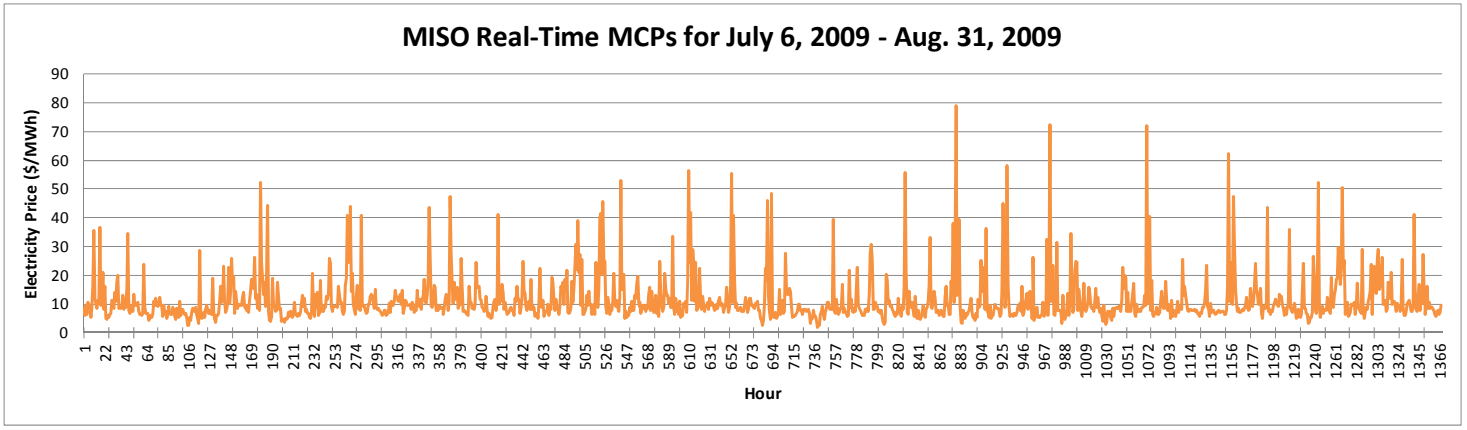

Figure 6.9: MISO Real-Time Market Clearing Prices

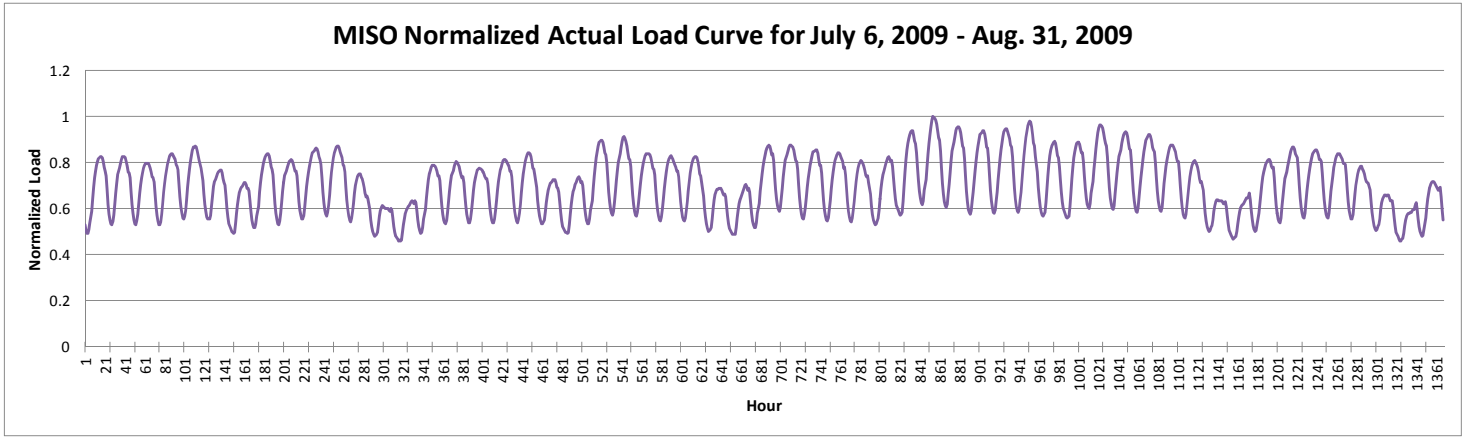

Figure 6.10: MISO Normalized Actual Load Curve

be located in less secure areas. Because of the critical functions provided by the deliberative layer agent, which must be secured to ensure 100% uptime, it was assumed that it was protected to withstand all such attacks.

A successful cyber attack on a coordination layer agent or a reactive layer substation agent was assumed to immobilize the agent for the hour during which the attack occurred, while a successful cyber attack on a reactive layer smart meter agent was assumed to trigger the agent into emergency operation mode where only critical load or "Must Have" load is served as shown in Figure 6.3 for the hour during which the attack occurred. Line failures were also enabled to occur, and a line failure was assumed to remove the line from operation for the hour during which the failure occurred.

In order to account for the variance in each simulation due to random cyber attacks and line failures, ten trials were performed, and the mean results were used for analysis. All simulations also used initial system configurations with minimum line losses. A summary of the simulation parameters used is shown in Table 6.2, and a flowchart outlining the simulation methodology is shown in Figure 6.11.

6.6.2 Wind Turbine

In addition, simulations were performed to assess the impact of an intermittent DER on the performance of the optimization algorithms and control architectures. To accomplish this task, a 750kW wind turbine was added to the IEEE 123 node test feeder as shown in Figure 6.12. Generation data for the wind turbine was obtained from a 1.65MW wind turbine located on the University of Minnesota Morris (UMM) campus in

Table 6.2: Dynamic Simulation Parameters

Parameter	Value
Periods	1,368
Trials	10
Price Data	
Maximum allowable electricity price ($\$/MWh$)	75.0
Load Data	
Maximum average peak load multiple	3
ALS Data	
Initial temperature, τ_o	0.4
Annealing rate, ρ	0.5
Outage Data	
Deliberative layer agent failure rate (%)	0
Coordination layer agent failure rate (%)	10
Reactive layer agent failure rate (%)	20
Line failure rate (%)	3

Morris, MN for the dates July 6, 2009 - Aug. 31, 2009. The 1.65MW wind turbine output was scaled down to a peak output of 750kW for use in the simulations. A graph of the wind turbine output for July 6, 2009 - Aug. 31, 2009 is shown in Figure 6.13.

For each simulation, if the generation from the wind turbine exceeded the total system load during a given period, the excess generation was fed back to the transmission system via a substation connection. If no substation connection was present, then any excess generation was curtailed after all system load had been served.

6.6.3 Results

The simulation results are shown below. Figure 6.14 shows the total LOEE for the different algorithms and control architectures, Figure 6.15 shows the total amount of

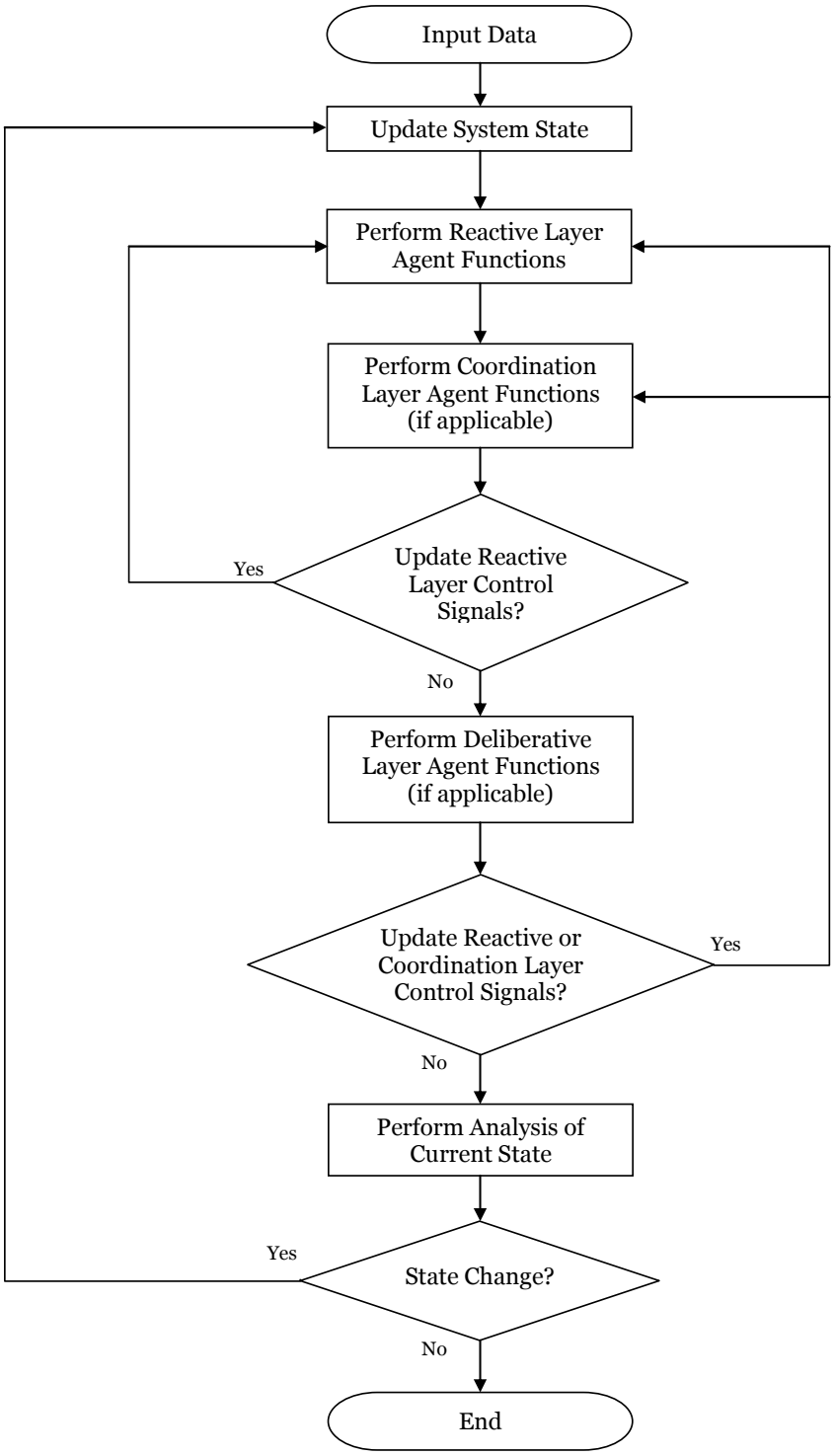

Figure 6.11: Dynamic Simulation Methodology

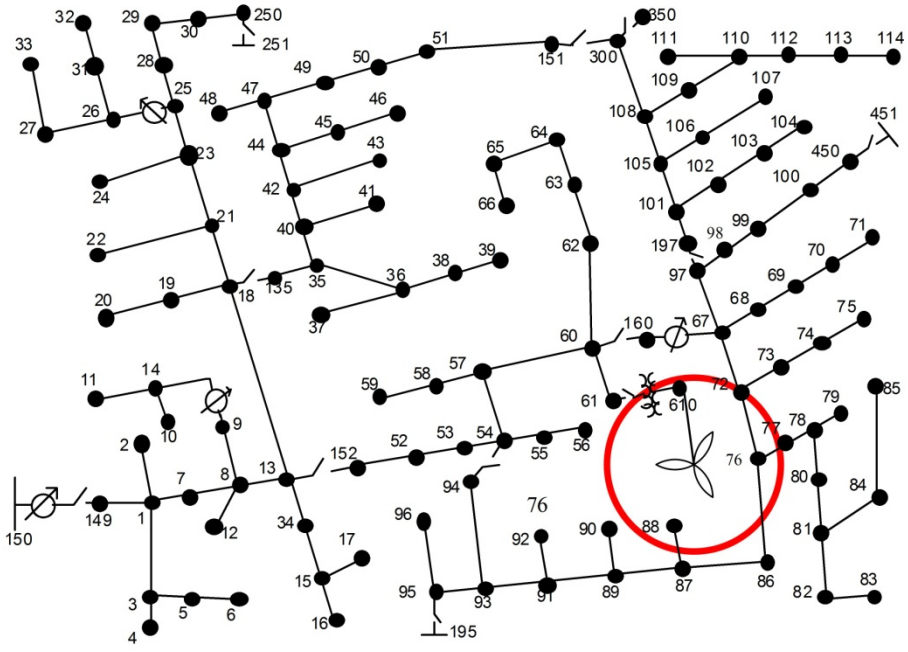

Figure 6.12: IEEE 123 Node Test Feeder One-line Diagram with Wind Turbine (Modified from [80])

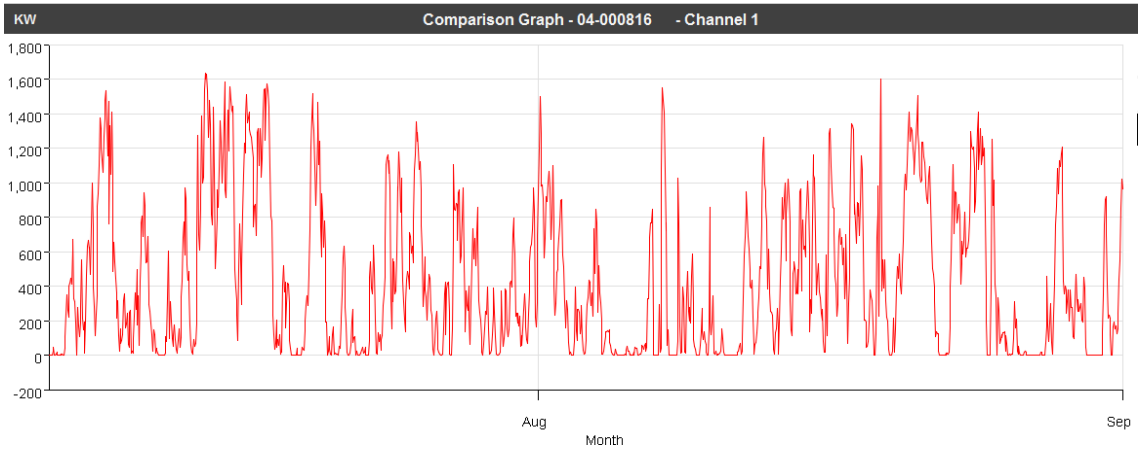

Figure 6.13: 1.65 MW Wind Turbine Output for July 6, 2009 - Aug. 31, 2009

line losses, Figure 6.16 shows the cumulative sum of the voltage violations, and Figure 6.17 shows the cumulative sum of the line flow violations.

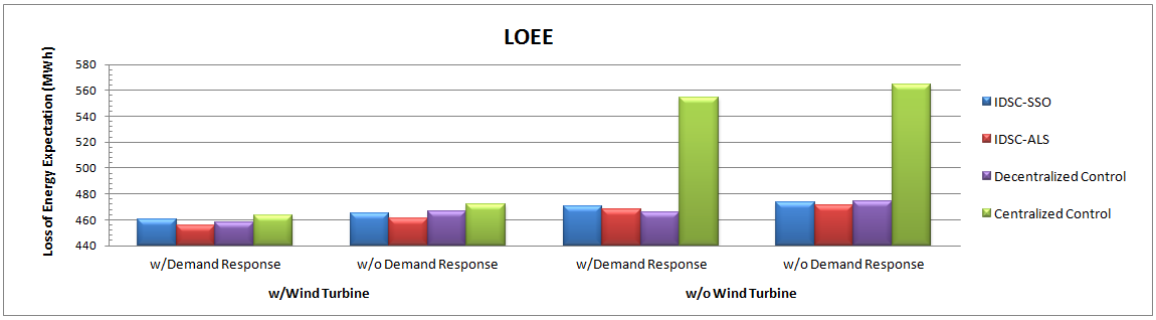

Figure 6.14: Loss of Energy Expectation (LOEE) Comparison

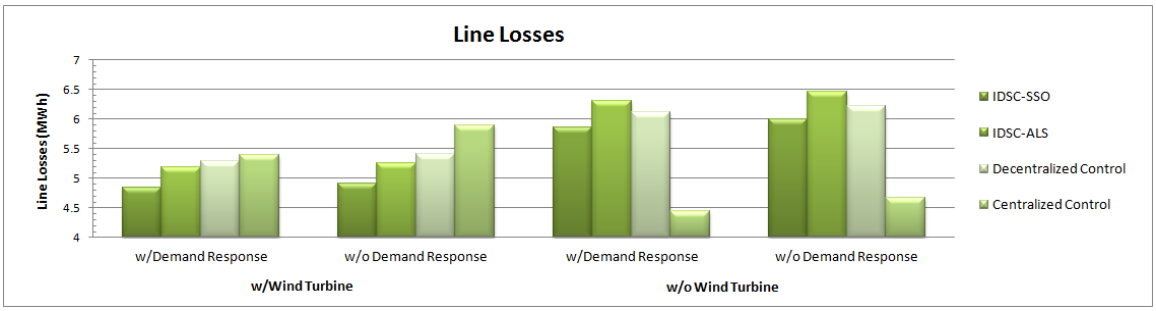

Figure 6.15: Line Losses Comparison

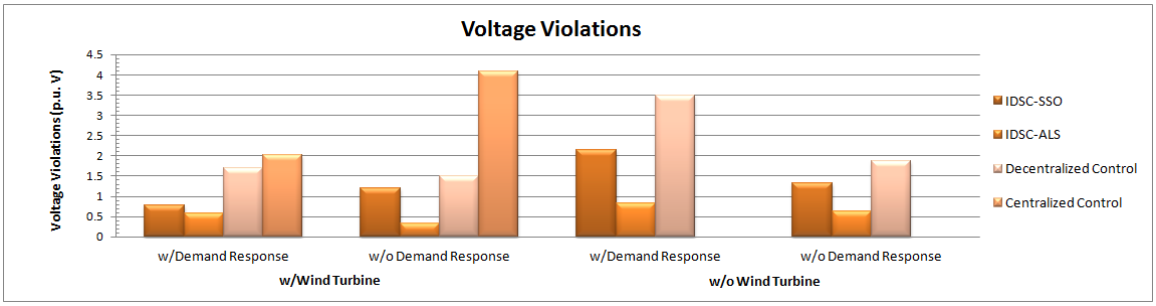

Figure 6.16: Voltage Violations Comparison

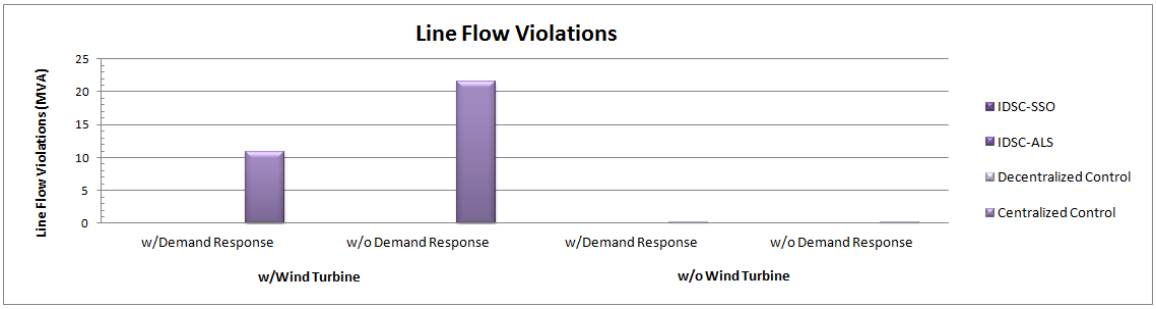

Figure 6.17: Line Flow Violations Comparison

Additionally, Figure 6.18 shows the discretionary energy cost, Figure 6.19 shows the discretionary energy served, Figure 6.20 shows the nondiscretionary energy cost, and Figure 6.21 shows the nondiscretionary energy served with system reconfiguration, with system reconfiguration without optimization, and without system reconfiguration capabilities enabled. The IDSC architecture uses system reconfiguration capabilities, the decentralized control architecture uses system reconfiguration capabilities without optimization, and the centralized control architecture does not use any system reconfiguration capabilities. Table 6.3 shows the average discretionary, nondiscretionary, and total energy costs for the results shown in Figure 6.18 - Figure 6.21.

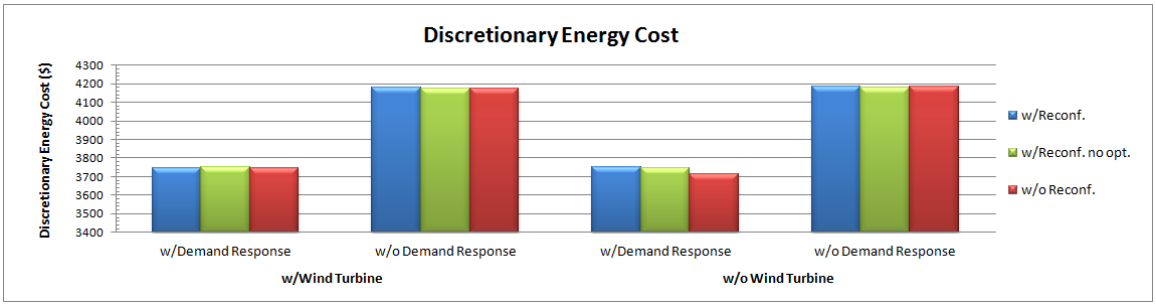

Figure 6.18: Discretionary Energy Cost Comparison

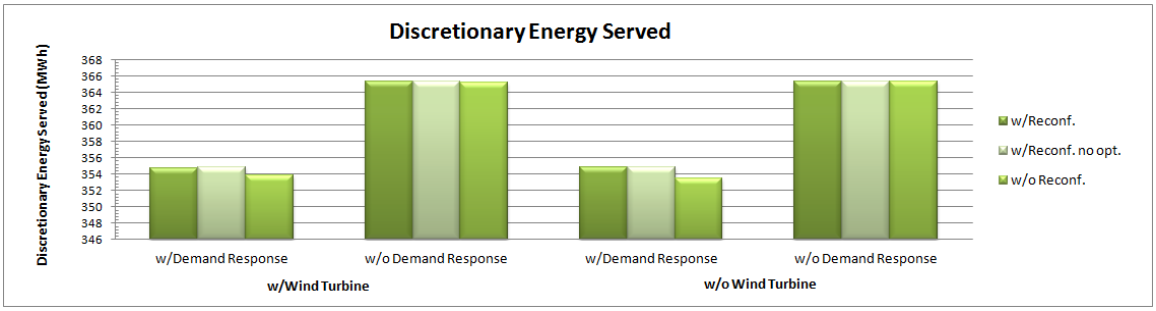

Figure 6.19: Discretionary Energy Served Comparison

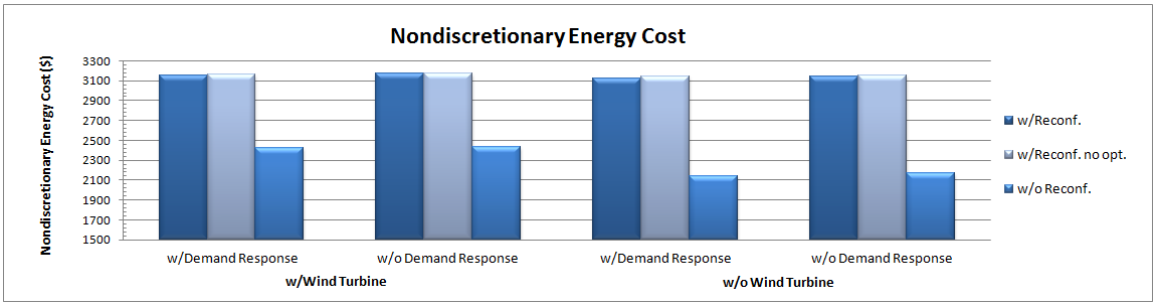

Figure 6.20: Nondiscretionary Energy Cost Comparison

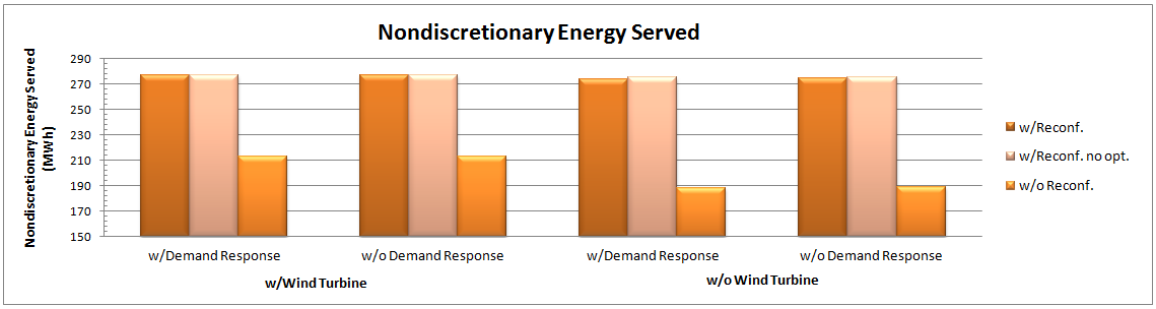

Figure 6.21: Nondiscretionary Energy Served Comparison

Table 6.3: Average Energy Cost Comparison
(w/DR – with Demand Response, w/o DR – without Demand Response)

	w/Wind Turbine		*w/o Wind Turbine*	
($/**MWh**)	*w/DR*	*w/o DR*	*w/DR*	*w/o DR*
Discretionary				
w/Reconfiguration	10.56	11.45	10.56	11.46
w/Reconfiguration (w/o opt.)	10.57	11.43	10.56	11.43
w/o Reconfiguration	10.58	11.43	10.51	11.45
Nondiscretionary				
w/Reconfiguration	11.40	11.46	11.41	11.46
w/Reconfiguration (w/o opt.)	11.41	11.44	11.42	11.45
w/o Reconfiguration	11.34	11.43	11.39	11.47
Total				
w/Reconfiguration	10.93	11.45	10.93	11.46
w/Reconfiguration (w/o opt.)	10.94	11.43	10.94	11.44
w/o Reconfiguration	10.87	11.43	10.82	11.46

6.7 Demand Response

6.7.1.1 Simulation Parameters

Next, an analysis of the effects of the demand response capabilities of the smart meter agents on the load demand curve was performed. The simulation parameters listed in Table 6.2 were again used, with the exceptions that random cyber attacks and line failures were disabled, and the upper price limit was set to $100\ \$/MWh$ so that brownout prevention measures would not occur. The electricity prices used were the real-time and day-ahead MCPs from the MISO for each hour during the period from July 6, 2009 - August 31, 2009. The day-ahead MCPs ranged from $2.34\ \$/MWh$ to $43.35\ \$/MWh$, and a plot of the day-ahead MCPs from July 6, 2009 - Aug. 31, 2009 is shown in Figure 6.22.

6.7.1.2 Results

A plot of the load served with and without demand response capabilities enabled using real-time MCPs is shown in Figure 6.23, and a plot of the load served with and without demand response capabilities enabled using day-ahead MCPs is shown in Figure 6.24.

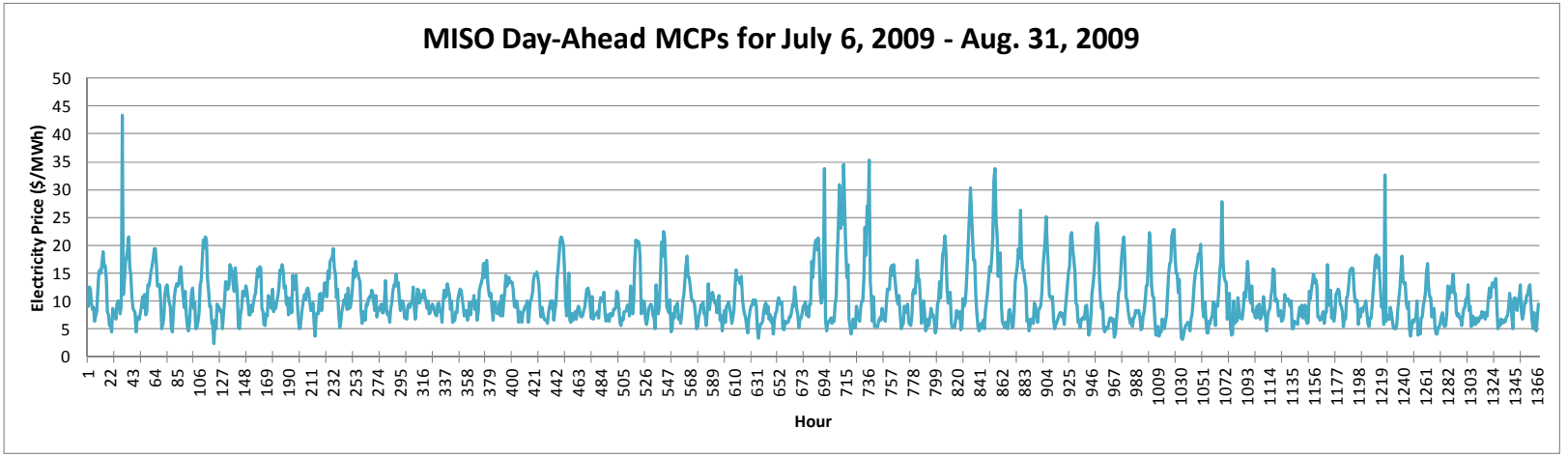

Figure 6.22: MISO Day-Ahead Market Clearing Prices

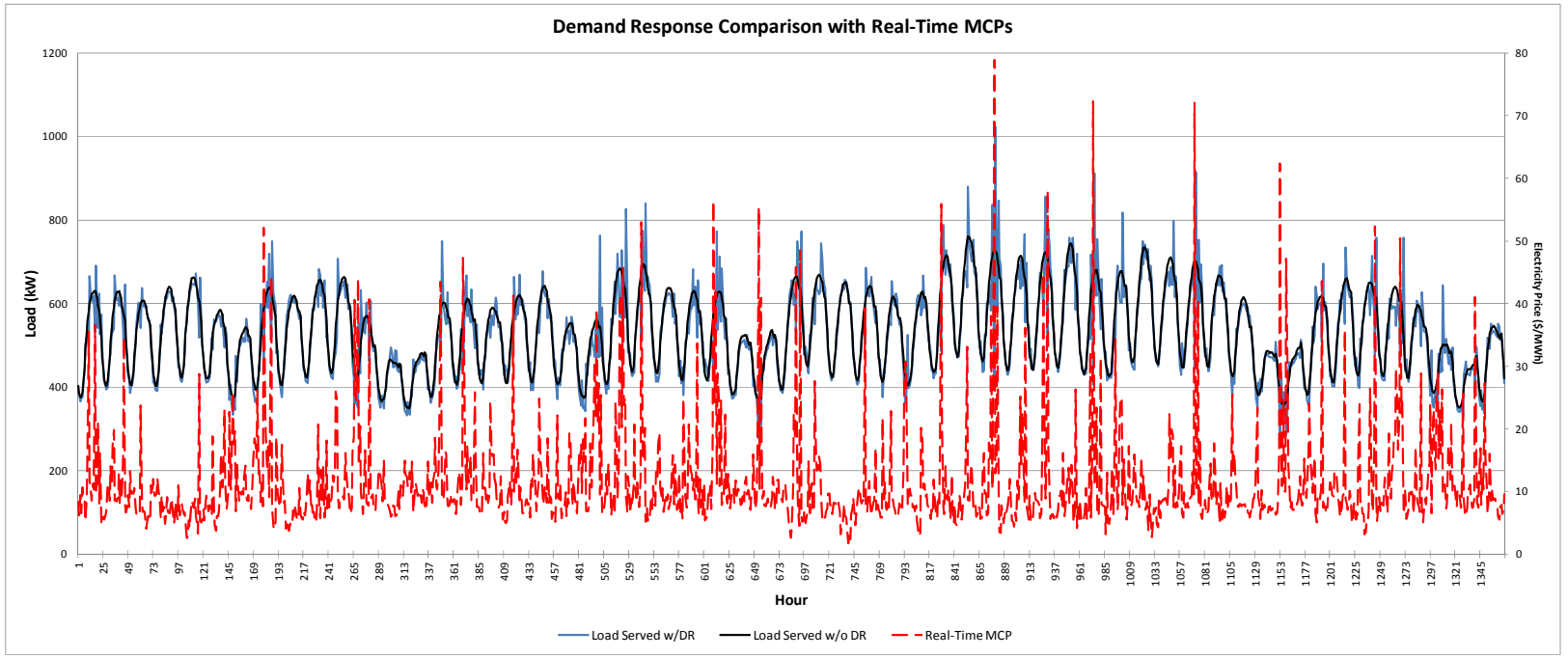

Figure 6.23: Demand Response Comparison with Real-Time Market Clearing Prices (w/DR-with Demand Response, w/o DR-without Demand Response)

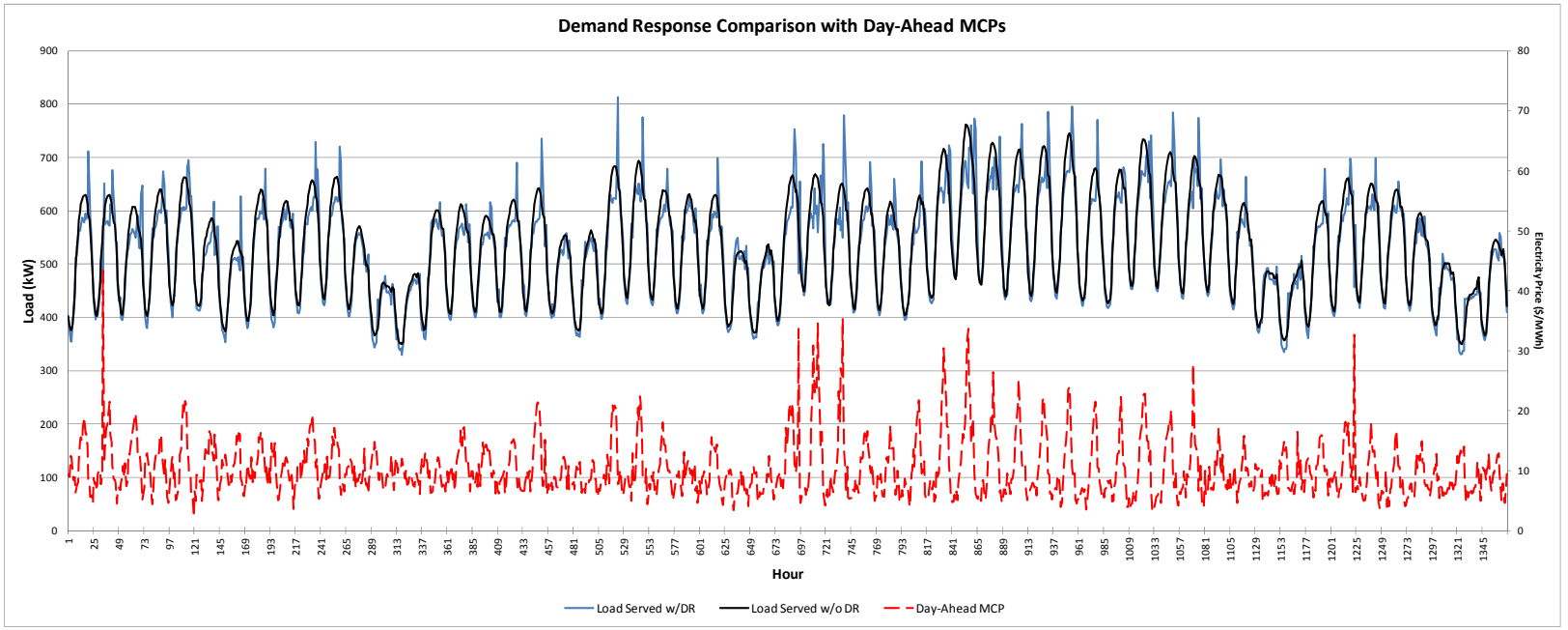

Figure 6.24: Demand Response Comparison with Day-Ahead Market Clearing Prices (w/DR-with Demand Response, w/o DR-without Demand Response)

6.8 Monte Carlo Simulations

6.8.1 Simulation Parameters

Finally, in order to evaluate the robustness of each of the control architectures and optimization algorithms, nonsequential Monte Carlo simulations [83] were performed where each scenario is treated as a random sample from a probability process. For each of the control architectures and optimization algorithms, 10,000 samples were generated and the LOEE and amount of line losses were calculated. Probability distributions for both metrics were then estimated from the generated samples.

For each node on the system, peak loads were used to maximize system stress, and the price of electricity was ignored. The state of each intelligent agent and line was modeled using a uniform probability distribution between [0,1] as shown in (6.1). The failure rates used were the same as those applied in the dynamic simulations listed in Table 6.2.

$$s_i = \begin{cases} 0 & \text{(success)} \quad \text{if } R_i > Q_i \\ 1 & \text{(failure)} \quad \text{if } 0 \leq R_i \leq Q_i \end{cases} \tag{6.1}$$

Where:

s_i - state of component i

Q_i - failure probability of component i

R_i - uniformly distributed random number between $[0, 1]$ for component i

A summary of the Monte Carlo simulation parameters used is provided in Table 6.4.

Table 6.4: Monte Carlo Simulation Parameters

Parameter	Value
Samples	10,000
ALS Data	
Initial temperature, τ_o	0.4
Annealing rate, ρ	0.5
Outage Data	
Deliberative layer agent failure rate	0%
Coordination layer agent failure rate	10%
Reactive layer agent failure rate	20%
Line failure rate	3%

6.8.2 Results

The simulation results for the nonsequential Monte Carlo simulations are shown below. Figure 6.25 shows the probability distributions for the LOEE for each of the control architectures and algorithms simulated, and Figure 6.26 shows the probability distributions for line losses.

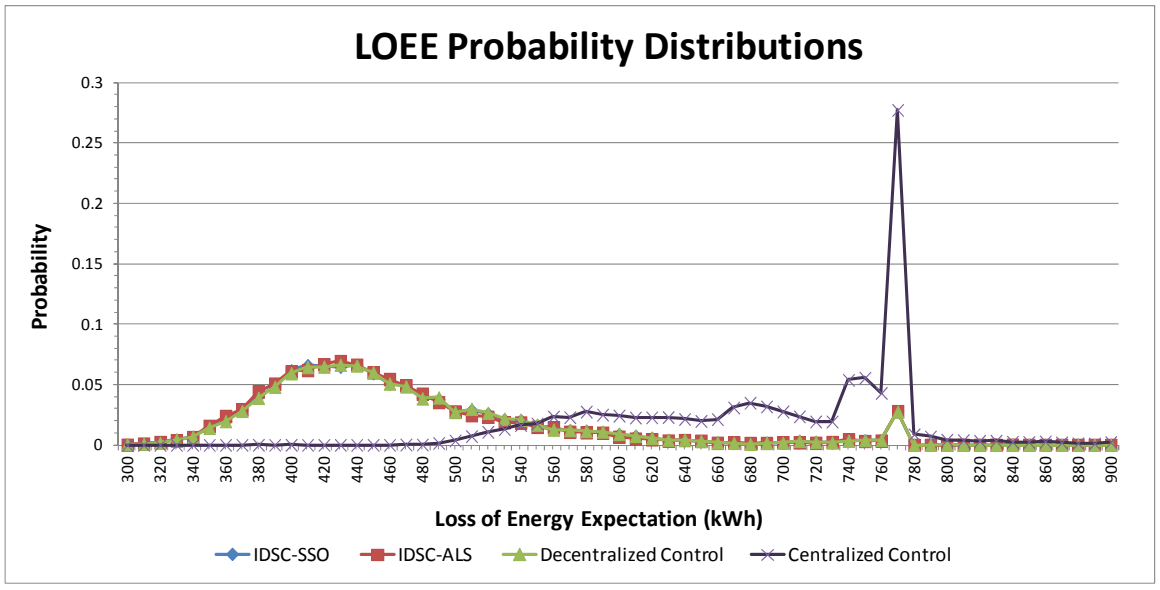

Figure 6.25: Loss of Energy Expectation (LOEE) Probability Distributions

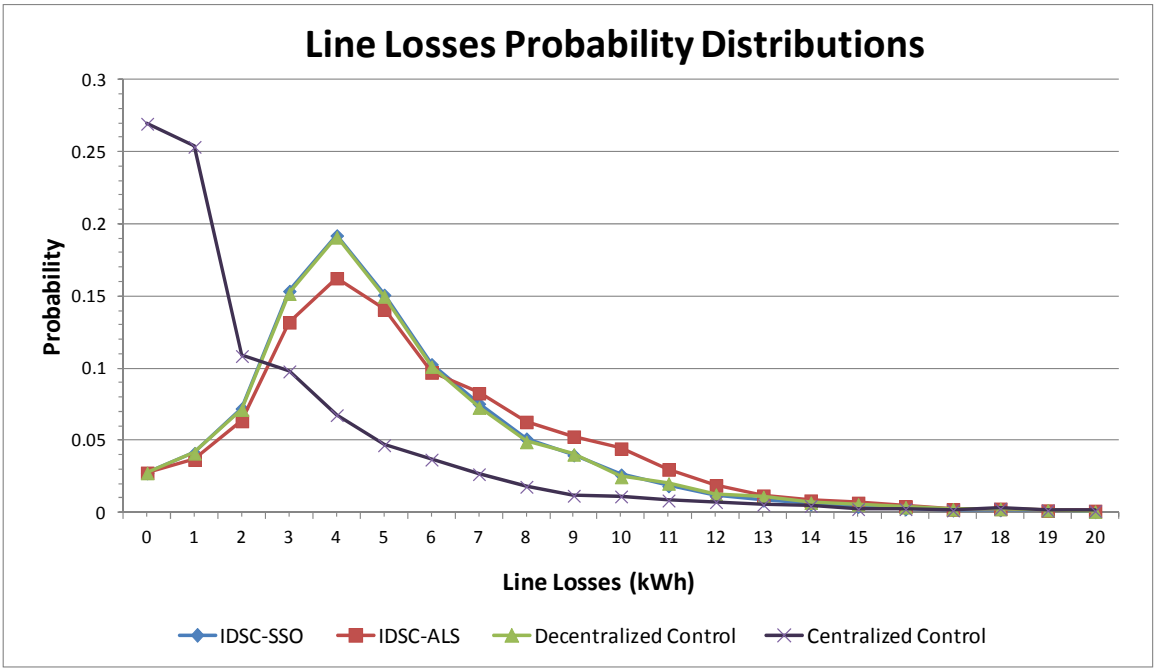

Figure 6.26: Line Losses Probability Distributions

6.9 Summary

In this chapter, several simulations are developed to investigate the performance of various distribution system control architectures and optimization algorithms on system operations. Results utilizing the IEEE 123 node test feeder are presented and show the trade-offs between system reliability, operational constraints, and costs. The simulation models include aspects of cyber-physical security, dynamic price and demand response, sensing, communications, intermittent DERs, and dynamic optimization and reconfiguration.

The next chapter provides a comprehensive discussion of the simulation results presented in this chapter, and describes some of the limitations of the simulation models.

7 Discussion

7.1 Dynamic Simulations

7.1.1 Without Wind Turbine

The results presented in Section 6.6 show the performance of the different control architectures and optimization algorithms simulated on several distribution system parameters. Figure 6.14 shows that the IDSC architecture using both the SSO and ALS methods and the decentralized control architecture greatly decreased the LOEE of the test feeder compared to the centralized control architecture due to the advanced reconfiguration capabilities enabled. Because of these capabilities, however, Figure 6.15 and Figure 6.16 show that the amount of line losses and the severity of voltage violations each greatly increased. Line flow violations did not have any measured effect on system operations except for the cases where the centralized control architecture was used as shown in Figure 6.17, although without the wind turbine present the size of the line flow violations was not large enough to show up on the graph. Comparing the ALS method to the SSO method for the IDSC architecture, it can be seen from Figure 6.14 - Figure 6.16 that while the ALS method further decreased the LOEE and the severity of voltage violations, it resulted in an increase in the amount of line losses.

Table 6.3 shows that the use of demand response significantly decreased the average cost of discretionary energy served, and Figure 6.14 and Figure 6.15 show that it decreased or had a very little effect on the LOEE and line losses respectively for all

algorithms and control architectures simulated. However, it resulted in a significant increase in the severity of voltage violations for the IDSC architecture using the SSO method and the decentralized control architecture as shown in Figure 6.16.

Thus, for the test feeder, the price for minimizing cyber and physical disturbances or LOEE using the IDSC architecture is increased line losses and voltage violations. To determine the most beneficial control architectures and algorithms to implement, the benefits from improved performance must be balanced against operational costs.

7.1.2 With Wind Turbine

When the wind turbine, an intermittent DER, was added to the system, the results changed significantly as shown in Figure 6.14 - Figure 6.17. The IDSC architecture using both the SSO and ALS methods resulted in the least LOEE, line losses, voltage violations, and line flow violations. Thus, with the wind turbine present, the IDSC architecture outperformed the others for all measured parameters. Comparing the ALS method to the SSO method for the IDSC architecture, it can be seen from Figure 6.14 - Figure 6.16 that while the ALS method minimized the LOEE and the severity of voltage violations on the system, the SSO method minimized the amount of line losses.

Furthermore, the addition of the wind turbine resulted in an increase in the amount of nondiscretionary energy served as shown in Figure 6.21, but did not have any significant affect on the average energy costs as shown in Table 6.3.

7.2 Demand Response

The results of the simulations presented in Section 6.7 show the impact of demand response on the load demand curve when both real-time and day-ahead MCPs are used. When real-time MCPs are used, demand response does not flatten the peaks in the load demand curve as one might expect, but instead introduces significant oscillations as shown in Figure 6.23. This effect is due to the high volatility of the real-time MCPs and the fact the peaks in the real-time MCPs do not correspond well to the peaks in demand.

When day-ahead MCPs are used, however, a significant portion of each daily peak load is shifted as shown in Figure 6.24. The reason for this improvement in performance is because the day-ahead MCPs are much less volatile than the real-time MCPs, and the peaks in the day-ahead MCPs corresponded much better to the peaks in demand.

Nevertheless, the use of day-ahead MCPs produced new peaks in the demand curve, sometimes much larger than the original peaks in demand, after each large drop in price due to large amounts of load being shifted to those periods. The reason for this is partly due to the demand model used for each customer and partly due to the demand response control scheme implemented. Modeling individual customer load demand curves with additional price steps, and by programming the smart meters to serve shifted load over a greater period of time, rather than just shifting it to the first period when the price drops below one's WTP, could reduce, or prevent such spikes from occurring.

It must be noted that the preceding simulations operated under the assumption that the system load was too small to influence the price of electricity. However, if a large enough percentage of customers in a specific region have real-time demand response capabilities enabled, the MCPs will be affected. The market restructuring necessary to make the preceding situation a reality, nevertheless, faces numerous technological and regulatory barriers that are not likely to be overcome in the near future. Several of these barriers are described in detail in [84]. As a result, several utilities are allowing customers to enroll voluntarily in demand response programs, such as Con Edison [85], and Southern California Edison [86], while the vast majority of customers still receive fixed rate prices.

7.3 Monte Carlo Simulations

The results of the nonsequential Monte Carlo simulations presented in Section 6.8 compare the robustness of the different control architectures and optimization algorithms. Figure 6.25 shows that the IDSC and the decentralized control architectures are significantly more robust to disturbances as measured by the LOEE than the centralized control architecture for the test system. One reason for this is due to the advanced reconfiguration capabilities enabled by both control architectures. The differences between the two were found to be negligible.

Figure 6.26 shows that the centralized control architecture results in the least amount of line losses, followed by the IDSC architecture with the SSO method, and the decentralized control architecture. The architecture with the greatest amount of line

losses is the IDSC architecture with the ALS method. It must be noted, however, that one of the reasons that the centralized control architecture results in the least amount of line losses is because it has the worst reliability (Figure 6.25). If a system is frequently unable to serve load due to disturbances, then its line losses will consequently be lower since less power is often flowing on the system.

Moreover, the results of the Monte Carlo simulations presented in Section 6.8 are consistent with the results of the dynamic simulations presented in Section 6.6.

7.4 Model Limitations

The simulation model described in Section 6 integrates aspects of cyber-physical security, dynamic price and demand response, sensing, communications, and dynamic optimization and reconfiguration. This work represents a novel approach toward developing an analytical and multi-domain methodology to assess the effects of smart grid technologies on distribution system operations and performance. Nevertheless, the model contains several limitations that must be noted.

First, it was assumed that all elements were balanced in both impedances and loadings, which is often referred to as a one-line AC-model. Traditionally, such a model has been regarded as the best compromise between available resources and required results for such an analysis. Even so, it is not a highly accurate depiction of reality. For example, using a one-line model means that one will not be able to observe the effects that load-imbalances have on system operations, and the effects of one- and two-phase

elements in the system will be approximate at best [76]. To obtain a more accurate depiction of reality, a full three-phase circuit model is needed.

Second, the Newton-Raphson algorithm [87] was used to solve the power flows for the test system. While the Newton-Raphson algorithm is widely used to solve power system power flow problems, it has been shown in [81] and [88] that special power flow algorithms that take advantage of the unique structure of radial distribution systems are much more efficient and reliable for solving such problems. For example, it was found that the Newton-Raphson method had trouble converging for heavily loaded radial distribution system cases. Reference [88] describes a method referred to as the "ladder iterative technique" that has been found to overcome such shortcomings.

8 Case Study: University of Minnesota Morris Campus

In this chapter, an analysis of the potential benefits from the integration of smart grid technologies throughout the University of Minnesota Morris (UMM) campus is performed.

8.1 University of Minnesota Morris Campus

The UMM campus is a small residential campus of about 1,800 students located in Morris, MN. The campus is a nationally recognized leader in sustainability, having been one of the first public colleges in the U.S. to generate on-site renewable power from local resources, such as corn stover. The campus's impressive array of renewable energy resources includes a biomass gasification plant fueled by crop residues from nearby farms, solar thermal panels, a solar photovoltaic system, and two 1.65MW wind turbines. The most recent wind turbine was installed in February 2011 [89].

The wind turbines provide a large portion of the daily electricity used on the UMM campus. Before the installation of the second wind turbine, wind energy provided over 50% of the campus's electricity needs. It is estimated that with the second wind turbine, wind will provide an average of 70% of the campus's electricity needs, with the potential for 100% on good wind days. When the energy produced by the wind turbines exceeds the campus's demand, the excess is sold to Otter Tail Power Company (OTPC),

the local utility serving the Morris region, at a prenegotiated rate. An example of the electricity produced by the original wind turbine and the portion consumed by the Morris campus for May 15, 2010 - May 31, 2010 is shown in Figure 8.1.

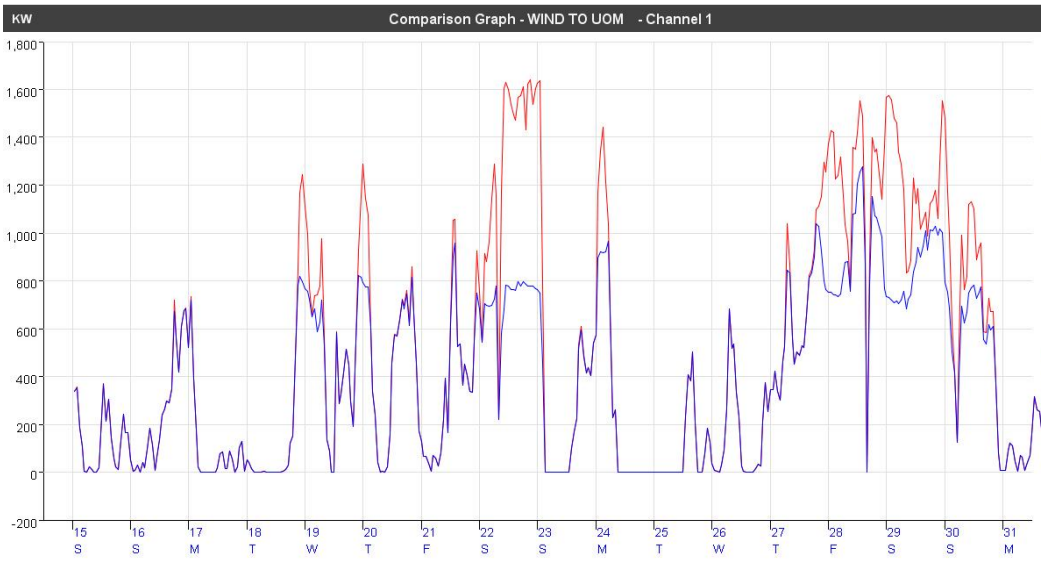

Figure 8.1: Wind Turbine Output (red) and Portion Consumed by UMM (blue) for May 15, 2010 - May 31, 2010

For 2010, UMM's electricity usage ranged from approximately 300,000kWh to 750,000kWh per month depending on the time of year with the peak occurring during the summer. A graph of the load duration curve for the UMM campus for the 2010 calendar year is shown in Figure 8.2.

8.2 Electricity Rate Schedules

OTPC is an investor owned utility headquartered in Fergus Falls, MN serving approximately 423 communities and 129,500 customers [90]. Their service area spans 50,000 square miles and encompasses western Minnesota, including the UMM campus,

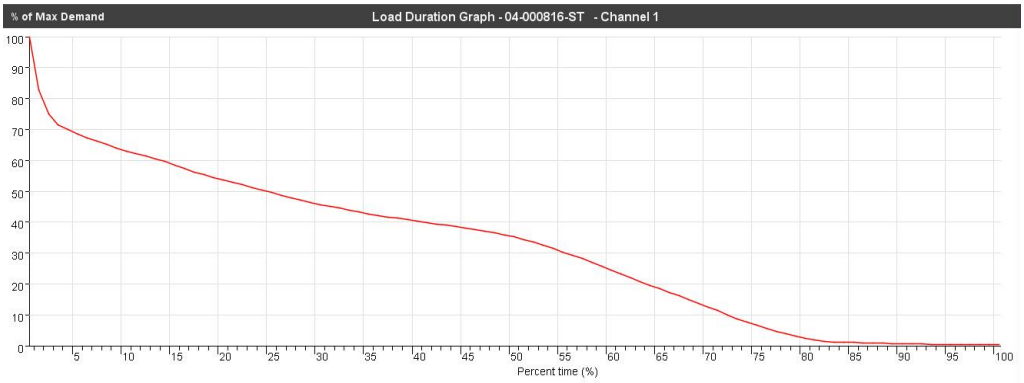

Figure 8.2: UMM Campus Load Duration Curve for 2010

and eastern North and South Dakota. A map of OTPC's service area is shown in Figure 8.3.

Figure 8.3: Otter Tail Power Company Service Area [90]

OTPC offers a variety of rate schedule options for large non-residential customers. These include large general service, large general service-time of day, commercial service-time

of use, and real-time pricing rate schedules. Details for each of these rate schedules are provided in [91].

Currently, the UMM campus subscribes to the large general service rate schedule, which charges a fixed energy and demand rate depending on the season. The summer is defined as lasting from June through September and the winter includes the remaining months. The large general service rate schedule for primary service customers is shown in Table 8.1. The energy charge is used to recover the variable costs of producing energy, and the demand charge is used to recover the fixed costs associated with the system capacity necessary to produce and deliver electricity.

Table 8.1: Large General Service - Primary Service Rate Schedule [91]

Charge	Rate	
Facilities Charge (per annual max kW)	$\$0.14/kW$	
	Summer	**Winter**
Energy Charge	$4.476\ ¢/kWh$	$4.238\ ¢/kWh$
Demand Charge	$\$6.46/kW$	$\$4.02/kW$

In contrast to the traditional large general service rate schedule, the large general service-time of day rate schedule charges varying rates depending on the time of day, day of the week, and season during which the energy is consumed. Each hour is designated as one of three different price periods: on-peak, shoulder, and off-peak. A chart depicting the time of day price period designations for each season is shown in Figure 8.4, and the rate schedule for primary service customers is shown in Table 8.2.

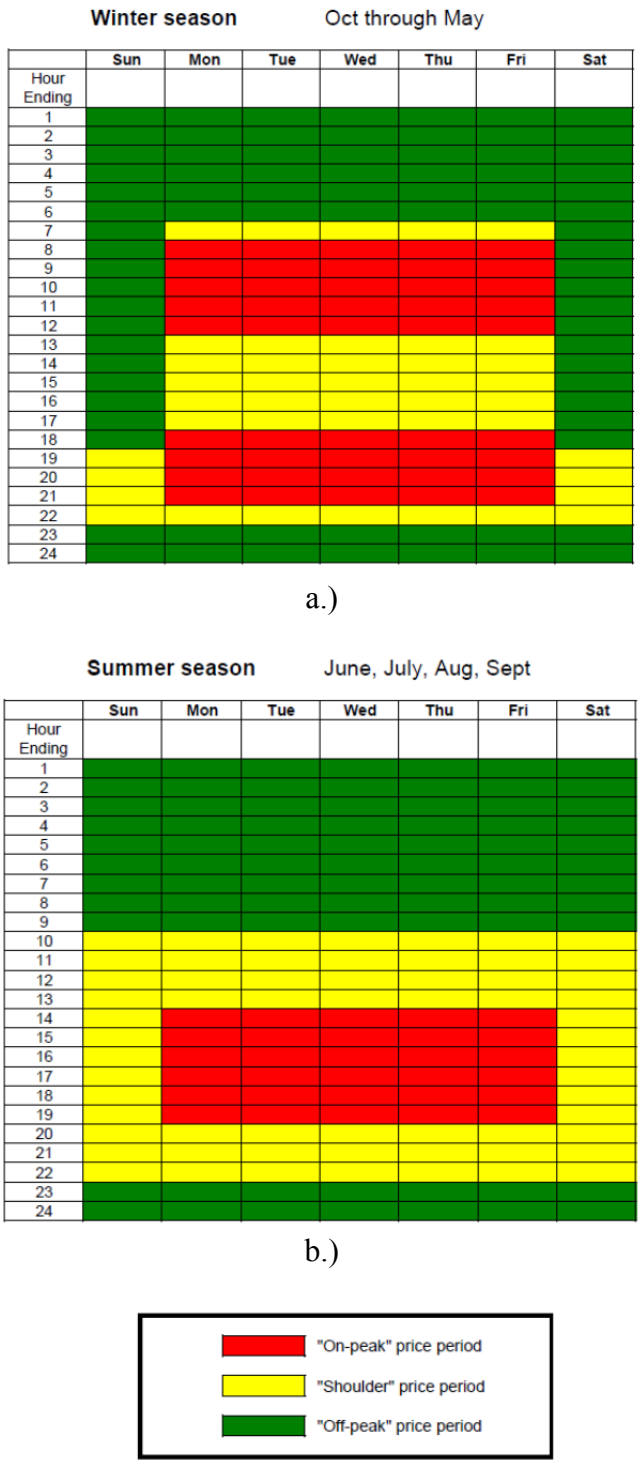

Figure 8.4: Time of Day Price Period Designations a.) Winter b.) Summer [91]

Table 8.2: Large General Service - Time of Day Primary Service Rate Schedule [91]

Charge	Rate	
Facilities Charge	$\$0.00/kW$	
Energy Charge	**Summer**	**Winter**
On-Peak	$8.415\ ¢/kWh$	$6.754\ ¢/kWh$
Shoulder	$5.315\ ¢/kWh$	$4.678\ ¢/kWh$
Off-Peak	$1.725\ ¢/kWh$	$1.982\ ¢/kWh$
Demand Charge		
On-Peak	$\$4.25/kW$	$\$3.01/kW$
Shoulder	$\$1.74/kW$	$\$0.98/kW$
Off-Peak	$\$0.00/kW$	$\$0.00/kW$

8.3 Energy Conservation

With the ambitious goal of becoming energy self-sufficient and carbon neutral, UMM is looking to decrease its energy use, costs, and carbon footprint by installing various smart grid technologies throughout its campus to make further use of its wide array of renewable DERs. DERs are much more efficient than traditional centralized energy systems. Traditional centralized power stations waste over 60% of the primary energy in fuel as heat released into the atmosphere. In addition, another 3.5% of the energy is lost through high-voltage transmission and distribution over long-distances [92]. Energy losses inherent in a centralized energy system are shown in Figure 8.5. In contrast, DERs can be up to 80-90% efficient [92].

Furthermore, numerous studies have shown that when consumers are provided with real-time energy use information they use less amounts of electricity. For example, a study by McClelland and Cook [93] over a period of 11 months found that consumers that were provided continuous feedback on their electricity use in cents per hour used 12% less electricity than those without this information over the same period. Assuming

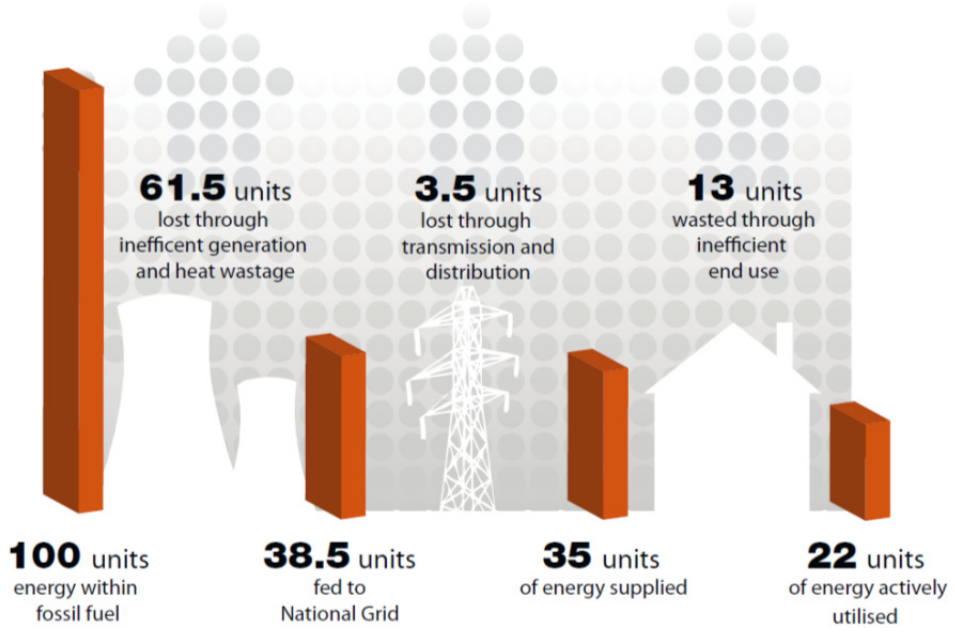

Figure 8.5: Energy Losses Inherent in Centralized Energy Systems [92]

a similar 12% reduction in energy usage for the UMM campus from real-time energy use information would have resulted in electricity cost savings of approximately $40,000 for the 2010 calendar year.

The ultimate vision is that each member of the UMM community will be able to observe and manage his/her personal energy use and carbon footprint via a downloadable smart phone application. Already, a smart phone application is under development to provide real-time production data for the campus's second wind turbine.

8.4 Time of Day Pricing

To further achieve its energy goals, UMM can take advantage of time of day pricing offered by OTPC to manage its load utilizing AMI, which is being planned for installation throughout the campus. Time of day pricing coupled with the capabilities

provided by AMI will facilitate both energy conservation and cost savings by allowing load to be shifted from on-peak and shoulder price periods to off-peak ones. Time of day pricing provides the most beneficial rate schedule for a large customer such as UMM since rates are predetermined and large loads can be scheduled in advance. Furthermore, UMM lacks the flexibility to reschedule load on short notice as would be necessary to benefit from real-time pricing options since campus events and classes cannot be canceled or postponed due to spikes in real-time electricity prices.

Using data on UMM's electricity consumption for the 2010 calendar year, the benefits from switching to a time of day rate schedule and actively managing its load were calculated. A graph comparing the total monthly electricity charges for 2010 for both the large general service and the large general service-time of day rate schedules is shown in Figure 8.6. The costs include facility, energy, and demand charges along with a 3.8% interim rate adjustment. Graphs comparing the monthly energy and demand charges for 2010 for both rate schedules are shown in Figure 8.7 and Figure 8.8 respectively.

Annually, the large general service rate schedule results in a charge of approximately $331,400, while the time of day rate schedule results in a charge of approximately $327,700. Thus, the time of day rate schedule represents a $3,700 or 1.1% costs savings with no active load management implemented. It can be seen from Figure 8.7 and Figure 8.8 that the reason for this cost savings is due to the lower demand charges even though the energy charges are higher. This is aided by the fact that the peak load for the UMM campus during each month tends to occur during a shoulder or off-peak

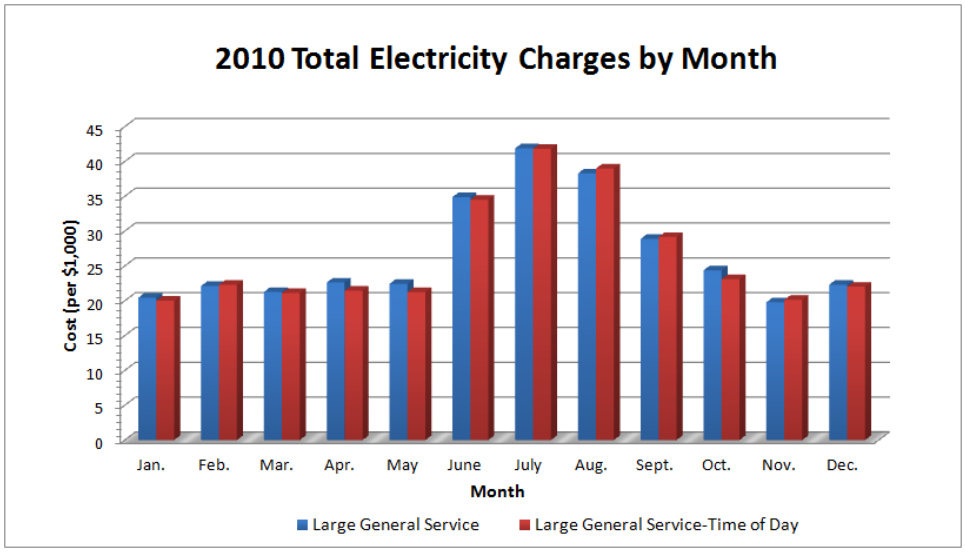

Figure 8.6: 2010 Total Electricity Charges by Month

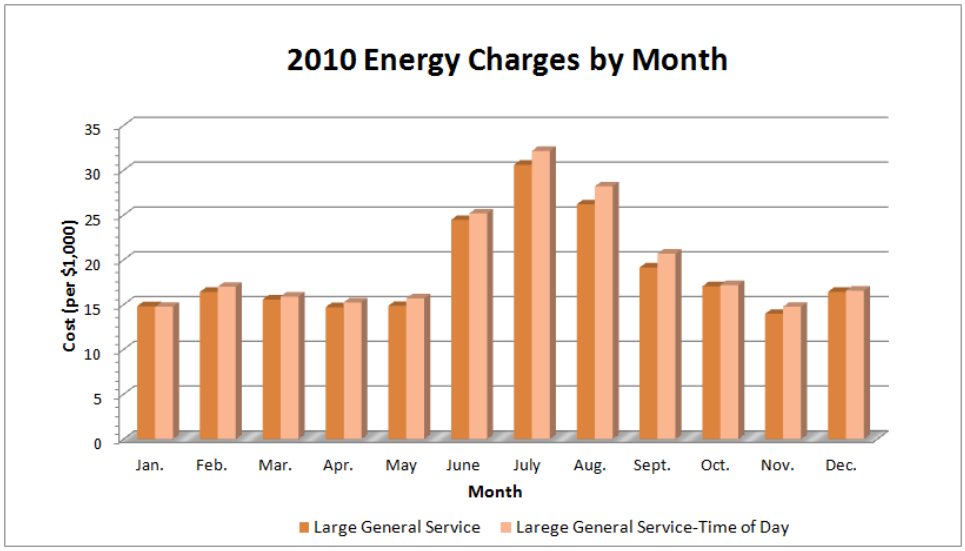

Figure 8.7: 2010 Energy Charges by Month

pricing period.

Thus, the UMM campus is advantageously positioned to benefit from an aggressive load management program utilizing time of day pricing. Small changes made to their current energy consumption patterns could lead to significant cost savings.

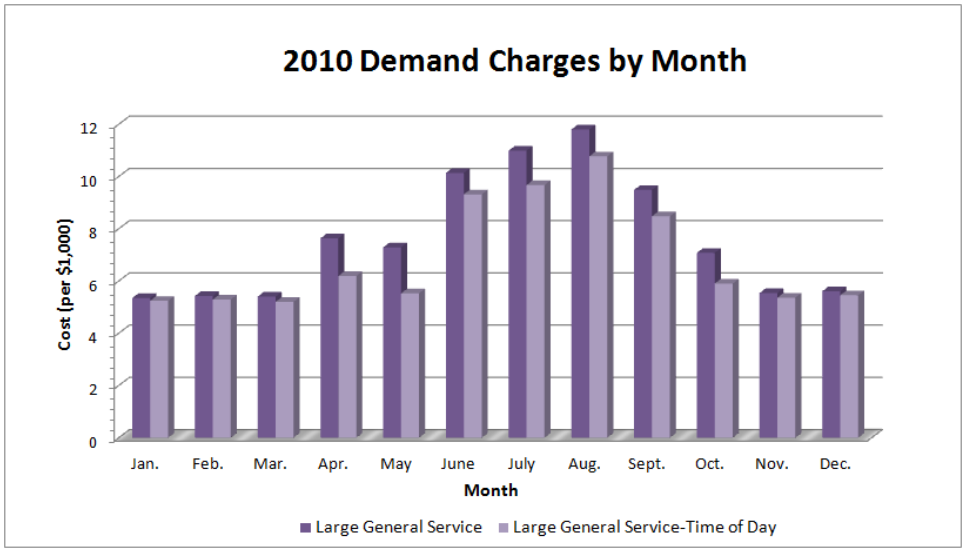

Figure 8.8: 2010 Demand Charges by Month

8.5 Active Load Management

Several additional calculations were performed to determine the benefits to the UMM campus from actively managing its load while utilizing time of day pricing. Calculations for when load is shifted to the next lowest price period and for when load is shifted to the lowest price period were performed. For example, shifting load to the next lowest price period would result in some amount of on-peak period load being shifted to the shoulder period, and some amount of shoulder period load being shifted to the off-peak period. Shifting load to the lowest price period would result in some amount of on-peak period load and shoulder period load both being shifted to the off-peak period. The cost savings for the 2010 calendar year for both load management schemes and various amounts of load when compared to time of day pricing without load management are shown in Table 8.3. A graph of the results is shown in Figure 8.9.

Table 8.3: Cost Savings from Load Management

Load Managed (%)	Savings ($)	Savings (%)
Load Shifted to Next Lowest Price Period		
10	9,573	2.9
20	19,146	5.8
30	28,719	8.8
40	38,292	11.7
50	47,865	14.6
Load Shifted to Lowest Price Period		
10	14,192	4.3
20	28,385	8.7
30	42,577	13.0
40	56,769	17.3
50	70,962	21.7

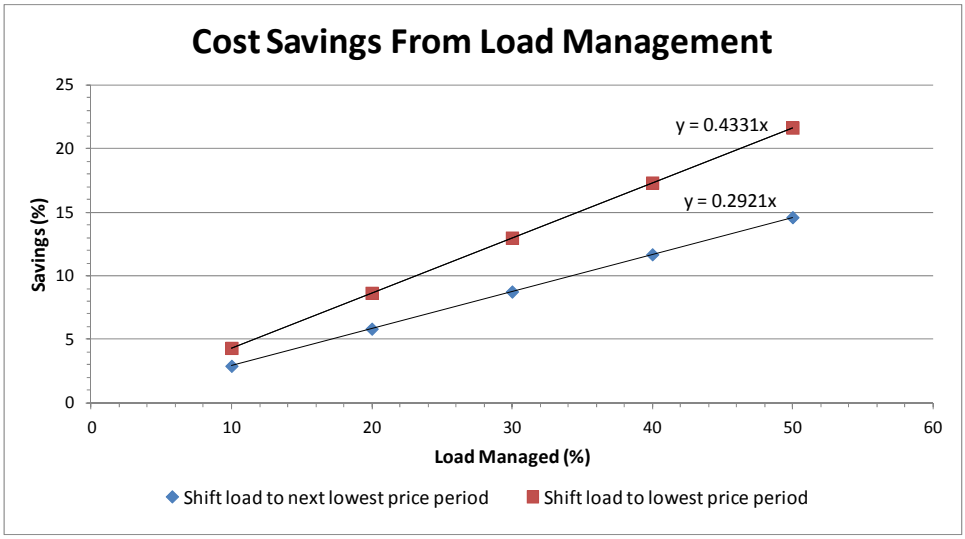

Figure 8.9: Cost Savings from Load Management

From Table 8.3 and Figure 8.9, it can be seen that with a modest effort UMM can achieve significant cost savings from actively managing its load. As one would expect, greater savings are achieved from shifting all load to the lowest price period, but this is more beneficial when a large percentage of load is managed. In addition, it can be seen from Figure 8.9 that when load is shifted to the next lowest price period, the percentage

of cost savings is approximately 29% of the percent of load shifted, while when load is shifted to the lowest price period, the percentage of cost savings is approximately 43% of the percent of load shifted.

8.6 Total Cost Savings

It must be noted that the load management calculations performed in Section 8.5 do not factor in cost savings from conservation efforts. The total cost savings from energy conservation, time of day pricing, and active load management for the 2010 calendar year for both load management schemes and various amounts of load when compared to large general service rate pricing are shown in Table 8.4. A graph of the results is shown in Figure 8.10. As a conservative estimate, it was again assumed that real-time energy use information would result in a 12% reduction in energy usage for the UMM campus.

From Table 8.4 and Figure 8.10, it can be seen that significant annual cost savings can be achieved from the combination of energy conservation, time of day pricing, and active load management. Approximately 13% of the cost savings are due to energy conservation and time of day pricing, while the remaining savings depend on the amount of load managed and the load management scheme implemented.

Furthermore, another cost savings opportunity exists from actively reducing established demand, which is used to determine demand charges. The monthly established demand is defined by OTPC as the maximum kW registered over any period of one hour during the month for which the bill is rendered adjusted for any excess

Table 8.4: Cost Savings from Energy Conservation, Time of Day Pricing, and Active Load Management

Load Managed (%)	Savings ($)	Savings (%)
Load Shifted to Next Lowest Price Period		
10	51,398	15.5
20	59,823	18.1
30	68,247	20.6
40	76,671	23.1
50	85,096	25.7
Load Shifted to Lowest Price Period		
10	55,463	16.7
20	67,952	20.5
30	80,442	24.3
40	92,931	28.0
50	105,420	31.8

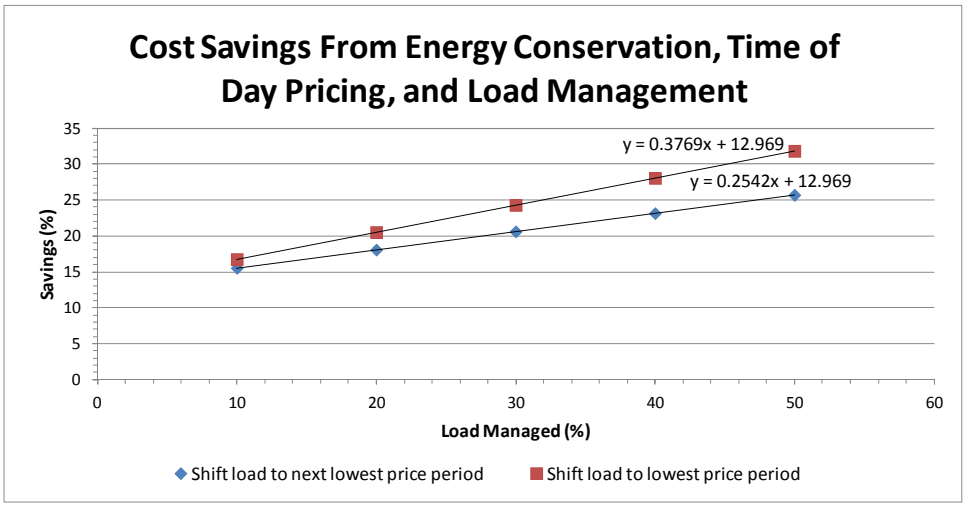

Figure 8.10: Cost Savings from Energy Conservation, Time of Day Pricing, and Active Load Management

reactive demand. Thus, additional cost savings can be achieved by reducing the established demand by shifting specific loads resulting in the established demand to a lower price period, or spreading such load out over a longer time period to reduce the demand during any specific hour.

While significant initial investments are required to install the necessary smart grid technologies to achieve the above costs savings, once installed, the annual savings can be used to pay back these initial investments. Given the costs and the expected life expectancies of the smart grid technologies, calculations can easily be completed to estimate their total long-term benefits. Moreover, as energy prices continue to rise in the future, the attractiveness of such investments will continue to increase.

8.7 Future Work

Full-scale implementation of smart grid technologies including demand response, two-way communication, DERs, supply-side management, and AMI on the UMM campus is being planned for the near future. Thus, future work will focus on measuring and quantifying the actual benefits realized as these technologies are implemented along with the effects of the technology on consumer's behavior, in this case the faculty, staff, and students of the UMM community. The project will serve as an important demonstration site and test platform for such technology, the results of which will then be able to be leveraged by other smart grid projects throughout the country.

From the above analysis, the UMM campus seems ideally situated to benefit from these investments in its campus energy infrastructure. UMM appears to be well on its way to achieving its goals of significantly reducing its energy costs, and becoming energy self-sufficient and carbon neutral.

9 Conclusions

A major transformation is taking place throughout the electric power industry to overlay existing electric infrastructure with advanced sensing, communications, and control system technologies. This transformation to a smart grid promises to enhance system efficiency, increase system reliability, support the electrification of transportation, and provide customers with greater control over their electricity consumption. Already, planning for the installation of such systems has begun at many utilities throughout the country, but regardless of how quickly various utilities embrace such concepts, technologies, and systems, "they all agree on the inevitability of this massive transformation" [62].

In this dissertation, a comprehensive systems approach is taken to minimize and prevent cyber-physical disturbances to electric power distribution systems using sensing, communications, and control system technologies. In particular, this research achieves each of the following:

1) The development of a control architecture for distribution systems to provide greater adaptive and self-healing protection, with the ability to proactively reconfigure, and rapidly respond to disturbances.
2) The development of an analytical and multi-domain methodology to assess the effects of smart grid technologies on distribution system operations and performance.

3) The integration of aspects of cyber-physical security, dynamic price and demand response, sensing, communications, intermittent DERs, and dynamic optimization and reconfiguration into one all-inclusive model.
4) An analysis of the trade-offs between system reliability, operational constraints, and costs for different control architectures and optimization algorithms.

A summary of the results presented in this dissertation is provided in Table 9.1. It lists the control architectures and optimization algorithms that achieved the best performance for each of the system objectives analyzed for each simulation scenario performed.

Table 9.1: Simulation Results Summary

	w/DR	**w/o DR**
Objective	**No Wind**	
Minimize LOEE	DC	IDSC-ALS
Minimize Line Losses	CC	CC
Minimize Voltage Violations	CC	CC
Minimize Line Flow Violations	IDSC-SSO IDSC-ALS DC	IDSC-SSO IDSC-ALS DC
	w/Wind	
Minimize LOEE	IDSC-ALS	IDSC-ALS
Minimize Line Losses	IDSC-SSO	IDSC-SSO
Minimize Voltage Violations	IDSC-ALS	IDSC-ALS
Minimize Line Flow Violations	IDSC-SSO IDSC-ALS	IDSC-SSO IDSC-ALS

Key
w/DR – with Demand Response
w/o DR – without Demand Response
IDSC – Intelligent Distributed Secure Control
SSO – Sequential Switch Opening
ALS – Annealed Local Search
DC – Decentralized Control
CC – Centralized Control

For multiple objectives, the optimal control architecture could not be determined directly from the simulation results. Such an assessment requires determining the value of one objective in relation to another, such as the value of minimizing LOEE versus minimizing line losses. As a result, in order to determine which distribution automation and control systems to implement, sound business practice stipulates that the costs of any systems implemented must be balanced against the cost savings realized by their implementation, although other factors often must also be taken into account.

In addition, the simulation results show that the use of day-ahead MCPs are much better suited for demand response programs than real-time MCPs due to their much lower volatility and greater correlation with load demand curves.

The research described in this dissertation lays the foundation for significant future work in this area to be completed. Areas for possible exploration include the impact of storage, additional types of DERs, and the location of DERs on distribution system operations and performance. In addition, significant enhancements can be made to the simulation models including the development of a full three-phase circuit model, and the simulation and analysis of larger test cases such as the recently released IEEE 8,500 node test feeder. A sensitivity analysis of the control architectures to various failure rates can also be performed.

9.1 Related Areas for Future Work

In order to defend and protect electric infrastructure control systems against cyber-physical attacks, significant work remains to be done and numerous research

questions remain unanswered. "Cyber connectivity, which provides a fairly inexpensive avenue to infiltrate control systems," has increased the complexity of control systems and the facilities it is intended to safely and reliably control. Therefore, "a better understanding and resulting optimization" of cyber security "will require a mathematical representation of this complexity" [38], which currently does not exist. In addition, minimizing the effects of cyber disturbances on a system introduces several complex challenges. According to [38]:

> Characterization of health or wellness from a cyber perspective is purely empirical, as prediction of the future is based on past events. While there are barriers in place to exclude known types of adversarial communication, state awareness cannot be assured because of the limited availability of diverse sensing. Determination of the actual cause of an abnormal event can only occur only [*sic*] after forensics are completed. Patterns or routines are analyzed and are used to provide comparisons to understand anomalies. However, while this understanding provides an interesting perspective, it may be very limited in predicting future behavior of the adversary.

Current research in the related area of terrorist attacks has found that such attacks tend to follow a specific pattern, known as a power law curve, which is often encountered in mathematics. In such a progression, the value of a variable (for example, the number of casualties) is always increased or decreased by the same exponent, or power. Furthermore, analyses of data from insurgencies in numerous countries have shown that for each set of data the resulting curves were characterized by a similar negative power [38]. (The negative power reflects a decrease rather than an increase in the number of events as the death toll rises.)

Nevertheless, a significant gap remains between the identification of mathematical patterns and being able to use them to predict attacks. Several researchers have expressed concern that mathematics might not be able to explain everything. "'Insurgencies are *sui generis*; each takes place within its own social, cultural, and political milieu. Trying to create a unified model is a fool's errand. I don't think there is enough cultural awareness of what moves people to do what they do'" [94]. Fallout from the 2008 Wall Street financial crash has already proven that finding patterns is not the same thing as understanding which ones are meaningful and acting on them in a responsible way [94].

Therefore, no matter how many layers of security or the degree of sophistication used in defense mechanisms, it will be essential that the industry hire qualified people. Research findings suggest that human and organizational factors do affect computer and information security performance in a multi-layered fashion. Often vulnerabilities are not the result of a single mistake or configuration error, but numerous latent organizational conditions, such as management support and decisions made by designers that combine to create scenarios where failures and vulnerabilities may occur [28]. Thus, staff must be well trained to respond to a wide variety of emergencies since no amount of technology can replace well-trained personnel [17].

In 1978, when Fred Schweppe first proposed the idea of an electric power grid with sophisticated hierarchical control systems, he stated that "there is a good chance that by the year 2000 the term blackout (societal definition) will be considered to be a term out of the Dark Ages" [5]. While the 2003 blackout that blanketed nearly the entire

Northeastern United States and parts of Canada proved this prediction false, one can hope that the transformation of the grid to an intelligent, self-healing system will continue, and this prediction will hold true in the near future.

10 Bibliography

[1] E. Santacana, G. Rackliffe, L. Tang, and X. Feng, "Getting smart," *IEEE Power and Energy Magazine*, vol. 8, no. 2, pp. 41-48, March/April 2010.

[2] Z. Jiang et al., "A vision of smart transmission grids," in *IEEE Power and Energy Society General Meeting*, Calgary, AB, 2009.

[3] "Needed: a grid operating system to facilitate grid transformation," EPRI, Palo Alto, CA, White Paper, May 2011.

[4] P. Fox-Penner, *Smart Power: Climate Change, the Smart Grid, and the Future of Electric Utilities*. Washington, D.C.: Island Press, 2010.

[5] F. C. Schweppe, "Power systems '2000': hierarchical control strategies," *IEEE Spectrum*, pp. 42-47, July 1978.

[6] Galvin Electricity Initiative. Fact Sheet: The Electric Power System is Unreliable. [Online]. http://www.galvinpower.org/resources/galvin.php?id=26

[7] Galvin Electricity Initiative. The Case for Transformation. [Online]. http://www.galvinpower.org/resources/galvin.php?id=27

[8] "Electricity sector framework for the future volume I: achieving the 21st century transformation," EPRI, Palo Alto, CA, 2003.

[9] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," *IEEE Security and Privacy*, vol. 7, no. 3, pp. 75-77, May/June 2009.

[10] Electricity Advisory Committee, "Smart grid: enabler of the new energy economy," Electricity Advisory Committee, 2008.

[11] R. Pratt et al., "The smart grid: an estimation of the energy and CO2 benefits," Pacific Northwest National Laboratory, Richland, WA, PNNL-19112, 2010.

[12] R. Davies, "Hydro One's smart meter initiative paves way for defining the smart grid of the future," in *IEEE Power and Energy Society General Meeting*, Calgary, AB, 2009.

[13] "Estimating the costs and benefits of the smart grid: a preliminary estimate of the investment requirements and the resultant benefits of a fully functioning smart grid," EPRI, Palo Alto, CA, 2011.

[14] "West Virginia smart grid implementation plan," DOE/NETL-2009/1386, 2009.

[15] P. Carson, "Regulators curb SmartGrid city recovery," *EnergyBiz*, January 26, 2011.

[16] T. Kropp, "System threats and vulnerabilities," *IEEE Power and Energy Magazine*, vol. 4, no. 2, pp. 46-50, March/April 2006.

[17] R. Schainker, J. Douglas, and T. Kropp, "Electric utility responses to grid security issues," *IEEE Power and Energy Magazine*, vol. 4, no. 2, pp. 30-37, March/April

2006.

[18] J. Clemente, "The security vulnerabilities of smart grid," *Journal of Energy Security*, June 2009.

[19] P. H. Corredor and M. E. Ruiz, "Against all odds," *IEEE Power and Energy Magazine*, vol. 9, no. 2, pp. 59-66, March/April 2011.

[20] "War in the fifth domain," *The Economist*, pp. 25-28, July 3rd-9th 2010.

[21] D. Watts, "Security & vulnerability in electric power systems," in *35th North American Power Symposium*, Rolla, MO, 2003, pp. 559-566.

[22] I. Winkler, "Opinion: the hackability of the smart grid," *Computerworld*, December 2009.

[23] S. M. Amin, "Securing the electricity grid," *The Bridge*, vol. 40, no. 1, Spring 2010.

[24] F. T. Sheldon, S. G. Batsell, S. J. Prowell, and M. A. Langston, "Position statement: methodology to support dependable survivable cyber-secure infrastructures," in *Proceedings of the 38th Annual Hawaii International Conference on System Sciences*, Big Island, HI, 2005, p. 310a.

[25] "Smart grid policy," Federal Energy Regulatory Commission, Policy Statement Docket No. PL09-4-000, July 2009. [Online]. http://www.ferc.gov/whats-new/comm-meet/2009/071609/E-3.pdf

[26] C.-W. Ten, M. Govindarasu, and C.-C. Liu, "Cybersecurity for electric power control and automation systems," in *IEEE International Conference on Systems, Man and Cybernetics*, Montreal, QC, 2007, pp. 29-34.

[27] J. E. Dagle, "Cyber security of the electric power grid," in *IEEE/PES Power Systems Conference and Exposition*, Seattle, WA, 2009, pp. 1-2.

[28] S. Kraemer, P. Carayon, and J. Clem, "Human and organizational factors in computer and information security: pathways to vulnerabilities," *Computers & Security*, vol. 28, no. 7, pp. 509-520, October 2009.

[29] "Complex interactive networks/systems initiative: final summary report: overview and summary report for joint EPRI and U.S. Department of Defense university research initiative," EPRI, Palo Alto, CA, 2002.

[30] J. Blum. (2004, August) MSNBC.com. [Online]. http://www.msnbc.msn.com/id/5659214

[31] G. N. Ericsson, "Information security for electric power utilities (EPUs)-CIGRE developments on frameworks, risk assessment, and technology," *IEEE Transactions on Power Delivery*, vol. 24, no. 3, pp. 1174-1181, July 2009.

[32] J. Salmeron, K. Wood, and R. Baldick, "Analysis of electric grid security under terrorist threat," *IEEE Transactions on Power Systems*, vol. 19, no. 2, pp. 905-912, May 2004.

[33] E. Camponogara, D. Jia, B. Krogh, and S. Talukdar, "Distributed model predictive control," *IEEE Control Systems Magazine*, vol. 22, no. 1, pp. 44-52, February 2002.

[34] K. Miller, "Layered security provides superior protection for plant control systems," *Oil & Gas Journal*, October 2005.

[35] NIST, "Smart grid cyber security strategy and requirements," The Smart Grid Interoperability Panel - Cyber Security Working Group, DRAFT NISTIR 7628, February 2010.

[36] M. Takano, "Sustainable cyber security for utility facilities control system based on defense-in-depth concept," in *SICE Annual Conference*, Takamatsu, Japan, 2007, pp. 2910-2913.

[37] M. A. McQueen and W. F. Boyer, "Deception used for cyber defense of control systems," in *2nd Conference on Human System Interactions*, Catania, Italy, 2009, pp. 624-631.

[38] C. G. Rieger, D. I. Gertman, and M. A. McQueen, "Resilient control systems: next generation design research," in *2nd Conference on Human System Interactions*, Catania, Italy, 2009, pp. 632-636.

[39] W. A. Johnson, "A utility program for enterprise security response," in *IEEE Power Engineering Society WPM*, Columbus, OH, 2001.

[40] F. Cohen, "Simulating cyber attacks, defences, and consequences," *Computers & Security*, vol. 18, no. 6, pp. 479-518, 1999.

[41] P. L. Campbell and J. E. Stamp, "A classification scheme for risk assessment methods," Sandia National Laboratories, Albuquerque, NM, SAND2004-4233, 2004.

[42] T. Sommestad, M. Ekstedt, and P. Johnson, "Cyber security risks assessment with bayesian defense graphs and architectural models," in *42nd Hawaii International Conference on System Sciences*, Waikoloa, HI, 2009, pp. 1-20.

[43] P. Helman, G. Liepins, and W. Richards, "Foundations of intrusion detection," in *Computer Secuirty Foundations Workshop V*, Franconia, NH, 1992, pp. 114-120.

[44] N. Ye, Y. Zhang, and C. M. Borror, "Robustness of the markov-chain model for cyber-attack detection," *IEEE Transactions on Reliability*, vol. 53, no. 1, pp. 116-123, March 2004.

[45] I. Kotenko, "Multi-agent modelling and simulation of cyber-attacks and cyber-defense for homeland security," in *IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications*, Dortmund, Germany, 2007, pp. 614-619.

[46] B. Awerbuch and R. Kleinberg, "Competitive collaborative learning," *Journal of Computer and System Sciences*, vol. 74, no. 8, pp. 1271-1288, December 2008.

[47] J. Darby et al., "Evidence-based techniques for evaluating cyber protection systems for critical infrastructure," in *IEEE Military Communications Conference*, Washington, D.C., 2006, pp. 1-10.

[48] "Strategic insights into security, quality, reliability and availability report," EPRI, Palo Alto, CA, 2005.

[49] C.-W. Ten, C.-C. Liu, and G. Manimaran, "Vulnerability assessment of cybersecurity for SCADA systems," *IEEE Transactions on Power Systems*, vol. 23, no. 4, pp. 1836-1846, November 2008.

[50] P. A. Ralston, J. H. Graham, and J. L. Hieb, "Cyber security risk assessment for SCADA and DCS networks," *ISA Transactions*, vol. 46, no. 4, pp. 583-594, October 2007.

[51] A. Mannikoff and H. Nilsson, "Sweden-reaching 100 percent 'smart meters' July 1, 2009," in *IEEE Power and Energy Society General Meeting*, Calgary, AB, 2009.

[52] F. Cleveland, "Cyber security issues for advanced metering infrastructure," in *IEEE T&D Conference*, Pittsburgh, PA, April 2008.

[53] G. Deconinck, "An evaluation of two-way communication means for advanced metering in Flanders (Belgium)," in *IEEE Instrumentation and Measurement Technology Conference Proceedings*, Victoria, BC, 2008, pp. 900-905.

[54] M. G. Morgan et al. (2009, July) The many meanings of "Smart Grid". [Online]. http://www.epp.cmu.edu/Publications/Policy_Brief_Smart_Grid_July_09.pdf

[55] Energy Insights, "2008 national residential online panel real-time pricing (RTP) survey," IDC, Framingham, MA, 2008.

[56] F. Barringer, "New electricity meters stir fears," *The New York Times*, p. A12, January 30, 2011.

[57] J. Cline, "Opinion: will the smart grid protect consumer privacy?," *Computerworld*, November 2009.

[58] M. Amin, "Scoping study and survey of electric utility industry chief information officers (CIOs): trends, challenges, opportunities, and plans regarding future information technology needs for the electric power industry," EPRI, Palo Alto, CA, White Paper 2007.

[59] Defense Science Board (DSB), "Report of the defense science board task force on DoD energy strategy," Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, Washington, D.C., February 2008.

[60] Packet Power. (2010, September) [Online]. http://www.packetpower.com/index.php

[61] A. Phillips, "Staying in shape," *IEEE Power & Energy Magazine*, vol. 8, no. 2, pp. 27-33, March/April 2010.

[62] H. Farhangi, "The path of the smart grid," *IEEE Power & Energy Magazine*, vol. 8, no. 1, pp. 18-28, January/February 2010.

[63] S. H. Horowitz, A. G. Phadke, and B. A. Renz, "The future of power transmission," *IEEE Power & Energy Magazine*, vol. 8, no. 2, pp. 34-40, March/April 2010.

[64] J. D. Bouford and C. A. Warren, "Many states of distribution," *IEEE Power & Energy Magazine*, vol. 5, no. 4, pp. 24-32, July/August 2007.

[65] E. Lakervi and E. J. Holmes, *Electricity Distribution Network Design*, 2nd ed., A. T. Johns and J. R. Platts, Eds. Exeter, United Kingdom: Peter Peregrinus Ltd., 1996.

[66] T. A. Short, *Electric Power Distribution Handbook*. New York: CRC Press, 2004.

[67] D. S. Bassett, K. N. Clinard, J. J. Grainger, S. L. Purucker, and D. J. Ward, "Distribution automation and the utility system," in *Distribution Automation*. Piscataway, NJ: IEEE, 1988, ch. 1, pp. 1-6.

[68] A. M. Giacomoni, S. M. Amin, and B. F. Wollenberg, "A control and communications architecture for a secure and reconfigurable power distribution system: an analysis and case study," in *IFAC World Congress*, Milan, Italy, 2011.

[69] C.-C. Liu, J. Jung, G. T. Heydt, V. Vittal, and A. G. Phadke, "The strategic power infrastructure defense (SPID) system: a conceptual design," *IEEE Control Systems Magazine*, pp. 40-52, August 2000.

[70] M. Amin and D. Ballard, "Defining new markets for intelligent agents," *IT Pro*, pp. 29-35, July/August 2000.

[71] M. Shouman, A. Salah, and H. M. Faheem, "Surviving cyber warfare with a hybrid multiagent-based intrusion prevention system," *IEEE Potentials*, vol. 29, no. 1, pp. 32-40, January/February 2010.

[72] A. Ahuja, S. Das, and A. Pahwa, "An AIS-ACO hybrid approach for multi-objective distribution system reconfiguration," *IEEE Transactions on Power Systems*, vol. 22, no. 3, pp. 1101-1111, August 2007.

[73] S. Jazebi, S. H. Hosseinian, M. Pooyan, and B. Vahidi, "Performance comparison of GA and DEA in solving distribution system reconfiguration problem," in *11th International Conference on Optimization of Electrical and Electronic Equipment*, Brasov, Romania, 2008, pp. 185-190.

[74] S. P. Karthikeyan, V. S. Verma, D. C. Agrawal, R. I. Jacob, and D. P. Kothari, "Assessment of distribution system feeder and its reconfiguration using fuzzy adaptive evolutionary computing," in *Annual IEEE India Conference*, Kanpur, India, 2008, pp. 240-245.

[75] D. Shirmohammadi and H. W. Hong, "Reconfiguration of electric distribution networks for resistive line losses reduction," *IEEE Transactions on Power Delivery*, vol. 4, no. 2, pp. 1492-1498, April 1989.

[76] H. L. Willis, *Power Distribution Planning Reference Book*. New York: Marcel Dekker, Inc., 1997.

[77] T. E. McDermott, I. Drezga, and R. P. Broadwater, "A heuristic nonlinear constructive method for distribution system reconfiguration," *IEEE Transactions on Power Systems*, vol. 14, no. 2, pp. 478-483, May 1999.

[78] L. A. Wolsey, *Integer Programming*. New York: John Wiley & Sons, Inc., 1998.

[79] R. E. Brown, "Distribution reliability assessment and reconfiguration optimization," in *IEEE/PES Transmission and Distribution Conference and Exposition,* Atlanta, GA, 2001, pp. 994-999 vol.2.

[80] W. H. Kersting, "Radial distribution test feeders," in *IEEE Power Engineering Society Winter Meeting*, Columbus, OH, 2001, pp. 908-912 vol. 2.

[81] D. Shirmohammadi, H. W. Hong, A. Semlyen, and G. X. Luo, "A compensation-based power flow method for weakly meshed distribution and transmission networks," *IEEE Transactions on Power Systems*, vol. 3, no. 2, pp. 753-762, May 1988.

[82] Midwest ISO. (2010, May) Midwest ISO - Documents. [Online]. http://www.midwestiso.org/publish

[83] W. Li, *Risk Assessment of Power Systems: Models, Methods, and Applications*. Piscataway, NJ: IEEE Press, 2005.

[84] M. Bollen, "Adapting electricity networks to a sustainable energy system - smart metering and smart grids," Energy Markets Inspectorate, Eskilstuna, Sweden, EI R2011:03, 2011.

[85] Con Edison. (2010, September) Demand Response/Day-Ahead Hourly Pricing Program. [Online]. http://www.coned.com/energyefficiency/vol_time_pricing.asp

[86] Southern California Edison. (2010, September) Demand Response Program. [Online]. http://www.sce.com/b-rs/demand-response-programs/demand-response-programs.htm

[87] J. J. Grainger and J. W. D. Stevenson, *Power System Analysis*. New York: McGraw-Hill, 1994.

[88] W. H. Kersting, *Distribution System Modeling and Analysis*, 2nd ed. Boca Raton, FL: CRC Press, 2002.

[89] University of Minnesota Morris. (2011, January) A Comprehensive Approach to Sustainability. [Online]. http://www.morris.umn.edu/sustainability/

[90] Otter Tail Power Company. (2011, January) Service area. [Online]. http://www.otpco.com/AboutCompany/ServiceArea.asp

[91] Otter Tail Power Company. (2011, January) Rates, rules, and regulations. [Online]. http://www.otpco.com/ElectricRates/RatesReferenceTable.asp

[92] M. King and R. Shaw, "Community energy: planning, development and delivery," Town and Country Planning Association, Gosport, United Kingdom, 2010.

[93] L. McClelland and S. W. Cook, "Energy conservation effects of continuous in-home feedback in all-electric homes," *Journal of Environmental Systems*, vol. 9, no. 2, pp. 169-173, 1979.

[94] A. Curry, "Mathematics of terror," *Discover*, pp. 38-43, July/August 2010.

Appendix A
Cyber Security Threat Categories

Table A.1: Authentication [47]

Category	Cyber Security Posture
I	No Passwords
II	Weak passwords. No periodic changes.
III	Strong passwords. No periodic changes.
IV	Strong passwords. Periodic Changes.
V	Strong passwords. Periodic Changes. Limits on failed password attempts. Passwords are cracked every month to find users with easily guessed passwords.

Table A.2: Network Access Control [47]

Category	Cyber Security Posture
I	Remote login via password-protected dial-up connections. No Firewall.
II	Remote logins allowed from Internet. IP Address Filtering and Port Blocking.
III	Remote logins allowed via VPN connection
IV	No remote logins. SCADA Controls accessible only from LAN terminals.
V	No remote logins. SCADA LAN is physically separate from other LANs.

Table A.3: User Access Control [47]

Category	Cyber Security Posture
I	Physical Access unmonitored. Rights given to everyone.
II	Physical Access monitored. Rights assigned to individual users.
III	Rights assigned to groups. All cyber equipment is physically secured.

Table A.4: Threat Categories: High (H), Medium (M), Low (L) [47]

Category	Funding	Goal Intensity	Stealth	Physical Access	Cyber Skills	Implementation Time	Cyber Org Size
I	H	H	H	H	H	Decades/Years	Hundreds
II	H	H	H	M	M	Years	Tens of Tens
III	M	H	M	M	M	Months	Tens
IV	L	M	H	L	H	Months	Tens
V	L	M	M	L	M	Months	Ones
VI	L	L	L	L	L	Weeks	One

Appendix B
Typical Distribution System Circuit Parameters

Table B.1: Typical Distribution System Circuit Parameters [66]

	Most Common Value	Other Common Values
Substation Characteristics		
Voltage	12.47 kV	4.16, 4.8, 13.2, 13.8, 24.94, 34.5 kV
Number of station transformers	2	1-6
Substation transformer size	21 MVA	5-60 MVA
Number of feeders per bus	4	1-8
Feeder Characteristics		
Peak current	400 A	100-600 A
Peak load	7 MVA	1-15 MVA
Power factor	0.98 lagging	0.8 lagging-0.95 leading
Number of customers	400	50-5000
Length of feeder mains	4 mi	2-15 mi
Length including laterals	8 mi	4-25 mi
Area covered	25 mi^2	0.5-500 mi^2
Mains wire size	500 kcmil	4/0-795 kcmil
Lateral tap wire size	1/0	#4-2/0
Lateral tap peak current	25 A	5-50 A
Lateral tap length	0.5 mi	0.2-5 mi
Distribution transformer size (1 ph)	25 kVA	10-150 A

Appendix C
IEEE 123 Node Test Feeder Data

Table C.1: IEEE 123 Node Test Feeder Line Data (Modified from [80])

From Node	To Node	Resistance (ohms)	Reactance (ohms)	Susceptance (S)	Line Flow Limit (kVA)	Line Reliability
1	2	0.044	0.0446	0	2496	0.97
1	3	0.0629	0.0638	0	2496	0.97
1	7	0.026	0.0612	0	2496	0.97
3	4	0.0503	0.051	0	2496	0.97
3	5	0.0818	0.0829	0	2496	0.97
5	6	0.0629	0.0629	0	2496	0.97
7	8	0.0173	0.0408	0	2496	0.97
8	12	0.0566	0.0574	0	2496	0.97
8	9	0.0566	0.0574	0	2496	0.97
8	13	0.026	0.0612	0	2496	0.97
9	14	0.107	0.1085	0	2496	0.97
13	34	0.0377	0.0382	0	2496	0.97
13	18	0.0729	0.1638	0	2496	0.97
14	11	0.0629	0.0638	0	2496	0.97
14	10	0.0629	0.0638	0	2496	0.97
15	16	0.0944	0.0957	0	2496	0.97
15	17	0.0881	0.0893	0	2496	0.97
18	19	0.0629	0.0638	0	2496	0.97
18	21	0.0265	0.0596	0	2496	0.97
19	20	0.0818	0.0829	0	2496	0.97
21	22	0.1321	0.1339	0	2496	0.97
21	23	0.0221	0.0496	0	2496	0.97
23	24	0.1384	0.1403	0	2496	0.97
23	25	0.0243	0.0546	0	2496	0.97
25	26	0.0303	0.0721	0	2496	0.97
25	28	0.0177	0.0397	0	2496	0.97
26	27	0.0238	0.0561	0	2496	0.97
26	31	0.0566	0.0574	0	2496	0.97
27	33	0.1259	0.1276	0	2496	0.97

28	29	0.0265	0.0596	0	2496	0.97
29	30	0.0309	0.0695	0	2496	0.97
30	250	0.0177	0.0397	0	2496	0.97
31	32	0.0755	0.0765	0	2496	0.97
34	15	0.0251	0.0255	0	2496	0.97
35	36	0.0563	0.1327	0	2496	0.97
35	40	0.0217	0.051	0	2496	0.97
36	37	0.0755	0.0766	0	2496	0.97
36	38	0.0629	0.0638	0	2496	0.97
38	39	0.0818	0.0818	0	2496	0.97
40	41	0.0818	0.0829	0	2496	0.97
40	42	0.0217	0.051	0	2496	0.97
42	43	0.1258	0.1276	0	2496	0.97
42	44	0.0173	0.0408	0	2496	0.97
44	45	0.0503	0.051	0	2496	0.97
44	47	0.0217	0.051	0	2496	0.97
45	46	0.0755	0.0766	0	2496	0.97
47	48	0.0131	0.0303	0	2496	0.97
47	49	0.0219	0.0504	0	2496	0.97
49	50	0.0219	0.0504	0	2496	0.97
50	51	0.0219	0.0504	0	2496	0.97
52	53	0.0173	0.0408	0	2496	0.97
53	54	0.0108	0.0255	0	2496	0.97
54	55	0.0238	0.0561	0	2496	0.97
54	57	0.0306	0.0706	0	2496	0.97
55	56	0.0238	0.0561	0	2496	0.97
57	58	0.0629	0.0638	0	2496	0.97
57	60	0.0655	0.1513	0	2496	0.97
58	59	0.0629	0.0638	0	2496	0.97
60	61	0.0486	0.1092	0	2496	0.97
60	62	0.072	0.0343	0	2496	0.97
62	63	0.0504	0.024	0	2496	0.97
63	64	0.1008	0.0481	0	2496	0.97
64	65	0.1224	0.0584	0	2496	0.97
65	66	0.0936	0.0446	0	2496	0.97
67	68	0.0503	0.051	0	2496	0.97
67	72	0.024	0.0555	0	2496	0.97
67	97	0.0219	0.0504	0	2496	0.97

68	69	0.0692	0.0702	0	2496	0.97
69	70	0.0818	0.0829	0	2496	0.97
70	71	0.0692	0.0702	0	2496	0.97
72	73	0.0692	0.0701	0	2496	0.97
72	76	0.0175	0.0403	0	2496	0.97
73	74	0.0881	0.0893	0	2496	0.97
74	75	0.1006	0.102	0	2496	0.97
76	77	0.0347	0.0817	0	2496	0.97
76	86	0.0612	0.1412	0	2496	0.97
77	78	0.0087	0.0204	0	2496	0.97
78	79	0.0195	0.0459	0	2496	0.97
78	80	0.0412	0.097	0	2496	0.97
80	81	0.0412	0.097	0	2496	0.97
81	82	0.0217	0.051	0	2496	0.97
81	84	0.1699	0.1722	0	2496	0.97
82	83	0.0217	0.051	0	2496	0.97
84	85	0.1195	0.1212	0	2496	0.97
86	87	0.039	0.0919	0	2496	0.97
87	88	0.044	0.0446	0	2496	0.97
87	89	0.0238	0.0561	0	2496	0.97
89	90	0.0566	0.0574	0	2496	0.97
89	91	0.0195	0.0459	0	2496	0.97
91	92	0.0755	0.0765	0	2496	0.97
91	93	0.0195	0.0459	0	2496	0.97
93	94	0.0692	0.0701	0	2496	0.97
93	95	0.026	0.0612	0	2496	0.97
95	96	0.0503	0.051	0	2496	0.97
97	98	0.024	0.0555	0	2496	0.97
98	99	0.0481	0.1109	0	2496	0.97
99	100	0.0262	0.0605	0	2496	0.97
100	450	0.0699	0.1614	0	2496	0.97
101	102	0.0566	0.0574	0	2496	0.97
101	105	0.024	0.0555	0	2496	0.97
102	103	0.0818	0.0829	0	2496	0.97
103	104	0.1762	0.1786	0	2496	0.97
105	106	0.0566	0.0574	0	2496	0.97
105	108	0.0284	0.0656	0	2496	0.97
106	107	0.1447	0.1467	0	2496	0.97

108	109	0.1133	0.1148	0	2496	0.97
108	300	0.0874	0.2017	0	2496	0.97
109	110	0.0755	0.0766	0	2496	0.97
110	111	0.1447	0.1467	0	2496	0.97
110	112	0.0315	0.0319	0	2496	0.97
112	113	0.1322	0.134	0	2496	0.97
113	114	0.0818	0.0829	0	2496	0.97
135	35	0.0328	0.0756	0	2496	0.97
149	1	0.0347	0.0817	0	2496	0.97
152	52	0.0347	0.0817	0	2496	0.97
160	67	0.0303	0.0715	0	2496	0.97
197	101	0.0219	0.0504	0	2496	0.97
51	151	0.0611	0.1412	0	2496	0.97
610	611	0.005	0.005	0	2496	0.97

Table C.2: IEEE 123 Node Test Feeder Switch Data (Modified from [80])

From Node	To Node	Resistance (ohms)	Reactance (ohms)	Susceptance (S)	Line Flow Limit (kVA)	Line Reliability
13	152	0.005	0.005	0	2496	1
18	135	0.005	0.005	0	2496	1
54	94	0.005	0.005	0	2496	1
61	610	0.005	0.005	0	2496	1
97	197	0.005	0.005	0	2496	1
300	350	0.005	0.005	0	2496	1
60	160	0.005	0.005	0	2496	1
151	300	0.005	0.005	0	2496	1
95	195	0.005	0.005	0	2496	1
150	149	0.005	0.005	0	2496	1
450	451	0.005	0.005	0	2496	1
250	251	0.005	0.005	0	2496	1

Table C.3: IEEE 123 Node Test Feeder Bus Data (Modified from [80])

Bus #	Real Power (kW)	Reactive Power (kVAR)	WTP ($/kWh)	Average Real Power (kW)	Minimum Bus Voltage (pu)
150	0	0	0.07788	0	0.94

195	0	0	0.04235	0	0.94
251	0	0	0.00908	0	0.94
451	0	0	0.02665	0	0.94
611	0	0	0.06812	0	0.94
1	10	10	0.01537	10	0.94
2	5	5	0.0281	5	0.94
3	0	0	0.04401	0	0.94
4	10	10	0.05271	10	0.94
5	5	5	0.04574	5	0.94
6	10	10	0.08754	10	0.94
7	5	5	0.05181	5	0.94
8	0	0	0.09436	0	0.94
9	10	10	0.06377	10	0.94
10	5	5	0.09577	5	0.94
11	10	10	0.02407	10	0.94
12	5	5	0.06761	5	0.94
13	0	0	0.02891	0	0.94
14	0	0	0.06718	0	0.94
15	0	0	0.06951	0	0.94
16	10	10	0.0068	10	0.94
17	5	5	0.02548	5	0.94
18	0	0	0.0224	0	0.94
19	10	10	0.06678	10	0.94
20	10	10	0.08444	10	0.94
21	0	0	0.03445	0	0.94
22	10	10	0.07805	10	0.94
23	0	0	0.06753	0	0.94
24	10	10	0.00067	10	0.94
25	0	0	0.06022	0	0.94
26	0	0	0.03868	0	0.94
27	0	0	0.0916	0	0.94
28	10	10	0.00012	10	0.94
29	10	10	0.04624	10	0.94
30	10	10	0.04243	10	0.94
31	5	5	0.04609	5	0.94
32	5	5	0.07702	5	0.94
33	10	10	0.03225	10	0.94
34	10	10	0.07847	10	0.94

35	10	10	0.04714	10	0.94
36	0	0	0.00358	0	0.94
37	10	10	0.01759	10	0.94
38	5	5	0.07218	5	0.94
39	5	5	0.04735	5	0.94
40	0	0	0.01527	0	0.94
41	5	5	0.03411	5	0.94
42	5	5	0.06074	5	0.94
43	10	10	0.01917	10	0.94
44	0	0	0.07384	0	0.94
45	5	5	0.02428	5	0.94
46	5	5	0.09174	5	0.94
47	8.75	12.5	0.02691	8.75	0.94
48	17.5	25	0.07655	17.5	0.94
49	8.75	12.5	0.01887	8.75	0.94
50	10	10	0.02875	10	0.94
51	5	5	0.00911	5	0.94
52	10	10	0.05762	10	0.94
53	10	10	0.06834	10	0.94
54	0	0	0.05466	0	0.94
55	5	5	0.04257	5	0.94
56	5	5	0.06444	5	0.94
57	0	0	0.06476	0	0.94
58	5	5	0.0679	5	0.94
59	5	5	0.06358	5	0.94
60	5	5	0.09452	5	0.94
61	5	5	0.02089	5	0.94
62	10	10	0.07093	10	0.94
63	10	10	0.02362	10	0.94
64	18.75	17.5	0.01194	18.75	0.94
65	8.75	12.5	0.06073	8.75	0.94
66	18.75	17.5	0.04501	18.75	0.94
67	0	0	0.04587	0	0.94
68	5	5	0.06619	5	0.94
69	10	10	0.07703	10	0.94
70	5	5	0.03502	5	0.94
71	10	10	0.0662	10	0.94
72	0	0	0.04162	0	0.94

73	10	10	0.08419	10	0.94
74	10	10	0.08329	10	0.94
75	10	10	0.02564	10	0.94
76	40	40	0.06135	40	0.94
77	10	10	0.05822	10	0.94
78	0	0	0.05407	0	0.94
79	10	10	0.08699	10	0.94
80	10	10	0.02648	10	0.94
81	0	0	0.03181	0	0.94
82	10	10	0.01192	10	0.94
83	5	5	0.09398	5	0.94
84	5	5	0.06456	5	0.94
85	10	10	0.04795	10	0.94
86	5	5	0.06393	5	0.94
87	10	10	0.05447	10	0.94
88	10	10	0.06473	10	0.94
89	0	0	0.05439	0	0.94
90	10	10	0.0721	10	0.94
91	0	0	0.05225	0	0.94
92	10	10	0.09937	10	0.94
93	0	0	0.02187	0	0.94
94	10	10	0.01058	10	0.94
95	5	5	0.01097	5	0.94
96	5	5	0.00636	5	0.94
97	0	0	0.04046	0	0.94
98	10	10	0.04484	10	0.94
99	10	10	0.03658	10	0.94
100	10	10	0.07635	10	0.94
101	0	0	0.06279	0	0.94
102	5	5	0.0772	5	0.94
103	10	10	0.09329	10	0.94
104	10	10	0.09727	10	0.94
105	0	0	0.0192	0	0.94
106	10	10	0.01389	10	0.94
107	10	10	0.06963	10	0.94
108	0	0	0.00938	0	0.94
109	10	10	0.05254	10	0.94
110	0	0	0.05303	0	0.94

111	5	5	0.08611	5	0.94
112	5	5	0.04849	5	0.94
113	10	10	0.03935	10	0.94
114	5	5	0.06714	5	0.94
135	0	0	0.07413	0	0.94
149	0	0	0.05201	0	0.94
151	0	0	0.03477	0	0.94
152	0	0	0.015	0	0.94
160	0	0	0.05861	0	0.94
197	0	0	0.02621	0	0.94
250	0	0	0.00445	0	0.94
300	0	0	0.07549	0	0.94
350	5	5	0.02428	5	0.94
450	0	0	0.04424	0	0.94
610	5	5	0.06878	5	0.94