NEW FRONTIERS FOR BLACKOUT PREVENTION:
A Study of the Vulnerability Frontier and its Use for
Contingency Analysis and Reliability Assessment

by
Jill D. Antonishen

A thesis submitted in partial fulfillment of
the requirements for the degree of

Master of Science
(Electrical Engineering)

at the
UNIVERSITY OF WISCONSIN-MADISON
2019
ABSTRACT

From infrastructure to healthcare to national security, global dependence on bulk power systems has never been more critical – placing reliability at a premium. Disruptions to power are consequential, and data on the frequency and size of blackouts over the past several decades is troubling. The existence of a power law in the frequency distribution of blackout size suggests the trends are no anomaly and more should be done in preparation for impending severe outages. The vulnerability frontier, defined as the set of points relating the maximum power disruption as a function of the number of lines removed from service, offers a unique screening approach to help examine certain worst-case events. To quantify grid reliability, associated scalar metrics influenced both by network topology and the pattern of power injections over the network are also framed. Existing contingency analysis practices typically rely on user-specified lists due to computational barriers faced when considering anything greater than N-1 or N-2 events. Thus, an opportunity is present for the frontier to better inform these lists with insightful selections of contingencies to assess.

The vulnerability frontier is studied on a 7977-bus synthetic grid model of the Midwest transmission network. A series of test scenarios are posed to probe the response of the frontier under seasonal and daily load profiles, transmission and generation outages, as well as in instances with increased renewable generation. These observational case studies show the effectiveness of the frontier in capturing grid weaknesses and lend a basis for further study. Modifications to the frontier formulation are provided in an effort to highlight cascading outage events in particular. Results are validated following a comparison to a modified version of the well-known Oak Ridge-PSERC-Alaska (OPA) blackout model.
ACKNOWLEDGEMENTS

I would first like to thank the University of Wisconsin-Madison Graduate School and Electrical Engineering Department for awarding me the Wisconsin Distinguished Graduate Fellowship. This generous funding permitted me to spend my first year focusing on coursework before ultimately landing in power systems. My experience at UW-Madison was supported by an amazing concentration of individuals with vast knowledge and resources. I have taken great pleasure in being a part of this learning community and am excited to begin my next chapter outside of academia – taking comfort in knowing that learning is never finished.

I must express my sincere gratitude to my advisor, Professor Bernie Lesieutre, for providing the opportunity to work on this project along with his tremendous guidance and advice throughout. I also thank Joe Eto for sponsoring this research. My colleagues Sogol Babaeinejad, Adria Brooks, and Jonathan Snodgrass along with my officemates deserve recognition, as well. They were always willing to discuss the intricacies of my work and offer advice on navigating the sometimes treacherous tides of graduate school. I am forever grateful for their welcoming nature, collaboration, and patience.

My roommate and friend Madeline Sena deserves a heartfelt thank you for providing comic relief, brain breaks, and great conversation. Completing this would have been significantly more difficult without your motivation, commiseration, and laughter.

Most of all, I would like to thank Brian Gammon for his unconditional support, my brothers for their (sometimes constructive) criticism, and my parents for their continued guidance. I am fortunate to be surrounded by such inspiring individuals who motivate me to pursue life with passion.
CONTENTS

ABSTRACT ........................................................................... i

ACKNOWLEDGEMENTS .......................................................... ii

LIST OF FIGURES ................................................................. v

LIST OF TABLES ................................................................. vii

ABBREVIATIONS ................................................................... ix

CHAPTERS

1. INTRODUCTION .............................................................. 1

1.1 Chapter Overview ......................................................... 1
1.2 Reliability Definition ..................................................... 2
1.3 NERC ........................................................................ 3
1.3.1 Reliability Standards .................................................. 4
1.3.2 Reliability Indicators .................................................. 6
1.4 Changing Nature of Reliability ........................................ 9
1.5 Blackout Causes and History ......................................... 11
1.6 Power Law and Self-Organized Criticality ....................... 15
1.7 Document Organization ................................................ 16

2. LITERATURE REVIEW ..................................................... 17

2.1 Chapter Overview ......................................................... 17
2.2 Cascading Failure Outages ............................................ 17
2.2.1 Self-Organized Criticality ........................................... 17
2.2.2 Blackout Models and Alternative Approaches ............... 19
2.3 Voltage Collapse ........................................................ 23
2.4 Renewables ................................................................ 25
2.5 Malicious and Cyber Attacks ......................................... 26
2.6 Topological Arguments and General Reliability Assessments ...... 27

3. THE VULNERABILITY FRONTIER ........................................ 31

3.1 Chapter Overview ......................................................... 31
3.2 Motivation ................................................................... 31
3.3 Model Foundation ........................................................ 33
3.4 Graph Partitioning ........................................................ 34
3.5 Model Description ........................................................ 37
3.5.0.1 Optimization Conversion Step ................................ 38
3.5.0.2 Finding Frontier Solutions ..................................... 41
4. ANALYSIS AND RESULTS .................................................. 52

4.1 Chapter Overview ........................................................ 52
4.2 Midwest Test System ...................................................... 52
4.3 Results Part I: Model Modifications ................................... 53
  4.3.1 30-bus Example ..................................................... 54
    4.3.1.1 Extension To OPA-v Model .................................. 56
    4.3.1.2 Modified Frontier Under $e_{di}$ ................................ 60
  4.3.2 Midwest Example I .................................................. 61
    4.3.2.1 Extension To OPA-v Model .................................. 63
  4.3.3 Midwest Example II ................................................ 65
    4.3.3.1 Extension To OPA-v Model .................................. 68
  4.3.4 Line Weighting Discussion ........................................ 70
  4.3.5 Radial Lines ........................................................ 71
4.4 Results Part II: Crafted Scenarios .................................... 71
  4.4.1 Vulnerability Frontier Over 12 Hours ............................ 71
  4.4.2 Vulnerability Metrics With Changing Load ....................... 74
  4.4.3 Seasonal Comparisons .............................................. 79
  4.4.4 Unplanned Outages ................................................ 81
    4.4.4.1 Generator Outages .......................................... 81
    4.4.4.2 Transmission Line Outages .................................. 84
  4.4.5 Variable Generation Patterns ..................................... 85
  4.4.6 Model Consistency Remarks ....................................... 91

5. CONCLUSIONS AND PROPOSED FUTURE WORK ....................... 93

  5.1 Summary ............................................................... 93
  5.2 Main Findings ........................................................ 94
  5.3 Future Work ........................................................... 95

REFERENCES ............................................................... 97
# LIST OF FIGURES

1.1 SAIDI and SAIFI metrics comparison by US state ............................... 3
1.2 Cascading outages flow chart ..................................................... 14
2.1 Cascading outage algorithm ........................................................ 22
3.1 4-node network ........................................................................... 35
3.2 4-node network graph partitioning example ..................................... 36
3.3 Converted min-cut/max-flow network .............................................. 38
3.4 Demonstration of iterative process for finding solutions on the vulnera-
   bility frontier ................................................................................. 42
3.5 30-bus network topology .............................................................. 43
3.6 Cost functions and vulnerability frontier plotted for 30-bus example ... 43
3.7 Revised frontier setup and edge weighting comparison ....................... 47
3.8 OPA-v blackout model algorithm .................................................. 51
4.1 Midwest test system one-line diagram ............................................ 53
4.2 Comparison of vulnerability frontiers under different edge weighting
   scenarios for 30-bus example ....................................................... 54
4.3 30-bus 2-cut scenario comparison ................................................ 55
4.4 30-bus 11-cut scenario comparison ............................................... 58
4.5 30-bus 14-cut scenario comparison ............................................... 58
4.6 OPA-v results for 30-bus network ................................................ 59
4.7 Modified vulnerability frontier under edge weights $e_d_i$ for 30-bus example 61
4.8 Comparison of vulnerability frontiers under different edge weighting
   scenarios for Midwest Example I .................................................... 62
4.9 Unique lines shared in Midwest Example I frontier solutions .............. 63
4.10 OPA-v results for Midwest Example I ............................................. 64
4.11 Unique lines shared in Midwest Example II frontier solutions ............ 66
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.12</td>
<td>Comparison of vulnerability frontiers under different edge weighting scenarios for Midwest Example II</td>
<td>67</td>
</tr>
<tr>
<td>4.13</td>
<td>OPA-v results for Midwest Example II</td>
<td>68</td>
</tr>
<tr>
<td>4.14</td>
<td>Vulnerability frontiers for the Midwest network over 12 hours</td>
<td>72</td>
</tr>
<tr>
<td>4.15</td>
<td>Modified vulnerability frontiers for the Midwest network over 12 hours</td>
<td>73</td>
</tr>
<tr>
<td>4.16</td>
<td>January and July Midwest system load</td>
<td>75</td>
</tr>
<tr>
<td>4.17</td>
<td>Equation 3.3 vulnerability metrics plotted for January and July hourly solutions</td>
<td>76</td>
</tr>
<tr>
<td>4.18</td>
<td>Equation 3.5 vulnerability metrics plotted for January and July hourly solutions</td>
<td>77</td>
</tr>
<tr>
<td>4.19</td>
<td>Equation 3.6 vulnerability metrics plotted for January and July hourly solutions</td>
<td>78</td>
</tr>
<tr>
<td>4.20</td>
<td>Vulnerability frontier for the Midwest network under three load profiles</td>
<td>80</td>
</tr>
<tr>
<td>4.21</td>
<td>Vulnerability frontier under unplanned generator outage Event I</td>
<td>82</td>
</tr>
<tr>
<td>4.22</td>
<td>Vulnerability frontier under unplanned generator outage event II</td>
<td>83</td>
</tr>
<tr>
<td>4.23</td>
<td>Vulnerability frontier under unplanned transmission outage Event III</td>
<td>84</td>
</tr>
<tr>
<td>4.24</td>
<td>Vulnerability frontier under unplanned transmission outage Event IV</td>
<td>85</td>
</tr>
<tr>
<td>4.25</td>
<td>Frontier comparison under varying wind generation</td>
<td>87</td>
</tr>
<tr>
<td>4.26</td>
<td>Small cut solutions to the modified vulnerability frontier under varying wind generation</td>
<td>90</td>
</tr>
</tbody>
</table>
# LIST OF TABLES

1.1 Classification of NERC enforced standards ............................................. 5
1.2 Summary of existing NERC reliability indicators ................................. 7
1.3 Selection of severe blackouts since 1965 ............................................. 13
2.1 Summary of simulation challenges .......................................................... 29
4.1 30-bus network branch information with line weightings ...................... 57
4.2 Percentage occurrence of select lines in OPA-v identified worse-case cascade events .......................................................... 60
4.3 Large cascade events from 10,000 OPA-v trials on the Midwest system (Example I) .......................................................... 63
4.4 Comparison of large cascade event data to vulnerability frontier solutions (Example I) .......................................................... 65
4.5 Large cascade events from 10,000 OPA-v trials on the Midwest system (Example II) .......................................................... 68
4.6 Comparison of large cascade event data to vulnerability frontier solutions (Example II) .......................................................... 69
4.7 Chi-squared statistics for Midwest Example II ...................................... 70
4.8 Vulnerability metrics for scenarios in Figure 4.14. ............................... 73
4.9 Vulnerability metrics for scenarios in Figure 4.15. ............................... 74
4.10 Vulnerability metrics for scenarios in Figure 4.20. .............................. 79
4.11 Seasonal comparison of smallest cut solutions .................................... 80
4.12 Vulnerability metrics for scenarios in Figure 4.22. ............................... 83
4.13 Vulnerability metrics for scenarios in Figure 4.24. ............................... 85
4.14 Wind generation by state for three scenarios ....................................... 86
4.15 Vulnerability metrics for scenarios in Figure 4.25. ............................... 88
4.16 Small cut solutions on the original frontier for increased wind and no wind cases .......................................................... 88
4.17 Lines in small cut solutions under increased wind case (modified model) 89
4.18 Lines in small cut solutions under no wind case (modified model) 90
4.19 Small cut solutions on the modified frontier for increased wind and no wind cases 91
## ABBREVIATIONS

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALR</td>
<td>Adequate Level of Reliability</td>
</tr>
<tr>
<td>BPS</td>
<td>Bulk Power System</td>
</tr>
<tr>
<td>CAIDI</td>
<td>Customer Average Interruption Duration Index</td>
</tr>
<tr>
<td>DOE</td>
<td>Department of Energy</td>
</tr>
<tr>
<td>EIA</td>
<td>Energy Information Administration</td>
</tr>
<tr>
<td>FERC</td>
<td>Federal Energy Regulatory Commission</td>
</tr>
<tr>
<td>HOT</td>
<td>Highly Optimized Tolerance</td>
</tr>
<tr>
<td>IEEE</td>
<td>Institute of Electrical and Electronics Engineers</td>
</tr>
<tr>
<td>ISO</td>
<td>Independent System Operator</td>
</tr>
<tr>
<td>MISO</td>
<td>Midwest Independent System Operator</td>
</tr>
<tr>
<td>NERC</td>
<td>North American Electric Reliability Corporation</td>
</tr>
<tr>
<td>OPA</td>
<td>Oak Ridge-PSERC-Alaska</td>
</tr>
<tr>
<td>OPF</td>
<td>Optimal Power Flow</td>
</tr>
<tr>
<td>PDF</td>
<td>Probability Distribution Function</td>
</tr>
<tr>
<td>SAIDI</td>
<td>System Average Interruption Duration Index</td>
</tr>
<tr>
<td>SAIFI</td>
<td>System Average Interruption Frequency Index</td>
</tr>
<tr>
<td>SOC</td>
<td>Self-Organized Criticality</td>
</tr>
<tr>
<td>SRI</td>
<td>Severity Risk Index</td>
</tr>
<tr>
<td>TRELSS</td>
<td>Transmission Reliability Evaluation of Large-Scale Systems</td>
</tr>
<tr>
<td>WECC</td>
<td>Western Electricity Coordination Council</td>
</tr>
</tbody>
</table>
CHAPTER 1

INTRODUCTION

1.1 Chapter Overview

Secure and reliable operation of the electric grid is essential to a nation’s economic vitality, national security, and societal quality of life. Engineers, grid operators, policymakers, and economists alike are tasked with maintaining the delicate balance of a dependable yet profitable network. Although most deem the North American power grid highly reliable, the power system is only designed to withstand single contingency events. Multiple component outages, though less likely, pose a tremendous threat to the bulk power system (BPS) – a network continuously growing in complexity.

There are compelling arguments to suggest more should be done in anticipation of catastrophic events resulting from multiple contingency outages. This is justified not only by trends in historical data and statistical predictions for the likelihood of future events, but also due to heightened risks of extreme weather as a result of global climate change. Consequently, there is a growing need for computationally feasible techniques to anticipate events that might disrupt the constant flow of electricity to which society has grown so accustomed. The vulnerability frontier technique offers a unique screening approach to help examine worst-case events to which the grid may be susceptible while also providing a method to quantify network reliability.

This chapter will begin by presenting the existing reliability definitions, standards, and assessments. The varying nature of reliability along with the impacts and causes of major blackouts will also be discussed as motivation for improved severe contingency analysis techniques.
1.2 Reliability Definition

As defined by the Department of Energy (DOE), reliability is the ability of a system or its components to withstand instability, uncontrolled events, cascading failures, or unanticipated loss of system components. This is closely related to the idea of resilience, which focuses on the ability to adapt to these disturbances, whether deliberate, accidental, or naturally occurring, and rapidly recover to bring system elements back online [1].

Today, there are several standard measures of reliability used by electric power utilities whose aim is to ensure the system operates within prescribed limits while avoiding instabilities or disruptions. For these institutions, reliability takes on a more formal designation involving well-defined metrics to quantify power availability along with the duration, frequency, and extent of various outages. One commonly used metric is the System Average Interruption Duration Index (SAIDI) which measures the average outage duration for each customer served. Another is CAIDI, or Customer Average Interruption Duration Index. CAIDI evaluates how long it takes to restore the system once an outage occurs. To accompany these, the System Average Interruption Frequency Index (SAIFI) computes the average number of times that a customer experiences an outage over the course of a year [1]. In the U.S. Energy Information Administration’s (EIA’s) Annual Electric Power Industry Report last year, measurements for SAIDI and SAIFI were compiled by state and summarized in Figure 1.1.

This figure highlights the highest and lowest measurements of average customer hours interrupted and average number of interruptions per customer by state in 2017. The presentation also allows for a comparison of results with and without major events included. One caveat with these traditional indicators is that they can misconstrue reliability performance when comparing across zones or states. This is due to the indicators being largely dependent on factors like regulatory standards, system configuration, customer density, hazard exposure, and other regional differences. It is also worth noting that not all utilities calculate and report these statistics in the same manner, some not reporting at all. The EIA found a 2017 reporting rate of just over 90% with about 78% following the IEEE (Institute of Electrical and Electronics
Engineers) standard and the remaining \sim 15\% using an alternative. There is a need for more uniform data collection processes as well as coordinated industry standards and metrics with enhanced sophistication [1], [2].

1.3 NERC

Key to this discussion is the North American Electric Reliability Corporation (NERC). NERC a nonprofit international regulatory authority founded and charged by the electric utility industry in 1968 to promote the reliability of the BPS. It was largely created in response to a 1965 blackout in the Northeastern United States, which at the time was the largest blackout in history. NERC has many roles in support of their mission statement of assuring the effective and efficient reduction of risks to the reliability and security of the grid. Tasks include assessing resource adequacy, developing and enforcing reliability standards for system operation and monitoring, as well as educating, training, and certifying industry personnel. Additionally, they

**Figure 1.1**: A comparison of SAIDI and SAIFI measurements by US state as reported by the EIA. The figure was reprinted from their 2018 Annual Electric Power Industry Report [2].
are called upon to investigate the cause of significant power system disturbances and analyze how to prevent these from reoccurring. This aspect of their work is closely linked to the subject of this report as we aim to detect and measure the severity of extreme events [3].

1.3.1 Reliability Standards

The reliability of the BPS is governed by a comprehensive set of standards many of which require active planning and real-time monitoring. The Federal Energy Regulatory Commission (FERC) oversees NERC and approves all accompanying standards. Meanwhile, eight Regional Entities across the US and Canada under NERC are responsible for compliance monitoring and enforcement. With regards to severe event analysis, some of these standards call on Balancing Authorities to perform network simulations and related assessments periodically to aid in developing reliable systems that meet specified performance requirements. This also ensures that systems continue to be modified or upgraded as needed to meet present and future demands [4]. More specifically, contingency events are sorted into four categories:

- No contingencies (Category A)
- Events resulting in the loss of a single system element (Category B)
- Event(s) resulting in the loss of two or more elements (Category C)
- Extreme event resulting in two or more elements removed or cascading out of service (Category D).

Category B is often referred to as an “N-1” contingency event and it should be noted that all systems are operated to be at least N-1 secure, meaning they can withstand the loss of any individual component. There are several families under which each individual standard can be classified and this information is summarized in Table 1.1.

TPL standards establish transmission system planning performance requirements to ensure the BPS will operate reliably following a range of contingencies deemed probable. Requirements are outlined for each of the four categories of contingencies
Table 1.1: Classification of mandatory standards subject to enforcement.

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Standard Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>BAL</td>
<td>Resource and Demand Balancing</td>
</tr>
<tr>
<td>COM</td>
<td>Communications</td>
</tr>
<tr>
<td>CIP</td>
<td>Critical Infrastructure Protection</td>
</tr>
<tr>
<td>EOP</td>
<td>Emergency Preparedness and operations</td>
</tr>
<tr>
<td>FAC</td>
<td>Facilities Design, Connections, and Maintenance</td>
</tr>
<tr>
<td>INT</td>
<td>Interchange Scheduling and Coordination</td>
</tr>
<tr>
<td>IRO</td>
<td>Interconnection Reliability Operations and Coordination</td>
</tr>
<tr>
<td>MOD</td>
<td>Modeling, Data, and Analysis</td>
</tr>
<tr>
<td>NUC</td>
<td>Nuclear</td>
</tr>
<tr>
<td>PER</td>
<td>Personal Performance, Training, and Qualifications</td>
</tr>
<tr>
<td>PRC</td>
<td>Protection and Control</td>
</tr>
<tr>
<td>TOP</td>
<td>Transmission Operations</td>
</tr>
<tr>
<td>TPL</td>
<td>Transmission Planning</td>
</tr>
<tr>
<td>VAR</td>
<td>Voltage and Reactive</td>
</tr>
</tbody>
</table>

A through D in the TPL-001-4 standard. It stipulates that periodic simulations and assessments are needed to ensure the grid can maintain safe and secure operating conditions. In more detail, the standard outlines specific contingencies to be simulated along with regulations on items like whether or not load loss or interruptions of firm transmission services are allowed. Importantly, it also clarifies that although the transmission planning entities may judge a number of Category D extreme contingencies as critical, it is not expected that all identified events can be evaluated and prepared against [4]. Related MOD standards determine consistent modeling and data reporting procedures to develop planning horizon cases needed to support such reliability analyses.

The transmission operations or TOP standards accompany the planning requirements with a focus on prompt action to mitigate disturbances and the necessary tools and quality of data to fulfill these responsibilities. For example, one of these standards establishes real-time monitoring and analysis capabilities which must be met to prevent instability, uncontrolled separation, or cascading outages. The family of CIP standards address the minimum network security requirements and impose rules for protecting all critical cyber assets. This detailed cluster of requirements and
procedures is constantly undergoing alterations and receiving amendments to improve the reliability of the interconnected transmission system [5].

At present, various system operators and utilities have developed their own methods for anticipating, preparing for, and protecting against multiple contingency events. Con Edison established an automated approach to determine the initiating events that cause cascading outages and identify optimal remedial actions to mitigate the effects or prevent them altogether. They employ the Physical and Operational Margins applications suite to help perform their massive contingency analysis. MISO has also implemented an automated technique to perform NERC compliance studies. The tool incorporates many computational features like identifying critical contingencies, determining transmission system bottlenecks, and minimizing load curtailment [6], [7]. The issue with these existing tools is that while they can perform exhaustive N-1 or N-2 contingency analyses, they require user-specified lists to test further N-k events. This selection of elements is certainly limited in size due to computational barriers and subject to what operators judge as most vulnerable. This limitation is also present in the NERC standards as they cannot require a more comprehensive analysis to prepare against category D contingencies. This presents a unique opportunity to improve severe event screening tactics and offer more robust contingency lists to undergo further analyses.

In addition to developing standards, NERC produces seasonal and long-term reliability risk assessments and special reports to assist in locating and mitigating potential threats. Their annual State of Reliability report, for example, evaluates the BPS performance for the previous year and identifies positive or negative performance trends. A series of reliability indicators or metrics are used to express their findings. A brief overview of select metrics will be discussed next [8].

1.3.2 Reliability Indicators

The metrics outlined in Table 1.2 were designed to link BPS performance to the NERC Adequate Level of Reliability (ALR) definition and address some of its fundamental characteristics and objectives. ALR is defined as the state that the design, planning, and operation of the BPS will achieve when the five predefined
performance objectives are met. These objectives range from maintaining frequency and voltage stability to restoring the BPS in a coordinated and controlled manner following major disturbances. In support of ALR, the objectives are also utilized to evaluate levels of reliability risk [9].

Table 1.2: Summary of existing NERC metrics [10].

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>M-1</td>
<td>Planning Reserve Margin</td>
</tr>
<tr>
<td>M-2</td>
<td>BPS Transmission-Related Events Resulting in Loss of Load</td>
</tr>
<tr>
<td>M-4</td>
<td>Interconnection Frequency Response</td>
</tr>
<tr>
<td>M-6</td>
<td>Average Percent Non-Recovery Disturbance Control Standard Events</td>
</tr>
<tr>
<td>M-7</td>
<td>Disturbance Control Events Greater than Most Severe Single Contingency (MSSC)</td>
</tr>
<tr>
<td>M-8</td>
<td>Interconnection Reliability Operating Limit/System Operating Limit (IROL/ISOL) Exceedances</td>
</tr>
<tr>
<td>M-9</td>
<td>Correct Protection System Operations</td>
</tr>
<tr>
<td>M-11</td>
<td>Energy Emergency Alerts</td>
</tr>
<tr>
<td>M-12</td>
<td>Automatic AC Transmission Outages Initiated by Failed Protection System Equipment</td>
</tr>
<tr>
<td>M-13</td>
<td>Automatic AC Transmission Outages Initiated by Human Error</td>
</tr>
<tr>
<td>M-14</td>
<td>Automatic AC Transmission Outages Initiated by Failed AC Substation Equipment</td>
</tr>
<tr>
<td>M-15</td>
<td>Automatic AC Transmission Outages Initiated by Failed AC Circuit Equipment</td>
</tr>
<tr>
<td>M-16</td>
<td>Element Availability Percentage (APC) and Unavailability Percentage</td>
</tr>
</tbody>
</table>

The 2018 State of Reliability recognized a few key indicators as M-2, M-9, and M-12 through 14. M-2 tracks BPS transmission-related events (excluding weather-related outages) that result in the loss of load. This metric has proven useful for planners and operators as they consider the appropriateness of designs and operating criteria in assuring acceptable system performance. Protection system misoperation has recently been recognized as a major area of concern and the M-9 metric was carefully surveyed in 2018 as a result. The metric reflects the performance of protection systems by computing the ratio of correct protection system operations to total system protection system. M-12, M-13, and M-14 are in place to survey the impacts of failed protection system, human error, and failed AC substation equipment for both momentary and sustained outages. These are computed separately for transformers
and AC circuits as factors in the performance of the AC transmission system. The 2018 report saw moderate reductions in each of these metrics [11]. The entire set of metrics is explained more thoroughly in [12].

On an individual bases, many of these metrics serve to quantify inherent risks, indicate potential high risk areas, or evaluate areas for significant risk reduction [13]. However, it is specified that no metric alone can indicate exceptional or poor performance of the BPS. They should be considered collectively when inspecting overall reliability qualifications and diagnosing where improvements are necessary. Many see these performance evaluations as a means to align the motives between organizations, people, and technology.

In an effort to synthesize the metrics and their threats to the system into a single number, events stemming from transmission, generation, and load loss are aggregated into what is referred to as the Severity Risk Index (SRI). The SRI is calculated daily as a measure of the overall performance of the BPS. For the generation portion, lost capacity is divided by the total generation fleet for the year. Transmission line outages are first weighted by their average line MVA ratings and then divided by the total inventory’s average capacity. Finally, when considering load losses, only those upstream of the distribution system are considered and they are computed based on outage frequency for the day and normalized to the system daily peak loading. Each component is weighted and incorporated into the final value – the generation piece at 10%, transmission at 30%, and load loss at 60%. The most common way yearly SRI results are presented and analyzed involves plotting the values in order or descending severity. Examples of this with comparisons across several years can be seen in various State of Reliability reports [10], [13].

Presently, the SRI acts as the only comprehensive measure of overall system reliability. The daily, blended metric is limited in scope and used only retrospectively to analyze yearly data and illuminate major disturbances. Some have suggested applying it regionally to search for correlations between localized performance and corresponding weather data, noting the metric could be useful to hone in on particular issues such as this [11]. Additionally, a more refined integrated reliability index (IRI) was under development in past years but has yet to be introduced officially. The IRI
was intended to serve as a more complete, quantitative picture of total BPS reliability [13]. Moreover, the existing assessments and accompanying metrics do little to screen for potential severe events and leave room for alternative measures which could be used for both after-the-fact analyses and on-line monitoring systems.

1.4 Changing Nature of Reliability

Many argue that these assessments require attention as a result of our changing reliability needs. In the age of technology, there are more two-way flows of energy, communications, and data than ever before throughout the entire electricity generation to end-use process. Consumers are taking on a larger role with increased participation in demand-side management in the face of new technologies such as smart meters, controllable loads, and batteries. There is also a growing presence of variable generation sources on the grid from renewables. Virtually every sector of the economy along with critical infrastructures like oil, transportation, and water depend on successful grid operation. From food production to healthcare to national security, the importance of this service cannot be understated. In summary, these changes are continually demanding innovation in technologies, market strategies, and operational procedures for our electricity system to remain as robust and accountable as possible [1], [14].

A few topics are shaping the conversation around modern day electric grid reliability and resilience. These include, but are certainly not limited to, our changing resource-mix, cyber security vulnerabilities, and extreme weather as a result of global climate change.

The changing resource-mix refers to a handful of relevant issues most of which stem from the increased penetration of renewable resources. Due to their variability and the lack of large-scale energy storage devices, many are concerned about reliability effects should renewables hold more substantial portions of generation capacity in the coming years. To mitigate some of these effects, advanced power electronic and inverter technologies are adding new sources of flexibility and responsiveness to the market when coupled with modern communications networks. In the future, one can imagine grid-interactive inverters which react to instantaneous feedback and adjust
their output accordingly while providing voltage stabilization, frequency regulation, and enabling storage [15]. Weather forecasting data analyzed by operators has easily been expanded to include solar and wind predictions which aid in utilities’ unit commitment process. Demand response programs use price signals during periods of high congestion or threatened vulnerability to encourage consumers to make short-term reductions in demand. These are just a few tools and techniques that can be used for not only managing peak days and variations in demand, but also for load reduction, load shaping, and consumption management [1], [16], [17].

As a byproduct of more renewables, natural-gas-fired capacity has become an increasingly important fuel source. It has the ability to provide both direct load service and the rapid backup that intermittent sources of electricity generation require. Unlike other parts of the world, natural gas is very inexpensive in the US in part due to revolutionary innovations like hydraulic fracking, 3D seismic imaging, and horizontal drilling. These technologies have allowed the US to take advantage of an abundant (for now) domestic resource and begin phasing out coal power plants. As this plays an important role in global energy markets, it is worth mentioning the history of natural gas prices have proven extremely volatile. This could inflict massive strains on the power grid as our resource mix continues to demand fast-start generators to account for inevitable and expanding variability. Finally, unlike other fossil fuels, natural gas is delivered as it is consumed rather than being stored onsite. This fact, paired with the growing dependence discussed above, boasts new reliability concerns as interruptions in deliveries could have significant impacts to the grid [10], [16].

Most of the information and communications technologies mentioned above while aiding reliability in some aspects, also expand the grid’s vulnerability to cyber-attacks. These technologies may present unique opportunities for consumers to interact with the electricity system, but unfortunately, they also pave new avenues for intrusions and attacks. To make matters worse, attempts to alleviate these risks are hindered by insufficient information-sharing practices between government and industry. There is also a lack of security specific technological and workforce resources available. Existing control systems have been indirectly connected to the Internet without added
technologies to ensure their security. As our use of automation increases and we navigate the grey area between centralized and decentralized electricity systems, it is essential to consider security threats in our design criteria. The electricity network will only continue to grow in complexity, making cybersecurity a profound system-wide concern [16].

Lastly, comments can be made regarding weather-related events, which pose the greatest risk to the BPS. Strong winds are cited the primary cause of damage to transmission and distribution infrastructures. Beyond this, extreme weather puts excessive strain on the system in the form of increased cost, maintenance, and repairs. In the face of a warming climate, the grid will require additional capacity to meet higher peak demand. This is exacerbated as rising air temperatures simultaneously reduce the generation capacity and efficiency of existing thermal generation units. Extreme temperatures on either end of the spectrum increase the likelihood of electric equipment malfunction. In addition, a rise in sea-level inflates the frequency with which electricity assets are exposed to inundation during storm events. As severe weather events appear more and more often, Mother Nature will likely act as a principal contributor to grid vulnerabilities [1].

1.5 Blackout Causes and History

Ensuring the reliable delivery of electricity services through carefully balanced supply and demand has historically been a success. Large blackouts quickly become national news headlines due to their infrequency. However, a growing dependence on the grid’s interconnectedness leaves us susceptible to a host of new risks and vulnerabilities.

Current standards only require the BPS to be resilient to single failure events as computational limitations prevent multiple failures from being exhaustively considered at this time. Interestingly enough, researchers investigating the August 14th, 2003 blackout that took place in the Eastern US and Canada concluded the event likely resulted from just three key line outages. Nearly 50 million people saw the impacts of this event across eight states and two Canadian provinces with some regions requiring almost two weeks to restore power. At the height of the outage,
load managed by the New York Independent System Operator dropped to about 5700 MW – a stark difference from the 28,700 MW being carried just minutes before the event. In total, roughly 62 GW of load was interrupted or about 11% of the total served in the Eastern Interconnection [18], [19].

A few notable factors contributed to the prevailing operating conditions that afternoon. These include significant reactive power supply problems, critical system failures, inoperative software, and operator decision-making errors. To begin, high generator reactive power loadings in Ohio and Indiana quickly became an issue, limiting the margins to support the system for potential outages while causing protection and control issues. The Midwest ISO’s (MISO’s) state estimator and real time contingency analysis software also began to malfunction. This prevented MISO from performing early-warning assessments of the system. Adding to this was the August heat, causing power lines to sage as elevated current levels traveled along them. This did not pair well with poor vegetation management, or lack of tree-trimming, which the NERC investigation identified as the cause of one 138-kV and three 345-kV line outages. Eventually, due to overloaded transmission and a cascading outage of around 400 lines, 531 generating units, and 261 power plants, the voltage collapsed and an entire region faced a blackout [18], [19].

Events of this size are not cheap. One source estimates blackouts and brownouts caused by severe weather cost Americans approximately $150 billion per year in spoiled food, lost productivity, and other indirect costs [20]. The DOE estimated the total damages associated with the Northeast blackout alone at around $6 billion. Another study reflected this figure in a different manner, assessing the economic value to roughly $5 per forgone kWh or 50 times more than the average retail electricity price in the United States [1]. Though the monetary losses are staggering, it is important to consider the cost to consumers and the havoc that ensues in an electricity dependent world. During this blackout in New York City for example, traffic lights and subways quickly failed, hundreds of people were stuck in elevators, and water and sewer pumps became inoperable straining many essential services. In addition, indirect costs were sustained in the form of multimillion-dollar losses for a few metal fabrication plants when metals hardened inside machinery [21].
The autumn of 2003 proved a tumultuous time for electric grid operation. Two more major outages followed in Scandinavia and Italy, both as a result of cascading outages. Table 1.3 shows a selection of some of the worst blackouts in North America along with their impacts and causes.

Table 1.3: A collection of the worst blackouts since 1965 is presented in a table adapted from [21] with supplementary information from [19], [22], [23]. Events are sorted by the MW lost column.

<table>
<thead>
<tr>
<th>Date</th>
<th>Location</th>
<th>MW lost</th>
<th>#people affected</th>
<th>Cause</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>8/14/03</td>
<td>Canada, Eastern US</td>
<td>61,800</td>
<td>50 million</td>
<td>cascading failure</td>
<td>up to 2 weeks</td>
</tr>
<tr>
<td>8/10/96</td>
<td>West Coast US</td>
<td>28,000</td>
<td>7.5 million</td>
<td>cascading failure</td>
<td>several hours</td>
</tr>
<tr>
<td>11/9/65</td>
<td>Canada, Northeastern US</td>
<td>20,000+</td>
<td>30 million</td>
<td>cascading failure</td>
<td>up to 13h</td>
</tr>
<tr>
<td>3/13/89</td>
<td>Quebec, New York</td>
<td>19,400</td>
<td>5.8 million</td>
<td>cascade, solar flare</td>
<td>9h</td>
</tr>
<tr>
<td>10/29/12</td>
<td>Canada, East Coast</td>
<td>18,246</td>
<td>8.2 million</td>
<td>hurricane Sandy</td>
<td>up to 2 weeks</td>
</tr>
<tr>
<td>12/22/82</td>
<td>West Coast US</td>
<td>12,350</td>
<td>5 million</td>
<td>high winds</td>
<td>several hours</td>
</tr>
<tr>
<td>6/29/12</td>
<td>Midwestern US</td>
<td>12,144</td>
<td>4.2 million</td>
<td>Derecho storm</td>
<td>up to 1 week</td>
</tr>
<tr>
<td>7/2/96</td>
<td>West Coast US</td>
<td>11,850</td>
<td>2 million</td>
<td>voltage instability</td>
<td>1-2h</td>
</tr>
<tr>
<td>9/8/11</td>
<td>Southwest US</td>
<td>7900</td>
<td>2.7 million</td>
<td>human error</td>
<td>12h</td>
</tr>
<tr>
<td>7/13/77</td>
<td>New York City</td>
<td>6000</td>
<td>9 million</td>
<td>high winds</td>
<td>up to 24h</td>
</tr>
</tbody>
</table>

These events illuminate some of the main causes for large scale blackouts like the one discussed previously. Natural events such as hurricanes or high winds appear most frequently, followed by cascading outages. Note that malicious attacks or terrorist attacks do not appear on the list but are an emerging threat currently receiving a lot of industry and private research attention. Although this table and many other comprehensive analyses arrive at a single cause, it is typically a perfect storm of events that eventually spiral out of control. Any combination of unusual operating conditions, excessive customer load demand, equipment failure, or near simultaneous disruptions can bring the system to its tipping point.

Consider the following cascading outage scenario where disturbances propagate through the network causing significant load loss and potentially leading to a system
collapse. “When a fault occurs, or if the system is stressed and equipment removed without sufficient adjustment, the chain of events may start. For example, some generators and/or lines may be out for maintenance, and another line may trip due to a fault. Other lines may become overloaded and start to sag, contact a tree, and trip. There may be a hidden failure in the protection system (e.g., outdated settings or hardware failures) that may cause another line or generator to trip. At that stage, the power system is faced with overloaded equipment and multiple disturbances evolving in different time scales. If fast actions (e.g., load shedding, system separation) are not undertaken, the system cascades into unplanned islands. Based on the severity of the disturbance felt by the system, and the strength of interconnection, parts of the islanded systems may enter into a complete blackout” [24]. Figure 1.2 presents a common scenario of the cascading outage process suggested in [25].

Figure 1.2: A flow chart demonstrating a typical cascading outage scenario. This figure was adapted directly from [25].

Large blackouts are relatively rare, but the if the sheer economic cost and human impact is not enough to convince readers of the importance of contingency analysis research, perhaps introducing this next study will.
1.6 Power Law and Self-Organized Criticality

Careful observation of major blackout frequency over the past several decades reveals that severe outages are much more likely than mathematicians might predict when extrapolating from regular occurring small outage data. These observations led to several lines of research attempting to explain this discrepancy. Most notably, chaos theory was highlighted and Carreras, Newman, and Dobson [26] were among many researchers eager to investigate the connection of chaos and real blackout data.

They first analyzed a 15-year time series of NERC documented transmission system blackouts – a set of events noticeably diverse in magnitude and of varying causes. When plotting the probability distribution functions (PDFs) for several different measures of blackout size they observed that the curves fit a power law – a signature of complex, chaotic systems. Measures of blackout size considered include energy unserved [MWh], amount of power lost [MW], and number of customers affected. This observed power tail, unlike conventional systems that might fit a Gaussian distribution and decay exponentially with event size, showed data that tapered off more slowly implying that large blackouts occur in higher frequency than expected. A simple explanation of this could be that as component failures occur, the power system is weakened and results in an elevated risk of additional (larger) failures.

To take it a step further, Carreras et al. explored their results for evidence of Self-Organized Criticality (SOC). They compared their findings to a time series from a sandpile model known to have these characteristics. In an SOC system, the average state is organized near, but not at, a critical point on the fringe of disruptions. This is attributed to nonlinear dynamics and the presence of perturbations. The sandpile model, a common representation of a chaotic system, is a physical system where grains of sand are continually added to a pile. At times, certain locations will exceed their threshold and cause avalanches to erupt. Eventually, the addition of sand will be balanced by the loss off the edges and the pile will reach a state of equilibrium. This new state will be near a critical point where its behavior becomes chaotic and another avalanche is likely to materialize. In short, avalanches of varying magnitudes occur, and the PDF of their size fits a power law [27]. In this comparison, the authors found
correlations between the PDFs strong enough to claim the two models as statistically indistinguishable. In summary, they proposed that SOC-like dynamics could play an important role in modeling power systems and in understanding why we may need to brace ourselves for more severe blackouts in the years to come [26],[28].

Although the SOC explanation paints an elegant picture of power grid dynamics, it is not universally accepted. Alternative theories exist and claim that criticality is not the only possible origin of power law distributions. Doyle and Carlson [29] argue that complex systems like the internet, traffic, and the power grid instead favor descriptions where performance and reliability are determined by factors like detailed structure and external conditions. Unlike SOC models where external forces only serve to initiate events, the Highly Optimized Tolerance (HOT) mechanism places a much greater weight on uncertainty when generating a broad distribution of outcomes. One key difference between HOT and SOC worth noting is the dependence of the power law exponent on dimensionality. Under SOC, large collective fluctuations or large-scale events are reduced with increasing system dimensionality, whereas HOT predicts just the opposite.

Though alternative methodologies like the one mentioned above do exist, the evidence is convincing in any case that blackouts, similar to earthquakes and other natural events, appear to follow a power law. This trend has also been observed outside of North America in Sweden, Norway, New Zealand, and China [30]. The overall message rings clear that there are profound risks to the complex electric grid we so heavily rely on.

1.7 Document Organization

The remainder of the report will be organized in the following manner. Chapter II will continue the discussion above with an in-depth review of literature and active research areas. Chapter III will present the Vulnerability Frontier model along with relevant supporting literature. Details for model modifications and additional tools to aid in analyses will also be described. Results for an assortment of test scenarios will be reported and analyzed in Chapter IV. Finally, conclusions will be drawn and areas of future work identified in chapter V.
CHAPTER 2

LITERATURE REVIEW

2.1 Chapter Overview

Electric grid reliability and severe contingency analysis can be modeled and analyzed through a variety of lenses. Important dynamic properties and complex features can be better understood through the simulation of cascading outages, voltage collapse, or other blackout event phenomena. With a higher penetration of renewables on the grid and heightened concerns for malicious attacks, blackout models and reliability assessment tools help paint a better picture of the past, present, and future state of grid vulnerabilities. This chapter explores many of these areas to better frame current gaps in the field.

2.2 Cascading Failure Outages

One common factor often identified as the leading cause of large blackouts in the bulk power system is cascading failures in which an initiating event produces a sequence of successive failures that trigger outages over large portions of the grid. These failures stem from a variety of causes that can be grouped into the following categories: natural disasters, human activity, unexpected component failures, and system failures [31]. A discussion of several lines of research and existing modeling techniques are presented next.

2.2.1 Self-Organized Criticality

The occurrence of a power tail in the frequency distribution of blackout size suggests the power system has been operated near a critical point. Some propose that as more elements are added to the grid in conjunction with increased power flows and consumer demand, the swelling complexity will continually cause the electric grid to
approach criticality. System operators are forced to accept higher and higher power levels on the system – typically making necessary upgrades following blackouts. This is the idea that economic forces and engineering practices seeking to minimize cost and maximize returns might set the system up for failure. Throughout the evolution of the power system, this trend of reactive rather than preventative measures has persisted [28].

To investigate these notions further, Carreras et al. [32] continued their work, constructing a simplified transmission system model to examine cascading failures as load is steadily increased. This analytically tractable blackout model employs the DC power flow equations and standard linear programming optimization of generation dispatch. It was first tested on tree networks before being applied to the IEEE 118-bus network. Two types of transitions were identified as these outages were simulated, the first due to limits on generation capacity and the second resulted from network line power flow limits. Results confirmed that some of these transitions have properties of critical transitions and when the load is increased to near a critical value, the PDF of blackout size is governed by a power law. These blackout distributions were statistically significant to those from their previous findings on real data. They have continued to validate their claims more recently with expanded data sets from NERC [33]. Now having tested both theoretical models and empirical blackout data, their compelling arguments are gaining traction.

The same authors next tried to explain why the power system is operated near critical points in [34]. To do so they called upon two cascading failure models, OPA and CASCADE, that will be discussed momentarily. They claim that system operating margins slowly and naturally evolve towards critical points in response to economic, societal, and engineering forces. In an attempt to model cascading failures, they constructed scenarios with regular increases in load or consumer demand while also including system upgrades (boosting rated line capacity) following blackouts. Inputting occasional line outages as random events, they could simulate typical afflictions to power lines which sometimes overload nearby lines and cause them to fail subsequently. They found that these upgrades, while initially reducing blackout frequency, ultimately lead to an increased number of severe blackouts. Yet again, the
power law was visible under these circumstances bolstering their claim that the power system was loaded near a critical point.

Though critics certainly disagree with these author’s statistical methods and overall approach ([29], [35]), there is common ground amongst researchers in acknowledging that major blackouts are a byproduct of a complex system and require fundamental changes to eliminate.

2.2.2 Blackout Models and Alternative Approaches

Two models of cascading failure pioneered by Dobson, Carreras, and Newman include the CASCADE model [36] as well as the Oak Ridge-PSERC-Alaska (OPA) model [37]. CASCADE is a simple probabilistic model that aims to uncover and describe some of the salient features of cascading blackout events. The algorithm is fairly straightforward and begins by giving all components an initial loading taken from a uniform distribution. After adding some disturbance, each component is tested for failure and those that do surpass their limit have their load redistributed to the remaining components. Though it neglects event timing and other complex component interactions, applications of this model have helped understand global system effects that have been seen in real blackout events or from other more detailed modeling techniques.

The OPA model on the other hand, consistent with some basic network and operational constraints, includes representations of power flows on the grid using circuit laws. A DC load flow approximation is used for a fixed network of transmission lines, loads, and generators. Beginning with a solved base case, independent random line outages are introduced and the load is re-dispatched using linear programming methods with a cost function that is weighted to avoid load shedding whenever possible. There also exists some probability that lines which became overloaded under the new dispatch will lead to an outage. This entire process is iterated until no more outages arise and the total load shed becomes a measure of the size of the blackout. This process represents a fast time scale on the order of minutes to hours, but a slow time scale corresponding to days through years, is also considered. This element offers opportunities to include system upgrades (boosted line flow limits or generator
capacity while maintaining original topology), typically in response to blackouts, as well as regular demand increases. These gradual opposing forces permit the authors to study the self-organization of the system in a dynamic equilibrium [34], [37].

With aims of validating this cascading blackout model, the authors have tested OPA on various large transmission networks including a 9402, 1553, and 19402-bus model of the Western Electricity Coordination Council (WECC) interconnect. These processes have permitted them to upgrade the model to better accommodate networks that contain significant tree structures rather than just mesh. They also highlighted the need for researchers to be mindful of the heterogeneous structure of large power system networks [38], [39]. Another use of this model required extending it slightly to simulate the impacts of two reliability principles – the n-1 criterion and a direct response policy. They amend the algorithm and incorporate these upgrades before introducing the initial disturbance. In doing so, they can simulate the slow evolution of the transmission grid incorporating an average 2% load increase per year and upgrades corresponding to either of the reliability policies mentioned above. This application allowed for the analysis of long-term electric grid impacts from steady load growth and required reliability standards [37].

Another way to understand cascading failure more thoroughly involves risk assessment. Ni et al. [40] use an online risk-based security assessment to rapidly quantify the security level of existing or forecasted operational conditions. This approach, unlike deterministic online security assessments, uses a probabilistic model of uncertainty in their computation of risk indices. These prove useful in control room decision making and improve understanding of potential network problems. The security evaluations incorporate not only line flow violations and cascading overloads, but also voltage magnitude violations and voltage instability. As an expectation of severity, the risk index is calculated by the product of the outcome probability and its severity and is summed over all feasible outcomes. A notable feature of this method is that it performs analyses on near-future conditions rather than past conditions as in traditional security assessments.

Beginning with a given contingency scenario, their algorithm identifies and removes circuits with flows that exceed their emergency overload rating. They then
resolve a power flow and repeat the process until either no more circuits are identified or the solution diverges, and compute the severity index. The assessment is rather flexible, allowing for global or regional views of risks and for individuals to efficiently investigate specific components or contingencies as the root cause of a disturbance. The authors surmise this assessment will prove useful in control-room security decision making scenarios that are frequently encountering stressed conditions.

Anghel, Werley, and Motter [41] created a stochastic model for describing quasi-static dynamics of a transmission network under various perturbations. Their model includes optimization over different risk factors balancing scenarios with heavy load shed in avoidance of cascading outages against scenarios with reduced load shed and higher risks of propagating cascades. They also adjust the model to incorporate operator actions to various contingency events that may or may not be optimal. Chen, Thorp, and Dobson [42] developed a technique to model protection system hidden failures, thermal overloads, and generator re-dispatch. Hidden failures in the power system, prominent in cascading failure events, refer to permanent defects causing relays to incorrectly or inappropriately react to disturbances. To study the effects of network degree and component interaction on both the size and duration of cascading failures, Roy et al. [43] employ a Markov model to generate component failures within randomly generated tree networks.

In another noteworthy approach which has proven useful for transmission expansion planning, Hardiman, Kumbale, and Makarov [25] simulate cascading outages and rank them in order of severity. For this method, an advanced reliability analysis software, Transmission Reliability Evaluation of Large-Scale Systems or TRELSS, enables them to model protection control groups and islanding in large AC networks. TRELSS was originally developed by Electric Power Research Institute in conjunction with Southern Company Services. The commercially available software is versatile in its modes of operation and can also compute reliability indices to quantify the vulnerability of the system in terms of problems such as overloads, voltage violations, and network separation.

Their method provides an interesting comparison to this work as well as to the OPA model. The authors offer a simplified cascading outage algorithm depicted
in Figure 2.1 to pair with the TRELSS Simulation Approach tool. This figure highlights another cascading outage method and contrasts with the OPA algorithm which focuses on overloaded lines rather than voltage violations.

![Flowchart](image)

**Figure 2.1**: Simplified cascading outage algorithm to pair with TRELSS software for contingency screening practice. This figure was adapted directly from [25].

Beginning with a prepared list of potential initiating events, hundreds of contingencies are screened and organized following a ranking methodology which hones in on those that are most probable and severe. The rank, $R_i$, is computed as the product of event severity, $S_i$, and the likelihood of event $i$, $L_i$. The likelihood term aims to capture the expected relative frequency of occurrence for the cascade event. The calculation of severity comes from a combination of several components including load loss from voltage collapse, load loss from other sources, the number of voltage and transmission problems, as well as the number of cascading steps. Each term is weighted by an experimentally selected coefficient to reflect the relative likelihood of such event.

Pairing the TRELSS software with this event screening algorithm and ranking strategy has proven useful in analyzing numerous high-consequence contingencies.
However, the requirement of having a predefined contingency list is restrictive and the large number of subjective quantities may hinder results.

Though it is only a research-grade tool, the Manchester model aims to characterize a wide array of interactions present in cascading outages. Among these are the tripping of transmission lines, generator instability, under frequency load shedding, and emergency shedding to prevent voltage collapse phenomena. The model employs an AC power flow model, Monte Carlo simulations, and is well-rounded in its inclusion of generation and transmission component failure probabilities as well as probabilities of hidden failures in the protection system [44]. Many have taken advantage of the expansive literature and modeling tools available and introduced modifications to improve robustness or illustrate shortcomings. For instance, one group offers an “Improved OPA” method to address limitations with accuracy [45] while another suggests combining AC power flow aspects in the Manchester models with the OPA model [46].

This diverse group of methodologies and analyses each have their own primary focus and advantages, while confirming that no existing approach can capture all of the mechanisms associated with cascading failure or extreme event analysis.

2.3 Voltage Collapse

Voltage collapse events, or events defined by a progressive decline in voltage magnitude at system buses, are also recognized frequently as the cause of major blackouts. This typically occurs in response to unmet reactive power load when support devices are not numerous enough or simply do not have enough capacity to remedy this. Automatic voltage regulators are used in real-time to stabilize this, but protective devices may still observe the abnormal conditions and cause a circuit breaker to open, de-energizing parts of the system and potentially building to total voltage collapse. This is becoming an increasingly serious problem as the electric grid becomes more heavily loaded and only grows in complexity.

Voltage collapse dynamics represent another area of substantial exploration and modeling. A key obstacle in anticipating these types of events lies in the use of capacitor banks which can shield a low stability margin in the network. The capacitor
banks maintain voltage levels at substations, holding the system within operational constraints while making operators blind to its true risk level. Thus, it is necessary to develop physically insightful stability conditions under which a network is safe from voltage collapse. Simpson-Porco, Dörfler, and Bullo [47] work to ameliorate this problem as they derive a closed-form condition that yields a connection between reactive power loading demands, the complex structure of the system, and the resulting voltage profile of the grid. Their computationally friendly stability condition provides node-by-node measures of grid stress and predicts the largest nodal voltage deviation while also estimating the distance to collapse. They argue this tool could not only be impactful in contingency analyses as operators screen for failure scenarios, but also in identifying weak network areas and locating geographical origins of voltage instability to assess the optimal placement of voltage control equipment. This works in tandem with the idea of a self-healing network in which the automatic dispatch of generation serves to mitigate voltage fluctuations as they appear.

Despite many complex, intricate properties, voltage collapse events typically have a fundamental effect in which the system falls out of equilibrium in a saddle-note bifurcation. One approach hones in on this aspect by computing closest bifurcations and their associated minimum load power margins for secure operation [48]. This is to say they identify the point on the feasibility boundary in which the smallest change in power injections would cause the operating point to shift to the edge of feasibility. These two points offer a minimum load power margin which can be a useful index of proximity to voltage collapse, providing a measure of the security margin (for a fixed network topology). Their technique also proposes a best direction for load shedding which could be of use during remedial actions following disturbances. The significance of computing minimum load power margins in this context is not to be understated as they characterize the worst case scenarios in terms of load growth.

Though numerous numerical simulation techniques exist for monitoring and predicting voltage collapse, little has been done to investigate nonlinear instabilities from a network perspective. There is also a need for an improved theoretical understanding of voltage collapse and reactive power flow in complex networks. Finally, it is worth noting that due to an increased presence of utility-scale wind and photovoltaic
generation sources, heightened voltage fluctuations are becoming more common [47]. This leads to another important discussion of the impacts of elevated renewable energy portfolios on the reliability of the grid along with a few examples of modeling techniques to do so.

### 2.4 Renewables

Highly variable renewable generation sources cause inadvertent stress on the stability of the power system and some traditional modeling approaches fall short in capturing this behavior. One newer technique combines power flow, economic dispatch, unit commitment, and historical time-series data to more closely reflect system stability [49]. Linking these components allows the authors to characterize wind variability in a single simulation and observe true worst-case scenarios under high penetrations of the variable resource. Their claim is that alternative studies aiming to pinpoint the worst-case scenarios miss out on the big picture by oversimplifying power flow studies involving wind generation. Moreover, this methodology could aid in proper implementation of voltage control strategies in wind turbines and increase voltage stability margins. For example, they demonstrate that the doubly-fed induction generator machine, the most popular installed wind turbine technology to date, could improve these margins if using voltage control features and permit larger levels of wind generation to penetrate the system without degrading stability.

Eftekharenejad et al. [50] embraced a similar issue except in the presence of photovoltaic (PV) systems. The authors study the static performance and transient stability of a large power transmission network that represents the Western US interconnection and find both favorable and unfavorable impacts. Observations showed bus voltage magnitudes having the most adverse effects during transients and they conclude that distributed PVs may require a measure of voltage tolerance. More recently, Obi and Bass [15] offered a few words on addressing some of the issues with PV integration calling on Maximum Power Point Tracking, Solar Tracking, and transformer-less inverters. These technological advances along with the potential construction of inverters with reactive power control and frequency regulation handles, ultimately surmount to minimized grid interference and efficiency gains.
Revisiting the OPA method discussed previously, the same group used the blackout model to probe the impacts of increased distributed generation on the power grid’s reliability [51]. To do so, they modified their existing model by adding a new generation class which enables them to vary the fraction of power from distributed generation, the fraction of nodes with distributed generation, and the reliability of this generation. They find an increased risk of severe blackouts when distributed generation proves more variable, despite observing improved system characteristics when the generation is reliable.

2.5 Malicious and Cyber Attacks

Reliability studies from another class of problems involving intentional, malicious attacks, both cyber and physical, require differing approaches than many of those discussed above. These attacks, unlike natural events or systemic failures which occur on a random basis, are more coordinated as individuals seek targets with the most disruptive outcome, embedding a strategic interaction between attackers and defenders. In this context, one study presents a game-theory model to illustrate these interactions and perform risk assessments of the various attacks against individual power-system components [52]. They presume that attackers look to balance the difficulty of the attack and its effects to the defender’s countermeasures and ability to reduce its impact. By exploiting this in their model, they assess the likelihood of attacks on specific components based on the outcome as well as the efficiency of the defense resources. Following tests on a standard IEEE RTS-96 system, they contend this type of analysis will be of use in designing defense plans and in properly allocating resources to protect a network’s most sensitive targets.

Salmeron, Wood, and Baldick [53] offer a min-max model to identify the most severe attack scenarios. In searching for these coordinated, maximally disruptive cases, they can locate critical sets of components and gain insight into how to lessen the vulnerability of the grid. The inner loop of their bilevel, mixed-integer optimization approach is used to solve a DC optimal power flow model with an objective function that minimizes generation costs plus a cost penalty for any unmet demand. The outer loop maximizes the disturbance by selecting the most disruptive interdiction plan from
a discrete set of potential attacks. They conclude that with moderate computational
efforts, these practices can help mitigate the disruptions to power grids by locating
critical components or attacks that a terrorist group might undertake. Furthermore,
they suggest that the components that reoccur over a wide range of attacks and
assumed terrorist resources, would be excellent candidates for hardening.

Investigation into cyber attacks and the risk they introduce to control systems is
not well-understood. Stamp, McIntyre, and Richardson [54] chip away at the prob-
lem by developing a cyber-to-physical bridge which relates cyber attack trajectories
to their subsequent disturbances on the grid. Also adding to the conversation is
Pasqualetti, Dörfler, and Bullo [55], who provide a mathematical framework for cyber
attacks and design attack detection monitors, while simultaneously identifying flaws
in alternative graph-theoretic methodologies. Moreover, research surrounding both
cyber and physical attacks are in preliminary stages and require new, unique tools to
pinpoint their fundamental attributes and reliability influences.

2.6 Topological Arguments and General Reliability
Assessments

With respect to reliability, some researchers are using blackout models to answer
more directed questions about network size, topological arguments, or the computa-
tional boundaries of multiple contingency analysis. Beginning with Carreras et al.
who pose questions surrounding the optimal size of a complex network, the OPA
model is put to use again [56]. In response to gross demand increases and high
levels of interconnectivity, they are curious if these networks, while supplying power
from distant points and to individuals in remote locations, are growing too large and
becoming more susceptible to sizable propagating failures. To study this cost-benefit
trade-off, they begin by evaluating failures in large networks to those of an equivalent
size network made up of several unconnected smaller systems. It is notable that
the disconnected small networks are governed by an exponential fit, rather than a
power law, in the PDF of blackout size. In comparing integrated risks, they show
the existence of an optimal size to manage blackout risks beyond which, the cost of
failure deems the network disadvantageous economically.
To a similar tone, Dey et al. [57] were interested in if the topology of the grid could drastically affect the propagation levels of disturbance events. They examine basic topological characteristics employing a variety of statistical measures to compute the average propagation of failure as a branching process parameter. This is done under varying topological conditions generated from three standard IEEE networks where they study the variation in mean propagation further. They require more work to make any firm conclusions, but remark that a correlation does exist between the propagation rate and the variations in topological parameters.

Topological studies and arguments for ideal network size could have significant implications for electric grid planning, design, and operation. These discussions will become more prominent as distributed resources, typically in the form of renewable generation, continue to penetrate the grid at higher and higher levels.

The following works focused on assessing or quantifying relative reliability levels from a general contingency analysis perspective. One source suggests an assessment based on a full topology model to simulate accurate system failure responses [58]. They employ a state enumeration method with probabilistic reliability measures to evaluate associated system disturbances. Their method is distinctive in the way they rank contingencies and apply filtering techniques to reduce the number of states requiring further analysis. Another study defines a metric referred to as “net-ability” that measures grid performance under normal operating conditions as a manner in which grid vulnerability can be quantified [59]. Traditional topology based graph approaches for depicting the electric grid have also been called upon and one group in particular offers modifications by weighting the network graph based on the reactance matrix [60]. The authors pair this alteration with minor changes to the power flow constraints and load definitions for an updated dynamic model and compare it to other vulnerability analyses of the same IEEE test systems . Finally, a paper focusing on “N-k” contingency analysis will be noted as it brings to light the computational capabilities for enumerating all possible component failures [61]. The authors demonstrate that with numerous parallel processors they are able to enumerate all single contingencies for a test WECC network in 30 seconds. However, anything above one or two contingencies becomes infeasible even for high performance cluster machines.
and enhanced screening techniques are thus required to reduce the massive number of combinations.

This section summarized several approaches including some that hone in on very specific operating conditions and triggering phenomena, along with others that aim to broadly characterize the vulnerability of an entire system. These advancements just scratch the surface of existing literature and their simulation, modeling, and analysis techniques many of which address various obstacles and interesting frameworks to surpass them. However, there are certainly challenges and complications yet to be resolved. For instance, many simulation techniques face a trade-off between speed and accuracy which can greatly alter result patterns [30]. Some of the pros and cons of common tactics in modeling cascading outages are described in Table 2.1.

**Table 2.1**: Summary of modeling challenges reprinted and adapted from [30].

<table>
<thead>
<tr>
<th>Approach</th>
<th>Strengths</th>
<th>Weaknesses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Historical data</td>
<td>Reality - no modeling assumptions</td>
<td>Long observation time for good statistics for rare large blackouts; data inaccurate or missing; no 'what if' experiments.</td>
</tr>
<tr>
<td>Deterministic simulation</td>
<td>Similar to standard reliability framework, e.g. N-1 security</td>
<td>Subjective choice of credible contingencies; no probability or risk evaluation; few mechanisms represented; many modeling approximations.</td>
</tr>
<tr>
<td>Probabilistic simulation</td>
<td>Enables quantitative risk evaluation</td>
<td>Slower simulation; few mechanisms represented; many modeling approximations.</td>
</tr>
<tr>
<td>High-level statistical models</td>
<td>Describes overall propagation of cascade; simple and tractable</td>
<td>Ignores all details of cascading.</td>
</tr>
</tbody>
</table>

To better understand the nature of severe blackouts and cascading events, contingency analysis beyond the N-1 requirement must be improved. Unfortunately, in the case of N-k events, there are severe computational burdens due to the large number of components and their respective combinations. Combating this requires intelligent contingency selection practices, high performance computing hardware, and innovative visualization methods. These will provide operators with the situational awareness in real-time allowing them to anticipate, recognize, and respond to
impending risks [44]. The search to find a vulnerability assessment tool that is both analytically tractable and flexible in its application is not an easy one. However, as the global population without access to electricity shrinks to near one billion and we have become dependent on the grid’s services for every facet of our daily lives, reliability grows evermore valuable.
CHAPTER 3
THE VULNERABILITY FRONTIER

3.1 Chapter Overview

The discussion of relevant literature surrounding power grid blackouts and contingency analysis in the previous chapter identified several areas in need of attention. Most notably, the presence of a power law showing increased risk of large blackouts paired with a lack of effective screening techniques for multiple failure events is of particular interest. The focus of this discussion will be on the motivation for the vulnerability frontier technique along with its evolution and development. A series of metrics will also be defined to help characterize the vulnerability of an entire system. To illustrate some of the practical uses of this method, results from a small test case will be presented.

The final section of this chapter will outline a slight variation on the existing technique to be considered in the analysis. In addition, a representation of the OPA blackout model will be explicitly defined. This cascading outage model will serve as a useful comparison tool with aims to improve understanding of results and potentially validate critical contingencies.

3.2 Motivation

The grid is monitored and operated under the requirement that network security must be guaranteed for all single component failures. In practice, this famous “N-1 criterion” is easily achievable as all single contingencies or multiple contingencies of sufficiently high likelihood can be anticipated. The grid can therefore be designed to be resilient to any system instability, cascading outages, or voltage collapse [62]. Preparing for multiple contingencies is not as straightforward and many deem less important despite their potential to trigger extreme events. True, large disturbances
do occur much less often than small, short-term outages, but, instead of decaying exponentially, PDFs of the frequency of blackout event size have been repeatedly shown to fit a power law making them of much greater concern. Adding to this is the sheer cost, both direct and indirect, inflicted from severe blackouts on related infrastructure, the economy, and customers. When the dependence on electricity services has grown as strong as it is today, maintaining the security of the power grid, what some consider the most complex “machine” in the world, requires taking a closer look at multiple contingency event screening.

Typically, the initiating event from a severe blackout can be traced back to a few critical, near-simultaneous component outages. The important thing to note is that these events are not typically independent events, and particular single or multiple contingencies may initiate subsequent failures very quickly. Unlike single contingencies which can be easily evaluated over all possible combinations, there are serious computational burdens to performing a brute-force enumeration over all multiple contingency events, $\sum_{i=1}^{k} \binom{n}{i}$. Consider a system with 10,000 components and a supercomputer with the ability to evaluate 10,000 contingencies per second. There are approximately 50 million combinations of N-2 contingencies, 160 trillion combinations of N-3 contingencies, and $4 \times 10^{14}$ combinations of N-4 contingencies which would take nearly 84 minutes, 6 months, and 1300 years to compute, respectively [63]. Thus, anticipating and planning for rarer events of this nature is challenging.

The main motivation behind this method is the need to establish intelligent screening protocols to search for contingencies that may precipitate severe events. In an effort to bound a worst case analysis, the vulnerability frontier approach helps evaluate power system weaknesses and reliability. Generally speaking, the frontier describes a boundary relating the worst-case power disruption as a function of the number of lines removed from service. The frontier and various operating conditions also aid in defining related metrics to quantify relative vulnerability. Next, the evolution of this model along with important advances that lead to its development will be presented.
3.3 Model Foundation

Initial work on power system worst-case studies began with a two-stage approach in which a screening process recognizes a subset of potentially important lines and subsequent analyses identify critical combinations that may lead to severe blackouts [64]. The main question of interest lies in finding the smallest change in operating conditions that forces the edge of the feasibility boundary to shrink to the present operating point. The method employs a graph theoretic approach which partitions the network into subgraphs. The lines separating the regions are taken as vulnerable components which may pose a threat to grid security. In this way, a constrained optimization problem can be formulated to minimize the number of line removals that guarantee a disturbance severity greater than some user-defined threshold. An alternate framework exists in which the objective function instead maximizes severity while forcing the number of line removals to be less than a user-defined maximum. In either case, the severity is measured from a power imbalance perspective and computed as a shortage or surplus of power within the resulting subgraphs. The benefit of this multi-step procedure is the massive reduction of important contingencies. In considering only the subset of lines deemed most severe, time is freed up to perform a more detailed, dynamic analysis of contingency events over all possible combinations from the reduced subset.

Continuing to probe the same fundamental question, a variant on the previous model came a few years later [65]. A primary difference between the two methods lies in how they measure the severity of an event; the prior formulation relying strictly on power imbalance while the updated one instead focuses on the magnitude of required load shed. This time, the nonlinear optimization problem enforces a minimum load loss quantity defined by the user in order to maintain grid integrity while the objective function minimizes component failures. Rearranged slightly, it can also be designed to maximize the loss of load necessary to withstand a specific number of disturbances. The authors approach this in two stages by first shrinking the feasibility region, causing the nominal operating point to be outside the boundary by at least some user-specified distance. This step employs a partial line outage relaxation technique to lessen the computational burden and aid in identifying a small set of line outages.
that will contract the feasibility boundary as needed. The second stage allows for a detailed N-k analysis on a much smaller subset of lines identified in stage one. I will refer the reader to the original publications [64] and [65] for specific details and peculiarities in setting up these optimization problems.

Both approaches are fairly similar as they consider the network in a static sense and pose questions relating event severity to the number of failure events. The formulations are reminiscent of past literature with aims of analyzing the proximity of an operating point to the power flow feasibility boundary and most notably a method derived by Alvarado, Dobson, and Hu [48] that offers minimum load power margins which would move a particular operating point to the edge of feasibility. Another similar formulation mentioned in the literature review was the bilevel optimization setup posed by Salmeron et al. [53] which finds the worst multiple contingency attack that may be performed by a terrorist group.

### 3.4 Graph Partitioning

These foundations established an important trade-off between the number of component failures and the severity of an event. Most relevant to the vulnerability frontier formulation was the application of this trade-off within a graph partitioning problem in [63]. The authors exploit graph theoretic properties to solve a problem which weighs two objective functions – minimizing cuts, or line removals, and maximizing power imbalance between partitions – and varies their importance with a trade-off parameter, $c$.

A few principles relevant to graph partitioning will be presented next, along with a simple example to illustrate the important features. Imagine a four node network connected by five branches as depicted in Figure 3.1.
Figure 3.1: 4-node example graph.

The directed graph can be described mathematically by the following incidence matrix, $A \in \mathbb{R}^{m \times n}$:

$$
A = \begin{bmatrix}
1 & -1 & 0 & 0 \\
1 & 0 & -1 & 0 \\
0 & -1 & 1 & 0 \\
0 & -1 & 0 & 1 \\
0 & 0 & -1 & 1 \\
\end{bmatrix}.
$$

The matrix will have $m$ rows corresponding to the number of branches and $n$ columns corresponding to the number of nodes. Each row (branch) is filled with a 1 in the entry matching the node $n$ where it originates, a $-1$ in the entry for the node where it terminates, and zeros otherwise. Multiplying the incidence matrix with itself forms the Laplacian matrix, $L$ – a square, symmetric matrix with many favorable properties. This positive semi-definite matrix is made up of off-diagonal elements equal to either 0 or $-1$ and diagonal elements corresponding to the absolute sum of the off-diagonal entries across each row. An important property to highlight in the case of connected graphs, which generally applies with the power grid, is the existence a single zero eigenvalue whose associated eigenvector is a vector of all ones, $1$. Observe that irregardless of the branch ordering in $A$, the Laplacian will work out to
\[ L = \begin{bmatrix} 2 & -1 & -1 & 0 \\ -1 & 3 & -1 & -1 \\ -1 & -1 & 3 & -1 \\ 0 & -1 & -1 & 2 \end{bmatrix} \]

for this sample network.

The graph can be partitioned into two groups by assigning each node to one group or the other with an indicator variable, \( x \). For example, it may take the form \( x = \begin{bmatrix} -1 & 1 & -1 & 1 \end{bmatrix}^T \) which separates nodes 1 and 3 from nodes 2 and 4 (see Figure 3.2). The product of the incidence matrix with this indicator variable provides a vector whose nonzero entries correspond to the branches that separate the two groups:

\[ y = Ax = \begin{bmatrix} -2 & 0 & -2 & 0 \end{bmatrix}^T. \]

\[ \text{Figure 3.2: 4-node sample graph with selected partition.} \]

Upon inspection, it can be seen that multiplying \( y^T y \) will yield four times the number of separating branches. Rearranged slightly, we have

\[ \frac{1}{4} y^T y = \frac{1}{4} x^T (A^T A) x = \frac{1}{4} x^T L x = \# \text{ of separating branches}. \]

Similarly, given a power injections vector, \( p \), it follows that the product of \( p^T x \) would give twice the power flow between the two groups. Rephrased, this product appears as:

\[ \frac{1}{2} p^T x = \text{power imbalance between groups}. \]
In the case of electric power systems, the network nodes are treated as buses which may have some generation, load, or both specified at each and the branches represent transmission lines delivering power to the loads. Note that in a lossless system, the power injections vector must sum to zero, implying that the power flow into the generation-poor partition must be equal to the sum of the injections in the generation-rich partition [63].

In general, graph partitioning techniques can be applied in a variety of ways to satisfy a particular goal while observing chosen criteria for decomposing the graph into smaller subgraphs. The aim here is to identify a small number of lines that when removed will partition the system into two groups and result in a severe power imbalance. This is to say, we are searching for an indicator variable, \( x \) which can balance these two competing objectives.

### 3.5 Model Description

The vulnerability frontier can be defined as the set of points relating the number of lines removed from service to the maximum amount of power disrupted by such an event. Considering a \( k \)-line outage scenario, this worst case analysis provides a measure of the maximum immediate power imbalance the grid is vulnerable to for any \( k \)-line cut. An important distinction here lies in the use of power imbalance rather than eventual power disrupted, or load shed, which would likely be a much smaller quantity (and much more difficult to compute). Note that even forming a solution with this reduced set of particular worst-case contingencies falls into the class of NP-Hard problems. However, the following algorithm developed by Lesieutre, Pinar, and Roy [66] allows for the calculation of points that bound the frontier as well as many that lie on it.

The following optimization problem minimizes a quadratic cost over all possible partition indicator vectors, \( x \):

\[
\min_{x \in \{-1,1\}} \frac{x^T L x}{4} - c \frac{p^T x}{2}.
\]  

(3.1)

Again, the two quantities reflect the number of lines removed and the effective power imbalance weighted by a trade-off parameter, \( c \). For small \( c \), the solution
will simply minimize the number of cuts. For large $c$, the problem heavily favors maximizing power imbalance and this will effectively find a solution which separates generation from load. In between, the goal is to find solutions with increasing number of cuts and increasing power imbalances to form the bound on worst-case contingencies.

### 3.5.0.1 Optimization Conversion Step

Equation 3.1 can be solved exactly by converting the optimization to a related min-cut/max-flow problem for specified trade-off parameter, $c$. The converted network for the 4-node example is shown in Figure 3.3 and a min-cut problem can be posed as:

$$\min_{x_\dagger \in \{-1,1\}} \frac{x_\dagger^T L_\dagger x_\dagger}{4},$$

where $x_\dagger$ and $L_\dagger$ reflect new variables due to the inclusion of a source and sink node.

![Figure 3.3: Converted min-cut/max-flow network for 4-node example with flow capacities specified on each edge. Blue nodes indicate net generation buses, while green indicate net load buses.](image)

More generally, given a network graph with $N$ buses and $M$ lines, each line can be weighted uniformly with capacity 1. A power flow solution for the network indicates which of the $N$ nodes are net generation or net load buses. The net generation buses can be connected to a source node, $s$, and the net load buses to a sink node, $t$. Each $s$ and $t$ connected branch will be weighted by $c \cdot p_i$. The next several steps show that solving the problem posed in Equation 3.2 is equivalent to the optimization in Equation 3.1.

To begin, observe that this network contains two more nodes and requires a new
incidence matrix, $A_\dagger$, to describe it. The initial incidence matrix $A$ can be reorganized to group the nodes which are net generation and net load separately, designating them as $A_1$ and $A_2$, respectively: $A = \begin{bmatrix} A_1 & A_2 \end{bmatrix}$. This allows for the following definition:

$$
A_\dagger = \begin{bmatrix} A_1 & A_2 & 0 & 0 \\
I & 0 & -1 & 0 \\
0 & I & 0 & -1 
\end{bmatrix},
$$

where the $s$ and $t$ nodes appear as the last two columns. Note the vectors of all -1’s in the last two columns. In this way, each net generation or net load bus is connected exactly once to the source or sink node. A weighted Laplacian is necessary as the additional lines have non-unity weight. This can be expressed as $L_\dagger = A_\dagger^T W A_\dagger$ where $W$ is a diagonal matrix in the following form:

$$
W = \begin{bmatrix} I & 0 & 0 \\
0 & [cP_g] & 0 \\
0 & 0 & [cP_d] 
\end{bmatrix}.
$$

The first set of rows represent the transmission lines present in the original network, weighted at unity. The next two sets are those connected to nodes $s$ and $t$ weighted by the product of the trade-off parameter, $c$, and the power injection at the corresponding bus. The $[cP_g]$ and $[cP_d]$ components represent diagonal matrices of relevant edge weights. These definitions allow for a calculation of the Laplacian matrix:

$$
L_\dagger = \begin{bmatrix} A_1^T & I & 0 & 0 \\
A_2^T & 0 & I & 0 \\
0 & -1^T & 0 & 0 \\
0 & 0 & -1^T & 0 
\end{bmatrix} \begin{bmatrix} I & 0 & 0 & 0 \\
0 & [cP_g] & 0 & 0 \\
0 & 0 & [cP_d] & 0 \\
0 & 0 & 0 & -1 
\end{bmatrix} \begin{bmatrix} A_1 & A_2 & 0 & 0 \\
I & 0 & -1 & 0 \\
0 & [cP_g] & 0 & -cP_g \\
0 & [cP_d] & 0 & -cP_d 
\end{bmatrix}
$$

$$
= \begin{bmatrix} A_1^T A_1 + [cP_g] & A_1^T A_2 & -cP_g & 0 \\
A_2^T A_1 & A_2^T A_2 + [cP_d] & 0 & -cP_d \\
-cP_g & 0 & c \sum P_g & 0 \\
0 & -cP_d & 0 & c \sum P_d 
\end{bmatrix}.
$$
In this representation, \(cP_g\) or \(cP_d\) terms correspond to vectors whereas \([cP_g]\) and \([cP_d]\) reflect diagonal matrices. A new indicator vector, \(x_\dagger\), is utilized in this framework with two added elements for the assignment of the \(s\) and \(t\) nodes:

\[
x_\dagger = \begin{bmatrix} x_1 \\ x_2 \\ s \\ t \end{bmatrix}.
\]

Similar to the incidence matrix organization, \(x_1\) and \(x_2\) represent the net generation and net load buses, respectively. The final step involves evaluating and simplifying the min-cut objective function, \((1/4)x_\dagger^T L x_\dagger\) with the new terms defined above. Ignoring the constant for a moment, the product appears as:

\[
x_\dagger^T L x_\dagger = \begin{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \begin{bmatrix} A_1^T A_1 + [cP_g] \\ -cP_g^T \end{bmatrix} \begin{bmatrix} A_2^T A_2 + [cP_d] \\ 0 \end{bmatrix} \end{bmatrix} + \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \begin{bmatrix} [cP_g] \\ 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} - x_1 cP_g s - x_2 cP_d t - scP_g^T x_1 - tcP_d^T x_2 + s^2 c \sum P_g + t^2 c \sum P_d.
\]

Taking a closer look at the second term, the resulting summation is made up solely of constant terms:

\[
\begin{bmatrix} x_1^T \\ x_2^T \end{bmatrix} \begin{bmatrix} [cP_g] \\ 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = x_1^T [cP_g] x_1 + x_2^T [cP_d] x_2 = c \sum P_g + c \sum P_d.
\]

Next, the source and sink nodes are assigned to opposite groups and thus the corresponding elements in \(x_\dagger\) are sent to 1 and -1. This implies that \(s^2 c \sum P_g + t^2 c \sum P_d = c \sum P_g + c \sum P_d\), reducing them to constants as well. Finally, this leaves

\[
x_\dagger^T L x_\dagger = \begin{bmatrix} x_1^T \\ x_2^T \end{bmatrix} \begin{bmatrix} A_1^T A_1 + A_2^T A_2 + [cP_g] \\ -cP_g^T \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} - 2cP_g^T x_1 + 2cP_d^T x_2 + \text{constant}
\]

\[
= x^T L x - 2cP^T x + \text{constant},
\]

where \(x = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}^T\) and \(p = \begin{bmatrix} P_g \\ -P_d \end{bmatrix}^T\). Note that these are identical to the
indicator vector $x$ and power injection vector $p$ defined for the original problem and the constants do not impact the optimization solution. Similarly, it follows that for the original incidence matrix $A = [A_1 \ A_2]$, the product $A^T A$ provides $L$ in the format above. It can now be observed that

$$\min_{x \in \{-1,1\}} \frac{x^T L x}{4} = \min_{x \in \{-1,1\}} \frac{x^T L x}{4} - \frac{c}{2} p^T x + \text{constant},$$

or that minimizing the number of cuts in the network shown in Figure 3.3 is identical to the bi-level optimization under investigation for the vulnerability frontier. In this way, employing a min-cut or max-flow solver for the related problem posed here will identify the desired indicator variable $x$ and solution to Equation 3.1. In this work, the proposed min-cut problem is evaluated with a max-flow solver using flow capacities as designated in Figure 3.3.

### 3.5.0.2 Finding Frontier Solutions

Following the derivation described previously, it is easy to obtain solutions to the optimization for a specified value of $c$. The interesting part comes in selecting the values of $c$ that yield points on the frontier. Observe that there are $2^N$ possible groupings for a network consisting of $N$ nodes. It is infeasible to exhaustively consider each grouping, however, the following algorithm guarantees the calculation of all points that lie on the boundary. To begin, consider the two extreme cases for large and small $c$ – each will provide a linear objective function and when plotted, their intersection point will separate where one case has a lower objective value than the other. This point, call it $c^*$, also provides a new value with which Equation 3.1 can be resolved to find a new $x$ or partition vector. Plotting the next objective function obtained from $c^*$ may intersect neighboring lines and provide two more $c^*$ values to try. See Figure 3.4 for a visualization of these first two steps. Each additional solution is verified for uniqueness and the process will continue until no more solutions exist. In general, although the number of points on the frontier is unknown initially, the process is bounded by the total number of lines in the system and is expected to be much less [66].
3.5.1 30-bus Example

The IEEE 30-bus test case is called upon to demonstrate the features of this technique. Figure 3.5 shows the topology of this model containing 6 generators, 20 loads, and 41 branches. Following the iterative process described above, the objective functions corresponding to solutions over the identified $c$ values are presented in Figure 3.6a. Tracing along the lowest cost function and identifying all intersection points form the solution set of the frontier. Lastly, the accompanying information for line removals and power imbalance are gathered from the solutions to produce the vulnerability frontier plot. Figure 3.6b shows this compilation.
3.5.2 Vulnerability Metrics

To accompany this methodology, an assortment of reliability metrics were offered to help quantify the overall system vulnerability with a single number. The goal is to construct scalar metrics that serve as an indicator of how susceptible various operating conditions are to large disturbances.

The first metric stems from a variation on the original optimization problem
presented in Equation 3.1. Rather than weighting the linear power imbalance term by a trade-off parameter, \( c \), the problem could be cast as a ratio of terms shown here:

\[
\max_{x \in \{-1,1\}} \frac{2p^T x}{x^T L x}.
\] (3.3)

This interpretation maximizes the ratio of a linear power imbalance term to the number of cuts expression from the original formulation. Exact solutions are attainable as this represents the initial slope of the vulnerability frontier. Although this permits straightforward calculations in the presence of the frontier, it does not have a closed-form solution generally.

Considering another related problem, the ratio could be revised to capture a quadratic power balance term as shown here:

\[
\max_{x \in \{-1,1\}} \frac{x^T pp^T x}{x^T L x}.
\] (3.4)

This formulation, however, requires a relaxation technique as it is not efficiently solved to an exact value. Relaxing the integer constraints on the indicator variable, \( x \), will help obtain realistic solutions and provide two additional metrics for consideration. Without this requirement, the solution to Equation 3.4 yields \( x = L^\dagger p + \alpha 1 \), where \( L^\dagger \) represents the pseudo-inverse of the Laplacian, \( \alpha \) is a constant, and \( 1 \) is vector of all ones, or a zero eigenvector from the Laplacian matrix. If interested in using this formulation, this simplification technique can guide the result to a least-cost integer solution by assigning values of positive entries of \( x \) to +1 and sending negative entries to −1. The addition of \( \alpha \) aids in toggling the result until it reaches a local optimum.

The first metric that can be extracted from this evaluation arises from directly substituting the relaxed solution into Equation 3.4:

\[
\beta = p^T L^\dagger p.
\] (3.5)

This closed-form representation is convenient and easily computed with knowledge of the system topology and present operating point. The third and final metric offered applies integer solutions on the vulnerability frontier directly to the formulation in
Equation 3.4:
\[
\max_{x \in \{-1, 1\}} \frac{x^* p^T p^T x^*}{x^* T L x^*}.
\] (3.6)

An important observation with these assessments is their reliance not only on system topology, but also the pattern of power injections over the network configuration. With regards to all three metrics presented in Equations 3.3, 3.5, and 3.6, it follows that vulnerability will decrease as topology grows more dense with the addition of lines [67].

### 3.6 Practical Uses

The vulnerability frontier itself can be useful in a variety of settings within extreme event analysis. The authors observed three in particular worth mentioning. First, the frontier serves as a screening technique to identify specific severe disturbances that deserve more attention. This greatly reduces the aforementioned computational burdens associated with a brute-force approach while providing an insightful list of important contingencies to prepare against. Second, it could be used to compare relative system vulnerability as the frontier is a byproduct of the network topology and power injections. Finally, it has been observed that cutsets typically appear in distinguishable patterns and may indicate critical corridors. This offers another area for secondary analysis with reduced computational efforts as groups of lines occurring in high frequency may illustrate other features or vulnerabilities in the grid [66].

Many of the tools currently utilized in industry by ISO’s or utilities require a user-specified list of contingencies to evaluate at a higher level. This screening technique could provide more sophisticated critical contingency lists worthy of further assessment. Moving forward, the vulnerability frontier method will be applied to a much larger test system in an effort to show its effectiveness and versatility while applying slight modifications for improved robustness.

### 3.7 New Additions

The final section of this chapter discusses the modified vulnerability frontier formulation. This is followed by a description of a revised version of the OPA
3.7.1 Alternate Model Formulation

Many worst case events involve cascades which propagate quickly throughout an interconnection. Recall in the OPA blackout model [37], this feature is captured through the increased probability that overloaded lines will trip following an initial random outage event. The original vulnerability frontier method can be amended to more closely reflect this phenomenon. The formulation is altered in the way transmission lines are weighted – the initial method giving all lines an equal weight while this instead designates them based on how close to its limit a line is loaded. We propose two alternative weighting formulas to reflect this.

The first determines the edge weight by the percent of available capacity remaining for a given transmission line. This marginal weighting is expressed in the following way:

\[ e_{p_i} = \frac{S_{\text{max}} - S_0}{S_{\text{max}}} \]  

(3.7)

where \( e_{p_i} \) represents the capacity of each edge \( i \), \( S_{\text{max}} \) is the maximum apparent power line rating in MVA, and \( S_0 \) is the flow on the line under the given operating point. In this way, as a line reaches its capacity constraints, the weight will tend towards zero. Comparatively, a line that is lightly loaded will have a weight closer to one.

The second variation will be defined as the absolute distance between the flow on a line and its maximum capacity (in per unit):

\[ e_{d_i} = |S_{\text{max}} - S_0|. \]  

(3.8)

Again, this formula gives heavily loaded lines a smaller weight rendering them less expensive to cut and more likely to appear in frontier solutions (as they would be more likely to trip in a cascade). To visualize this change, Figure 3.7 shows a 5-bus network for each scenario. The figure includes \( s \) and \( t \) nodes along with their connections to net generation (blue) or net load (green) buses to demonstrate the min-cut/max-flow setup. Figure 3.7a reflects the original vulnerability frontier structure while 3.7b
presents the revised structure.

(a) Unity weight for transmission lines

(b) Alternate weight for transmission lines based on MVA capacity remaining. Edge weight, \( e \), can be determined by Equation 3.7 or 3.8.

**Figure 3.7:** A comparison of two model formulations on a 5-bus network and the associated min-cut/max-flow problems. Flow capacities are provided on each edge.

This revision also requires a change to the Laplacian and objective function in Equation 3.1. The use of a weighted Laplacian, \( L_w = A^T W A \), is now utilized where
$W$ corresponds to a diagonal matrix of branch or edge weightings. Inserting this into the original optimization problem gives

$$\min_{x \in \{-1, 1\}} \frac{x^T L w x}{4} - c \frac{p^T x}{2}. \quad (3.9)$$

The goal is to capture a more robust set of multiple contingency scenarios by including a relative line weighting element. Thus, the algorithm will effectively treat a heavily loaded line as more vulnerable than one with low power flow when compared to its limit. The idea is that the revised method will be more practical in detecting and screening for contingencies that are often apart of cascades. It is unclear whether or not this formulation is superior at identifying triggering events, however.

### 3.7.2 OPA-v Model As Comparative Tool

As a comparison tool, the OPA-v method is called on to help in the analysis of results obtained with the frontier. The algorithm will be discussed explicitly below as some changes were made from the original formulation derived in [37]. A flow chart for this algorithm is presented in Figure 3.8.

To begin, an initial dispatch is obtained with a standard DC optimal power flow (OPF) solution. The previously defined incidence matrix, $A$, a diagonal matrix of susceptances, $W$, and a vector of bus angles, $\theta$, will be used to aid in setting up the constraints. From these definitions, the line flows, $F$, can be computed through the product of $W \cdot A$. Again, introducing a Laplacian matrix $L = A^T W A$ sets up the DC power flow constraint ensuring that $L \theta = P$. The power injection vector, $P$, is defined here as the sum of generation and load at each bus where the loads are expressed as negative values. Equations 3.10a - 3.10f express this optimization problem in full.

As in a traditional DC optimal power flow solution, the aim is to minimize generation cost while ensuring power flow (3.10b) and line flow constraints (3.10d) are satisfied. Additionally, the load is fixed to its initial set point, $P_{d0}$, and upper and lower bounds are enforced for all bus angles, $\theta$, and generator dispatch, $P_g$. Note that Equation 3.10a uses only the linear cost associated with each generator.
\[
\min_{P_g, P_d, \theta} \quad c^T P_g \tag{3.10a}
\]
\[
\text{s.t.} \quad L\theta = P \tag{3.10b}
\]
\[
P_d = P_{d_0} \tag{3.10c}
\]
\[
-P_{\text{FlowLimit}} \leq F\theta \leq P_{\text{FlowLimit}} \tag{3.10d}
\]
\[
0 \leq P_g \leq P_{g_{\text{max}}} \tag{3.10e}
\]
\[
-\pi \leq \theta \leq \pi \tag{3.10f}
\]

Once the initial dispatch is obtained, independent random line outages are triggered with probability \( p_0 = 0.106 / N \) where \( N \) represents the total number of branches in the network. This calls for an updated generator dispatch and DC power flow solution with a quadratic program shown here:

\[
\min_{P_g, P_d, \theta} \quad K(P_g - P_{g_0})^2 + 100P_d \tag{3.11a}
\]
\[
\text{s.t.} \quad L\theta = P \tag{3.11b}
\]
\[
P_{d_0} \leq P_d \leq 0 \tag{3.11c}
\]
\[
0 \leq P_g \leq P_{g_{\text{max}}} \tag{3.11d}
\]
\[
-\pi \leq \theta \leq \pi \tag{3.11e}
\]

A few changes to make note of include constraint 3.11d and cost function 3.11a. The constraint on loads, \( P_d \), is altered to allow load shedding when necessary (observe the direction of the inequality as a result of the negative values assigned to loads). The objective function has two terms – the first aims to keep the generation close to its previous dispatch while the second serves to avoid load loss whenever possible by placing a high cost on load variables. The addition of a tuning parameter, \( K \), allows for the weight of the generation term to be modified as necessary. Note that for the remainder of this work, \( K \) will be fixed at unity as this weighting provided reasonable results. Sensitivity analysis with this parameter represents an area of future work. The inequality enforcing line constraints has been omitted to allow for closer observations of lines that may become overloaded. Thus, the results from this secondary dispatch may contain lines with flows that have surpassed their capacity.
An intermediate step was required in the modeling process which applied this quadratic optimization before introducing the initial disturbances. Essentially, due to the nature of this objective function and removal of the transmission constraint, it was necessary to ensure that without disturbances the dispatch remains very close to the original and lines do not become overloaded. Results typically produced slight deviations in dispatch with a few lines becoming overloaded (by extremely small margins). To remedy this, the line capacities were upgraded to match what is needed under this solution. This step was performed between items one and two described in Figure 3.8, calling upon the optimization in item three.

The cascade process begins by including additional outages from the potential set of newly overloaded lines. Unlike the original OPA formulation, in this model the overloaded lines will be tripped based on the percentage overload (PO) incurred. The probability $p_1$ will be assigned as follows:

$$p_1 = \begin{cases} 
0 & \text{if } PO \leq 1 \\
1 & \text{if } PO \geq 1.5 \\
(2 \cdot PO) - 2 & \text{if } 1 < PO < 1.5 
\end{cases} \tag{3.12}$$

where $PO$ is the ratio of the apparent power flow $S$ to the respective line’s maximum capacity, $S_{\text{max}}$. Thus, lines overloaded by 150% will have 100% chance of tripping and lines loaded less than 100% will have 0% chance of tripping. In between, the probability of a line outage will increase linearly. From here, the probabilities will dictate if more outages occur. If they do, the loop will continue. Otherwise, the trial is completed and the number of lines outaged along with quantity of load shed can be recorded.
Figure 3.8: A flow chart demonstrating the OPA-v cascading outage algorithm.
CHAPTER 4

ANALYSIS AND RESULTS

4.1 Chapter Overview

The main contributions of this work include both modifications to the model along with crafted scenarios to illustrate some of its salient features. In this way, the results generally fall into two classes. The first contains demonstrations of the alternate vulnerability frontier technique and evaluations of its effectiveness. Examples will provide insight into where and how this can be best utilized. The second class, and the bulk of this work, will rely on carefully crafted test scenarios to illustrate how the frontier works on a larger, more realistic test system. The use of load profiles and manipulated case information will help characterize the behavior of the frontier (modified or original) and, in some cases, ensure it performs as expected.

4.2 Midwest Test System

The test system used for the majority of this analysis is a synthetic model of the transmission grid in Illinois, Iowa, Minnesota, and Wisconsin. The four-state network was created by a group of researchers at the University of Wisconsin-Madison in response to the growing demand for realistic large-scale synthetic power systems. These can be of use in a variety of settings including dynamics and transient stability studies, contingency analysis, and reliability assessments. The network includes 7977 buses, 610 generators, and 11,701 lines. Note that while generation and load information were derived based on publicly available data to closely represent this geographic area, the transmission network is entirely fictitious. A one-line diagram of this system can be seen in Figure 4.1.

The transmission lines are printed in different colors according to voltage level:

- 69 kV - grey
4.3 Results Part I: Model Modifications

The previously outlined modified frontier formulation will be assessed in the following three examples. Initial insight suggests that taking transmission line loadings under consideration will improve the selection process of lines that may appear in severe cascading outage events. Typical cascading scenarios are perpetuated by heavily loaded lines that continue to trip in succession. Thus, adding this element to the frontier computation might better serve in screening for this type of multiple contingency event.
4.3.1 30-bus Example

Returning again to the IEEE 30-bus network (Figure 3.5), the effects of the revised vulnerability frontier can be visualized and interpreted. Note that the comparison in this section is only performed between the original model and the modified model with edge weights based on percentage capacity remaining, calling on $e_{p_i}$ from Equation 3.7.

Figure 4.2: A comparison of frontier solutions under different edge weighting scenarios for 30-bus example. Red circles indicate selected cutsets that will be investigated in more detail.

Figure 4.2 shows the frontiers produced from a uniform edge weighting case (4.2a) and a marginal edge weighting case (4.2b) with $e_{p_i}$ weightings. Note that in order to preserve the shape of the graph (such that it remains monotonic increasing), the revised formulation requires plotting the sum of the edge weights for all lines in a given cutset along the $x$-axis. For this reason, the true number of lines within each solution are printed next to each point in Figure 4.2b. In general, when observing the collection of lines gathered throughout the solution in either case, there is heavy overlap. The uniform weighting case contains a selection of 15 different lines while the marginal case contains 17. Thirteen of these are similar between both cases. The key differences instead occur in the combinations of lines along the curve.

Another observation from Figure 4.2 is the difference in severity for the two-line
outage results. The original frontier identifies a two-line outage event that disrupts 40 MW of power while the modified frontier selects the worst outage as one that disrupts around 30 MW. In these circumstances, the original frontier with uniform edge weights has identified the more severe outcome. This is an important observation that illustrates the fact that each method is solving a different problem and depending on the operating point or the context with which the frontier is being applied, one method may outperform the other.

To understand how this revised model changes the solution set, we can look to the lines selected in a common 2-cut, 11-cut, and 14-cut scenario. These are indicated by the red circles in Figure 4.2. Beginning with the 2-cut scenario, the lines selected in each method can be visualized in Figure 4.3.

**Figure 4.3**: A comparison of two-line cuts as determined by the original and modified frontier models (using $e_{pi}$ weights).

The original model chose to isolate the generator at bus one, while the revised model found isolating the load at bus eight as more vulnerable. This difference comes as a result of the varying powerflow along each of the lines. The lines connected to bus eight are closer to their limit than those connected to bus one – rendering...
them less "expensive" to cut. Table 4.1 lists each line in the 30-bus network and their corresponding edge weighting. Recall that this weighting is determined by the AC powerflow solution based on the given operating point. A weight of zero implies the line has reached capacity, while a weight of one indicates the line is completely unloaded.

In this scenario, line ten (connecting buses six and eight) is likely the limiting factor as it only has 10% of its capacity remaining. Thus, pairing line 10 and line 40 proved a greater risk than pairing lines one and two. Continuing on, the solutions for a 11-cut and 14-cut scenario are detailed in Figures 4.4 and 4.5. Note that in these cases, eight out of eleven and thirteen out of fourteen lines, respectively, are common among both solutions as shown in purple. For the line choices that do disagree, these differences can be explained by inspecting Table 4.1.

4.3.1.1 Extension To OPA-v Model

It is beneficial to extend these results further with a comparison to several cascading outage scenarios. By employing the OPA-v model, the lines which occur in large cascade scenarios can be compared to those selected by the vulnerability frontier method.

Each OPA-v solution will contain 50,000 trials on the 30-bus system. Recall that within each trial, there is an initial dispatch, followed by random outage events, and then an iterative loop to redispach and shed load as outages accumulate. An example of the results gathered in an OPA-v simulation are presented in Figure 4.6. This plot illustrates the number of lines and corresponding load shed for each trial. In this case, the largest cascade occurred with 15 line outages and 108.7 MW of load shed.

This process was repeated 100 times and after each 50,000-trial simulation was completed, the largest cascade scenario was recorded. This allows for an evaluation of lines typically involved in a large scale cascade event. Over all 100 repetitions, the average maximum load shed event was 100.37 MW, or about 53% of the total active power load. The standard deviation was found to be 24.05 MW. With regards to the lines involved in such cascades, the average event triggered about 14 of the 41 lines. These sets of lines frequently overlapped with those that were identified in the
Table 4.1: 30-bus network branch information and edge weightings as determined by AC powerflow solution. Highlighted lines indicate those selected in each two-line outage scenario.

<table>
<thead>
<tr>
<th>Line Number</th>
<th>From Bus</th>
<th>To Bus</th>
<th>Edge Weighting, $e_{p_i}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>0.8371</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>3</td>
<td>0.8405</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>4</td>
<td>0.6995</td>
</tr>
<tr>
<td>4</td>
<td>3</td>
<td>4</td>
<td>0.8603</td>
</tr>
<tr>
<td>5</td>
<td>2</td>
<td>5</td>
<td>0.8894</td>
</tr>
<tr>
<td>6</td>
<td>2</td>
<td>6</td>
<td>0.6605</td>
</tr>
<tr>
<td>7</td>
<td>4</td>
<td>6</td>
<td>0.7947</td>
</tr>
<tr>
<td>8</td>
<td>5</td>
<td>7</td>
<td>0.7959</td>
</tr>
<tr>
<td>9</td>
<td>6</td>
<td>7</td>
<td>0.9025</td>
</tr>
<tr>
<td>10</td>
<td>6</td>
<td>8</td>
<td>0.0100</td>
</tr>
<tr>
<td>11</td>
<td>6</td>
<td>9</td>
<td>0.8274</td>
</tr>
<tr>
<td>12</td>
<td>6</td>
<td>10</td>
<td>0.7978</td>
</tr>
<tr>
<td>13</td>
<td>9</td>
<td>11</td>
<td>1.0000</td>
</tr>
<tr>
<td>14</td>
<td>9</td>
<td>10</td>
<td>0.8258</td>
</tr>
<tr>
<td>15</td>
<td>4</td>
<td>12</td>
<td>0.6981</td>
</tr>
<tr>
<td>16</td>
<td>12</td>
<td>13</td>
<td>0.3936</td>
</tr>
<tr>
<td>17</td>
<td>12</td>
<td>14</td>
<td>0.8398</td>
</tr>
<tr>
<td>18</td>
<td>12</td>
<td>15</td>
<td>0.7858</td>
</tr>
<tr>
<td>19</td>
<td>12</td>
<td>16</td>
<td>0.7711</td>
</tr>
<tr>
<td>20</td>
<td>14</td>
<td>15</td>
<td>0.8997</td>
</tr>
<tr>
<td>21</td>
<td>16</td>
<td>17</td>
<td>0.7749</td>
</tr>
<tr>
<td>22</td>
<td>15</td>
<td>18</td>
<td>0.4925</td>
</tr>
<tr>
<td>23</td>
<td>18</td>
<td>19</td>
<td>0.7017</td>
</tr>
<tr>
<td>24</td>
<td>19</td>
<td>20</td>
<td>0.8237</td>
</tr>
<tr>
<td>25</td>
<td>10</td>
<td>20</td>
<td>0.7498</td>
</tr>
<tr>
<td>26</td>
<td>10</td>
<td>17</td>
<td>0.7574</td>
</tr>
<tr>
<td>27</td>
<td>10</td>
<td>21</td>
<td>0.6094</td>
</tr>
<tr>
<td>28</td>
<td>10</td>
<td>22</td>
<td>0.6888</td>
</tr>
<tr>
<td>29</td>
<td>21</td>
<td>22</td>
<td>0.0022</td>
</tr>
<tr>
<td>30</td>
<td>15</td>
<td>23</td>
<td>0.2855</td>
</tr>
<tr>
<td>31</td>
<td>22</td>
<td>24</td>
<td>0.6774</td>
</tr>
<tr>
<td>32</td>
<td>23</td>
<td>24</td>
<td>0.8040</td>
</tr>
<tr>
<td>33</td>
<td>24</td>
<td>25</td>
<td>0.2740</td>
</tr>
<tr>
<td>34</td>
<td>25</td>
<td>26</td>
<td>0.7339</td>
</tr>
<tr>
<td>35</td>
<td>25</td>
<td>27</td>
<td>0.0100</td>
</tr>
<tr>
<td>36</td>
<td>28</td>
<td>27</td>
<td>0.5981</td>
</tr>
<tr>
<td>37</td>
<td>27</td>
<td>29</td>
<td>0.6016</td>
</tr>
<tr>
<td>38</td>
<td>27</td>
<td>30</td>
<td>0.5446</td>
</tr>
<tr>
<td>39</td>
<td>29</td>
<td>30</td>
<td>0.7670</td>
</tr>
<tr>
<td>40</td>
<td>8</td>
<td>28</td>
<td>0.6552</td>
</tr>
<tr>
<td>41</td>
<td>6</td>
<td>28</td>
<td>0.5203</td>
</tr>
</tbody>
</table>
Figure 4.4: A comparison of 11-line cuts as determined by the original and modified frontier models (using $e_{pi}$ weights).

Figure 4.5: A comparison of 14-line cuts as determined by the original and modified frontier models (using $e_{pi}$ weights).
Figure 4.6: OPA-v results summarizing line outage events and corresponding load shed quantities for 50,000 trials on a 30-bus network. The maximum load shed event is indicated in orange.

frontier cutsets – typically more than 70% being shared.

Notice in the 11-cut comparison performed above (see Figure 4.4) the two solutions differed by three lines. The original model included line numbers 5, 37, and 38 while the revised model found lines 8, 33, and 35 in their place. Table 4.2 reports the percentage that each of these lines occurred in the 100 OPA-v simulated worst case event. The three lines that are included in the revised frontier solution are selected much more often in the OPA-v simulations than those of the original frontier, with two of them occurring in 93% of simulations. These results support the claim that the revised frontier method – which considers line loadings – is a better predictor of lines that would be triggered in a cascade event. There is still cause to argue, however, that initiating events are more likely to be identified from the uniform weighting scenario. This aspect is more difficult to pinpoint and requires further assessment in a scenario more targeted for this feature. Beyond this, the commonalities between the vulnerability frontier cutsets and OPA-v cascading outage line predictions help validate the assessment of severe contingencies being preformed here.
Table 4.2: The percentage occurrence out of 100 50,000-trial OPA-v simulations for selected lines. Teal highlighting indicates lines in the modified frontier model (using $e_{pi}$ weights) whereas red indicates lines identified in the original frontier.

<table>
<thead>
<tr>
<th>Frontier Version</th>
<th>Line Number</th>
<th>% occurrence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Original</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Modified</td>
<td>8</td>
<td>78</td>
</tr>
<tr>
<td>Modified</td>
<td>33</td>
<td>93</td>
</tr>
<tr>
<td>Modified</td>
<td>35</td>
<td>93</td>
</tr>
<tr>
<td>Original</td>
<td>37</td>
<td>3</td>
</tr>
<tr>
<td>Original</td>
<td>38</td>
<td>4</td>
</tr>
</tbody>
</table>

4.3.1.2 Modified Frontier Under $e_{di}$

The modified frontier solution under $e_{di}$ from Equation 3.8 is provided in Figure 4.7. Though not compared explicitly in the proceeding tables and figures, the result is presented here to address a few relevant observations. This form of the modified model denotes edge weights based on the absolute distance from the power flow on a line to its maximum rating and contributes another deviation from the original results. The first obvious change comes from the maximum cut solution which requires 15 lines rather than 14 to disrupt the same amount of power. The 14-line event in this model disrupts only 125.7 MW. Though not visible in the curve, it was noted that a larger subset of lines were identified throughout this frontier than in the two other cases, it is clear that altering the edge weights generates less severe cuts, but may detect transmission lines reminiscent of those tripped in a cascade event.
4.3.2 Midwest Example I

It is necessary to move to a larger test system and observe if similar conclusions can be drawn regarding the identification of critical components in cascading outages. For this, the Midwest 7977-bus case will be utilized. Figure 4.8 presents vulnerability frontiers for a snapshot of the Midwest test case under three model formulations. The snapshot is taken from an operating point in late September with a total system load of 34,470 MW. Subfigures (b), (d), and (f) show small cut portions of (a), (c), and (e) respectively. The labels in Figures 4.8d and 4.8f declare the number of lines involved in several cuts since it is no longer plotted along the $x$-axis.

Considering all unique lines selected in cutsets along the frontiers in Figures 4.8a, 4.8c, and 4.8e, 880 are members of all three solution sets. In total, the original formulation finds 1152 lines, the modified formulation under $e_{pi}$ finds 1128, and the modified formulation under $e_{di}$ finds 1166 from the Midwest system with 11,693 total branches in service. The intersection of lines in each case are compared in Figure 4.9.

The large number of common lines is similar to what was seen in the 30-bus example and again, the differences lie in how the lines are organized along each frontier. Figures 4.8b, 4.8d, and 4.8f show this as different size cutsets form the boundary of the frontier for small cut scenarios.

A common 11-cut scenario exists between the modified model under $e_{pi}$ and the
Figure 4.8: A comparison of frontier results under different edge weighting scenarios for Midwest Example I.
original model solutions with 10 shared lines. The modified result appears to have selected an alternate line closer to its capacity limit (4.7% remaining rather than 12%). Similarly, a common 28-cut event shares 26 lines and the same trend can be observed where the modified model finds a superior optimum by exchanging two lines for alternatives with smaller edge weights (or ones that are more heavily loaded). It can also be seen that both modified frontiers find less severe cuts than the original when comparing those of a similar size outage event.

### 4.3.2.1 Extension To OPA-v Model

Using the OPA-v model, results can be simulated for the same operating point on the Midwest network. One example of this can be seen in Figure 4.10. Four large load shed events arose from this 10,000 trial OPA-v simulation. These can be labeled as Events A, B, C, and D and are depicted in Table 4.3.

**Table 4.3:** A summary of four large cascade events observed in Figure 4.10.

<table>
<thead>
<tr>
<th>Event</th>
<th>Number of Line Outages</th>
<th>Loadshed [MW]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event A</td>
<td>158</td>
<td>408</td>
</tr>
<tr>
<td>Event B</td>
<td>191</td>
<td>670</td>
</tr>
<tr>
<td>Event C</td>
<td>214</td>
<td>890</td>
</tr>
<tr>
<td>Event D</td>
<td>236</td>
<td>967</td>
</tr>
</tbody>
</table>
Figure 4.10: OPA-v results summarizing line outage events and corresponding load shed quantities for 10,000 trials on the Midwest network (Example I). The operating point is taken from a September evening.

An evaluation of the lines involved in each cascade event showed only five common lines between all four cascades. However, Events B, C, and D (the three larger cascades) shared 88 lines. This indicates some repetition in what events are causing the most severe disturbances. It follows to examine whether these solutions share any resemblance to lines involved in the vulnerability frontier cutsets.

Table 4.4 compares each cascade event to both the original (Figure 4.8a) and the modified versions (Figure 4.8c and 4.8e) of the vulnerability frontier. The comparison finds the intersection of lines in each cascade event and all unique lines contained in frontier cutsets. In each event, a larger quantity of lines are shared with the modified frontiers than those in the original. The significance of the quantity shared between any case and the OPA-v result will be addressed further in the next example. Note that under this operating point and power flow solution, nearly 80% of all lines are loaded at less than 25% of their total capacity.

This example highlights many similarities between solutions of the original and modified frontiers while also hinting at a slight correlation to OPA-v cascading outage results. One explanation for the close resemblance of frontier solutions despite
Table 4.4: A comparison of large cascade events to vulnerability frontier solutions in Midwest Example I.

<table>
<thead>
<tr>
<th>Event</th>
<th>Lines Shared With Original Frontier</th>
<th>% of Cascade Event</th>
<th>Lines Shared With Modified Frontier ((e_{pi}))</th>
<th>% of Cascade Event</th>
<th>Lines Shared With Modified Frontier ((e_{di}))</th>
<th>% of Cascade Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event A</td>
<td>26</td>
<td>16.5%</td>
<td>32</td>
<td>20.3%</td>
<td>37</td>
<td>23.4%</td>
</tr>
<tr>
<td>Event B</td>
<td>13</td>
<td>6.8%</td>
<td>24</td>
<td>12.6%</td>
<td>42</td>
<td>22%</td>
</tr>
<tr>
<td>Event C</td>
<td>15</td>
<td>7%</td>
<td>26</td>
<td>12.1%</td>
<td>45</td>
<td>21%</td>
</tr>
<tr>
<td>Event D</td>
<td>13</td>
<td>5.5%</td>
<td>21</td>
<td>8.9%</td>
<td>41</td>
<td>17.4%</td>
</tr>
</tbody>
</table>

Alternate formulations could be the loading level of this scenario. Since the system is relatively under-loaded, the impact of considering line weightings is small. The correlation to the OPA-v results may be stronger in a case that contains a higher system load. Furthermore, the two frontier solutions will likely be more distinct. Example II explores these claims.

4.3.3 Midwest Example II

The same procedure was followed for a July operating point with system load at 49,493 MW. This case along with other peak operating conditions in July provided similar trends to those in Example I. It was observed that even these scenarios kept lines flows and generator dispatches well below their capacity limits, providing only slight variations between the modified and original frontiers. To truly capture a heavily loaded case, the July snapshot was utilized with load scaled by 120% to achieve loading level near 60 GW. Due to shortfalls in the Midwest test system, this forced the results to be performed under DC power flow analysis rather than AC.

The vulnerability frontiers under this operating point are detailed in Figure 4.12. Subfigures (b), (d), and (f) show small cut portions of (a), (c), and (e), respectively. The labels in Figures 4.12d and 4.12f declare the number of lines involved in various cuts under the marginal weighting scenario for comparison to Figure 4.12b. The curves contain around 350 bounding solutions formed by different combinations of lines from a selection of 1152 (original), 1114 (modified \(e_{pi}\)), or 1183 (modified \(e_{di}\))
out of the total 11,693 that are in service. The intersection of lines in each case are compared in Figure 4.11.

\[ \text{Figure 4.11: Unique lines shared in Midwest Example II frontier solutions under the original and two modified models.} \]

This highly loaded example is interesting in its own right and two observations can be noted before moving on to OPA-v comparisons. First, the initial solution on the original frontier represents a 43-line outage event that disrupts 14,332 MW. The same size event is found in the modified frontier under $e_p$ weighting but disrupts slightly less power at 11,537 MW. This result is unique in that both sets of 43 lines are severe contingencies but have very little in common, only sharing two lines between them. Although the modified frontier identified a less severe 43-line outage in terms of immediate power imbalance, this is not to say the event will actually prove less disruptive. Moreover, the true amount of load shedding that might be required from such an event is unknown. It is known, however, that the modified frontier identified a line outage event with a selection of lines loaded closer to their maximum and may reflect a more dangerous cascading scenario. A similar comparison was made between the original frontier and modified frontier under $e_d$ for a 70-line cut where only six lines were shared. Again, the outage event was more severe on the original frontier, creating an imbalance of 19,759 MW as opposed to 13,236 on the modified frontier.

Second, both modified frontiers allow for a more in-depth analysis of minimum cut scenarios as they find several bounding contingencies smaller than the 43-line outage.
Figure 4.12: A comparison of frontier results under different edge weighting scenarios for Midwest Example II.
4.3.3.1 Extension To OPA-v Model

Cascading outages were simulated for the Midwest case under scaled July operating conditions following the OPA-v algorithm (see Figure 4.13). Four resulting large blackout events are detailed in Table 4.5 and compared to frontier solutions in Table 4.6.

![Figure 4.13](image)

**Figure 4.13**: OPA-v results summarizing line outage events and corresponding load shed quantities for 10,000 trials on the Midwest network (Example II). The operating point is taken from a July evening and with load scaled by 120%.

**Table 4.5**: A summary of four large cascade events observed in Figure 4.13.

<table>
<thead>
<tr>
<th>Number of Line Outages</th>
<th>Loadshed [MW]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event E</td>
<td>56</td>
</tr>
<tr>
<td>Event F</td>
<td>72</td>
</tr>
<tr>
<td>Event G</td>
<td>55</td>
</tr>
<tr>
<td>Event H</td>
<td>198</td>
</tr>
</tbody>
</table>

Despite seeing more distinct results from each frontier technique under increased system load (Figure 4.12), the correlation to OPA-v is not as strong as predicted under the modified frontier. Still, an argument can be made that these results are
Table 4.6: A comparison of large cascade events to vulnerability frontier solutions in Example II.

<table>
<thead>
<tr>
<th>Event</th>
<th>Lines Shared With Original Frontier</th>
<th>% of Cascade Event</th>
<th>Lines Shared With Modified Frontier ($e_{pi}$)</th>
<th>% of Cascade Event</th>
<th>Lines Shared With Modified Frontier ($e_{di}$)</th>
<th>% of Cascade Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event E</td>
<td>7</td>
<td>12.5%</td>
<td>6</td>
<td>10.7%</td>
<td>13</td>
<td>23.2%</td>
</tr>
<tr>
<td>Event F</td>
<td>25</td>
<td>34.7%</td>
<td>31</td>
<td>43.1%</td>
<td>35</td>
<td>48.6%</td>
</tr>
<tr>
<td>Event G</td>
<td>12</td>
<td>21.8%</td>
<td>17</td>
<td>30.9%</td>
<td>15</td>
<td>27.3%</td>
</tr>
<tr>
<td>Event H</td>
<td>38</td>
<td>19.2%</td>
<td>46</td>
<td>23.2%</td>
<td>54</td>
<td>27.3%</td>
</tr>
</tbody>
</table>

not random. The original and modified frontiers include a subset of 9.85%, 9.5%, and 10.1% of the total system branches, respectively. If the results could be explained by randomness, one would expect the same percentages of the OPA-v lines to fall in the subset of frontier solutions. Table 4.6 illustrates that Events F, G, and H share much larger portions of the OPA-v event lines than the ∼10% expected from a random result. The overlap with OPA-v is slightly greater under the modified frontier which might suggest this method is preferred when analyzing cascades. Note that this only holds true under elevated load levels as Example I did not provide the same outcome.

A chi-squared independence test can be applied to validate the statistical significance with null hypothesis, $H_0$, assuming no association between the frontier and OPA-v models. The alternate hypothesis $H_A$ assumes there is an association. Under the null hypothesis, randomness would explain any overlap and ∼10% is expected. The $\chi^2$ statistics are computed with the following formula:

$$\sum_i \frac{(E_i - O_i)^2}{E_i}.$$ 

Values for each event are presented in Table 4.7 and report all three models reject the null hypothesis in events F, G, and H.
Table 4.7: Chi-squared statistics for Midwest Example II.

<table>
<thead>
<tr>
<th>Event</th>
<th>$\chi^2$ (uniform)</th>
<th>$\chi^2$ (modified $e_{pi}$)</th>
<th>$\chi^2$ (modified $e_{di}$)</th>
<th>Hypothesis Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event E</td>
<td>0.4427</td>
<td>0.0960</td>
<td>10.61</td>
<td>uniform, modified $e_{pi}$ = fail to reject $H_0$; modified $e_{di}$ = reject $H_0$</td>
</tr>
<tr>
<td>Event F</td>
<td>50.16</td>
<td>94.30</td>
<td>117.60</td>
<td>reject $H_0$</td>
</tr>
<tr>
<td>Event G</td>
<td>8.87</td>
<td>29.32</td>
<td>17.86</td>
<td>reject $H_0$</td>
</tr>
<tr>
<td>Event H</td>
<td>19.46</td>
<td>43.43</td>
<td>64.31</td>
<td>reject $H_0$</td>
</tr>
</tbody>
</table>

4.3.4 Line Weighting Discussion

While investigating the original and modified model solutions, results found a trade-off in terms of pinpointing the most severe cuts verses identifying lines expected to perpetuate cascades. The original model is superior at locating the worst-case power disruptions, but less efficient at selecting lines that may trip in a cascade event. It is presumed, however, that the original model would better serve in identifying the random initiating events which precipitate cascading outages. Cross comparing each modified result under $e_{pi}$ and $e_{di}$ weights shows that the absolute distance formula finds more in common with the OPA-v cascade events.

The two line weighting formulas assessed in the preceding examples both reflect a marginal measurement of the remaining capacity on a given transmission line. Constructed as a percentage and an absolute distance measurement, there are instances where each choice fails to reflect the relevant features of a cascade. While both rank lines near their max rating as more likely to be cut, neither takes into account the relative loading level. As a result, lines with small and large capacity, if loaded near their respective maximums, will be treated the same. Moreover, it is also important to consider lines that simply transport a large quantity of power. One remedy to this could be the following weighting formula:

$$e_i = \frac{S_{\max} - S_0}{S_0},$$  \hspace{1cm} (4.1)

which computes the remaining margin and normalizes it to the absolute flow on that line, $S_0$. Evaluating the frontier using this variation, or improving upon it, represents
another topic for future study.

For the remainder of this report, examples typically rely on the original model as the basis for any discussion. When cases do include a modified frontier, however, only the percentage edge weights $e_{pi}$ from Equation 3.7 are considered.

4.3.5 Radial Lines

A few comments can be made regarding the consideration of radial lines in this analysis. Radial lines, or lines linked to buses with no other connection to the grid, are vulnerable by construction. No new information is gained by presenting them in solutions. These are obvious choices and some may wish to exclude them from analyses altogether. In the original frontier formulation, this is an easy task. Simply weighting radial lines heavily will ensure they do not appear in cutsets.

For the modified frontier with edge weights based on line loadings, this would require more work due to the setup of the optimization problem. Simply over-weighting the lines does not eliminate them from the frontier. This could be an area of future work, however, at this time it is not a priority as radial lines do not occur in high frequency in the solutions. For instance, the results in Figure 4.8 are made up of about 1100 different lines and only 105 of these are radial. The Midwest system is constructed with 1556 radial lines in total.

4.4 Results Part II: Crafted Scenarios

The Midwest network and accompanying yearly load profile is further probed in this section to evaluate the performance and effectiveness of the vulnerability frontier. Results from a series of examples are presented next.

A logical starting point for expanding this work lies first in analyzing the vulnerability frontier on a larger system and second in incorporating hourly load profiles. In this way, a basic understanding can be attained for how the frontier changes under varying load settings as well as under unplanned outages faced in the grid.

4.4.1 Vulnerability Frontier Over 12 Hours

It is interesting to observe the frontier and its characteristics with changes in load. In this example, an hourly load profile is used for a half-day in August. For
each frontier, an AC power flow solution is utilized to redispacth the generation. The expectation is that the curve will shift upwards and downwards with the total load. Recall the maximum point on the curve aims to bisect the network into two groups in which all generation is separated from load. This creates a power imbalance of the entire active power demand. The relevant differences worth exploring further will come from varying combinations of lines, cutsizes, and power disruption along the curves. Figure 4.14 presents these results.

![Diagram](image.png)

(a) Entire frontier  
(b) Small cuts within frontier

**Figure 4.14**: Vulnerability frontiers for the Midwest 7977-bus network with changing hourly load. Load profiles were chosen from an August day.

Overall, despite variations in the magnitude of power disruptions, the solutions change very little. Each curve contains between 1170 and 1194 lines combined into around 340 bounding contingencies. In total, the 12 curves share 1099 lines in the makeup of their cutsets. Furthermore, upon observing the smaller cutsets shown in Figure 4.15b, each operating point contains the exact same four smallest cuts.

In this uniform edge weights example, many identical solutions appear on each frontier. They are identical in that they select the same transmission lines for a given size outage – the only difference lies in the amount of power disrupted, which increases simply following the load pattern throughout a day. The 70-line outage events in Figure 4.15b are an example of this. See Table 4.8 for the related vulnerability metrics.
An important element restricting this analysis could be the lack of a unit commitment strategy. This could drastically change the power flow solution and in turn the frontier as it is directly related to the topology and power injections throughout the network. This example can be scrutinized further by applying the modified vulnerability frontier which considers line loadings in its selection process. The edge weightings based on percentage capacity available, $e_{pi}$, from Equation 3.7 are utilized.

Table 4.8: Vulnerability metrics computed for each scenario presented in Figure 4.14

<table>
<thead>
<tr>
<th>Time</th>
<th>System Load [MW]</th>
<th>Load Trend</th>
<th>Eqn 3.3</th>
<th>Eqn 3.5</th>
<th>Eqn 3.6</th>
</tr>
</thead>
<tbody>
<tr>
<td>1:00PM</td>
<td>43815</td>
<td>-</td>
<td>307.69</td>
<td>$3.09 \times 10^7$</td>
<td>$3.43 \times 10^6$</td>
</tr>
<tr>
<td>2:00PM</td>
<td>44800</td>
<td>↑</td>
<td>307.61</td>
<td>$3.19 \times 10^7$</td>
<td>$3.59 \times 10^6$</td>
</tr>
<tr>
<td>3:00PM</td>
<td>45350</td>
<td>↑</td>
<td>307.57</td>
<td>$3.25 \times 10^7$</td>
<td>$3.68 \times 10^6$</td>
</tr>
<tr>
<td>4:00PM</td>
<td>45603</td>
<td>↑</td>
<td>307.52</td>
<td>$3.27 \times 10^7$</td>
<td>$3.72 \times 10^6$</td>
</tr>
<tr>
<td>5:00PM</td>
<td>45654</td>
<td>↑</td>
<td>307.52</td>
<td>$3.28 \times 10^7$</td>
<td>$3.73 \times 10^6$</td>
</tr>
<tr>
<td>6:00PM</td>
<td>45268</td>
<td>↓</td>
<td>307.57</td>
<td>$3.23 \times 10^7$</td>
<td>$3.67 \times 10^6$</td>
</tr>
<tr>
<td>7:00PM</td>
<td>44414</td>
<td>↓</td>
<td>307.68</td>
<td>$3.12 \times 10^7$</td>
<td>$3.55 \times 10^6$</td>
</tr>
<tr>
<td>8:00PM</td>
<td>43090</td>
<td>↓</td>
<td>307.82</td>
<td>$2.97 \times 10^7$</td>
<td>$3.35 \times 10^6$</td>
</tr>
<tr>
<td>9:00PM</td>
<td>42309</td>
<td>↓</td>
<td>307.85</td>
<td>$2.91 \times 10^7$</td>
<td>$3.24 \times 10^6$</td>
</tr>
<tr>
<td>10:00PM</td>
<td>41076</td>
<td>↓</td>
<td>307.93</td>
<td>$2.79 \times 10^7$</td>
<td>$3.07 \times 10^6$</td>
</tr>
<tr>
<td>11:00PM</td>
<td>38636</td>
<td>↓</td>
<td>307.69</td>
<td>$2.62 \times 10^7$</td>
<td>$2.76 \times 10^6$</td>
</tr>
<tr>
<td>12:00AM</td>
<td>35892</td>
<td>↓</td>
<td>306.20</td>
<td>$2.72 \times 10^7$</td>
<td>$2.83 \times 10^6$</td>
</tr>
</tbody>
</table>

*Figure 4.15:* Modified vulnerability frontiers (under edge weights $e_{pi}$) for the Midwest 7977-bus network with changing hourly load. Load profiles were chosen from an August day.
As seen in Figure 4.15, the curves are not as redundant as in the original frontier solution. A few small cuts are shared among all solutions, but the curves diverge quickly and find varying size cutsets organized with different components. There exist some similarities to the previously solution, however. Each curve still identifies a quantity of about 10% of the total system branches and all 12 curves share 1039 lines. When comparing the elements identified in the original to the modified frontier, they also share a large proportion of identified lines at around 950. Vulnerability metrics for this case are presented in Table 4.9.

Table 4.9: Vulnerability metrics computed for each scenario presented in Figure 4.15

<table>
<thead>
<tr>
<th>Time</th>
<th>System Load [MW]</th>
<th>Load Trend</th>
<th>Eqn 3.3</th>
<th>Eqn 3.5</th>
<th>Eqn 3.6</th>
</tr>
</thead>
<tbody>
<tr>
<td>1:00PM</td>
<td>43815</td>
<td>-</td>
<td>1016.41</td>
<td>5.57x10^7</td>
<td>6.57x10^6</td>
</tr>
<tr>
<td>2:00PM</td>
<td>44800</td>
<td>↑</td>
<td>1020.14</td>
<td>5.79x10^7</td>
<td>6.58x10^6</td>
</tr>
<tr>
<td>3:00PM</td>
<td>45350</td>
<td>↑</td>
<td>1022.73</td>
<td>5.92x10^7</td>
<td>6.70x10^6</td>
</tr>
<tr>
<td>4:00PM</td>
<td>45603</td>
<td>↑</td>
<td>1020.99</td>
<td>5.98x10^7</td>
<td>6.79x10^6</td>
</tr>
<tr>
<td>5:00PM</td>
<td>45654</td>
<td>↑</td>
<td>1019.81</td>
<td>5.99x10^7</td>
<td>6.82x10^6</td>
</tr>
<tr>
<td>6:00PM</td>
<td>45268</td>
<td>↓</td>
<td>1022.12</td>
<td>5.89x10^7</td>
<td>6.73x10^6</td>
</tr>
<tr>
<td>7:00PM</td>
<td>44414</td>
<td>↓</td>
<td>1026.16</td>
<td>5.69x10^7</td>
<td>6.59x10^6</td>
</tr>
<tr>
<td>8:00PM</td>
<td>43090</td>
<td>↓</td>
<td>1022.09</td>
<td>5.38x10^7</td>
<td>6.58x10^6</td>
</tr>
<tr>
<td>9:00PM</td>
<td>42309</td>
<td>↓</td>
<td>1016.91</td>
<td>5.24x10^7</td>
<td>6.57x10^6</td>
</tr>
<tr>
<td>10:00PM</td>
<td>41076</td>
<td>↓</td>
<td>1018.81</td>
<td>5.01x10^7</td>
<td>6.57x10^6</td>
</tr>
<tr>
<td>11:00PM</td>
<td>38636</td>
<td>↓</td>
<td>1031.55</td>
<td>4.74x10^7</td>
<td>6.57x10^6</td>
</tr>
<tr>
<td>12:00AM</td>
<td>35892</td>
<td>↓</td>
<td>1031.56</td>
<td>4.98x10^7</td>
<td>6.49x10^6</td>
</tr>
</tbody>
</table>

This example illustrates that no matter which frontier formulation is used, a similar set of critical lines are identified. They key variations in cut size and line combinations are a result of the varying edge weights. The optimization will vary depending on these parameters and occasionally identify a different k-line outage as the most severe.

4.4.2 Vulnerability Metrics With Changing Load

This section examines the associated metrics for hourly solutions to the vulnerability frontier over two separate months. Though difficult to analyze extensively, several remarks can be made regarding general trends. For comparison, the total
system load at each hour for the months of January and July is shown in Figure 4.16.

**Figure 4.16**: Total system load plotted for each operating point in January (top) and July (bottom).

Figures 4.17, 4.18, and 4.19 present the monthly solutions for the Equation 3.3, 3.5, and 3.6 metrics, respectively. The figures are separated into subfigures by month and within each month, the metrics are computed under original and modified \( (e_{pi}) \) frontier models.

Beginning with Figure 4.17, recall that Equation 3.3 assesses reliability based on the initial slope of the frontier. Thus, if the smallest cut solution disrupts a large amount of power (steep initial slope) rather than gradually approaching the maximum power imbalance solution, this metric will increase sharply. The other two do not reflect the small cut solutions and initial curve shape as closely. The July results show larger variations in this regard than those of January. This could be due to the increased system load which caused a greater variation in worst-case
Figure 4.17: Equation 3.3 vulnerability metric for January and July hourly solutions.
Figure 4.18: Equation 3.5 vulnerability metric for January and July hourly solutions.
Figure 4.19: Equation 3.6 vulnerability metric for January and July hourly solutions.
small outage events. Though this will be scrutinized in future examples, it is worth mentioning that this metric often disagrees with trends seen with the other two. This may be of use when the initial slope or small cut vulnerability is valued higher than the shape of the entire curve when interpreting system reliability.

Figures 4.18 and 4.19 appear to follow load trends more closely. However, the instances where they differ show the frontier responding to conditions other than system load level. The metric described by Equation 3.5 aims to characterize both the power injections and topology of the network by computing the product $p^T L^\dagger p$. The Equation 3.6 summarizes reliability by identifying the maximum ratio of squared power imbalance to line outage size for the set of points on the frontier.

Unsurprisingly, the magnitude increases for the metrics in July scenarios over their respective pair in January. This can be explained due to the increase in load. Note that in the July case, AC OPF solutions are not attainable at every operating point. This explains subtle irregularities in the graphs as not every hour has a solution.

### 4.4.3 Seasonal Comparisons

Following the previous analysis of the frontier throughout a typical daily load sequence, it is interesting to observe seasonal changes as well. For this, snapshots from March, July, and December are called upon to reflect a low, high, and average load profile that might be seen throughout a year. This scenario will also be used to delve into what lines are involved in each respective small cut solution. Figure 4.20 shows these results and Table 4.10 examines the respective metrics.

<table>
<thead>
<tr>
<th></th>
<th>Equation 3.3</th>
<th>Equation 3.5</th>
<th>Equation 3.6</th>
</tr>
</thead>
<tbody>
<tr>
<td>March</td>
<td>295</td>
<td>$2.34 \times 10^7$</td>
<td>$2.21 \times 10^6$</td>
</tr>
<tr>
<td>July</td>
<td>279</td>
<td>$3.51 \times 10^7$</td>
<td>$4.41 \times 10^6$</td>
</tr>
<tr>
<td>December</td>
<td>273</td>
<td>$3.02 \times 10^7$</td>
<td>$2.82 \times 10^6$</td>
</tr>
</tbody>
</table>

In contrast to the 12-hour example, this seasonal comparison shows a greater variety of distinct small-cut solutions that bound each frontier (see Figure 4.20b).
Figure 4.20: Vulnerability frontier for the Midwest 7977-bus network under three different load profiles.

Table 4.11 examines lines in the first cut for each frontier.

Table 4.11: A comparison of the smallest cut on each frontier. The lines in each respective cutset are presented along with the percentage occurrence of each line in the complete set of points in the frontier.

<table>
<thead>
<tr>
<th>March</th>
<th>July</th>
<th>December</th>
</tr>
</thead>
<tbody>
<tr>
<td>Line Number</td>
<td>%</td>
<td>Line Number</td>
</tr>
<tr>
<td>312</td>
<td>77</td>
<td>312</td>
</tr>
<tr>
<td>314</td>
<td>40</td>
<td>316</td>
</tr>
<tr>
<td>316</td>
<td>92</td>
<td>317</td>
</tr>
<tr>
<td>317</td>
<td>92</td>
<td>318</td>
</tr>
<tr>
<td>318</td>
<td>71</td>
<td>319</td>
</tr>
<tr>
<td>319</td>
<td>71</td>
<td>320</td>
</tr>
<tr>
<td>320</td>
<td>71</td>
<td>321</td>
</tr>
<tr>
<td>321</td>
<td>71</td>
<td><strong>322</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Lines involved in the first cut solution appear heavily throughout the remainder of the frontier. This has been observed consistently among the scenarios under investigation and provides justification for focusing on the small cut results in this
report. Lines which do not appear frequently in their frontier are highlighted in the table. Despite heavy repetition of the other lines in their respective frontier and multitude of common lines shared between the seasonal results, the inclusion of these components illustrates the uniqueness of the chosen worst-case line outage. This suggests the frontier method is identifying intelligent combinations of lines to which the system is most vulnerable.

A few final remarks can be made about the frontier results in this scenario. As usual, approximately 10% of total lines in the system appear throughout frontier solutions. Within the lines in the frontier, only 10% of this reduced subset are radial lines. Notably, none of the lines in the first cutsets presented in Table 4.10 are radial.

4.4.4 Unplanned Outages

The performance of the frontier under various generation and transmission outage events is key to our understanding of network reliability and the effectiveness of this technique in characterizing it. The following examples will show the response of the frontier to unplanned component outages. In this case, unplanned implies that the contingencies are unexpected and thus the grid will not be able to redispatch to a new optimum. Instead, a sub-optimal power flow solution is assumed and simulated.

4.4.4.1 Generator Outages

Consider a frontier solution from an August snapshot with system load of 44,414 MW. To simulate an unplanned generation outage expected to cause a sizable disturbance, we will assume the ten generators supplying the greatest magnitude of power under this operating point go offline. This effectively shuts down five powerplants completely and half of the generators at three additional plants. The resulting scenario will be referred to as outage Event I. Although this may be unrealistic, the goal is to show the system response and evaluate the performance of the frontier technique under such a scenario. Since it is unplanned, instead of redispatching the generation using an economic dispatch or OPF solver, the lost generation will be picked up equally by the remaining generators whose capacity will allow it. Figure 4.21 illustrates the results of this scenario where nearly 14% of total generation was redispached sub-optimally.
It is important to note that since no load is being shed, it is not expected that the curve should shift a great distance. Smaller changes such as altered curvature along the trajectory to the maximum power imbalance point or variations in the cutsets (including their size and selected lines) are anticipated.

**Figure 4.21**: Vulnerability frontier under unplanned generator outage Event I.

Figure 4.21b reflects some of the subtle changes that were predicted. Although some initial cuts went unchanged, the system appears to have grown more vulnerable. This is seen as the Event I solution finds similar size cutsets that provide a greater power imbalance due to the shift in generation and flow patterns. The system was forced to call on generators that were not as well-connected to the grid and likely more expensive.

Further exploration in this scenario involves looking at the original solution to aid in the selection of generators to decommit. The first cut on the frontier corresponds to 13 transmission lines. Several of these lines connect to three major power plants. Rather than turning off the largest generation sources as in Event I, Event II turns off all generators at the three power plants identified by the existing frontier solution. This corresponds to a loss of about 13% of supply which will again be redistributed equally to the remaining generators. It is important to note that the generators selected in Event II represent an entirely different set than those of Event I. This implies the frontier is not simply selecting lines connected to the largest generators.
as the most critical elements.

Figure 4.22: Vulnerability frontier under unplanned generator outage event II.

Figure 4.22 displays outage Event II alongside the previous cases. Under this generation outage, the curve shrinks and earlier cuts are less vulnerable than before. A possible explanation for this response is that by selecting generators based on existing frontier solutions – meaning they were deemed vulnerable to begin with – we may have removed a source of vulnerability. The generation sources that were supplying power on the critical lines are now out of service. In this case the resulting network is more secure. Certainly, there exist examples that do just the opposite, however, it is reasonable to assume the frontier is reacting effectively.

Table 4.12: Associated vulnerability metrics computed for each scenario presented in Figure 4.22.

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Equation 3.3</th>
<th>Equation 3.5</th>
<th>Equation 3.6</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Outages</td>
<td>308</td>
<td>3.12x10^7</td>
<td>3.55x10^6</td>
</tr>
<tr>
<td>Outage Event I</td>
<td>322</td>
<td>3.69x10^7</td>
<td>3.64x10^6</td>
</tr>
<tr>
<td>Outage Event II</td>
<td>266</td>
<td>2.93x10^7</td>
<td>3.15x10^6</td>
</tr>
</tbody>
</table>

The metrics presented in Table 4.12 suggest that Outage Event I created the most vulnerable network while outage Event II produced the least. Under the modified
vulnerability frontier technique, similar results are obtained and are left out to avoid redundancy.

4.4.4.2 Transmission Line Outages

Moving on to transmission outages, the loss of lines can be implemented and impacts on the frontier observed. Outage Event III includes six transmission lines removed from service. These were selected from the original frontier solution. Specifically, the six lines are all elements of the first cutset. See Figure 4.23 for this result.

![Vulnerability frontier under unplanned transmission outage Event III.](image)

(a) Entire frontier
(b) Small cuts within frontier

**Figure 4.23**: Vulnerability frontier under unplanned transmission outage Event III.

Another selection of lines could come from those that are heavily loaded under the base operating conditions. Removing six of these lines depicts outage Event IV.

Figures 4.23 and 4.24 show slight variations in response to the loss of transmission lines. The accompanying vulnerability metrics are expressed in Table 4.13. Aside from the Equation 3.3 calculation under outage Event III, the remaining metrics show subtle changes to reflect the minimally altered network. Outage Event III caused the largest disruption and appears as the most vulnerable case. This large change in Equation 3.3 is not surprising given the shape of the frontier. Recall this metric is a measure of the initial slope of the frontier which increases sharply under the outage event of interest.

The synthetic Midwest test system proved over-constrained when testing for line outages. The system often fails to find power flow solutions when removing more
than a few lines. This could be a caveat of the network construction, as a system of over 11,000 lines is not likely to be unsolvable with a contingency event of only a few components. This is not to overlook cases in which certain critical contingency events will cause instability and it should be noted that the frontier method successfully identified a large number of those.

4.4.5 Variable Generation Patterns

The Midwest test system contains a fair share of renewable generation in the form of wind energy. The base model has generation fleet with nearly 9% of its capacity coming from wind farms, though transmission line constraints limit a non-trivial portion of this from being distributed to load centers. Still, this presents an opportunity to evaluate system reliability with and without high concentrations of wind generation present.

To begin, the frontier was computed for a July operating point with total system
load at 49,553 MW. This will act as the base case to be compared against two alternate scenarios. First, after evaluating transmission line capabilities, it was decided to increase the wind by more than 300% from its base contribution. Following the examples in the previous section, it is assumed this drastic influx of wind is unplanned. As a result, only natural gas power plants are asked to reduce supply. It is also useful to pair this with a scenario where it is no longer windy. Thus, the final case will remove all wind generation and call on natural gas spinning reserves to make up the lost supply.

This system in particular is interesting due to the large proportion of wind power produced in Iowa. Table 4.14 details each of these three cases and where the wind is produced. An unequal distribution of the wind resource along with known transmission limitations in the midwest grid led to the decision to study this case under the original and modified models. The edge weights determined by \( e_p \) (Equation 3.7) are utilized with aims of capturing some of these features.

**Table 4.14**: Wind generation dispatch by state for three different scenarios.

<table>
<thead>
<tr>
<th>Wind Dispatch [MW]</th>
<th>Illinois</th>
<th>Iowa</th>
<th>Minnesota</th>
<th>Wisconsin</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Case</td>
<td>318</td>
<td>940</td>
<td>683</td>
<td>129</td>
<td>2070</td>
</tr>
<tr>
<td>Increased Wind</td>
<td>1357</td>
<td>3084</td>
<td>1712</td>
<td>446</td>
<td>6599</td>
</tr>
<tr>
<td>No Wind</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Beginning with frontier results under the original formulation presented in Figures 4.25a and 4.25b, several observations can be made. The increased wind scenario showed the largest shift to a more vulnerable state. This is reflected in the shape of the curve as well as in the metrics in Table 4.15. The case with no wind generation altered the curve only slightly when compared to the base case. One possible interpretation could be that the no wind scenario called solely on natural gas generators, which are well-distributed in and well-connected to the grid, to adjust their output. In contrast, the high wind case saw more drastic shifts in the dispatch pattern calling
on fewer generators to increase supply in areas that were already congested. Table 4.16 presents the small cut solutions for the high and low wind cases on the original frontiers demonstrating that for similar size line outages, the high wind scenario proves more severe.

Next, the modified frontiers (Figures 4.25c and 4.25d) can be discussed. This case is especially relevant for investigation under the formulation considering line weights due to current transmission problems in the Midwest network. This issue is more pronounced when looking at transmission output from renewable generators. Furthermore, large concentrations of wind power produced in Iowa and Minnesota are
Table 4.15: Associated vulnerability metrics computed for each scenario presented in Figure 4.25.

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Original Frontier</th>
<th>Modified Frontier ($e_{pi}$ weights)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Equation 3.3</td>
<td>Equation 3.5</td>
</tr>
<tr>
<td>Base Case</td>
<td>307</td>
<td>3.87$x10^7$</td>
</tr>
<tr>
<td>Increased Wind</td>
<td>321</td>
<td>4.73$x10^7$</td>
</tr>
<tr>
<td>No Wind</td>
<td>320</td>
<td>3.98$x10^7$</td>
</tr>
<tr>
<td></td>
<td>993</td>
<td>7.26$x10^7$</td>
</tr>
<tr>
<td>Increased Wind</td>
<td>16851</td>
<td>1.24$x10^8$</td>
</tr>
<tr>
<td>No Wind</td>
<td>1137</td>
<td>7.70$x10^7$</td>
</tr>
</tbody>
</table>

Table 4.16: Small cut solutions on the frontiers (original model) for increased wind and no wind cases. Identical size cut solutions are highlighted for comparison.

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Increased Wind Case</th>
<th>No Wind Case</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td># Lines Cut</td>
<td>Power Imbalance [MW]</td>
</tr>
<tr>
<td></td>
<td>42</td>
<td>13486</td>
</tr>
<tr>
<td></td>
<td>44</td>
<td>14013</td>
</tr>
<tr>
<td></td>
<td>45</td>
<td>14205</td>
</tr>
<tr>
<td><strong>69</strong></td>
<td><strong>18373</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>72</td>
<td>18865</td>
</tr>
<tr>
<td></td>
<td>73</td>
<td>19014</td>
</tr>
<tr>
<td></td>
<td>77</td>
<td>19532</td>
</tr>
<tr>
<td><strong>82</strong></td>
<td><strong>20163</strong></td>
<td></td>
</tr>
<tr>
<td><strong>90</strong></td>
<td><strong>21123</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>97</td>
<td>21936</td>
</tr>
<tr>
<td></td>
<td>100</td>
<td>22259</td>
</tr>
<tr>
<td></td>
<td>95</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

causing significant congestion on existing lines. This effect is reflected in the results.

Increasing wind generation led to a limited number of transmission lines becoming more heavily loaded. Under the modified frontier model, this produced very distinct subsets of lines in the small cutsets when comparing across wind and no wind scenarios. This is unique in that many of the past examples showed only small changes in
cutsets regardless of the operating point or outage event status. Comparing the next two tables will help illustrate this effect.

**Table 4.17**: Lines included in small cut frontier solutions (modified model) under the increased wind scenario. Highlighted buses indicate those which are connected to generators and the cutset column specifies of which cuts each line is a member.

<table>
<thead>
<tr>
<th>Line #</th>
<th>From Bus</th>
<th>To Bus</th>
<th>Generation Type</th>
<th>State</th>
<th>Cutset</th>
</tr>
</thead>
<tbody>
<tr>
<td>259</td>
<td>63</td>
<td>768</td>
<td>Wind</td>
<td>IA</td>
<td>13</td>
</tr>
<tr>
<td>267</td>
<td>66</td>
<td>511</td>
<td>Wind</td>
<td>IA</td>
<td>13</td>
</tr>
<tr>
<td>676</td>
<td>147</td>
<td>3574</td>
<td>Wind</td>
<td>IL</td>
<td>1,3,5,6,7,10,11,13</td>
</tr>
<tr>
<td>814</td>
<td>186</td>
<td>212</td>
<td>NG (186)/Wind (212)</td>
<td>MN</td>
<td>7,10,11,13</td>
</tr>
<tr>
<td>898</td>
<td>202</td>
<td>252</td>
<td>Wind</td>
<td>MN</td>
<td>10,11,13</td>
</tr>
<tr>
<td>899</td>
<td>202</td>
<td>252</td>
<td>Wind</td>
<td>MN</td>
<td>10,11,13</td>
</tr>
<tr>
<td>901</td>
<td>203</td>
<td>513</td>
<td>Wind</td>
<td>MN</td>
<td>5,6,7,10,11,13</td>
</tr>
<tr>
<td>914</td>
<td>207</td>
<td>5352</td>
<td>Wind</td>
<td>MN</td>
<td>10,11,13</td>
</tr>
<tr>
<td>917</td>
<td>209</td>
<td>228</td>
<td>Wind</td>
<td>MN</td>
<td>6,7,10,11,13</td>
</tr>
<tr>
<td>920</td>
<td>211</td>
<td>4860</td>
<td>Wind</td>
<td>MN</td>
<td>3,5,6,7,10,11,13</td>
</tr>
<tr>
<td>930</td>
<td>216</td>
<td>4441</td>
<td>Wind</td>
<td>MN</td>
<td>3,5,6,7,10,11,13</td>
</tr>
<tr>
<td>935</td>
<td>218</td>
<td>4934</td>
<td>Wind</td>
<td>MN</td>
<td>11,13</td>
</tr>
<tr>
<td>1013</td>
<td>255</td>
<td>4308</td>
<td>Wind</td>
<td>MN</td>
<td>5,6,7,10,11,13</td>
</tr>
</tbody>
</table>

Under elevated wind generation, the set of critical lines in Table 4.17 are all connected to wind generators. The set of lines in Table 4.18 are less significant in that they deviate little from past examples and do not isolate wind generators. For the next set of observations, it is beneficial to look closer at the small cut solutions in the modified frontier. Figure 4.26 and Table 4.19 compile the results.

A larger number of small cut solutions were identified in the increased wind case, however, in general this method identified less severe cuts. Although the increased wind frontier in Figure 4.26 looks most severe, Table 4.19 tells a different story. Recall that when identifying small cut solutions, the method is weighted towards minimizing the sum of the edge weights rather than maximizing power imbalance. For this reason, several small cut solutions appear with lines approaching their load limits but power disruptions less extreme. In the no wind case, the transmission lines are under-loaded and thus a different 13-line outage event was identified with much more significant
Table 4.18: Lines included in small cut frontier solutions (modified model) under the no wind scenario. Highlighted buses indicate those which are connected to generators and the cutset column specifies of which cuts each line is a member.

<table>
<thead>
<tr>
<th>Line #</th>
<th>From Bus</th>
<th>To Bus</th>
<th>Generation Type</th>
<th>State</th>
<th>Cutset</th>
</tr>
</thead>
<tbody>
<tr>
<td>312</td>
<td>83</td>
<td>2830</td>
<td>Nuclear</td>
<td>IL</td>
<td>13</td>
</tr>
<tr>
<td>316</td>
<td>83</td>
<td>3999</td>
<td>Nuclear</td>
<td>IL</td>
<td>13</td>
</tr>
<tr>
<td>317</td>
<td>83</td>
<td>4000</td>
<td>Nuclear</td>
<td>IL</td>
<td>13</td>
</tr>
<tr>
<td>318</td>
<td>83</td>
<td>6722</td>
<td>Nuclear</td>
<td>IL</td>
<td>13</td>
</tr>
<tr>
<td>319</td>
<td>83</td>
<td>6722</td>
<td>Nuclear</td>
<td>IL</td>
<td>13</td>
</tr>
<tr>
<td>320</td>
<td>83</td>
<td>6722</td>
<td>Nuclear</td>
<td>IL</td>
<td>13</td>
</tr>
<tr>
<td>321</td>
<td>83</td>
<td>6722</td>
<td>Nuclear</td>
<td>IL</td>
<td>13</td>
</tr>
<tr>
<td>322</td>
<td>84</td>
<td>86</td>
<td>Nuclear</td>
<td>IL</td>
<td>13</td>
</tr>
<tr>
<td>360</td>
<td>89</td>
<td>3957</td>
<td>NG</td>
<td>IL</td>
<td>4,13</td>
</tr>
<tr>
<td>362</td>
<td>89</td>
<td>6733</td>
<td>NG</td>
<td>IL</td>
<td>4,13</td>
</tr>
<tr>
<td>363</td>
<td>89</td>
<td>6733</td>
<td>NG</td>
<td>IL</td>
<td>4,13</td>
</tr>
<tr>
<td>662</td>
<td>143</td>
<td>3967</td>
<td>NG</td>
<td>IL</td>
<td>13</td>
</tr>
<tr>
<td>6678</td>
<td>3971</td>
<td>4003</td>
<td></td>
<td></td>
<td>4</td>
</tr>
<tr>
<td>10334</td>
<td>6728</td>
<td>6733</td>
<td></td>
<td></td>
<td>13</td>
</tr>
</tbody>
</table>

Figure 4.26: Small cut solutions to the modified vulnerability frontier presented in Figures 4.25c and 4.25d.
Table 4.19: Small cut solutions on the frontiers for increased wind and no wind cases under modified edge weightings, \( e_p \). Identical size cut solutions are highlighted for comparison.

<table>
<thead>
<tr>
<th># Lines Cut</th>
<th>Power Imbalance [MW]</th>
<th># of Lines Cut</th>
<th>Power Imbalance [MW]</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>169</td>
<td>4</td>
<td>1034</td>
</tr>
<tr>
<td>3</td>
<td>453</td>
<td>13</td>
<td>4158</td>
</tr>
<tr>
<td>5</td>
<td>681</td>
<td>21</td>
<td>6370</td>
</tr>
<tr>
<td>6</td>
<td>777</td>
<td>22</td>
<td>6420</td>
</tr>
<tr>
<td>7</td>
<td>868</td>
<td>27</td>
<td>7511</td>
</tr>
<tr>
<td>10</td>
<td>1106</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>1184</td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>1340</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>1476</td>
<td></td>
<td></td>
</tr>
<tr>
<td>28</td>
<td>5257</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Power imbalance. In this way, the two methods disagree in what they suggest as the most vulnerable system. However, each method can be useful in different settings.

The small cut scenarios found only under the modified formulation are of interest and still disrupt significant amounts of power. Additionally, nearly all of the lines making up the first several cutsets in the increased wind case are connected to wind generators in Minnesota. This may suggest a critical corridor that presents itself when renewable generation is especially high. This example shows consistency in the model in its response to different circumstances faced in the grid.

4.4.6 Model Consistency Remarks

Throughout this analysis, several instances occurred where consistencies in the model were observed despite shortfalls in the Midwest test case itself. Depending on the operating point, the frontier occasionally identified single contingency events, which, when removed, prevented the system from converging to an AC or DC power flow solution. Some of the lines involved in small cut solutions or those that appeared frequently in the entire frontier also led to system instabilities. Thus, the frontier was able to successfully detect critical contingencies in a model that fails to be N-1 secure. Note that none of these were radial lines. In an attempt to validate this
further, simulations of the OPA-v model were compiled with and without the critical lines removed. It was observed that the quantity and magnitude of large cascades increased when these lines were out of service in some simulations. However, this was not seen often enough to report any conclusive evidence.
CHAPTER 5
CONCLUSIONS AND PROPOSED
FUTURE WORK

5.1 Summary

In the absence of any modeling or simulation restrictions, one could imagine a technique which considers all internal dynamics, nonlinear behavior, and complex interactions within the electric grid. A more complete model could also include representations of hidden failures, human error, or operator decision-making criteria. Without computational barriers or in the presence of quantum computers, every possible contingency could be evaluated and neutralized in advance. However, the present computing and modeling capabilities are limited in what can be done. Simplified and analytically tractable techniques like the OPA cascading outage model or the vulnerability frontier must be analyzed, altered, and improved to better serve in severe event detection.

The vulnerability frontier provides a worse case analysis of contingency events, forming a boundary relating the most severe power disruption as a function of the number of lines removed from service. Relying on a graph partitioning algorithm, this approach helps evaluate power system weaknesses and reliability. While existing contingency analysis tools require a selection of user-specified events to evaluate (typically a small subset of the total possible combinations for multiple component outages), the vulnerability frontier analyzes worst-case events from the entire collection of components. Detailed in this report is a study of the frontier on a 7977-bus synthetic test system. In addition, the model was amended to consider line loadings in its selection process with the aim of better representing the specific class of cascading outage events. The key outcomes and proposals of future work are detailed below.
5.2 Main Findings

The case studies and comparisons performed in this report illustrate the versatility and effectiveness of the frontier technique. First and foremost, it should be noted that the frontier reduced the number of lines to consider to approximately 10% of the total number of branches in the Midwest network. A variety of smaller line outage events can be obtained from the original or modified frontier formulations. These reduced subsets could be of use in existing software used by ISOs and utilities for NERC compliance studies. They offer an intelligent selection of contingencies which can be exhaustively analyzed with more comprehensive modeling tools.

The frontier responded to generator and transmission line outages in a reasonable manner, with metrics suggesting the model is capable of performing system-wide reliability assessments. The renewable generation cases were especially promising, demonstrating the unique critical corridors or areas of increased vulnerability that may present themselves when variable generation spikes. The modified frontier under this scenario also amplified some of the known transmission problems present in the Midwest network.

The three metrics proposed help to characterize the behavior seen in the frontier. Depending on the nature of an assessment, an individual may favor one metric over the others in an attempt to quantify and capture reliability with a single number. For instance, the metric depicted by the initial slope of the frontier (Equation 3.3) provides a representation of the severity of a small cut solution. On the other hand, the metric in Equation 3.5 considers network topology as well as power injections, but will not reflect the severity of small line outage events as precisely.

The addition of a marginal weighting element to the model helped detect an increased number of transmission lines that tripped in OPA-v events. Though the improvements were subtle, modified frontier results provide confidence in this direction for investigating the specific class of cascading outage events. Several test scenarios suggest the revised model is also more relevant in assessing heavily loaded cases. However, the marginal frontiers are not as efficient at identifying the most severe contingencies. Marginal weights were proposed both as a percentage and an absolute distance, but it was observed that neither formulation is sufficient to capture
all of the features of interest. In the current state, any line with power flow near its limit will be given a small edge weight – increasing its likelihood to be cut. This does not consider the relative loading factor or that we may be interested in lines that simply have a large amount of flow, regardless of their maximum rating. Generally, correlations between critical lines in any of the frontier models and the OPA-v results further validate the line selection in the vulnerability frontier.

5.3 Future Work

Based on the model developments and case study results, several areas of future work have emerged. The implementation of a unit commitment strategy is perhaps the most important feature that is lacking in this research. It was shown that the frontier effectively responds to changes in generation dispatch and one could deduce this would remain consistent with any committing or de-committing of generators. Still, adding this element and re-examining results may further validate the technique and identify new areas to improve model robustness. This addition may also aid in comparing each of the vulnerability frontier techniques and their application towards cascading outage events in particular.

Several of the case studies produced frontiers in which the first bounding solution contains a large number of lines. Smaller cut outages were left out as they were not severe enough to shift the boundary. Identifying these smaller cut solutions is still important, however, and new ways of deriving them should be considered. Additionally, there is room to explore model revisions that shift the focus to cascading outages and their triggering events in particular. To this effect, a sensitivity analysis on the tuning parameter $K$ in the OPA-v model is necessary along with improvements in the way transmission lines are weighted in the model. The proposed edge weighting formula in Equation 4.1, serves as a starting point for future analyses.

Although the Midwest network used in the majority of the analysis is a fairly realistic system with varied generation fleet, some shortfalls were identified. The system behaved poorly under modifications of operating points, decommissioning of generators, or removals of transmission lines. It was also difficult to attain heavily loaded operating points. Thus, continuing work on an alternate network model that
can withstand larger outages and increased load levels is recommended.

Applying this method to a real system model with historical data would also prove beneficial. Utilizing real data would offer opportunities to verify if the metrics and component selection processes are capable of detecting amplified vulnerability levels before blackouts or severe events.
REFERENCES


