Identification and Ranking of Critical Assets within an Electrical Grid under Threat of Cyber Attack

By

Blake R. Boyer

A thesis submitted to the

Graduate School–New Brunswick

Rutgers, The State University of New Jersey

In partial fulfillment of the requirements

For the degree of

Master of Science

Graduate Program in Mechanical and Aerospace Engineering

Written under the direction of

Professor Michael R. Muller

And approved by

New Brunswick, New Jersey

May 2011

Abstract of Thesis

Identification and Ranking of Critical Assets within an Electrical Grid under Threat of Cyber Attack

By Blake R. Boyer

Thesis Director:

William J. Bottega

This paper examines the ranking of critical assets within an electrical grid under threat of cyber attack.[1] Critical to this analysis is the assumption of zero hour exploits namely, the threat of an immediate attack as soon as a vulnerability is discovered. Modeling shows that over time load fluctuations as well as other system variations will change the importance of each asset in the delivery of bulk power. As opposed to classic stability studies where risk can be shown to be greatest during high load periods, the zero hour exploit-cyber-risk assumes that vulnerabilities will be attacked as soon as they are discovered. The probability of attacks is made uniform over time to include any and all possible attacks. Examining the impact of an attack and how the grid reacts immediately following an attack will identify and determine the criticality of each asset.

This work endeavors to fulfill the NERC Critical Infrastructure Protection Requirements CIP-001-1 through CIP-009-2, cyber security requirements for the reliable supply of bulk power to customers throughout North America.

[1] Critical assets will here refer to facilities, systems, and equipment, which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System, NERC Glossary of Terms Used in Reliability Standards, 2009

Acknowledgements

First and foremost I would like to thank my advisor Dr. Michael R Muller for his insight into this thesis topic and the thesis writing process. His aid and advice in formulating a suitable topic and his confidence in my ability as an engineer as well as researcher helped me to approach this new topic intrepidly.

I would also like to extend a warm thanks to my parents Richard and Sharon Boyer who have supported me tirelessly and always encouraged me to pursue my interests, whatever they may be.

Contents

List of Figures

List of Equations

List of Tables

Chapter 1 Introduction

The electric power grid in the United States is one of the largest and most complex systems in today's world. While the physics of generating, transmitting, and distributing power has remained the same, the ways in which the grid is managed, controlled, and regulated has changed drastically from the early days when utilities were responsible for every aspect of the electric grid.

This thesis gives an over view of today's electrical grid and how it is managed, controlled, and regulated in the United States. The thesis then offers a protocol for identifying critical assets within the grid as it faces the ever-present risk of cyber attack. The ideas presented in this paper endeavor to fulfill the North American Electric Reliability Corporation's reliability standards, specifically the identification of critical assets according to Critical Infrastructure Protection Standard CIP-001-1.

1.1.1 Electric Power Grid

Electric power system reliability and stability are of increasing importance in today's electricity dependent society. Today's grid faces challenges that were not anticipated during planning and construction namely, higher than expected demand and subsequently increased transmission.[i] Total retail sales of electricity in 2007 were 3,765 million MWh, compared to 3,670 million MWh in 2006. This increase reflects an annual growth in electricity sales of 2.6 percent, which equal the growth in sales from 2005 to 2006 and out paces the 1.8 percent average annual growth since 1995.[ii]

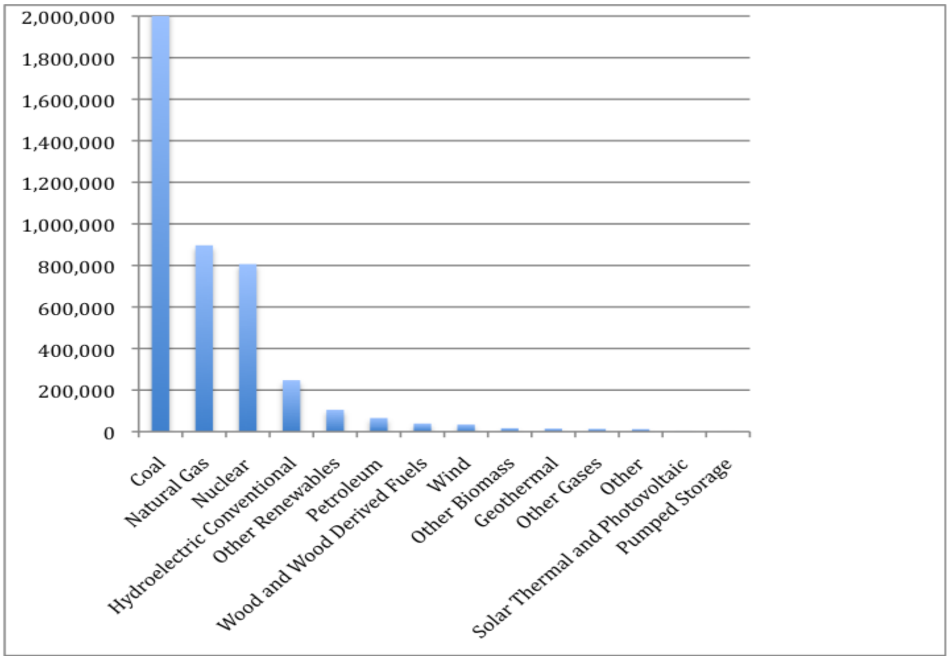


Figure 1 United States Annual Net Generation by Source 2007

The electric power grid is a series of interconnected transmission and distribution lines separated by substations. Substations consist of: transformers, switchgears or circuit breakers, bus bars, current transformers, capacitor banks, and a control system. The purposes of substations are to convert voltage, adjust voltage, direct power flow, correct power factor, and ultimately distribute power to end-users. And because of the way substations are configured, they act as isolators in the event of a fault2. This intricate network of pathways connects the power generators to the power customers, offering multiple pathways in which power can be transmitted and distributed.

1.1.2 Generation

Figure 1 illustrates the types of generation used in the United States as a whole, and it must be noted that regional generation types varying widely in some areas. Generating units vary in size. Nuclear and fossil-fuel steam-electric units typically have large capacities, many over 1,000 megawatts (MW), while hydroelectric dams range from less than 1MW to thousands of MW at some of the large Federal dams. Although some are larger, gas turbines, combustion turbines, and combined-cycle units are typically less than 200 MW. Wind and solar plants are similarly small. Distributed generation, which can be installed at or near the customer's site can be quite small, examples include rooftop photovoltaic arrays or fuel cells ranging from several, to a few hundred, kilowatts.

[2] A fault is an event occurring on an electric system such as a short circuit, a broken wire, or an intermittent connection. Faults can result from a short between any or all phases of a three-phase system or a short between any or all phases and a ground, NERC Glossary of Terms Used in Reliability Standards, 2009.

Electric power is generated at relatively low voltages, approximately 30 KV, and is then converted with transformers to its transmission voltage, above 30 KV. The first substation in the supply of bulk power is the generation substation. These facilities connect to the generators to the utility grid and also provide off-site power to the plant. Generator switchyards step up the generation voltage, approximately 30 KV, to the transmission voltage, anywhere from 230 to 736 KV in the United States.

Transmission voltages can reach over one million volts and because losses are proportional to the current squared, the higher the voltage, the lower the transmission losses. In the case of long distances, high voltage DC is used because its relatively low losses can offset the cost of rectifier (AC to DC converter) at the generation end and inverter (AC to DC converter) at the distribution end.

1.1.3 Transmission and Distribution

Figure 2 is the layout of high voltage transmission lines in the United States ranging from 230 to 765 KV and high voltage DC. [3] There are three distinct regions: Eastern, Western, and Texas Interconnect. All three maintain a frequency of 60 hertz to ensure continuity but only the Eastern and Western Interconnections are physically connected. The Texas Interconnect is connected to the Eastern and Western Interconnections by high voltage direct current lines and it is also connected to parts of Mexico.

Transmission substations perform the transfer of bulk power across the network and may only provide switching facilities but can also include transformers for voltage

[3] High voltage transmission is an interconnected group of lines and associated equipment for the movement or transfer of electric energy between points of supply and points at which it is transformed for delivery to customers or is delivered to other electric systems, NERC Glossary of Terms Used in Reliability Standards, 2009

conversion as well.

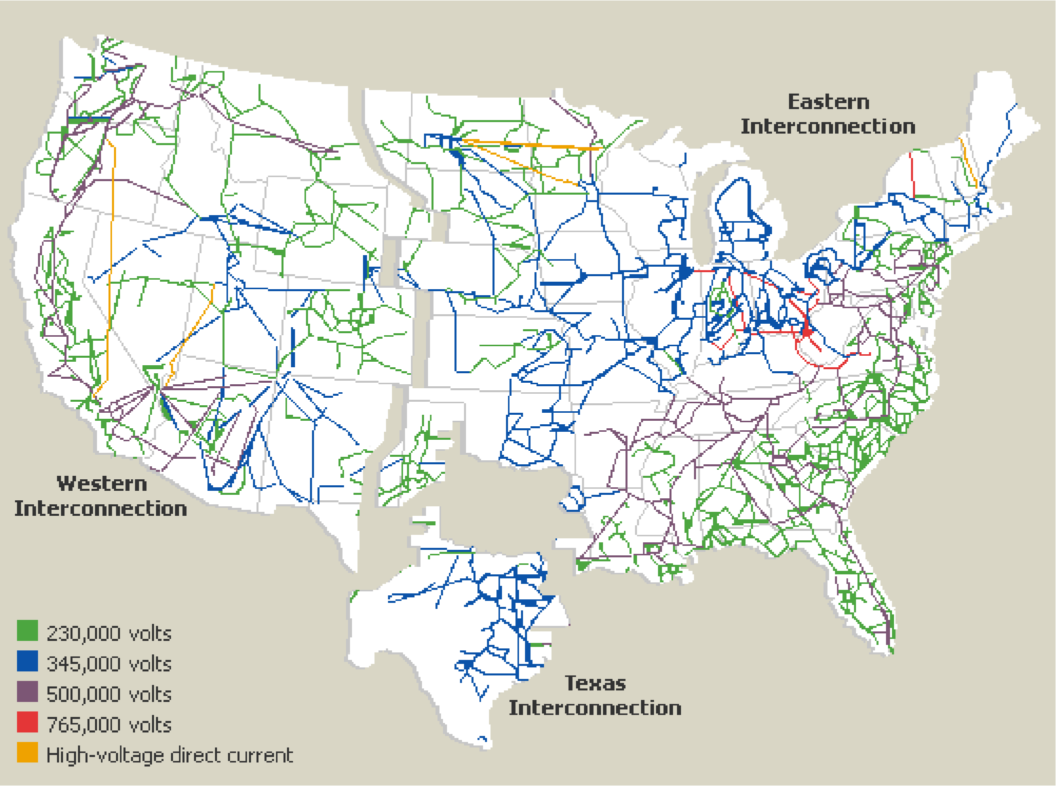


Figure 2 High voltage transmission lines of the three United States interconnections

The bulk power remains at transmission voltages, typically from 230-765 kV, until it is converted to lower distribution voltages. A distribution provider, often a utility, operates the “wires” between the transmission system and the end-use customer. For those end-use customers who are served at transmission voltages, the transmission owner also serves as the distribution provider. Thus the distribution provider is not limited to a specific voltage, but rather is able to perform the distribution function at any voltage.

Distribution substations are the most common facilities in power electric systems and provide the distribution circuits that directly supply most electric customers.

Distribution stations are commonly accepted as receiving or providing power below 69 KV.

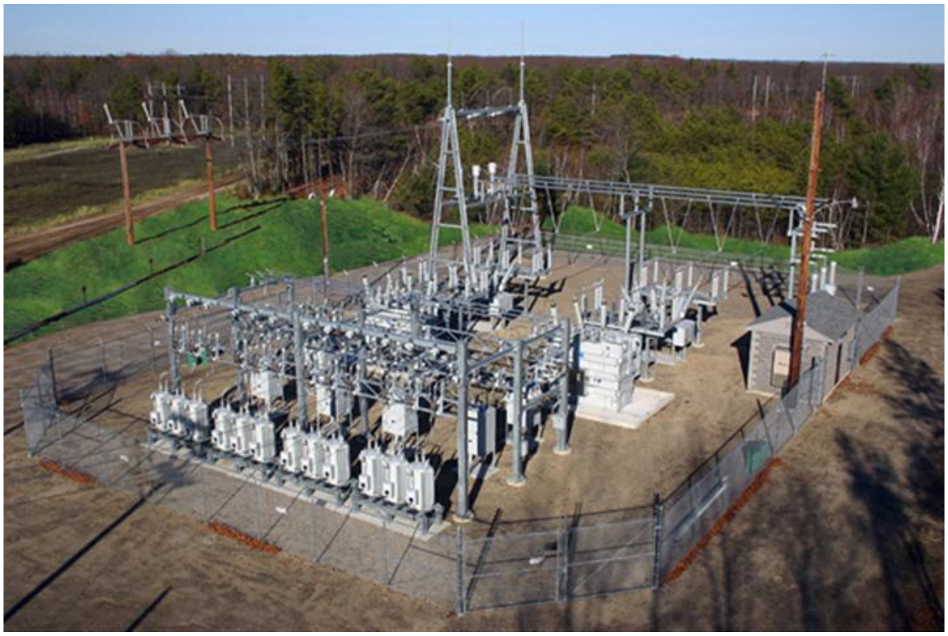


Figure 3 Distribution Substation

Substation design varies from a single bus bar to a full mesh and combinations thereof. A given substation can have multiple pathways to ensure the flow of power. This allows substations to direct power flow and maintain grid stability. Ideally, substations would be robust enough to allow for simultaneous maintenance and uninterrupted power delivery, but reality shows a balance between supply reliability and capital cost.

1.1.4 Deregulation of the Electric Power Grid

In the earliest power plants in the late 19th century, like the one George Westinghouse ran in Massachusetts, the proprietor controlled all aspects of generation, transmission, and distribution. This monopolization of utilities continued until The Public Utility Company Holding Act (PUCHA) was enacted in 1935. This act attempted to break-up the unconstrained and excessively large trusts that controlled the nation's electric and gas distribution networks. These trusts were accused of many abuses, including the attempted "Control of an entire system by means of a small investment at the top of a pyramid of companies, sale of services to subsidiaries at excessive prices, buying and selling properties within the system at unreasonable prices, intra-system loans at unfair terms, and the wild bidding war to buy operating companies."[iii] In the early years of industrialization, utilities had complete control over the production, transmission, and distribution of power and were able to manipulate costs and services as they saw fit.

PUCHA required large monopolies to divide themselves into smaller utilities that supplied specific areas and subjected them to state regulations. PUCHA also forced holding companies to decouple their utility business from non-utility business so as to avoid double-recovery when operating in more than one state. Under this new legislation all service companies were then regulated by the Securities and Exchange Commission and Federal Energy Regulator Commission.

The next major piece of legislation in the energy sector was *The Public Utility Regulatory Policies Act* of 1978, a result of the energy crisis of that time, this legislation encouraged higher efficiency and the use of renewables for power generation. It also allowed non-utility companies who were deemed Qualified Facilities (QF) to generate and sell power unilaterally to utilities. This act made it easier for newer smaller generators to enter into the power market.[iv]

It wasn't until *The Energy Policy Act* of 1992 that the power market changed into its present form. This act created a new class of power generators called Exempt Wholesale Generators (EWGs). These EWGs were not required to meet the *Public Utility Regulatory Policy Act* of 1978's cogeneration or renewable fuels limitations. Although utilities were not required to purchase power from EWGs, the 1992 act made it possible for customers to purchase power directly from generators. Marketing of EWG power is facilitated by transmission provisions that give The Federal Electric Reliability Council (FERC) the authority to order utilities to provide generators access to their transmission systems.

This essentially changed the traditional vertically integrated system, where generation and transmission are jointly controlled, to a more deregulated system where generators are separated from their customers by utilities and grid operators. Customers are now able to choose whom they purchase their power from, whether it is from traditional sources like coal, or renewables like solar or wind. "Wheeling" is a term used to describe power that is transmitted over long distances to reach a customer; the evolution of such practices shows how wide the gap between customer and generator has grown.

Some states like New Mexico have repealed legislation requiring the dismantling of the traditional vertically integrated utilities. In order to avoid problems like those experienced during the California Energy Crisis, New Mexico started allowing utilities to build or acquire new unregulated power plants for selling electricity in the wholesale market in 2001. The repeal of the legislation prevented residential customers from purchasing electricity from competitive retailers until 2007.

Deregulation of the electric power market and its infrastructure has had three major effects. First, it encourages new generators to enter the market, thereby increasing competition between generators. Second, it allows generators to bid their power to a much larger market, which also gives customers more choices. Thirdly, and most profoundly, it has created the need for a transmission system operator to manage and control the flow of power from generator to customer.

1.2.1 Electrical Grid Management and Control

1.2.2 Transmission System Operators

A Transmission System Operator (TSO) along with the distribution provider are the entities responsible for the reliability of the “local” transmission system. The TSO operates or directs the operation of the transmission facilities. The Transmission Operator Area is the collection of transmission assets over which the Transmission Operator is responsible for operating.

In the United States there are two types of transmission system operators. An Independent System Operators (ISO) is an organization formed at the direction or recommendation of the Federal Energy Regulatory Commission. In the areas where an ISO is established, it coordinates, controls and monitors the operation of the electrical power system, usually within a single US State (e.g. California), although such an entity will occasionally encompass multiple states. A Regional Transmission Operator (RTO) performs the same duties as an ISO but over larger areas encompassing several states.

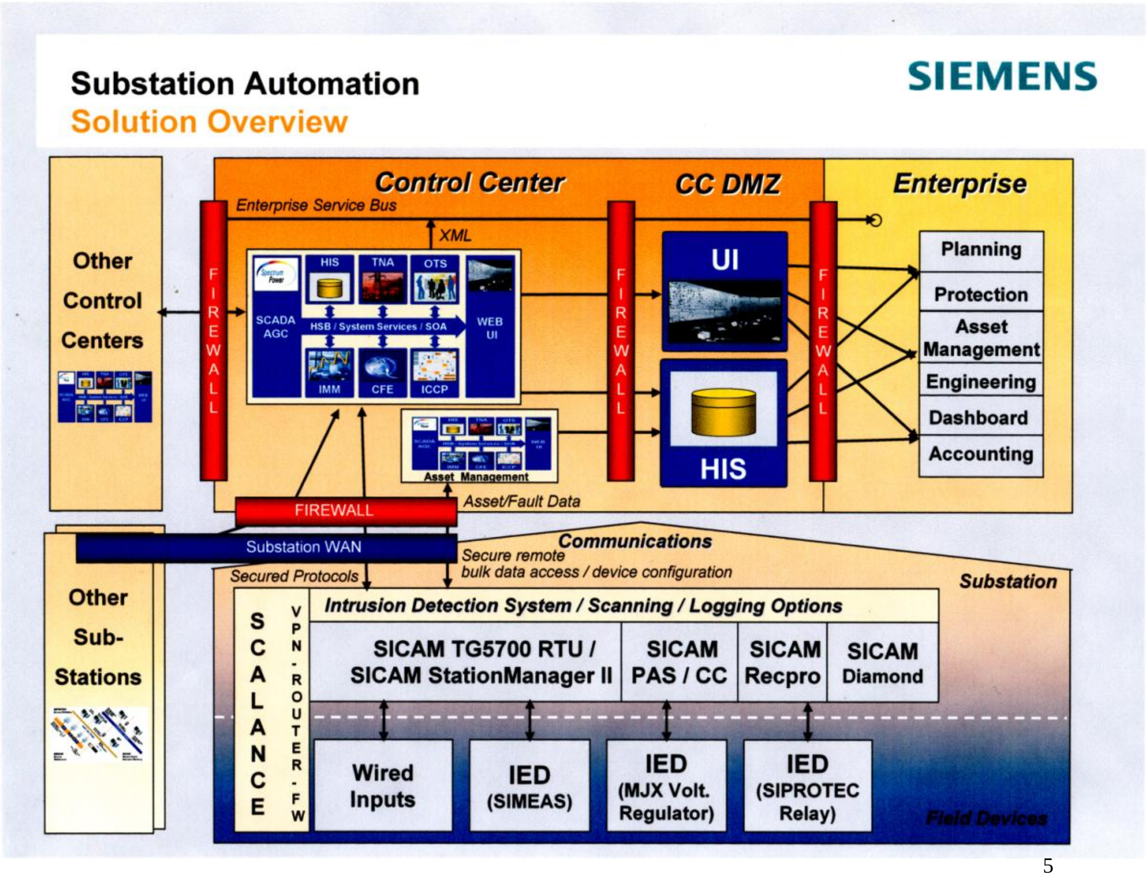
ISOs and RTOs have remote control over their respective transmission systems and are constantly monitoring and directing the flow of power between generators and customers. Operators at control centers perform monitoring and control. A Control Center is capable of performing one or more of the functions listed below for multiple (i.e., two or more) Bulk Power Supply (BPS) assets, such as generation plants and transmission substations. Functions that support Real-time operations of a Control Center typically include one or more of the following:

- Supervisory control of BPS assets, including generation plants, transmission facilities, substations, Automatic Generation Control systems, and automatic load-shedding systems
- Acquisition, aggregation, processing, inter-utility exchange, or display of BPS reliability and/or operability data, used for Real-time operations
- BPS and system status monitoring and processing for reliability and asset management purposes (e.g., providing information used by Responsible Entities to make operational decisions regarding reliability and operability of the BPS)
- Alarm monitoring and processing specific to operation and restoration functions
- Coordination of BPS restoration activities[v]

Clearly as computers have automated much of everyday life, the electric grid is no exception. Substations, themselves can often have complicated control systems and the interactions between them are normally managed by a sophisticated control center.

One example of this is the Siemens control system[4]. Figure 1 shows a schematic of the control center whose job is to manage multiple substations. The various components include user interfaces, historical information systems, training simulators (OTS),

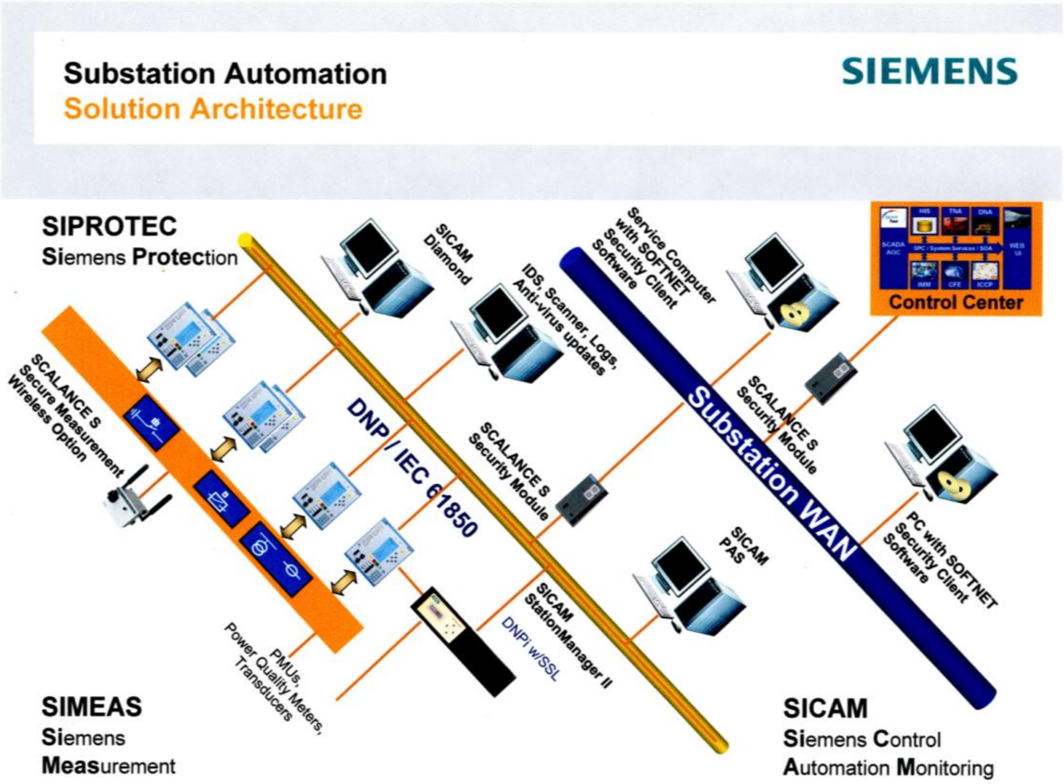
[4] Siemens supported the research contained herein and this example was selected only because of the extent of details they could provide on their products.



[5]

Figure 4 Modern Control Hierarchy for Electric Grids

[5] Siemens supported the research contained herein and this example was selected only because of the extent of details they could provide on their products.



[6]

Figure 5 Electrical Substation Automation and Control

Safety and reliability are a critical issue for transmission system operators, since any failure on their grid or of their electrical generation sources might affect a large number of customers, causing personal and property damages. Natural hazards and generation/consumption imbalances are a major cause of concern. To minimize the probability of grid instability and failure, regional or national transmission system operators are interconnected and their operation is dictated by security constrained economic dispatch.

[6] Siemens supported the research contained herein and this example was selected only because of the extent of details they could provide on their products.

1.2.3 Security Constrained Economic Dispatch

Security Constrained Economic Dispatch is an area-wide optimization process designed to meet electricity demand at the lowest cost, given the operational and reliability limitations of the area's generation fleet and transmission system. The following two sections explain the economic drivers in the power market and the establishment of secure operating conditions.

Economic Dispatch in The Power Market

Power and energy are commodities, and because electric power is not easily stored, sales and purchases are made on an on-going basis. Competition in day-ahead deregulated electricity markets has been established through auctions where generators and loads bid prices and quantities[vi]. These day-ahead-prices are used as place holders until the real-time prices are calculated every hour, adjusted for real-time grid operation.

The economic dispatch of power relies on market forces to determine the most cost effective ways of generating power. Starting with the most economical generators and moving to more expensive generation as loads increase. For example, when the most economic generators can supply all areas of the grid, those per unit electricity prices will be reflected. As the grid becomes more congested, certain areas of the grid will become congested and have to rely on more expensive generators to supply loads and in turn higher electricity prices are seen.

RTOs and ISOs develop load forecasts based on historical usage, day-ahead auctions, and weather data. These load forecasts give an idea of what to expect in day-ahead planning. But like predicting the weather, the transmission operators can only forecast so far, they also have to make real time decisions on how to direct power flows. When the grid becomes more loaded, operators become more concerned with reliable service and economics are less of an issue.

Secure Operation

Once the day-ahead auctions have been made it is up to the transmission operators to decide the most secure scenarios for power transmission. This operational protocol relies on the establishment of “secure” operating conditions which manage the generation, transmission, and distribution of power. The most common means of establishing operating parameters, which provide the highest reliability, is to constantly assess the grid’s reaction to changes in operation.

While maintaining safe operating conditions, transmission operators are constantly assessing the effects of possible faults either for the purposes of scheduling maintenance or in case of a random weather related fault. Operators want to make sure that secure operation will continue in the aftermath of a fault. This analysis, commonly referred to as N-1 analysis is the main tenet of secure grid operation. The analysis is a way to assess the impact of outages, foreseen or not. ISOs and RTOs perform this N-1 analysis continuously to address changing loads and grid configurations while directing the flow of power.[vii]

Spinning reserve is another feature of secure grid operation where generators have units idling or unloaded, ready to supply power in the event of a generation loss or significant load increase. NERC has introduced standards for spinning reserve requiring asset owners and transmission operators to have a certain amount on hand. This amount will vary by region depending on the types of generation available and how fast those generators can react. Some large RTOs like PJM have created a spinning reserve market to encourage even more spinning reserve than is required.

Secure Growth

The N-1 analysis can also be used to forecast growth and plan infrastructure improvements. The North American Electric Reliability Corporation (NERC) predicts the total usage for the United States to rise from 4,087,626 GWH in 2008 to 4,725,815 GWH by 2017.[ii] In order for the grid to remain robust with the increasing capacity, and to meet energy demands, NERC as well as transmission operators conduct tests to decide when and where to increase capacity and how to direct power more reliably. The table below illustrates the energy growth rate for The United States' largest Regional Transmission Operator Pennsylvania, New Jersey, Maryland (PJM). With the exception of 2005, we can determine a steady increase since 1998.[viii]

PJM RTO HISTORICAL NET ENERGY (GWH)

YEAR	ENERGY	GROWTH RATE
1998	620,061	0.8%
1999	636,404	2.6%
2000	651,190	2.3%
2001	651,319	0.0%
2002	673,526	3.4%
2003	674,471	0.1%
2004	689,008	2.2%
2005	682,441	-1.0%
2006	694,989	1.8%
2007	724,541	4.3%
2008	713,910	-1.5%

PJM's annual *Regional Transmission Planning Report* summarizes the results of reliability tests on the current system with respective load conditions. Projected load increases are applied to the existing infrastructure over a 5 to 10 year period and the results are recorded. Due to the annual increase in demand and the static infrastructure, the grid system will begin to violate over-limits.[7] Where and when these violations occur will determine when and where PJM increases capacity. Strategies for increasing capacity include constructing new transmission lines, substations, and reactive power correction. [8]

PJM's 2008 assessment of expected 2013 system conditions examined more than 18,000,000 combinations of facility outages.[9] Several hundred potential violations were identified, the majority of which appeared on lower voltage Bulk Electric System facilities (less than 230 kV).[ii] These violations did not result in significant systemic impacts.

Power systems make use of their capacity by allowing more development in a given area. As a result, the power grid can reach critical load levels, during which, the failure of one or more elements can cause cascading failures.[10] "Cascading" is the uncontrolled successive loss of system elements triggered by an incident at any location within the grid. "Cascading" results in widespread electric service interruption that

[7] System operating limits are the values (such as MW, MVar, Amperes, Frequency or Volts) that satisfies the most limiting of the prescribed operating criteria for a specified system configuration to ensure operation within acceptable reliability criteria, NERC Glossary of Terms Used in Reliability Standards, 2009.

[8] Reactive power is the portion of electricity that establishes and sustains the electric and magnetic fields of alternating-current equipment. Reactive power must be supplied to most types of magnetic equipment, such as motors and transformers. It also must supply the reactive losses on transmission facilities. Reactive power is provided by generators, synchronous condensers, or electrostatic equipment such as capacitors and directly influences electric system voltage. It is usually expressed in kilovars (kvar) or megavars (Mvar), NERC Glossary of Terms Used in Reliabilty Standards, 2009.

[9] A facility is a set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.), NERC Glossary of Terms Used in Reliability Standards, 2009.

[10] An element is any electrical device with terminals that may be connected to other electrical devices such as a generator, transformer, circuit breaker, bus section, or transmission line. An element may be comprised of one or more components, NERC Glossary of Terms Used in Reliability Standards, 2009.

spreads sequentially beyond the area determined by predictive data.

Cascading failures are the most severe types of failures and attempts are constantly being made to avoid them. Nevertheless they can occur, and incidence of cascading failures increases during warm summer months when reactive power loads are high[ix] (See Appendix A.2 Alternating Current and Reactive Power Compensation). This is, in part, attributed to high air-conditioning use, which utilizes induction motors in compressors and fans.

1.3.1 Grid Oversight and Regulations

The reliable supply of bulk power is tedious and requires constant monitoring and control in order to succeed. The United Sates Government created the Federal Energy Regulatory Commission (FERC) in 1977, part of the Department of Energy, to oversee the management and operation of the electric power grid within the United States.

The Federal Energy Regulatory Commission's original incarnation, the Federal Power Commission (FPC), was originally created to oversee hydropower development and later expanded to interstate electricity and natural gas pipelines. The original FPC was an independent organization before it became the Federal Energy Regulatory Commission, when it was absorbed by the Department of Energy (DOE). Despite being absorbed by the larger Department of Energy, FERC managed to retain some autonomy. FERC is responsible for creating and enforcing reliability standards to ensure the reliable supply of bulk power.

Since the Energy Policy Act of 2005 FERC's responsibilities have been expanded to include mandatory reliability standards on the bulk power system and penalties for those who do not comply. The Federal Energy Regulatory Commission has recently approved eight new mandatory Critical Infrastructure Protection (CIP) reliability standards to protect the nation's bulk power system against potential disruptions from cyber security breaches.[x] FERC has entrusted The North American Electric Reliability Corporation (NERC) to ensure that responsible entities comply with the new regulations.

The North American Electric Reliability Corporation's (NERC), a non-profit non-governmental corporation formed in 2006, has established its mission to ensure the reliability of the North American bulk power system. NERC is the electric reliability organization (ERO) certified by the Federal Energy Regulatory Commission to establish and enforce reliability standards for the bulk-power system. NERC develops and enforces reliability standards; assesses adequacy annually via a 10-year forecast, and summer and winter forecasts; monitors the bulk power system; and educates, trains and certifies industry personnel. ERO activities in Canada related to the reliability of the bulk-power system are recognized and overseen by the appropriate governmental authorities in that country.[xi]

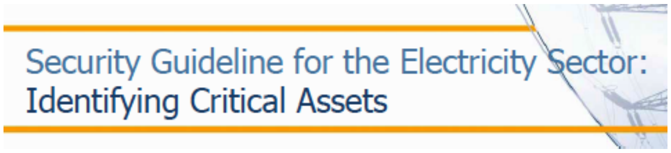
As of late, NERC has been tasked with enacting the reliability standards for Critical Infrastructure Protection, which calls for the identification of critical assets and their respective critical cyber assets within the electrical grid. FERC chairman Joseph T. Kelliher was overly optimistic when he stated, “Today we achieve a milestone by adopting the first mandatory and enforceable reliability standards that address cyber security concerns on the bulk power system in the United States,” FERC Chairman Joseph T. Kelliher also conveyed that, “The electric industry now can move on to the implementation of the standards in conjunction with improvement of these standards in order to increase the security and reliability of the bulk power system."[xii]

Kellihers optimism turns out to be transparently optimistic posturing because in a letter written to industry stakeholders on April 7, 2009 by NERC Vice President and Chief Security Officer Michael Asante, Asante explains his concern with the poor results of the preliminary Critical Asset Identification survey.

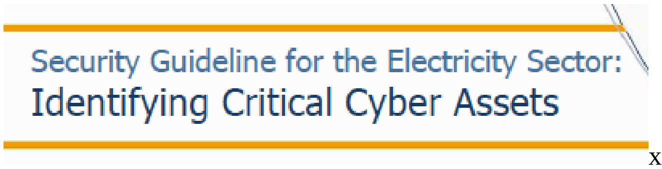
> The survey results, on their surface, raise concern about the identification of Critical Assets (CA) and the associated Critical Cyber Assets (CCA), which could be used to manipulate them. In this second survey, only 31 percent of separate (i.e. non-affiliated) entities responding to the survey reported they had at least one CA and 23 percent a CCA[xiii]

Of all generation owners and generation operators, only 29% identified at least one critical asset. Of all transmission owners, less than 63% identified at least one critical asset.

Because of anemic industry response to the Critical Infrastructure Protection standards, NERC has provided security guidelines for identifying critical assets and critical cyber assets.[xiv]



Security Guideline for the Electricity Sector:
Identifying Critical Assets



Security Guideline for the Electricity Sector:
Identifying Critical Cyber Assets

[xiv]

These security guidelines are to assist asset owners and operators in identifying critical assets and critical cyber assets within the electrical grid. The appearance of these guidelines is a testament to the difficulty of the task at hand. This work utilizes aspects of these guidelines to build a methodology for *identifying critical assets within an electrical grid under threat of cyber attack*.

1.4.1 Motivation for Research

The vulnerability of the electric power system to natural disasters and other causes such as hidden faults has been established.[xv] [xvi] [xvii] More recently the threat of cyber attack has become a concern to the U.S. Government, utilities, and asset owners and operators. Over the past decades power systems have become more intelligent and more accessible via network cables and phone lines. In return these improvements have made them more susceptible to cyber attacks. A massive blackout of the North East in 2003, and more recently, a massive blackout in Brazil on November 10th 2009, although not thought to be an act of sabotage, are a reminder of the fragility of interconnected power systems. It is important to be able to analyze today's power grids under the assumption that cyber attacks are real and ever present.

1.5.1 Identifying the Risk of Cyber Attack

A commonly used definition of risk, provided by the National Institute of Standards and Technology states, “Risk is the net negative effect of the exercise of a vulnerability, considering both the probability and the impact of occurrence.”

The Probability of an occurrence is a combination of threat and vulnerability. A commonly used definition of threat is “the potential for a threat-source to successfully exercise a specific vulnerability.”[xviii] Quantitatively determining threat is a difficult and subjective task. For example the physical threat to an obscure low power substation would clearly seem to be different than that of a denial-of-service cyber threat on a transmission grid control system. However, the difference can be difficult to characterize or quantify. A simplifying approach is to assume that threats always exist.

Likewise, according to NIST a vulnerability is, “a weakness that can be accidentally or intentionally exploited.” Quantifying vulnerabilities is also difficult and dynamic. Cyber hackers discover new vulnerabilities every day but may or may not be able to exploit them. This means the probability of an attack is changing over time and in the case of this work, it is too difficult to decide when vulnerabilities will exist and when they wont.

The approach taken by this work is to look at every possible vulnerability, and assume each vulnerability could be intentionally exploited at any given time. It is important to note here that the probability of a cyber attack is not 1.0, but we must assume each vulnerability will be attacked in order to identify critical assets facing a cyber attack.

1.5.2 Cyber Attack Modes

When a hacker discovers a vulnerability, there are several ways in which an attack can be carried out. The range of attacks starts with a hacker only being able to view information and ends with the worst-case scenario. The hacker has complete and utter control over the system. Regardless of the severity, all actions within this range are considered cyber attacks. We present three specific ways in which a hacker can manipulate the operation of the power system.

Visual Intrusion - The hacker is able to access the system but is unable to affect it in any way. This attack is the easiest to achieve and rarely leads to significant impacts, but it is considered an attack nonetheless.

Loss of Data – In this scenario the hacker masks the data being transmitted between an element, e.g. voltage transformer, current transformer, etc, and a control center or intelligent-electronic-device.

Loss of Control – In this scenario a hacker limits or eliminates the ability of an operator to control elements within the power grid, e.g. circuit breakers, transformer taps, etc.

Assume Control – In this worst-case scenario a hacker gains control of elements within the power grid and is able to manipulate them freely.

According to NERCs Critical Infrastructure Protection Standard CIP-002-1, critical cyber assets will possess one or more of the following characteristics: The cyber asset uses a routable protocol, sends packets from one network to another, to communicate outside the electronic security perimeter. The cyber asset uses a routable protocol within a control center, or the cyber asset is dial-up accessible.[x]

For the purposes of this exercise, the threat of cyber attack and the existence of vulnerabilities are considered uniform throughout the year. The “zero-day” or “zero-hour” are terms used to describe the immediacy of a cyber attack. In other words, a hacker will exploit a vulnerability window as soon as he or she is able, not when it is most convenient for them or most detrimental to the system. This means cyber attacks are inherently stochastic and must be looked at over time, considering as many attack scenarios as possible.

The understanding of “zero-day” and “zero-hour” attacks is critical to the methodology. As opposed to classical stability studies where risk can be shown to be greatest during high load periods, the “zero-hour” exploitation scenario has to be treated as uniform over time. The result is an impact analysis that looks at a system over time. The critical assets are then those *whose invalidation will be most significant over time*.

1.5.3 Quantifying the Impact of a Fault

A fault is an event occurring on an electric system such as a short circuit, a broken wire, or an intermittent connection. The most common naturally occurring faults are caused by lighting striking an overhead line and that line becoming overloaded, triggering a protective circuit breaker. Faults can result from a short between any or all phases of a three-phase system or a short between any or all phases and a ground[xix]. Other naturally occurring faults are caused by high winds and falling objects such as trees, which can destroy and/or ground wires.

A man made fault can be caused either by a physical assault on the grid, or by compromising a cyber asset or supporting system, through misuse or unauthorized modification. This work takes a simplified approach and assumes that the potential for attacks always exist. Once that assumption has been made, the cause of the fault becomes irrelevant and it is the impact of the fault that is of utmost concern. *Thus the identification and ranking of critical assets in an electrical grid under threat of cyber attack is achieved through an impact study*.

There are several ways in which a system can react following a fault. Line Outage Distribution Factors (LODF) and Power Transfer Distribution Factors (PTDF) are two ways to gauge how a system will react after an outage. The LODF is the percent of flow from a downed line that will end up flowing on an active line, given a value between -1 and +1.

$$LODF_{l,k} = \frac{\Delta P_{l,k}}{P_k}$$

Positive 1 denotes that all the power from a downed line K is absorbed on line L and continues in the direction of flow prior to the outage. Negative 1 denotes that all the power of the downed line K is absorbed by line L but the power flow direction has changed.

The PTDF is a percentage of power that a monitored line will pick up from a downed line. For instance if a monitored line has a 20% PTDF and an outage occurs on a line carrying 100 MW, than the monitored line will take on 20 MW of additional power transfer.

There are quantifiable reactions to a fault, which take place and are referred to as fault metrics. The following are several examples:[xx]

Reactive Power – Following a fault, reactive power that was previously being corrected by capacitor banks, now islanded, can reappear on the grid. The amount of reactive power in KVAR can be recorded.

Over Limit – Following the occurrence of a fault, power will be rerouted by physical laws as well as operator intervention, and the rerouting can cause other equipments to exceed their rated limit values resulting in protective action. The duration and the magnitude of over limit violations can be recorded.

Loss of Load – When a fault occurs, load may be lost due to physical disconnection or load may be shed in order to maintain grid functionality. The impact of a fault can be categorized by the amount of load not supplied to customers, in MW.

Power System Restoration - Power system restoration is of paramount importance following a fault. Restoration requires the reconnection of loads, either remotely or physically, and depending on the grids configuration and reconnection capabilities, the restoration time can vary. A viable method for critical asset ranking is to look at the restoration time per element and normalizing such information on an averaged scale.

There are myriad problems with power system restoration and a few have been identified and are divided into several functional groups:

- Reactive power balance
- Switching transient voltages
- Interconnection assistance
- Load and generation balance
- Frequency response of prime movers
- Cold load pickup
- Load and generation coordination
- Remote cranking power
- Optimum sequencing of generating units startup
- Fault location
- Assessment of switching status
- Standing phase angles
- Low frequency isolation scheme
- Intentional islanding
- Local load shedding
- Under-frequency and switched capacitor relays[xxi]

Once an outage has taken place, power system recovery is tedious and time consuming. Looking at assets and their respective recovery times becomes a way to identify critical assets within an electrical grid. Computer modeling, knowledge base, and heuristic methods are all used to recover a grid after an outage and can in turn be used to identify critical recovery assets.

1.6.1 Identifying Critical Assets Through an Impact Assessment

N-1 impact analysis is a very useful tool and is widely used in power systems all over the world. Some agencies have also delved further into its usefulness to analyze the impact of N-1-1, where the loss of one element is corrected for, and subsequently causes the failure of another element. Performing N-1 impact analysis on an electric gird will directly convey the results of an attack resulting in the invalidation of an asset.

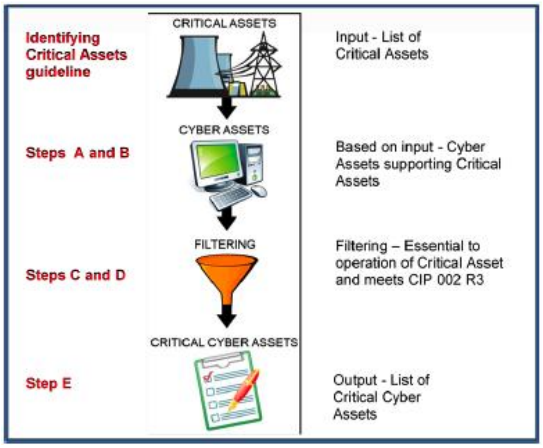

Identifying Critical Assets guideline
CRITICAL ASSETS
Input - List of Critical Assets
Steps A and B
CYBER ASSETS
Based on input - Cyber Assets supporting Critical Assets
FILTERING
Steps C and D
Filtering – Essential to operation of Critical Asset and meets CIP 002 R3
CRITICAL CYBER ASSETS
Step E
Output - List of Critical Cyber Assets

Figure 6 Protocol for Identifying Critical Cyber Assets

The NERC standards for Critical Infrastructure Protection are two-tiered Figure 5.[xxii] The first objective is identifying critical assets for the supply of bulk power and the second is the identification of their respective critical cyber assets. We focus here on identifying critical assets, namely substations, and do not deal with the associated critical cyber asset identification. It is assumed that a cyber attack on a substation will result in the incapacitation of the substation and that the substation will be physically removed from the grid via circuit breakers.

This thesis presents the following approach to quantifying the effect of an attack. Simulate the removal of a given substation during every hour of normal operation in a given year. This will show the impact of removing the substation during all load conditions and varying grid configurations. Summing the hourly impacts of the substation removal reveals the final impact metric (the total loss of load as a result of removing a given substation over a years time). This approach assumes an attack is possible at any given time and therefore the impact is assessed over time.

The following equation sums each load factor dependent fault metric to create the final impact metric.

$$\sum_{n=0}^{100}[(Fm)Hn] = IMPACT\_Metric$$

Equation 1

Where,

$\mathbf{F_m}$ - the fault metric of the mth bus

Note: One or more fault metrics can be used to quantify the impact of an attack. It is up to the user to choose which fault metric is most relevant and perform each impact analysis according the chosen metric.

n - is the load factor in percent of maximum load

m - corresponds to the bus number and

$\mathbf{H_n}$ - is the number of hours that the nth load factor occurs during one year of operation

The revelation in this impact assessment is the consideration of the time dimension. With the threat of cyber attack possible at any time, it is important to analyze each element over the same time interval.

Chapter 2 Technology Review

Before testing the methodology presented in Chapter 1, a review was conducted to evaluate the various tools capable of performing such a test. There are two main components needed for this study namely a grid modeling software and a test grid.

2.1.1 Grid Modeling Software

PowerWorld was selected was selected for this study because of its approachability for new users, its visualization, and educational roots. For non-electrical engineers, PowerWold's visualization offers the user the ability to physically construct a grid and view the power-flows in real-time.

The PowerWorld software started as a PHD dissertation conducted by Thomas J. Overbye and grew into a commercially used grid modeling software with emphasis on visualization.

Other Grid Modeling Software are listed below with their respective pros and cons compared to PowerWorld:

- MatPower is a package of MATLAB M-files for solving power flow and optimal power flow problems. It is intended as a simulation tool for researchers and educators that is easy to use and modify. MatPower is a powerful program but requires heavy coding and has no visualization.

- CYME power engineering software is a commercial product focusing on transmission and more extensively distribution side power grids. This tool is too specialized for the purposes of this study.
- Siemens' Power System Simulator for Engineering (PSSE) is a comprehensive commercial software for power grid analysis and one of the most widely used software in the industry. This software is much too expensive and requires professional training for useful operation.

2.2.1 Test Systems

Test systems were evaluated based on their availability, size, and source. The IEEE Reliability Test System was developed to, "Satisfy the need for a standardized data base to test and compare results from different power system reliability evaluation methodologies." The IEEE Reliability Test System is designed to encompass many aspects of an electrical grid but not to mimic an existing grid. The test system includes load levels above reliable operating conditions in order to study the effects of cascading failures.

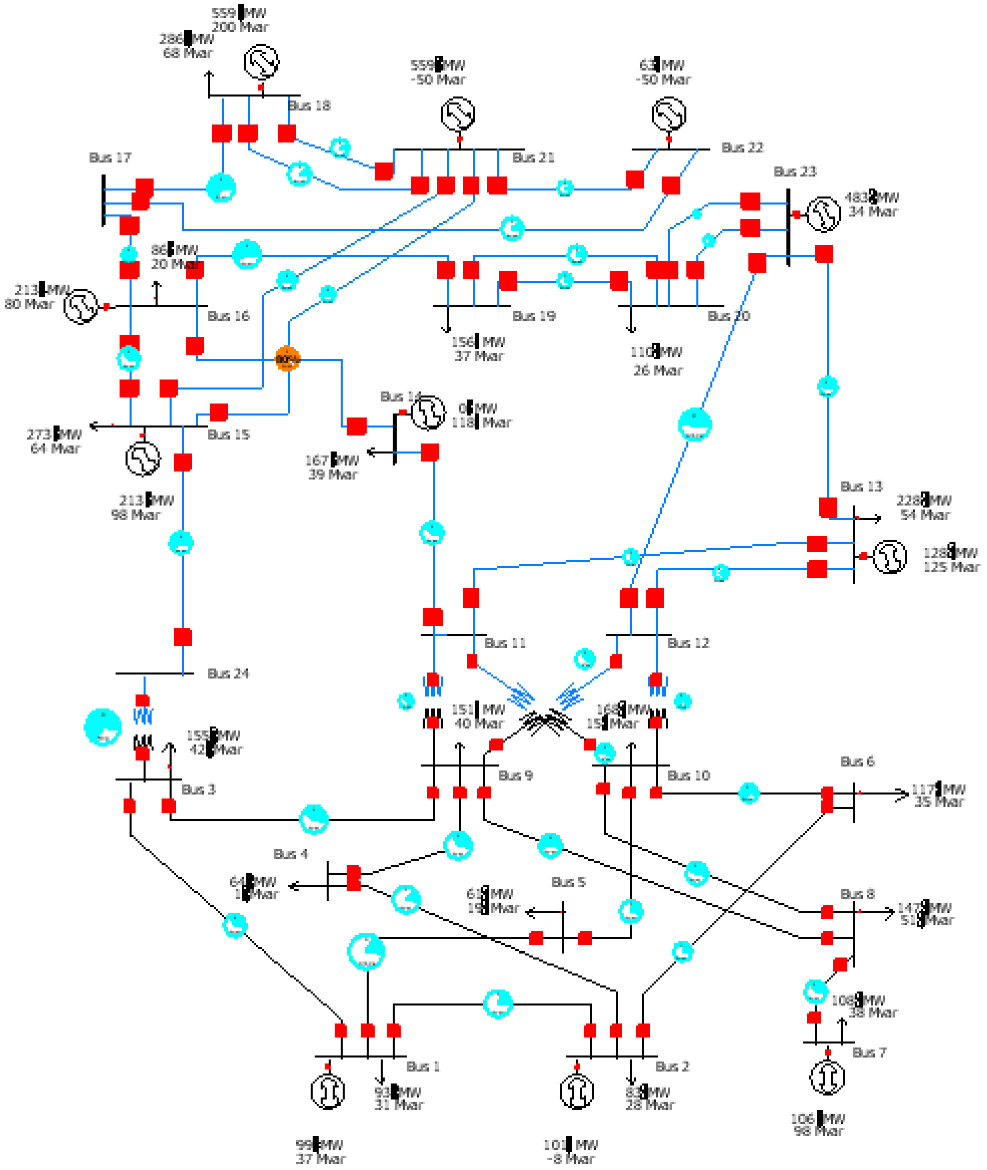


Figure 7 One line diagram of IEEE Reliability Test System

The fact that the IEEE system has been established allows repeatability and a chance to compare competing methodologies. Further studies of this methodology and its variances are easily cataloged with the IEEE test system.[xxiii]

2.2.2 Other Test Systems

Other test systems were experimented with before deciding on the IEEE System, the results of which will be presented and discussed in their respective sections. These included a 12 bus system built in PowerWorld to test initial theories and become familiar with the software, and a 118 bus system presented by PowerWorld as their test model. The 118-bus system proved too large for the purposes of this research.

Chapter 3 Results

3.1.1 Preliminary Tests Results and Discussion

The initial evaluation of this impact study was performed on the aforementioned 12-bus grid built in PowerWorld **Figure 8 Twelve-bus initial test system**, using load data from Pacific Gas and Electrics database on medium sized manufacturing customers. The data gives the percent of max load every half hour for an entire year, **Figure 9 Annual half hours at varying load factors**. Maximum loads were assigned close in value to one another and are illustrated in **Table 1 Max Load Values for 12 Bus Preliminary Grid**.

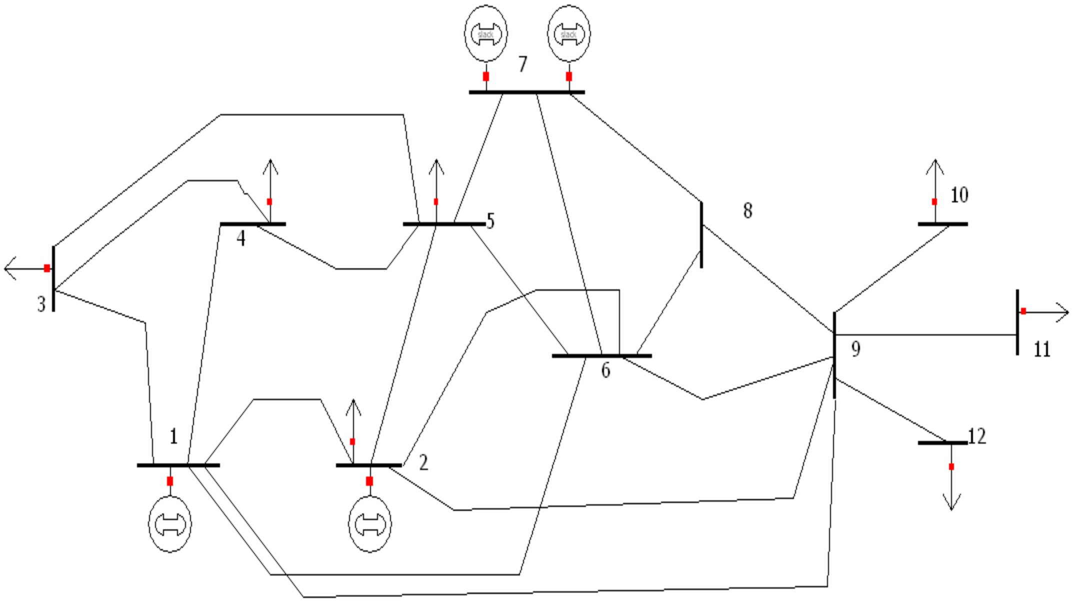


Figure 8 Twelve-bus initial test system

This grid was built for preliminary evaluation of the methodology, as well as preliminary software programming. It was important to begin with a clear example in order to get past initial hurdles: grid construction, over limit programming, contingency analysis, and data exportation.

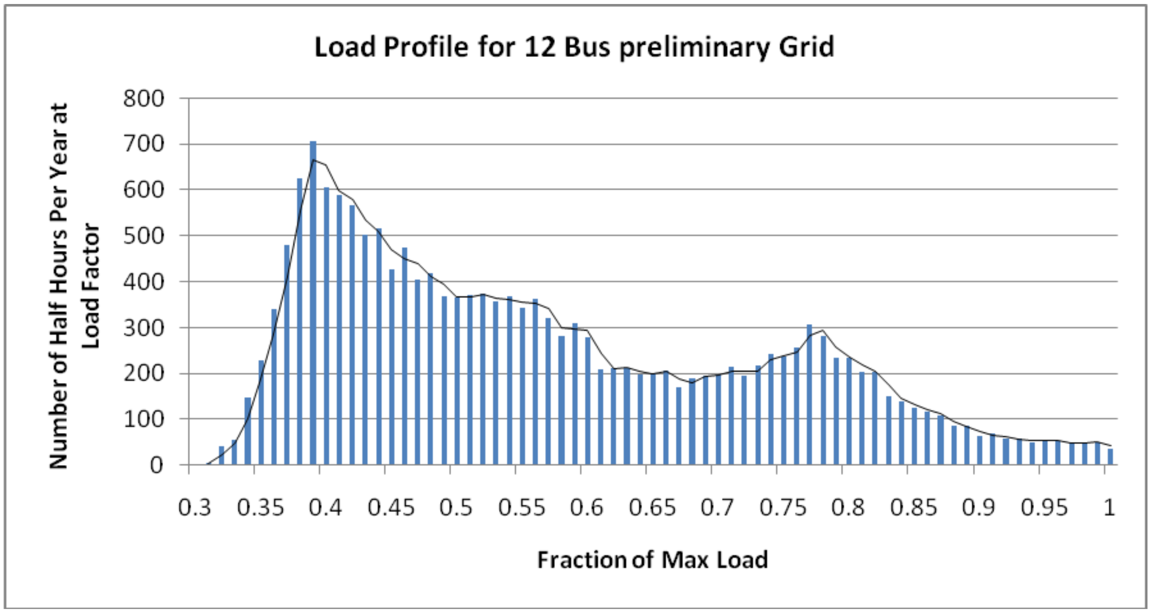


Figure 9 Annual half hours at varying load factors

The impact analysis was performed over the entire operational range, including load factors 0.3-1.0. Above 0.79, cascading failures occurred because of over limit violations. At 0.79 load factor and below, loss of load resulted from the removal of distribution substations.

From **Figure 8 Twelve-bus initial test system**, the distribution substations directly supplying load centers are: 2, 3, 4, 5, 10, 11, and 12. Bus 9 feeds buses 10, 11, and 12 directly with no rerouting available.

The test is designed to trip overloaded transmission lines once a substation has been removed so cascading is a possible impact of substation removal. This analysis used the *loss of load* failure metrics to determine the impact of a substation's removal. Other failure metrics were not considered.

Table 1 Max Load Values for 12 Bus Preliminary Grid

Substation	**Max Load (MW)**
Bus 12	57
Bus 11	56
Bus10	55
Bus 5	54
Bus 4	53
Bus 3	52
Bus 2	51

The bus records are nominal values from Power World software.

Table 2 Bus Records for 12 Bus Preliminary Grid

Number	**Nom kV**	**PU Volt**	**Volt (kV)**	**Load MW**	**Load Mvar**
1	138	1	138	0	0
2	138	1	138	34.17	10
3	138	0.99432	137.216	44.84	10
4	138	0.99241	136.953	45.51	10
5	138	0.99487	137.293	51.18	10
6	138	0.99919	137.888	0	0
7	138	1	138	0	0
8	138	0.99869	137.819	0	0
9	138	0.99312	137.051	0	0
10	138	0.98638	136.12	41.85	10
11	138	0.98928	136.521	42.52	10
12	138	0.98595	136.06	48.19	10

The branch data for the 12 bus preliminary grid, **Table 3 Branch Data for 12 Bus Preliminary System**, was assigned to ensure cascading loads at high load factors. The ratings are those of medium sized transmission lines and there are no transformers within the system.

Table 3 Branch Data for 12 Bus Preliminary System

From Number	**From Name**	**To Number**	**To Name**	**R**	**X**	**B**	**Lim A MVA**	**Lim B MVA**	**Lim C MVA**
1	1	4	4	0.01	0.12	0.03	75	100	100
1	1	9	9	0.01	0.12	0.03	75	100	100
1	1	3	3	0.01	0.12	0.03	75	100	100
1	1	6	6	0.01	0.12	0.03	75	100	100
1	1	2	2	0.01	0.12	0.03	75	100	100
1	1	3	3	0.01	0.12	0.03	75	100	100
2	2	5	5	0.01	0.12	0.03	75	100	100
2	2	9	9	0.01	0.12	0.03	75	100	100
2	2	6	6	0.01	0.12	0.03	75	100	100
3	3	5	5	0.01	0.12	0.03	75	100	100
4	4	3	3	0.01	0.12	0.03	75	100	100
5	5	4	4	0.01	0.12	0.03	75	100	100
5	5	6	6	0.01	0.12	0.03	75	100	100
6	6	7	7	0.01	0.12	0.03	75	100	100
6	6	9	9	0.01	0.12	0.03	75	100	100
6	6	8	8	0.01	0.12	0.03	75	100	100
7	7	5	5	0.01	0.12	0.03	75	100	100
7	7	8	8	0.01	0.12	0.03	75	100	100
9	9	12	12	0.01	0.12	0.03	75	100	100
9	9	12	12	0.01	0.12	0.03	75	100	100
9	9	11	11	0.01	0.12	0.03	75	100	100
9	9	11	11	0.01	0.12	0.03	75	100	100
9	9	11	11	0.01	0.12	0.03	75	100	100
9	9	10	10	0.01	0.12	0.03	75	100	100
9	9	10	10	0.01	0.12	0.03	75	100	100
9	9	8	8	0.01	0.12	0.03	75	100	100

The loss-of-load in megawatt hours is multiplied by the number of time intervals for which the loss of load occurs, at each load factor throughout the year. The result is the total islanded load due to the removal of a given substation for an entire year.

These results were calculated using the following equation:

$$\mathrm{I}\Gamma(1) = \sum_{n=0.3}^{1.0} IL(1)n \times t\eta$$

Equation 2

Where,

$\mathrm{I}\Gamma$ (1) – The lost load due to the removal of bus (1) over an entire year

$IL(1)n$ – The lost load from the removal of bus (1) at the nth load factor

$t\eta$ – The number of hours the nth load factor occurs during the year

Table 4 Aggregate Loss of Load per Year

Substation	Loss of Load (MWh)
9	947,226
12	278,557
11	273,670
10	268,783
5	263,737
4	259,053
3	254,038
2	249,230
6	140,185
1	82,519
7	0
8	0

This preliminary work illustrates how the criticality of elements changes over time and through a range of load factors. Bus 6 is a major transmission substation and at high load factors, those above the critical load factor, the removal of bus 6 causes over limit violations on other transmission lines and subsequent cascading. But over the course of a year, the impact of removing substation 3 is a loss of load greater than the removal of bus 6.

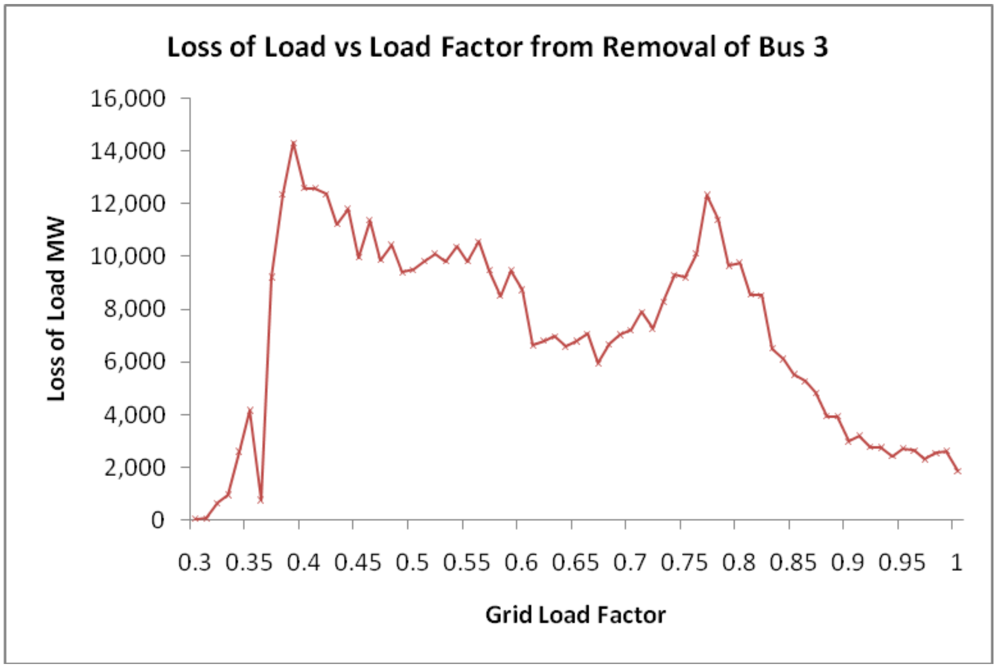


Figure 10 Bus 3 Contingency Results

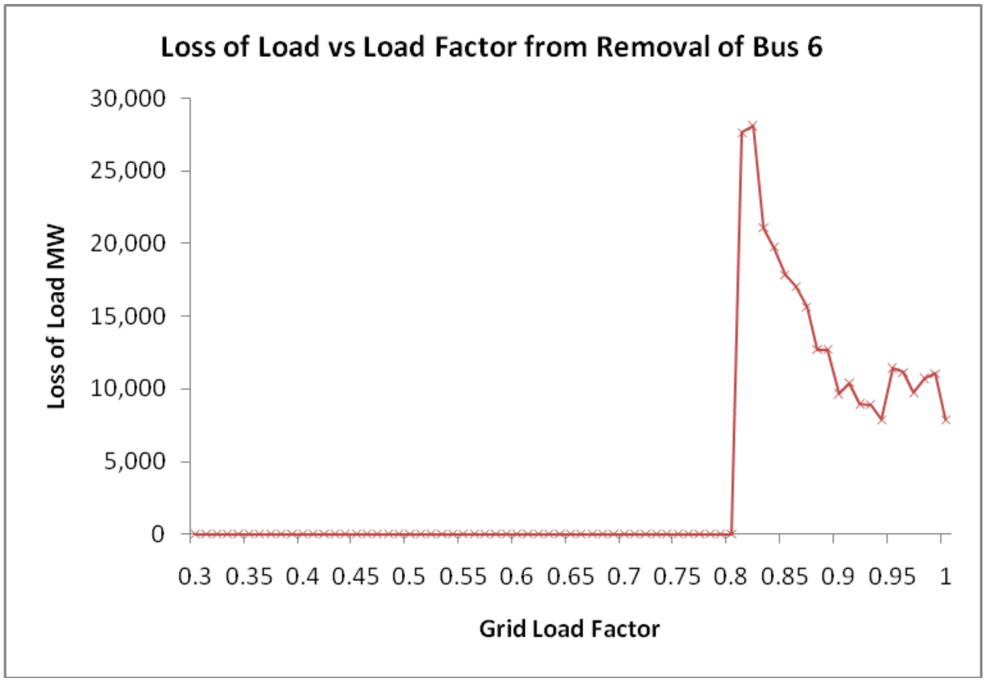


Figure 11 Bus 6 Contingency Results

An important finding is that over time, distribution stations become critical assets because of their criticality at lower load factors. This study is looking at the likelyhood of an attack at any time during a year. And identifying critical assets with respect to time reveals that criticality is a function of time.

It is important to note the other failure metrics not being considered in this test namely grid sensitivity, reactive power, and grid restoration. Assets used in the process of grid restoration, including transmision substations used for initial system restoration (e.g., blackstart generation connected at 69kV) should be evaluated as well according to NERC.

3.2.1 IEEE Test System Results

This research took the IEEE test system and performed aforementioned impact study for all hourly load factors in one year. The loss of load failure metric was used to rank each substation although any of the aforementioned metric(s) could have been used. The result is the total loss of load as the result of the removal of each substation during an entire year.

Throughout this test, bus 14 acted as a slack bus, and the generation was kept as close to zero as possible never moving outside plus or minus one megawatt. Branch data and load data was taken directly from the IEEE Reliability Test System.

3.3.1 Substation Identification

Classically, substations can be divided into three general types: generation stations are the sources of power for the electric grid, transmission substations transfer power along high-voltage transmission lines, and distribution substations are the final node before power is distributed by smaller feeders. Substation classification is based on voltage levels, as previously discussed[ix].

The IEEE reliability test system (2.2.1 Test System) is unique in that it encompasses many aspects of electrical power grids in a reasonably sized model and does not transform power enough to identify all types of substation.[xxiii] This paper takes a simplified approach to identifying each substation and the identification is as follows:

Generation

The bus bar is directly connected to a generator.

Transmission

The bus bar is connected only to transmission lines with no loads or generation.

Distribution

The bus bar delivers a load and is not connected to a generator.

NOTE:

NERC's guidelines for identifying critical assets offer example criteria when analyzing generation resources and transmission resources as well as control stations and specialty systems. These criteria also identify smaller distribution substations as potential critical assets especially when these smaller feeders are used in a cranking path (A portion of the electric system that can be isolated and then energized to deliver electric power from a generation source to enable the startup of one or more other generating units, less than 100 kV).

That said, it becomes important to include as many assets as possible in the risk based assessment because under varying circumstances all assets play a role in the bulk power supply and therefore must be considered.

Table 5 Substation Identification shows the each substation and its respective type.

Table 5 Substation Identification

Bus Number	MW to and from bus	Gen	Trans	Dist
Bus 1	289.6	X		
Bus 2	246.2	X		
Bus 3	513.8			X
Bus 4	128.2			X
Bus 5	122.2			X
Bus 6	234.9			X
Bus 7	216	X		
Bus 8	298.6			X
Bus 9	569.8			X
Bus 10	724.2			X
Bus 11	590.9		X	
Bus 12	604.9		X	
Bus 13	726.8	X		
Bus 14	786.69	Slack	Slack	Slack
Bus 15	1158	X		
Bus 16	1517.5	X		
Bus 17	762.9		X	
Bus 18	1236.7	X		
Bus 19	545.5			X
Bus 20	230.8			X
Bus 21	1125.2	X		
Bus 22	70.4	X		
Bus 23	962.7	X		
Bus 24	517.5		X	

Table 6 Substation Ranking According to Loss of Load Failure Metric shows a clear delineation of criticality. This impact analysis revealed the “critical load factor,” the load above which cascading failures occur. For the IEEE test system, at %86 of max load, cascading failures began to occur after the removal of some substations.

The load profile for the IEEE Test System, Figure 11, can serve as an indicator of grid stress. Looking at the load profile, the majority of hours are spent above the critical load factor of 0.86, which translates to high loads on transmission lines. Ideally a grid will spend no time above its critical load factor but history tells us this is not possible. There it is necessary to develop protocols for directing power during these high load times so that the risk of cascading is minimized.

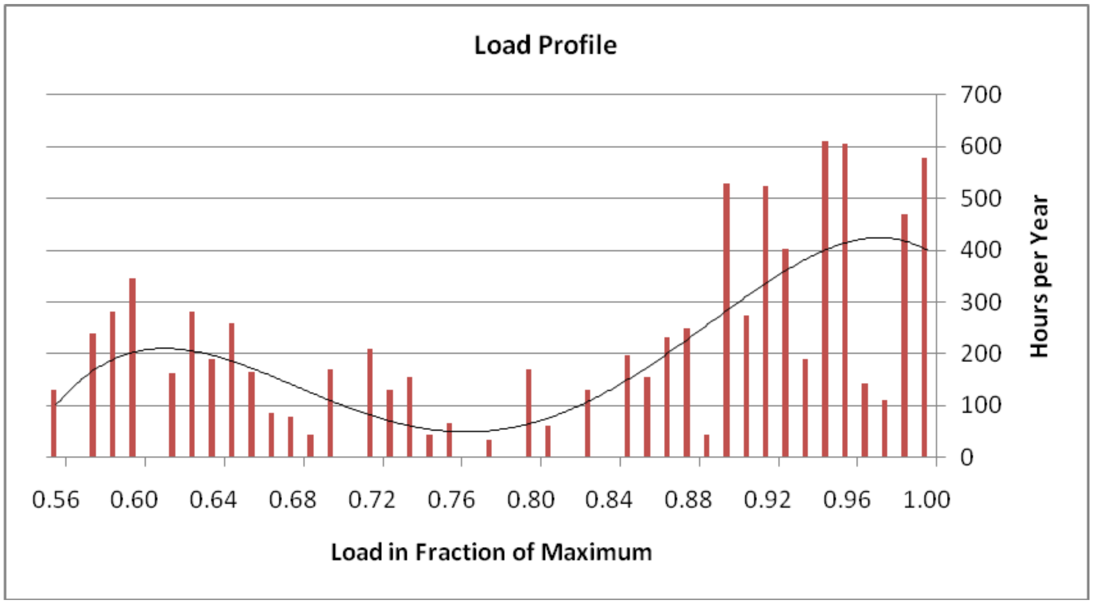


Figure 12 Load Factors and Respective Hours

It is clear that the load on this grid is too high and as a result, transmission substations are the most critical in supplying bulk power. The substation identities for the five most critical substations have been noted in Tables 7 and 8.

Table 6 Substation Ranking According to Loss of Load Failure Metric

bus	(MW) total islanded load/year	bus	(MW) total islanded load/year
8	2554267	20	918506
18	2530543	4	849212
15	2515752	5	754948
9	2138228	16	717271
10	2118894	14	416377
13	2066327	22	301863
2	1669557	11	263712
3	1302432	17	183168
19	1298593	21	142059
6	1292464	12	0
1	1012537	23	0
7	961566	24	0

When looking at the impact analysis results above the critical load factor versus below the critical load factor, the six most critical substations remain the same but are rearranged slightly. This is because the majority of load loss takes place when cascading failures occur. The loss of load below the critical load factor is less because it is only realized when a distribution station is removed and the amount of time spent below the critical load factor is 3,691 hours/yr versus the amount of time spent above the critical load factor 5,117 hours/yr.

Table 7 Five Most Critical Assets Above Critical Load Factor

Bus Number	**MW to and from bus**	**Gen**	**Trans**	**Dist**
Bus 8	298.6			X
Bus 15	1158	X		
Bus 9	569.8			X
Bus 18	1236.7	X		
Bus 10	724.2			X

Table 8 Five Most Critical Assets Below Critical Load Factor

Bus Number	**MW to and from bus**	**Gen**	**Trans**	**Dist**
Bus 18	1236.7	X		
Bus 15	1158	X		
Bus 8	298.6			X
Bus 13	726.8	X		
Bus 2	246.2	X		

This test grid spends the majority of operation hours above the critical load factor. Over time, the criticality does not shift to distribution stations. This grid is inherently overloaded.

Table 7 Five Most Critical Assets and **Table 8 Five Most Critical Assets** are the total loss of load above and below the critical load factor respectively. Looking at the substation identities it would appear that generation and distribution stations are the most critical. But it can be argued that the substations identified as distribution are equally as much transmission because of the amount of Mega Watts to and from the bus being transmitted.

A generation substation like 18 is producing hundreds of megawatts and when it is no longer in service, not only does the generation need to be made up, but the remaining lines are forced to shoulder the transmission load originating from 18. This is the reason for generation substations being most critical below the critical load factor.

3.4.1 Critical Ratio

The ratio of time spent above the critical load factor and time spent below the critical load factor can be an indicator of the overall grid stress. If the ratio is too high, the grid is not functioning properly and may need infrastructural improvements. If the ratio is zero, then the grid satisfies N-1 criterion at every load factor. Given the structure and load requirements of a given grid, this ratio will be an indicator of grid stress.

This critical ratio changes with time while the grid experiences load fluctuations as well as varying operation configurations. Techniques such as Power Transfer

Distribution Factors are employed to determine the maximum allowable power transfer, but are only a guideline because if a contingency were to occur, elements would overload. Together with the Line Outage Distribution Factor, a maximum allowable power transfer with available contingency can be calculated.

The load factors for the IEEE System and respective number of hours per year are illustrated in Figure 10. Variances in operation and control of the test system can yield varying critical load factors. The criteria used for this test, explained in the IEEE Results section, experienced a critical load factor of 0.86. The resulting critical ratio becomes 1.3. This ratio is very high and this test system spends the majority of operating hours above the critical load factor.

Table 9 Total Loss of Load Over One Year

Bus Number	**MW to and from bus**	**Gen**	**Trans**	**Dist**
Bus 8	298.6			X
Bus 18	1236.7	X		
Bus 15	1158	X		
Bus 9	569.8			X
Bus 10	724.2			X
Bus 13	726.8	X		
Bus 2	246.2	X		
Bus 3	513.8			X
Bus 19	545.5			X
Bus 6	234.9			X
Bus 1	289.6	X		
Bus 7	216	X		
Bus 20	230.8			X
Bus 4	128.2			X
Bus 5	122.2			X
Bus 16	1517.5	X		
Bus 14	786.69	Slack	Slack	Slack
Bus 22	70.4	X		
Bus 11	590.9		X	
Bus 17	762.9		X	
Bus 21	1125.2	X		
Bus 12	604.9		X	
Bus 23	962.7	X		
Bus 24	517.5		X	

Table 10 Total Islanded Load Above Critical Load Factor

Bus Number	**MW to and from bus**	**Gen**	**Trans**	**Dist**
Bus 8	298.6			X
Bus 15	1158	X		
Bus 9	569.8			X
Bus 18	1236.7	X		
Bus 10	724.2			X
Bus 13	726.8	X		
Bus 2	246.2	X		
Bus 6	234.9			X
Bus 19	545.5			X
Bus 3	513.8			X
Bus 1	289.6	X		
Bus 4	128.2			X
Bus 7	216	X		
Bus 20	230.8			X
Bus 5	122.2			X
Bus 16	1517.5	X		
Bus 14	786.69	Slack	Slack	Slack
Bus 22	70.4	X		
Bus 11	590.9		X	
Bus 17	762.9		X	
Bus 21	1125.2	X		
Bus 12	604.9		X	
Bus 23	962.7	X		
Bus 24	517.5		X	

Table 11 Total Islanded Load Below Critical Load Factor
with Substation Index Rating at 0.86

Bus Number	**MW to and from bus**	**Gen**	**Trans**	**Dist**
Bus 18	1236.7	X		
Bus 15	1158	X		
Bus 8	298.6			X
Bus 13	726.8	X		
Bus 2	246.2	X		
Bus 10	724.2			X
Bus 3	513.8			X
Bus 19	545.5			X
Bus 9	569.8			X
Bus 6	234.9			X
Bus 20	230.8			X
Bus 7	216	X		
Bus 1	289.6	X		
Bus 16	1517.5	X		
Bus 4	128.2			X
Bus 5	122.2			X
Bus 11	590.9		X	
Bus 12	604.9		X	
Bus 14	786.69	Slack	Slack	Slack
Bus 17	762.9		X	
Bus 21	1125.2	X		
Bus 22	70.4	X		
Bus 23	962.7	X		
Bus 24	517.5		X	

Chapter 4 Conclusions

4.1.1 Conclusions

Introducing the threat of cyber attack implies that vulnerabilities exist and can be exploited at any time. The assessment of the electrical grid becomes an impact study. The inclusion of the time dimension in the impact study takes care of this ever present threat. Integrating over time yields an aggregate impact from the removal of a given substation. It can be shown that the criticality of assets changes over time because the impact of an attack changes over time.

During peak load periods, cascading failures pose the highest risk and subsequent impact. Therefore it is those assets whose removal will cause cascading failures which are most critical during these high load times.

During low load periods, attacks may only impact directly connected loads but because of the ever present nature of a cyber attack and the zero hour exploit, these assets will remain critical, especially when they are responsible for grid recovery e.g. cranking path.

Another revelation of this impact study is the establishment of a critical load factor, above which cascading failures occur. Once the critical load factor has been established, the ratio of time spent above and below that threshold will be an indicator of grid stress.

Further studies using alternative failure metrics, e.g. recovery time, will expand the impact analysis and allow asset owners to decide which failure metric(s) best suites their security model. Likewise other individual or groups of elements can be removed and the subsequent impacts can be studied. Especially when dealing with larger substations, it may be more sensible to remove a single transmission line instead of an entire substation. As the size of the grid increases so do the number of elements and this analysis can be extended to N-2 if necessary.

This analysis is a risk based critical asset identification methodology capable of identifying critical assets under constant threat of cyber attack. This methodology uses an impact study to reveal critical assets based on the direct supply of bulk power. In formulation methodologies to comply with the NERC cyber security standards, responsible entities can reference this work when looking for directly applicable research.

4.2.1 Continued Research

In addition to the physical stress on the grid, it is important to address the grid’s control network and its exposure to cyber intrusion. A detailed analysis of the grid’s communication network coupled with the physical asset identification will provide a list of critical assets, which are at high risk of attack and if invalidated, could have large impacts.

These exercises in interpreting impacts to accompany the new threat of cyber attack are ongoing and will differ from system to system. As systems become more and more interconnected and remotely accessible, the parameters will change. Especially with the increased implementation of smart grid technology, our power system will be increasingly accessible to cyber attacks and grid security will be as it has always been, an integral part of our daily lives.

Appendix

A.1 Nomenclature

F_m(a), F_m(b), …, F_m(x) - are the failure metrics of the m^{th} bus

n - is the load factor in percent of maximum load

m - corresponds to the bus number and

H_n - is the number of hours that the n^{th} load factor occurs during one year of operation

IL(1) - The lost load due to the removal of bus 1 over an entire year

IL(1)*n* - The lost load from the removal of bus (1) at the nth load factor

t - The number of hours the nth load factor occurs during the year

V-Volts

I- Current (A)

A-Ampere

P-Power (W)

W- Watt

var- Volt-Amp-Reactive

R- Resistance (per unit)

X- Reactance (per unit)

B-Suseptance (per unit)

Lim A - Continuous Rating

Lim B - Long Term Rating (24 hour)

Lim C- Short Term Rating (15 minute)

A.2 Alternating Current and Reactive Power Compensation

Alternating current is the most ubiquitous method for generating, transmitting, distributing, and utilizing power in the United States. One of the unique characteristics of AC power circuits is the presence of reactive power. Reactive power is either generated or consumed in almost every component of the electrical grid system: generation, transmission, distribution, and eventually by the loads.

The impedance of a branch of a circuit in an AC system consists of two components, resistance and reactance. Reactance can be either inductive or capacitive, which contribute to reactive power in the circuit. Most of the loads supplied by the power grid are inductive and must be supplied with lagging reactive power. It is economical to supply this reactive power closer to the load in a distribution system.[xxiv]

NERC has established operational standards regarding reactive power and requires transmission owners to maintain voltages within established limits, to maintain reactive reserves to keep voltages within acceptable limits following a single contingency and that transmission operators be able to direct the operation of devices necessary to regulate transmission voltage and reactive flow.[xxv]

A.3 Hourly load factors for the IEEE test system

Table 12 Load Factor and Corresponding Number of Hours per Year

Load Factor	Hours
1	579
0.99	469
0.98	110
0.97	143
0.96	605
0.95	611
0.94	189
0.93	403
0.92	524
0.91	275
0.9	530
0.89	44
0.88	248
0.87	232
0.86	155
0.85	198
0.84	0
0.83	129
0.82	0
0.81	60
0.8	170
0.79	0
0.78	34
0.77	0
0.76	65
0.75	44
0.74	155
0.73	129
0.72	209
0.71	0
0.7	170
0.69	44
0.68	78
0.67	85
0.66	164
0.65	258
0.64	190
0.63	280
0.62	162
0.61	0
0.6	345
0.59	280
0.58	240
0.57	0
0.56	130

References

[i] North American Electricity Reliability Council Reliability Assessment 2000-2009, 2000

[ii] North American Electricity Reliability Council 2008–2017 Regional & National Peak Demand and Energy Forecasts Bandwidths

[iii] L. S. Hyman, *America's Electric Utilities: Past, Present and Future*, Fifth Edition (Arlington, VA: Public Utilities Reports, Inc., 1994), p. 111

[iv] Public Utility Regulatory Policies Act of 1978 (Public Law 95-617)

[v] NERC, Glossary of Terms Used in Reliability Standards, 2009

[vi] Contreras et al, Auction Design in Day-Ahead Electricity Markets, IEEE Transactions on Power Systems, Vol. 16, No. 1, 2001

[vii] Zima and Anderson, "On Security Criteria in Power Systems Operation," Swiss Federal Institute of Technology (ETH) 2005

[viii] PJM 2008 Regional Transmission Expansion Plan February 27, 2009

[ix] Weedy, B.M., *Electric Power Systems*, John Wiley and Sons 1987

[x] NERC CIP 002-1 and CIP002-2 Cyber Security-Critical Cyber Asset Identification

[xi] NERC Mission Statement, NERC.com

[xii] Federal Energy Regulatory Commission January 17, 2008 Docket No RM06-22-000 NEWS

[xiii] NERC CIP-002-Identification Letter April 7, 2009

[xiv] Security Guidelines for the Electricity Sector: Identifying Critical Assets, NERC 2009

[xv] Albert, Albert, and Naka, "Structural Vulnerability of The North American Power Grid," 2004

[xvi] Kirschen and Nedic, "Consideration of Hidden Failures in Security Analysis," PSCC 2002

[xvii] Kappenman, "Geomagnetic Disturbances and Impacts Upon Power System Operation," Electric Power Generation Transmission and Distribution

[xviii] National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30, Risk Management Guide for Information Technology Systems

[xix] Bayliss and Hardy, Transmission and Distribution Electrical Engineering, Elsvier 2007

[xx] Anjia M., Jiaxi Y., and Zhizhong G., "Electric Power Grid Structural Vulnerability Assessment," IEEE 2006

[xxi] *M.M. Adibi' and R.J. KakaL* Power System Restoration Issues IEEE 1991

[xxii] Jafari et al., Cyber-Related Risk Assessment and Critical Asset Identification within The Power Grid, IEEE 2010

[xxiii] C. Grigg et al., The IEEE Reliability Test System – 1996, IEEE Transactions on Power Systems, vol. 14, no. 3 August 1999

[xxiv] Grigsby, Leonard, *Electric Power Generation Transmission, and Distribution*, Taylor and Francis Group, 2007

[xxv] FERC, Principles for Efficient and Reliable Reactive power Supply and Consumption, 2005