How to Think About Resilient Infrastructure Systems

by

Daniel A. Eisenberg

A Dissertation Presented in Partial Fulfillment
of the Requirements for the Degree
Doctor of Philosophy

Approved December 2017 by the
Graduate Supervisory Committee:

Thomas Seager, Co-Chair
Jeryang Park, Co-Chair
David Alderson
Ying-Cheng Lai

ARIZONA STATE UNIVERSITY

May 2018

ABSTRACT

Resilience is emerging as the preferred way to improve the protection of infrastructure systems beyond established risk management practices. Massive damages experienced during tragedies like Hurricane Katrina showed that risk analysis is incapable to prevent unforeseen infrastructure failures and shifted expert focus towards resilience to absorb and recover from adverse events. Recent, exponential growth in research is now producing consensus on how to think about infrastructure resilience centered on definitions and models from influential organizations like the US National Academy of Sciences. Despite widespread efforts, massive infrastructure failures in 2017 demonstrate that resilience is still not working, raising the question: Are the ways people think about resilience producing resilient infrastructure systems?

This dissertation argues that established thinking harbors misconceptions about infrastructure systems that diminish attempts to improve their resilience. Widespread efforts based on the current canon focus on improving data analytics, establishing resilience goals, reducing failure probabilities, and measuring cascading losses. Unfortunately, none of these pursuits change the resilience of an infrastructure system, because none of them result in knowledge about how data is used, goals are set, or failures occur. Through the examination of each misconception, this dissertation results in practical, new approaches for infrastructure systems to respond to unforeseen failures via sensing, adapting, and anticipating processes. Specifically, infrastructure resilience is improved by sensing when data analytics include the modeler-in-the-loop, adapting to stress contexts by switching between multiple resilience strategies, and anticipating crisis coordination activities prior to experiencing a failure.

Overall, results demonstrate that current resilience thinking needs to change because it does not differentiate resilience from risk. The majority of research thinks resilience is a property that a system has, like a noun, when resilience is really an action a system does, like a verb. Treating resilience as a noun only strengthens commitment to risk-based practices that do not protect infrastructure from unknown events. Instead, switching to thinking about resilience as a verb overcomes prevalent misconceptions about data, goals, systems, and failures, and may bring a necessary, radical change to the way infrastructure is protected in the future.

DEDICATION

For those who keep us safe when we are in darkness.

For those who keep my life bright.

For my family.

ACKNOWLEDGMENTS

Prior to starting my Ph.D., I only cared about the degree as a means of advancement. I both admired the work of research professionals and yearned to be one, and a Ph.D. was a necessary step in realizing my future. Culminating my degree, I can finally appreciate the wisdom that a Ph.D. imparts. I am grateful for being able to add three letters to my name because the letters represent so much more than a title. It represents the people, relationships, and experiences that embraced and guided me throughout the last four and a half years. I am forever indebted to my friends, colleagues, and mentors who shaped my Ph.D., and I will always be thankful. If I am successful in reaching my goals in the future, it will not be because of the status conferred by a piece of paper, but from the way in which each of you changed my life. I am only a reflection of the people who surround me, and I am remarkably lucky to be a part of such a wonderful community.

I further acknowledge my Ph.D. committee for making my degree possible through mentorship, guidance, and support. Dr. Thomas Seager, in particular, has been an essential figure in my development. Tom, more than any other, fostered my endeavors by offering freedom to pursue new plans, ideas, and journeys and direction to overcome the inevitable trials faced as an academic. Because Tom was so willing and encouraging, I was able to travel, work under the guidance of other experts, and focus my dissertation on a topic I deeply cared about. I am equally grateful to Dr. Jeryang Park for welcoming me into his research group in South Korea, supporting me as one of your own students, and making this work possible. Dr. Alderson for offering external mentorship and support that has grown into one of my strongest professional relationships. And Dr. Lai sharing so many ideas and collaborations that have accelerated my thinking and my professional standing in research. Thank you all for your dedication to my growth as an individual.

The work in this dissertation is supported by the National Science Foundation (grant # 1311230, 1441352, and 1415060), the National Research Foundation of Korea (NRF-2016R1C1B1011770), and the Defense Threat Reduction Agency (DTRA-18681-M-FY17). Any opinions, findings and conclusions or recommendations expressed in this material are those of the author and do not necessarily reflect those of NSF, NRF, or DTRA.

TABLE OF CONTENTS

CHAPTER Page

CHAPTER Page

APPENDIX

LIST OF TABLES

Table Page

LIST OF FIGURES

Figure Page

CHAPTER 1

INTRODUCTION

Resilience is emerging as the preferred way for governments and academics to advance the protection of infrastructure systems beyond established risk management practices. Risk management centers on using risk analysis to identify the potential events that threaten infrastructure, the likelihood that threatening events may cause damages, and the resulting consequences of these damages to make decisions [1]. Past catastrophes like Hurricane Katrina (2005) and Superstorm Sandy (2012) which risk analysis deemed either too unlikely or too costly to consider led national and international organizations to reevaluate risk-based approaches for managing infrastructure failures. Experts found risk analysis ineffective to guide decisions that prevent unknown and unforeseen events, and shifted to endorsing infrastructure resilience to withstand surprising losses and quickly recover from catastrophe [2]. Growing efforts to promote resilience by government agencies sparked recent, exponential growth in resilience research by academic institutions to support lofty goals for a safer future [3]–[5]. Now a steady stream of research is promoting resilience-based catastrophe management and searching for ways to improve infrastructure protection [4], [6].

The vast majority of resilient infrastructure research hinges on few common definitions and illustrative models to advance resilience-based design, operations, and management. Influential organizations such as the Office of the President of the United States [7], [8], the US National Academies of Science (NAS) [9], and the United Nations International Strategy for Disaster Reduction [10] all have working definitions of resilience that guide infrastructure resilience research and applied practice. Although each uses different terminology, all emphasize improving the ways built systems respond to failures, exemplified by the NAS defining resilience as, “the ability to plan and prepare for, absorb, recover from, and adapt to adverse events,” [9]. A common model found across academic literature, *the critical functionality curve* (e.g., Fig. 1), operationalizes these influential definitions by mapping the loss of services over time like electricity, water, mobility, and communications with respect to failures [11]–[15]. The critical functionality curve makes the intuitive connection between the services provided by infrastructure

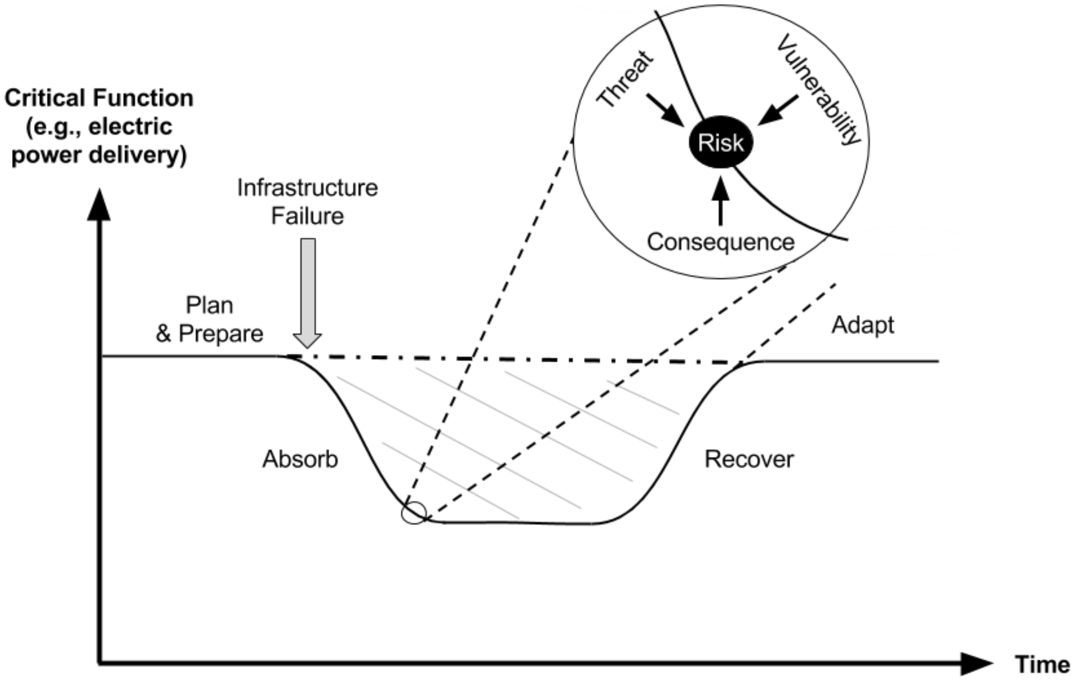


Figure 1 Relationships between National Academy of Sciences Definition of Resilience, Infrastructure Function, and Risk.
Infrastructure systems perform a critical function that is degraded and recovered over time after a system experiences a failure. Risk analysis focuses on single point on this line, where threats, vulnerabilities, and consequences are combined into a single metric. Resilience is often associated to the shaded area between the dot-dashed line and the critical functionality curve, where more resilient systems have a smaller area. Resilience is gained through planning and preparation, absorption, recovery, and adaptation capabilities. These four abilities comprise the NAS definition of resilience and are associated with different phases before and after infrastructure failures. Figure based on [12]**.**

systems and pre- and post-failure response practices identified in resilience definitions. In doing so it also offers a way to improve infrastructure resilience – flattening the curve, i.e., reducing the loss of services and speeding up recovery efforts. Together, a promising way to think about resilient infrastructure is emerging that emphasizes improved failure management activities and tracking system performance when losses occur.

Despite established definitions and models guiding research and applied work for the last 20 years [16], recent massive losses due to infrastructure failures raise the question: ***are the ways people thinking about resilience producing resilient infrastructure systems?*** The widespread adoption of the NAS definition and the critical functionality curve makes it tempting to accept them without significant examination. Their intuitive nature means that they also match established failure management practices for infrastructure systems and are easy to adopt across the numerous stakeholders involved in infrastructure protection. However, the very fact that these perspectives fit risk-based paradigms is an indication that they may only further risk management practices. If the promise of resilience is to change how infrastructure protection is done, then why would guiding theory deepen our commitment to outdated practices?

Moreover, infrastructure crises in 2017 provide a constant reminder that resilience is still not working. After a single year of massive fires caused by poor design or faulty equipment [17], [18], the near-breaching of the largest dam in the US [19], and series of catastrophic hurricanes [20], it appears as if national and international infrastructure systems may be in a worse predicament than before Hurricane Katrina.

What people need is a new way to *think* about resilient infrastructure systems that extends beyond these and other well-established perspectives. The problem with the NAS definition and critical functionality curve is not that they are wrong, but that they are too superficial to guide changes in infrastructure protection activities. Infrastructure owners and operators are already planning, preparing, absorbing, recovering, and adapting failed infrastructure all the time, rendering the definition meaningless for changing infrastructure protection away from risk. In practice, the critical functionality curve can only tell infrastructure stakeholders if they had resilience after a catastrophe happens, and offers limited prospective guidance to handle the next disaster. The fact that these two perspectives influence the majority of infrastructure resilience work today is symptomatic of a serious problem. Collectively, thinking about resilience is misplaced in the critical infrastructure literature. As the library that hinges on these ideas continues exponential growth, infrastructure systems will remain vulnerable to surprise.

The purpose of this dissertation is to come to terms with growing misconceptions about resilience that dominate the infrastructure discourse and offer new ways to think about resilient infrastructure systems. The NAS definition and critical functionality curve are the product of misconceptions held by experts across resilience literature. A new way of thinking about resilient infrastructure systems is needed to correct the fundamental misconceptions that lead to bad theory and advance entirely new definitions and models unlike those seen before. Thus, this work focuses on addressing four fundamental misconceptions to help move research towards the development of a new theory of resilient infrastructure systems. Each chapter is centered on understanding the building blocks that make up resilient infrastructure research – data, goals, systems, and failures – where the misconceptions about resilience that pervade the literature are summarized as:

- **Misconception 1:** More data and advanced computational techniques will result in faster and better decision-making, with fewer cascading losses, deaths, and economic impacts.
- **Misconception 2:** Resilience is a good thing that successful systems do, need, or have when faced with adversity, suggesting more resilience is always better.
- **Misconception 3:** Infrastructure resilience is achieved by hardening existing system components and designing automated, redundant, smart, or otherwise technological solutions to reduce the probability of losses.
- **Misconception 4:** Cascading failure models act as a means to simulate initiating events, study different failure mechanisms, and predict expected losses.

More succinctly, it is commonly believed that:

- more data and data analysis tools will improve infrastructure resilience,
- pursuing resilience will make infrastructure systems better,
- resilience is achieved by lowering the probability of component failure,
- the consequence of cascading failure events can predicted with engineering models.

On the surface, each statement summarizes a reasonable position guiding numerous studies across resilient infrastructure literature. However, like the NAS definition and critical functionality curve, these statements give superficial treatment to the way data, goals, systems, and failures influence action. In reality, each statement is preventing us from realizing the goal of creating resilient infrastructure systems, because:

- **Clarification 1:** More data is not better – being able to access the right information when needed *is*. Data analytics on their own may misinform failure management activities by focusing decisions on the wrong information at the wrong time.
- **Clarification 2:** Pursuing resilience does not guarantee that infrastructure will be protected from all hazards because the act of pursuing resilience, itself, has inherent risks. A single resilience strategy has both benefits and risks, and managing future failures requires infrastructure systems that can switch between multiple resilience strategies to match shifting stress contexts.
- **Clarification 3:** Technologies cannot solve resilience problems on their own because infrastructure systems are comprised of both technologies and people. Reducing the *probability* of infrastructure failure does nothing to reduce failure *consequences* dictated by human action.
- **Clarification 4:** Measuring the consequences after cascading failures occur does little to support decision-making *during* cascading failures as they happen. Again, ignoring the influence people have on the outcome of cascades means the predicted consequences from models may be entirely different from real, surprising situations.

Taken together, resilience is not gained by more data, better goals, novel technologies, or failure measures. Resilience is gained by understanding and improving the *processes* that dictate how data is used, goals are set, technologies are developed, and failures are studied. In other words, resilience is not gained from more *objects* (nouns), it is gained by changing and improving *actions* (verbs). Only with a better understanding of these processes can we reveal ways in which infrastructure systems succeed and fail when faced with unforeseen and unknown surprises. Only then can one begin to change infrastructure resilience, itself a verb rather than a noun, by shifting the processes themselves and changing the ways in which surprises are managed in the future.

Four processes defined in literature help frame this perspective on resilience: sensing, anticipating, adapting, and learning (SAAL) [4], [5], [21]–[25]. Since all SAAL processes are dynamic and interacting, a simple way to think about them is with a control loop linking an infrastructure system to the outside world (Fig. 2). Prior to studying any infrastructure system, researchers develop a conceptual model that delineates a boundary between what is included in analysis and what is ignored (the rest of the world). Within this model is a dynamic infrastructure system under consideration. Infrastructure dynamics such as the provision of electricity are dictated by the people and technologies act via the SAAL processes. Power grids sense power flows and system state, anticipate changes in service provision such as shifting weather and demand, adapt to shifting context to maintain power balance and delivery, and learn whether

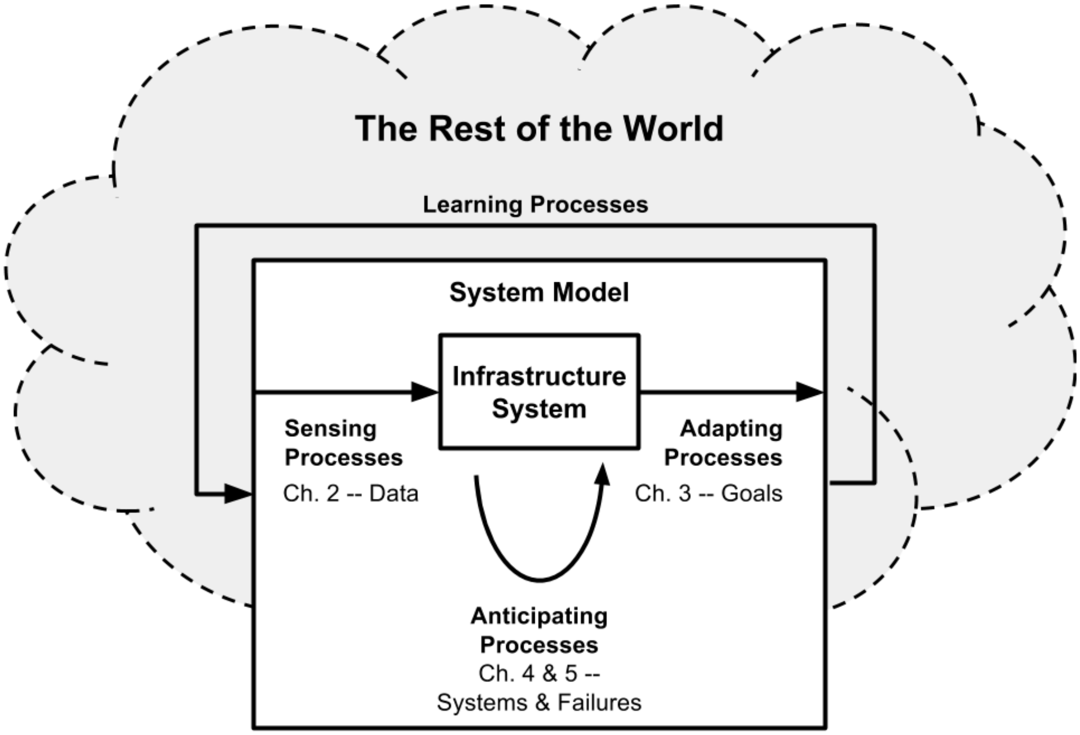


Figure 2 A Simple Control Loop Representation of SAAL Processes for Infrastructure Systems.
Sensing, anticipating, adapting, and learning processes dictate the way in which infrastructure systems interact with the world. The control loop representation is meant to signify that the processes are dynamic and any change to one processes will affect the interactions among all of them. The chapters of this dissertation correspond to new knowledge associated with specific processes, e.g., Ch. 2 advances sensing processes by analyzing the treatment of data for infrastructure resilience.

current practices are fulfilling intended goals. These processes are generic in Fig. 2, as all infrastructure systems sense information from the world, anticipate desired or undesired future states with internal processes, adapt to situations to change future states, and learn through interactions with its environment.

Fig. 2 also provides a structure to think about the papers presented in this dissertation. Chapter 2 discusses the meaning and use of data analytics to turn data into decisions and presents new ways to think about infrastructure sensing processes. Chapter 3 questions whether approaches to infrastructure adaptation are making infrastructure systems resilient, and presents a new way to advance infrastructure adaptation via resilience strategies for electric power, transportation, and water systems. Chapters 4 and 5 focus on anticipation of future large-scale blackouts in power grids, and uses a case study of South Korea to reveal the limitations of network science and cascading failure models for infrastructure design. These chapters demonstrate that system and failure models must include both social and technological perspectives to offer improvements to current emergency management practices. Additional summary and a key figure for each chapter is provided at the end of this introduction.

This dissertation concludes with a path forward to a new theory of resilience based on resilience processes. Where current approaches to infrastructure resilience research hinge upon having the best data, strategies, and models, future resilience theories will be more nuanced because more data is not necessarily good, there is no single best resilience strategy, and conflicting and new models are useful and important. Hopefully, building on this work, future resilient infrastructure systems will bring a safer future for society.

Chapter-wise summary

Table 1 Chapter 2 Summary

Chapter 2: Rethinking Resilience Analytics	
Research Questions	Do data analytics on their own offer a means to advance critical infrastructure resilience? What are the benefits and/or drawbacks to relying on data analytics for infrastructure resilience?
Approach	Review theoretical perspectives on data analytics, systems modeling, and resilience engineering.
Deliverable	Perspective article in the journal *Risk Analysis* for the special issue Resilience Analytics for Cyber-Physical-Social Systems
Intellectual Merit	Identifies pitfalls in using descriptive, predictive, and prescriptive data analytics for infrastructure resilience. Demonstrates how analytics are capable of responding to situational surprise, but will be challenged by fundamental surprises. Argues for caution and sets forth a research agenda that may help manage overuse of some analytic models that obviate the need for a human-in-the-loop

Key Figure for Chapter 2

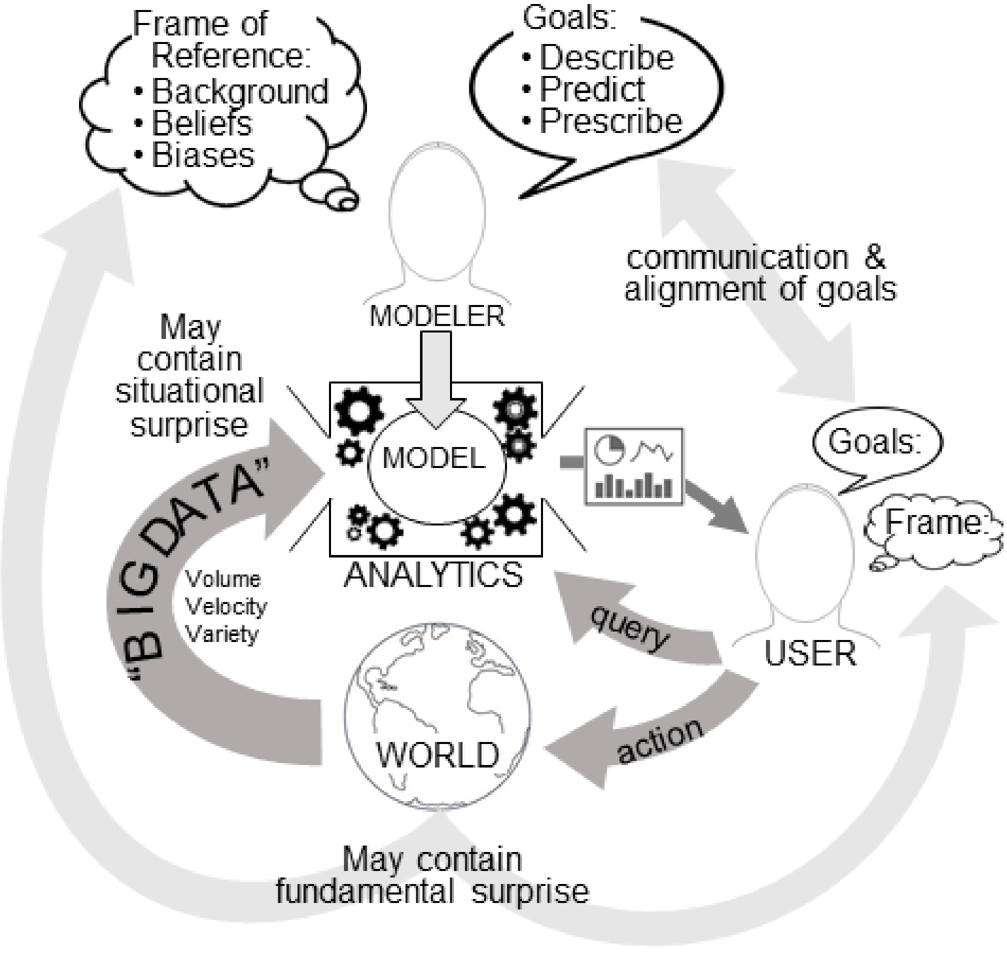


Fig 3 The Relationship Between Analytic Models, Users, Modelers, and the Real World.
The inner loop in this figure represents a simplified way for how resilience analytics are used in CPS networks. Big data inputs are transformed by analytic models for descriptive, predictive, and prescriptive decision support. Model users embedded in CPS networks then decide and act upon model outputs, where no action still constitutes a decision. Actions taken by users affect the real world and feeds new inputs back into analytic models. Within this simple loop, feedback from the real world may contain unexpected observations (i.e., a 'situational surprise') that can be accommodated within current models. However, the inclusion of a 'modeler' who creates and updates big data analytics introduces additional dependencies that form an outer feedback loop and confounds the simple model. Both the interpretation of a user's decision frame by the modeler and the influence of real world stimuli on modeler may produce an incomplete pre-analytic vision and lead to inappropriate analytic models. Moreover, novel and rare experiences may characteristically change a user's decision frame or a modeler's pre-analytic vision (i.e., fundamental surprise) which may upend previous model assumptions and require the development of entirely new analytics.

Table 2 Chapter 3 Summary

Chapter 3: Robustness and Extensibility in Infrastructure Systems	
Research Questions	Is there a single, universal strategy to make infrastructure systems resilient, or, do multiple competing resilience strategies exist? If multiple strategies exist, what makes each strategy distinct? What are the benefits and/or drawbacks to choosing one strategy over another? Are resilience strategies mutually exclusive?
Approach	Review risk analysis and resilience engineering literature for infrastructure resilience strategies. Identify real-world examples of resilient infrastructure to demonstrate benefits and drawbacks to resilience strategies in action. Define a list of possible resilient design strategies for infrastructure systems.
Deliverable	Peer-reviewed journal article.
Intellectual Merit	This work clarifies the meaning of the word resilience and its use in infrastructure systems. We find multiple, distinct strategies available to make infrastructure systems more resilient and demonstrate the advantages of this pluralistic view of resilience. We expound two of these strategies, robustness and extensibility, for infrastructure design, operation, and management. Resulting conclusions are: 1) robustness and extensibility are different strategies for resilience because they draw upon different system characteristics, 2) neither robustness nor extensibility can prevent all hazards, 3) while infrastructure systems can perform robustness and extensibility simultaneously, the drawbacks associated with each strategy are different.

Key Figure Chapter 3

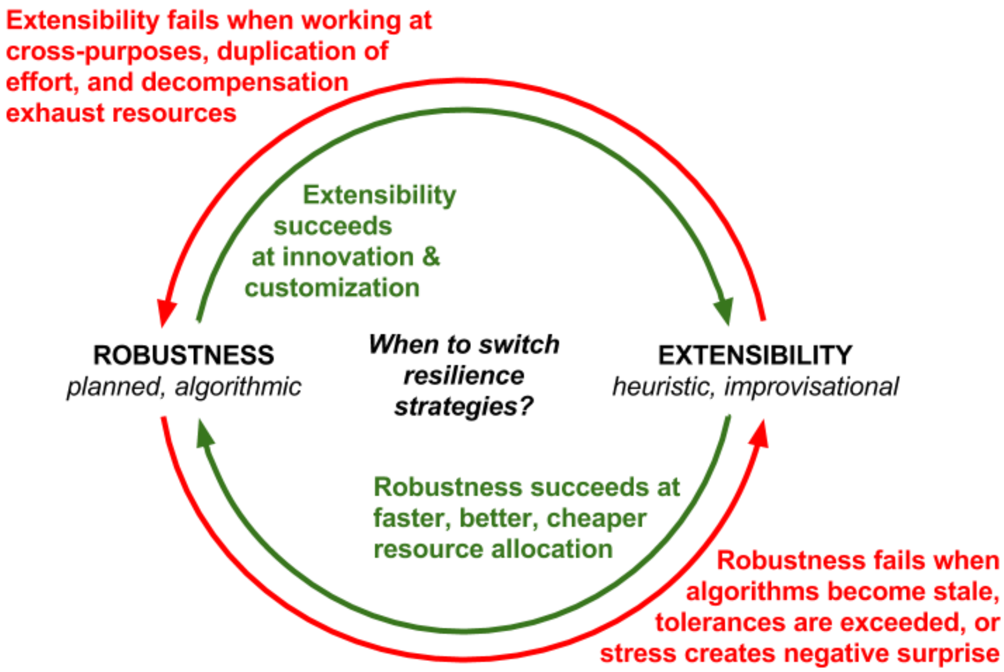

Extensibility fails when working at cross-purposes, duplication of effort, and decompensation exhaust resources
Extensibility succeeds at innovation & customization
ROBUSTNESS
planned, algorithmic
When to switch resilience strategies?
EXTENSIBILITY
heuristic, improvisational
Robustness succeeds at faster, better, cheaper resource allocation
Robustness fails when algorithms become stale, tolerances are exceeded, or stress creates negative surprise

Figure 4 Relationship between Robustness and Extensibility Strategies. Robustness and extensibility are two strategies used to help infrastructure systems manage disruptions. Robustness strategies are best at managing situation surprises, and where they fail, improvisational strategies of extensibility are required to succeed (represented by the red circle). Likewise, there are benefits gained from switching strategies (represented by the green circle) when serendipity enables new robust and extensible capabilities. Infrastructure resilience is not one strategy or another, but the ability to change strategies in response to changing stressors and organizational state

Table 4 Chapter 4 Summary

Chapter 4: Sociotechnical Network Analysis for Power Grid Resilience in South Korea	
Research Questions	How can network analysis inform critical infrastructure emergency management policies and practices? What is the sociotechnical blackout management context in South Korea? How does the identification of critical infrastructures within the South Korean Power Grid (KPG) offer improvements to existing blackout management policies and practices? How does the identification of information-sharing and decision-making organizations for blackout management in Korea offer improvements to national blackout management policies? What, if any, combined guidance do these parallel studies provide Korean blackout management policies?
Approach	Create corresponding power grid and social network models for South Korea based on national policies. Identify critical power transmission infrastructure and blackout management organizations using betweenness measures developed for power grid and social networks, respectively. Use infrastructure and organizational criticality results to recommend improvements to blackout management policies.
Deliverable	Research article published in the journal *Complexity*
Intellectual Merit	Developed first sociotechnical network analysis (STNA) for a critical infrastructure system. Found ways to offer broad recommendations to improve blackout management in Korea using infrastructure and social network analyses. Found that neither power grid nor social network analysis was sufficient on its own to offer specific recommendations, instead combined analyses and guidance is necessary to specify improvements to national policies.

Key Figure Chapter 4

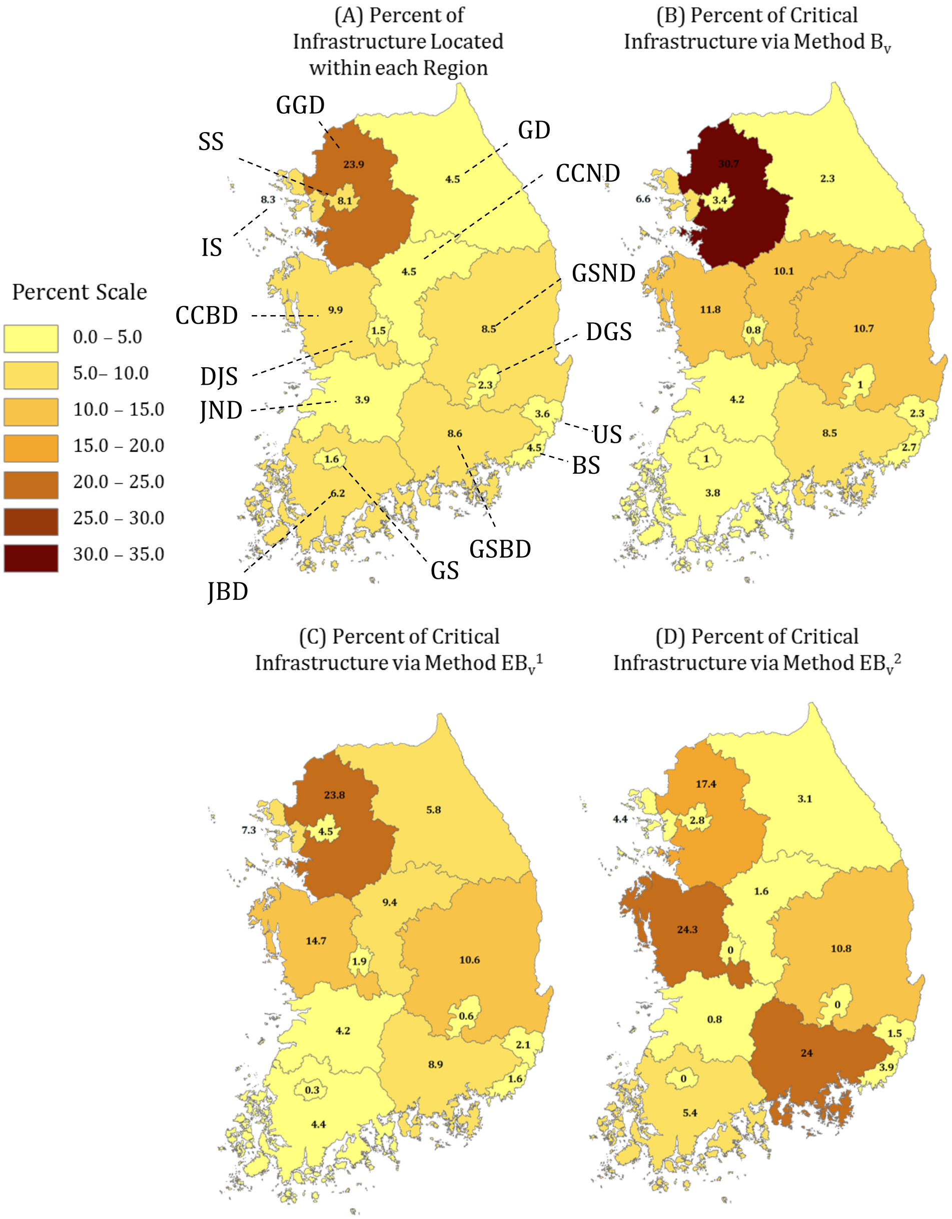


Figure 5 Aggregate Criticality Scores for Korean Power Grid Infrastructure by Emergency Management Region.
The top left image of Korea presents the amount of generation and substation buses located in each region (A), where all other images show the normalized total criticality score for each region (B, C, and D). Thus, percent scale refers to quantity of infrastructure (A) and aggregated criticality score (B, C, and D). Regions are labelled in (A) with abbreviations: Gyeonggi-Do (GGD), Gangwon-Do (GD), Chungcheongnam-Do (CCND), Chungcheongbuk-Do (CCBD), Gyeongsangnam-Do (GSND), Gyeongsangbuk-Do (GSBD), Jeollanam-Do (JND), Jeollabuk-Do (JBD), Seoul-Si (SS), Incheon-Si (IS), Daejeon-Si (DJS), Gwangju-Si (GS), Daegu-Si (DGS), Ulsan-Si (US), and Busan-Si (BS).

Table 5 Chapter 5 Summary

Chapter 5: Advancing Cascading Failure Models for Improved Blackout Management in South Korea	
Research Questions	How does the importance of South Korean blackout management organizations change during cascading failure events? What can models teach us about power failures *during* cascades, rather than after them?
Approach	Advance a failure model for measuring congestion-based cascades for power grids. Generate a weighted social network or South Korean organizations based on the frequency interorganizational partnerships are active during cascades. Measure shifting organizational importance across cascades with multiple betweenness measures for weighted networks. Identify critical organizations during normal operations and extended social network states.
Deliverable	Research article for submission to *Nature Energy*
Intellectual Merit	Developed first link between cascading failures and the complex social context influencing decision making as cascades occur. Found shifting importance of organizations that relate to shifting cascading failure risk across the South Korean Peninsula. Pinpoint organizations that can support surprising power grid failures by filling information sharing and decision-making roles when critical organizations are unavailable or overloaded.

Key Figure Chapter 5

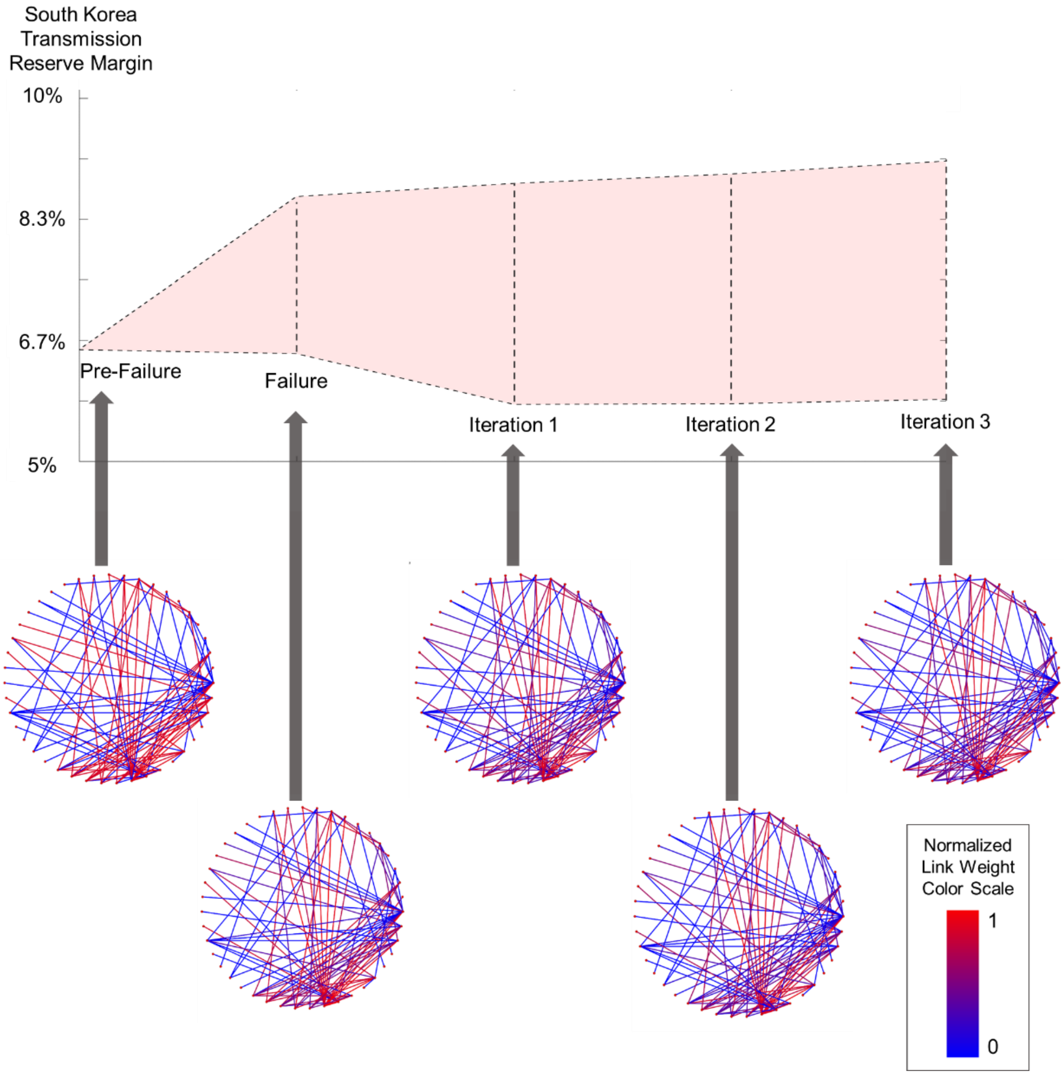


Figure 6 Cascading Failure Results for South Korea and Associated Weighted Blackout Management Social Networks.
When a single substation or generation bus fails, electricity redistributes across the grid and total dispatchable reserve margin changes. The light red region in the above graph encompasses all reserve margin gains and losses from N-1 failures in the South Korean power grid, where top and bottom dashed lines are the largest gains and losses, respectively. Social network links form based on which organization owns and operates stressed infrastructures, where stressed infrastructures are located, and how stressed they are (see Methods). The weight of each social network link is the mean weight across all N-1 failure scenarios with a normalized, maximum partnership strength of 1. Strong and weak partnerships are shown across the cascading process as red and blue links, respectively.

CHAPTER 2

RETHINKING RESILIENCE ANALYTICS

This chapter is in review in the journal *Risk Analysis* for the special issue on Resilience Analytics for Cyber-Physical-Social Systems and appears as submitted prior to review. The citation for this article is: Alderson, D.L., Eisenberg, D.A., Seager, T.P. (2018) Rethinking Resilience Analytics. *Risk Analysis*, in review.

The Allure of Resilience Analytics

Recent advances in information technologies have dramatically improved our ability to capture and use data. For instance, the trend towards an internet-of-things (IoT) means that everything from lightbulbs to appliances to traffic signals becomes both a type of internet-enabled sensor that measures the environment and/or an actuator that can attempt to control it. Similarly, social media applications now collect massive data from crowd-sourced observations, including earthquake and infectious disease detection that may improve responsive actions. This ability to connect data and decision--at large scale and in real time--means that we can potentially respond and adapt to an increasingly volatile world in ways previously unthinkable.

This recent revolution of so-called ‘big data’ requires associated analytics to reveal patterns, trends, and associations between physical systems and human behavior. In business, big data firms Alphabet (i.e., Google) and Facebook demonstrate the global impact of data analytics by using novel techniques like machine learning to guide searches and target customers. In academia, researchers further demonstrate the importance of analytics for investigating previously untenable phenomena, such as the function of the human brain. For the purposes of this work, we focus on data analytics developed for operating and managing critical infrastructure systems such as the electric grid, financial markets, communications, and transportation. These systems are critical because they provide services like electricity and mobility that ensure the safety and function of society, are complex due to their wide geographic scale, interdependencies, and human-technological interactions, and are producing significant amounts of data every second of the day. The picture that is commonly suggested is that continued advances in the use of data analytics will bring unprecedented levels of capability, efficiency, and new knowledge to infrastructure systems. Government [26], [27] and the military [28] are now working as quickly as they can to try to make sense of data analytics and turn it into tactical, operational, and strategic advantage.

Recently, Barker et al. coined the neologism resilience analytics to mean “the systematic use of advanced data-driven methods to understand, visualize, design, and manage interdependent infrastructures to enhance their resilience and the resilience of the communities and services that rely upon them" [29]. The term emphasizes the use of analytic models in support of infrastructure operations and management decisions. Given that the complexities of multi-layered, interdependent infrastructure systems are beyond comprehension of any single individual or organization, the promise of resilience analytics is that more data and advanced computational techniques will result in faster and better decision-making, with fewer cascading losses, deaths, and economic impacts. The authors categorize the decision support offered by analytic models through (1) descriptive analytics to understand how infrastructure systems work, (2) predictive analytics to comprehend the course disasters are likely to take, and (3) prescriptive analytics to offer recommendations to direct systems towards better outcomes. Moreover, they organize the recommended targets of this analysis as cyber-physical-social (CPS) systems comprised of:

- a) infrastructure networks "that enable essential 'lifeline' services for society (e.g., transportation, electric, power, communications)",
- b) service networks comprised of "human systems that engage with these infrastructure systems during a disruption (e.g., emergency responders, humanitarian relief, debris removal)"
- c) community networks of "the interconnected society that the other networks support (e.g., relationships among people and communities)".

Collectively, the combination of analytic category (1-3) and target network (a-c) presents a taxonomy that is intended to allow researchers to "argue for new frameworks for resilience of large-scale systems from a data-centric viewpoint," with considerable emphasis on crowdsourced social media.

It is certainly true that US infrastructure providers would benefit from the improved the decision-making that resilience analytics aims to offer. Essentially all major infrastructure crises in 2017 were exacerbated by maladaptive interactions across infrastructure, service, and community networks. For example, in February 2017 decisions across cyber-physical and service networks to use a broken and untested infrastructure led to the near collapse of largest dam in the United States, the Oroville Dam [19]. Later in the year, damages experienced during hurricanes Harvey in Houston and Maria in Puerto Rico were exacerbated due to risky building development practices and mismanaged recovery efforts [20] across cyber-physical and social networks. Considering these and other ongoing threats to infrastructure systems, it behooves all stakeholders involved in infrastructure, including government agencies, first responders, infrastructure providers, users, and others, to employ analytic techniques in service of reducing the impacts of future, potentially calamitous events.

The temptation to adopt and develop resilience analytics without question is almost overwhelming. However, without critical examination of the assumptions of existing analytics and the limitations they create, resilience analytics may ironically expose the public to grave dangers resulting from overconfidence, myopia, loss of adaptive or innovative capacity, or misconceptions that result in more brittle CPS systems. This paper offers just such an examination. We interrogate the initial 'framing' of resilience analytics by questioning whether analytic models will be able to handle surprising disruptions that cannot be predicted a priori. We find that resilience analytics may be capable to adapt to situational surprises, but will remain unable to adapt to fundamental surprises that motivate their need, the 9/11 terrorist attacks and the near-breaching of the Oroville Dam. We conclude that pursuit of resilience analytics is subject to limitation and premature, as CPS systems that adopt them may ironically become more vulnerable to these events in the future.

The Role of Models

In general, analytics harness the availability of big data to inform decisions through the application of statistical and mathematical *models*. Since there is no single definition of 'model', for simplicity we adopt the lexicon of Brown [30]: "A model is an abstraction that emphasizes certain aspects of reality to assess or understand the behavior of a system under study." This definition is broad enough to cover physical models (e.g., miniature vehicles or buildings), logical models (e.g., of software), and information models (potentially scaling to represent all the working cyber-physical infrastructure in a city). Big data analytic models are often classified in three sub-categories [29]:

- Descriptive analytics that describe and help visualize the performance of CPS networks.
- Predictive analytics that determine complex patterns, relationships among variables, and quantify the likelihood of future events.
- Prescriptive analytics that identify and evaluate a feasible course of actions given a set of constraints, possible interventions, and objectives.

Models are so important that even understanding the role of analytics for improving resilience requires a model for how analytics are used in CPS networks (see: Fig. 7, inner loop). Big data analytics interact with the real world by taking high velocity, volume, and variety information assets as inputs and transforming them with models into useful outputs for engineers, developers, operators, managers, regulators, and others embedded in CPS networks (i.e., users). Predictive and prescriptive analytics use explicit models to guide user decisions and actions. Although it is possible to describe and visualize systems without an explicit model, the choice of what to collect and any inference a user makes on such data implicitly depends on model of what is information assets are relevant and how to use those assets. Model users then take actions that change the real world which feeds back new information assets into analytic models. Together, the interaction between models, users, and the real world creates a simple sociotechnical feedback loop that influences CPS network dynamics and updates analytics to meet new challenges.

The development of resilience analytics also requires the inclusion of a modeler into this feedback loop that interprets the values of the users embedded in CPS networks and translates them into descriptive, predictive, and prescriptive analytics. The initial formation of a resilience analytic model requires a modeler to interpret a user's decision frame, i.e., the user's background, beliefs, goals, needs, and other personal and contextual values that influence their behavior. Existing definitions of resilience analytics guide model development by summarizing common values found across infrastructure sectors, federal agencies, and academic literature. For example, common user beliefs motivating the need for resilience include the increasing frequency and severity of large-scale disasters that challenge lifeline services [31], the growing existence and capacity to harness big data [29], and the increasing interdependence among cyber-physical and social networks [32]–[34]. Moreover, common user goals are captured in resilience definitions across the US Federal government, such as improving the ability for cyber-physical infrastructure systems, "to plan and prepare for, absorb, recover from, and adapt to adverse events," [9], the ability of service providers and organizations, "to recognize threats and hazards and make adjustments that will improve future protection efforts and risk reduction measures," [2], and the ability of communities, "to prepare for anticipated hazards, adapt to changing conditions, and withstand and recover rapidly from disruptions,” [35]. The challenge posed to modelers, then, is to produce analytics that embed these values and support users to make decisions that help CPS networks withstand, adapt to, and recover from disruptions.

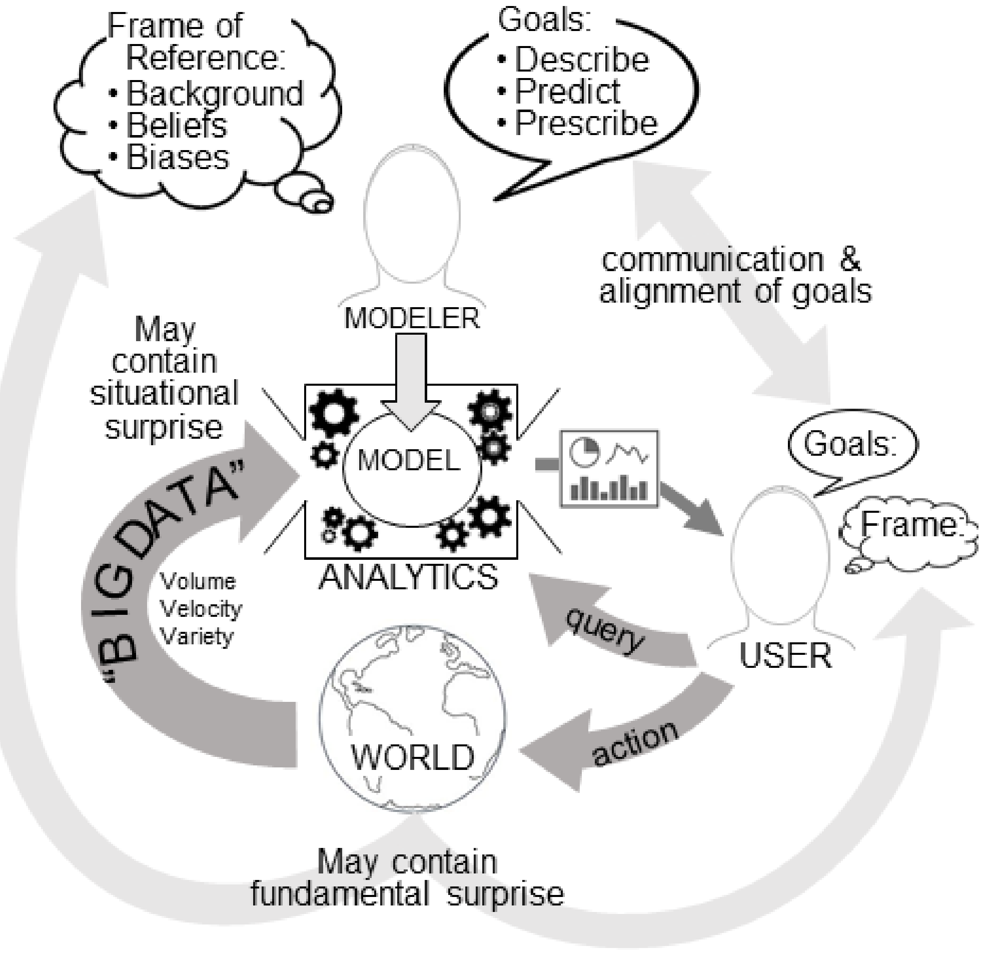


Fig 7 The Relationship Between Analytic Models, Users, Modelers, and the Real World.
The inner loop in this figure represents a simplified way for how resilience analytics are used in CPS networks. Big data inputs are transformed by analytic models for descriptive, predictive, and prescriptive decision support. Model users embedded in CPS networks then decide and act upon model outputs, where no action still constitutes a decision. Actions taken by users affect the real world and feeds new inputs back into analytic models. Within this simple loop, feedback from the real world may contain unexpected observations (i.e., a 'situational surprise') that can be accommodated within current models. However, the inclusion of a 'modeler' who creates and updates big data analytics introduces additional dependencies that form an outer feedback loop and confounds the simple model. Both the interpretation of a user's decision frame by the modeler and the influence of real world stimuli on modeler may produce an incomplete pre-analytic vision and lead to inappropriate analytic models. Moreover, novel and rare experiences may characteristically change a user's decision frame or a modeler's pre-analytic vision (i.e., fundamental surprise) which may upend previous model assumptions and require the development of entirely new analytics.

Unfortunately, the translation of a user's decision frame into models is not so simple. A modeler also has backgrounds, beliefs, goals, needs, and other personal and contextual values comprising a pre-analytic vision (Schumpter [36], Costanza [37]) that influences the act of modeling itself. Although a decision frame and a pre-analytic vision are comprised of similar values, we create a distinction between them because discrepancies among these two sets of values may limit resulting analytics. For example, it is common for a user's decision frame to change during model development and render previous modelling efforts useless. Likewise, a modeler's pre-analytic vision may include technical decisions that reduce the accuracy, throughput, and usability of analytics with or without user knowledge. These and other discrepancies may even exist when the user and modeler are the same individual. Thus, it is necessary to separate the modeler in the sociotechnical loop from the user and add additional feedback dependencies that can influence model development.

Bringing the modeler-in-the-loop introduces at least two confounding dependencies that challenge resilience analytics (see: Fig. 7, outer loop). The first dependency between the user and modeler represents the necessity for translation and interpretation of user values. This dependency emphasizes that analytics are limited by a pre-analytic vision that may obscure model outputs and decision support. George Box's famous aphorism "All models are wrong, but some are useful" reminds us that analytics are only meaningful in their decision context which may be unavailable to a modeler. The second dependency between the real world and the modeler represents the way in which a modeler's values and pre-analytic vision can be influenced by external stimuli. Analytic models must also be regularly updated and modified as both the user's and modeler's values also change over time. Costanza [37] elaborates this fact by emphasizing the credibility of analytics depends on constant reconciliation between a modeler's and user's values. "...[C]redibility proceeds from honest discussion of this underlying [pre-analytic] vision and its inherently subjective elements, as well as from constant, pragmatic testing of conclusions against real-world problems, rather than by appealing to a nonexistent objectivity....[T]he ultimate goal is therefore not truth, but quality and utility." Together, these two dependencies have a direct and possibly underappreciated impact on how analytics improve CPS resilience.

Surprise Happens

Linking inner loop decision-making to outer loop model development raises unresolved issues for analytic models that can inhibit CPS resilience. Specifically, for analytics to improve the resilience of CPS networks, they will need to be responsive to unforeseeable natural and man-made disruptions that challenge lifeline services, infrastructure management practices, and community safety and security. This means outer loop dependencies that include the modeler are critical for determining which disruptions CPS networks can handle. For simplicity, we refer to disruptions that are unknown a priori and challenge CPS networks as surprises. This notion of surprise frames an important question for resilience analytics: can analytic models adapt to surprise?

To answer this question we define two distinct surprises that challenge CPS networks: situational surprise and fundamental surprise. In general, surprises occur in CPS systems because their complex nature makes it difficult to know all relevant dependencies that may cause, exacerbate, or even help manage a disruption. Finding anomalies that cause surprises in cyber-physical systems is a normal activity (e.g., debugging) which often reveals underappreciated dependencies among physical and digital assets [38]. More rarely, surprises occur that cause astonishment in an individual or group that may change their background, beliefs, and goals in such a way that previous conceptions of the CPS system may be deemed irrelevant. Cognitive scientists typically distinguish these situations as experiencing a situational surprise vs. a fundamental surprise. Citing foundational work by Lanir [39], Webb and Wears [39] state four distinguishing features: "Fundamental surprise refutes basic beliefs about 'how things work', while situational surprise is compatible with previous beliefs. Second, in fundamental surprise one cannot define in advance the issues for which one must be alert. Third, situational and fundamental surprise differ in the value brought by information about the future. Situational surprise can be averted or mitigated by such foresight, while advance information on fundamental surprise actually causes the surprise. ...And finally, learning from situational surprise seems easy, but learning from fundamental surprise is difficult."

The central role models play in decision-making shown in Fig. 7 reveals at least two ways in which resilience analytics may be responsive to surprise: (1) feedback from real world inputs, and (2) feedback from modelers. Type-1 feedback depicted in the lower half of Fig. 7 is responsive to situational surprise in the form of updating model structure from real world inputs. Some analytic models automatically adjust behavior and even 'learn' from discrepancies between model outputs and observations from these surprises. However, Type-1 feedback is unresponsive to fundamental surprise because neither users and nor models can change the pre-analytic values embedded in the model. For example, learning algorithms must be trained prior to use, and are unable to access characteristically different inputs than what was chosen during model training. There is no way for analytic model to update its internal structure to a fundamental surprise that deems current model inputs obsolete. Even in situations that fundamentally change the user's decision frame, without Type-2 feedback there is no way to fundamently change the central model. In these situations, a user's best option would be to make decisions without the support of analytic model rendering it useless. Because fundamental surprise can only occur from Type-2 feedback, even the most advanced machine learning or artificial intelligence models cannot be fundamentally surprised. Simply put, analytic models cannot adapt to a fundamental surprise because they cannot experience a fundamental surprise.

The key point is that the modeler, not the model, creates both the limitations of resilience analytics as well as the solution for how to adapt to fundamental surprise. Including the modeler-in-the-loop makes analytics susceptible to having the wrong pre-analytic vision during initial model development. Analytics predicated on misconceptions, or draw our attention to the wrong things, cannot be improved by better data or machine learning processes. In fact, more and better information assets in the wrong model may reinforce misconceptions embedded in results, leading to greater danger resulting from a false sense of security and/or poor decision-making. A view of resilience analytics that only considers the inner loop in Fig. 7 is susceptible in this manner. Likewise, fundamental surprise requires a modeler-in-the-loop to update models and ensure CPS systems adapt to unforeseen events. When modelers identify new ways to structure analytics that where otherwise unknown during initial model development or users determine current model outputs obsolete, resilience requires the model to fundamentally change. Without Type-2 feedback, analytic models lack the capacity to adapt. Again, a view of resilience analytics that only considers the inner control loop in Fig. 7 is susceptible in this manner.

Thus, no analytic model on its own, no matter how well-informed with observation during its initial development, can ever result in a resilient CPS networks. At minimum, resilience analytics require Type-2 feedback to change pre-analytic visions when existing models are no longer working, even if this form of feedback is also the reason why George Box's aphorism remains true.

Implications for Cyber-Physical Social Systems

Fundamental Surprise without a Modeler-in-the-Loop

Many past disasters that challenged real CPS networks demonstrate the need for Type-2 feedback. CPS networks represent a diversity of lifeline infrastructure systems, including financial, transportation, electric power, and water systems among others. Prominent events that fundamentally surprised established models of infrastructure, service provider, or community response in these systems include the 9/11 terrorist attacks in 2001 and the near-breaching of the Oroville dam in 2017. Here, we present short explanations of these events, establishing when fundamental surprise occurred, when models changed, and the resilient results. These case studies are not meant to be comprehensive and further reading is provided at the beginning of each description. Moreover, for brevity, we present only few, well-known events during each disaster to focus on a single fundamental surprise (Fig. 8). Finally, to derive general principles of surprise we organize each case study with the following sub-events:

(1) People embedded in CPS networks realized that continued use of established models only exacerbated problems. (2) Realizing past models were flawed forced people to fundamentally change their values. (3) New values enabled users embedded in the CPS networks forming new decision frames. (4) Resilient response required Type-2 feedback that abandoned past analytics for new models. This was done either by modelers who changed

analytics for the users, or by the users who chose to ignore established models and improvise decisions. (5) Changing models resulted in resilience, i.e., less damages incurred and/or faster recovery of lifeline services.

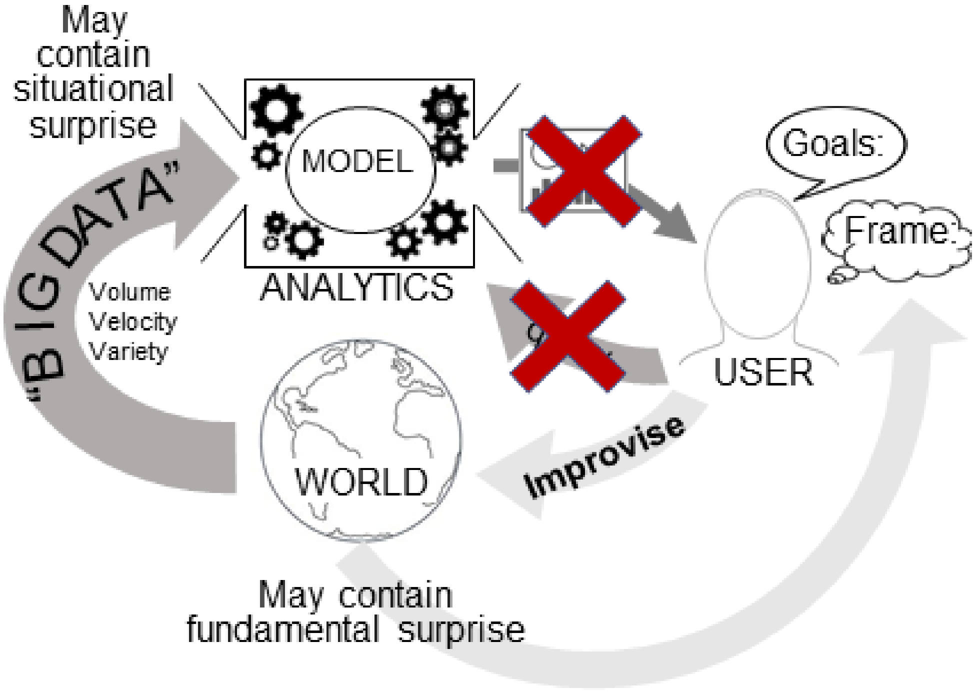


Fig 8 Fundamental Surprise Experienced By Users With No Modeler-In-The-Loop. Past crisis events such as Black Monday, the 9/11 terrorist attack, the Tohoku earthquake, and the near-breaching of the Oroville dam included fundamental surprises where users found existing analytics to be insufficient to meet emergency response needs. Because there was no "modeler-in-the-loop", users that experienced these surprises had no effective way to communicate new analytic needs and adapt models to fundamentally new situations. The result was users abandoned analytics (represented by red "x's"), and were forced to improvise actions without additional decision support.

The 9/11 Terrorist Attack

Based on summarized accounts from [40], [41].

(1) At the time, the mental model that flight crews were trained to adopt was that hijackers will have demands for money, freedom and political power. And that negotiations should

best left to the professionals, and not to flight crews. They were taught non-confrontational strategies that acquiesced to hijacker demands. Their observations indicated that they were being hijacked. They predicted that they would be directed to fly to somewhere and suffer prolonged and dangerous negotiations. They prescribed a strategy of acquiescence that they predicted would result in the eventual release of passengers and crew.

(2) By contrast, United Flight 93 benefited from cell phone calls (observations) that gave them enough information to form a new mental model. They made different predictions. They knew they were as good as dead. (3) The crew formed a new decision frame that focused on taking the plane from the hijackers or cause the plane to crash prematurely.

(4) Together, both the crew (service providers) and passengers (communities) abandoned established model for dealing with hijackers focused on waiting out negotiations and implemented the new model focused on taking the plane back from the hijackers in midair. (5) Implementing the new model led to the plane crashing before it could be used as a weapon and spared the White House from destruction. The crew and passengers lost their lives, but saved the lives of others.

The Near-Breaching of the Oroville Dam

Based on summarized accounts from [42], [43].

(1) Prior to the crisis, the frame of reference for California Department of Water Resources (DWR) and the Federal Energy Regulatory Commission (FERC) was to make decisions based on reservoir-wide risk analyses that identified potential dam failure modes. The most recent analysis in 2014 ignored structural problems from initial dam design, insufficient maintenance practices, and poor mountainside geological conditions that contributed to the crisis. (2) Forensic reports show significant evidence of each misgiving existed before the 2014 risk analysis.

Once the primary spillway failed, dam management was faced with the complex decision of whether to: a) continue using the broken primary spillway, or b) use the ungated, emergency spillway. Expertise divided decision-makers, as operations personnel, management executives, and regulators favored maintaining the frame of reference that the dame was safe and use the emergency spillway, yet (3) geologists, safety engineers, and emergency managers insisted on using the broken primary spillway. The eventual decision that split the difference between both options, to use the primary spillway at reduced discharge rates, is cited as the one that led to the near-collapse of the dam. Once the emergency spillway was activated, (4) geologist onsite warned of immediate dam collapse. (5) Operators controlling the sluice gates to the primary spillway opened it without direct order to decrease flow rate over the emergency spillway and prevent mountainside erosion.

Fundamental Surprise without a User-in-the-Loop

Type-2 feedback is unavoidable in the current study of CPS network resilience. Analytic models function at the scale and speed of real cyber-physical and social networks, effectively acting as a bridge between a user's decision frame, a modeler's pre-analytic vision, and real world phenomena. However, the increased use of some analytic techniques like machine learning and artificial intelligence that create their own internal algorithmic structure may circumvent the need or possibility for Type-2 feedback. These analytic techniques are able to answer certain types of questions (e.g., classification) based on data alone and generate their own internal algorithmic structure in ways people do not yet understand. These models may then produce descriptions, predictions, and prescriptions in such a way that neither a modeler nor a user may be able reflect on why the model produced this output. When using these analytics in situations where it is easy to check model outputs against expected results (e.g., classifying a known photograph), then it may be unnecessary to understand why recommendations were made for Type-2 feedback. The complexity of real world CPS networks, though, makes it impossible for the user to accurately compare outputs to pre-analytic expectations. This means using machine learning algorithms for CPS resilience is equivalent to replacing users with models that are incapable to recognize whether analytic outputs is a situational or a fundamental surprise (Fig. 9).

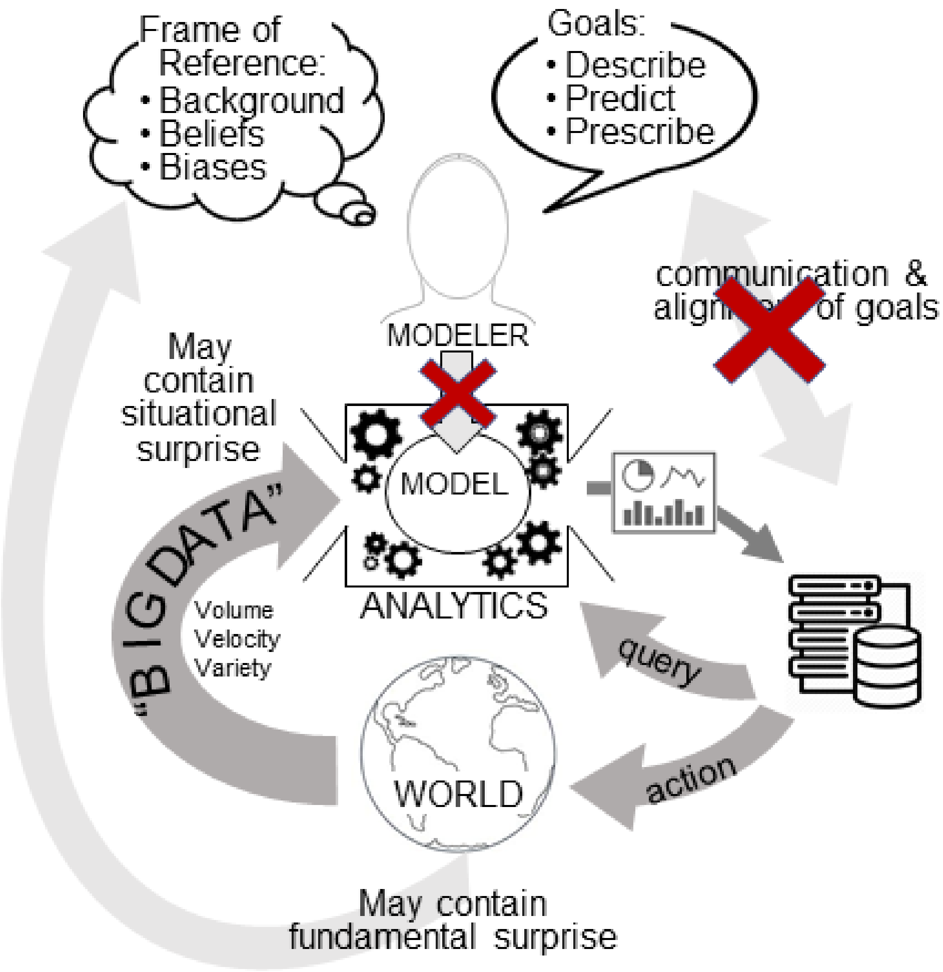


Fig 9 Fundamental Surprise Experienced By Modelers with No User-In-The-Loop. In some cases, the user-in-the-loop is a technological system that acts at the scale and speed of infrastructure. Moreover, increased use of some big data analytics like machine learning impede the ability for human users to compare model outputs to real-world situations, effectively limiting user ability to recognize fundamental surprise. In both cases, there was no "user-in-the-loop". Modelers that experience fundamental surprise have no effective way to align analytic needs to fundamentally new situations. Moreover, the translation of a new frame of reference into new analytic models may be too slow to interdict maladaptive actions hard coded into existing models and technologies. Type-2 feedback is lost where red "x's" are shown.

Because Type-2 feedback is crucial for resilience, increased use of machine learning and other big data analytics may have the unintended consequence of hindering CPS resilience, rather than helping it. The four case studies above demonstrate the necessity to adapt models to fundamental surprise. When models are untenable by humans, then pre-analytic values embedded in the model is also untenable by humans. The increased use of these models further inhibits the capacity for people to reflect on the dynamics of CPS systems effectively negating any attempt to adjust models to fundamental surprise. This inhibits Type-2 feedback and a necessary mode of adaptive response.

Removing the user-in-the-loop also forewarns the potential danger of embedding resilience analytics in autonomous processes. A key objective in the use of analytics is to process data of extreme volume, velocity, and variety, and the ability to leverage large-scale computational resources means that we can now tackle problems at scale--both in terms of size and speed--in a manner that humans could never fathom. Many CPS systems, such as the electric power grid and financial markets, already operate on timescales that make human-in-the-loop intervention impractical, and tales of their large-scale cascading failure are legendary. However, a push to make resilience analytics that are too fast to override and too complex to properly understand will preclude humans from being 'in the loop'. CPS systems will always be vulnerable to fundamental surprise in this context, because there is no ability to re-frame analytic models. When disruptions like Black Monday or the Tohoku Earthquake occur, all that will be left is to try to understand after the fact why things went inexplicably wrong (or right) in the aftermath.

Rethinking Resilience Analytics

A Revised Taxonomy

A first step towards analytics that include the modeler-in-the-loop would be the adoption of resilience taxonomies that make situational and fundamental surprise explicit. The taxonomy originally described in Hollnagel et al. [44] and discussed and refined by Park et al. [4], Hollnagel [45], and Seager et al. [5] offers one approach to frame analytic models relative to Type-1 and Type-2 feedback. Hollnagel [45] defines four abilities that built systems like CPS networks need to ensure that situational and fundamental surprise lead to positive outcomes:

- "Knowing what to do: how to respond to regular and irregular disruptions and disturbances either by implementing a prepared set of responses or by adjusting normal functioning."
- "Knowing what to look for: how to monitor that which is or can become a threat in the near term. The monitoring must cover both events in the environment and the performance of the system itself."

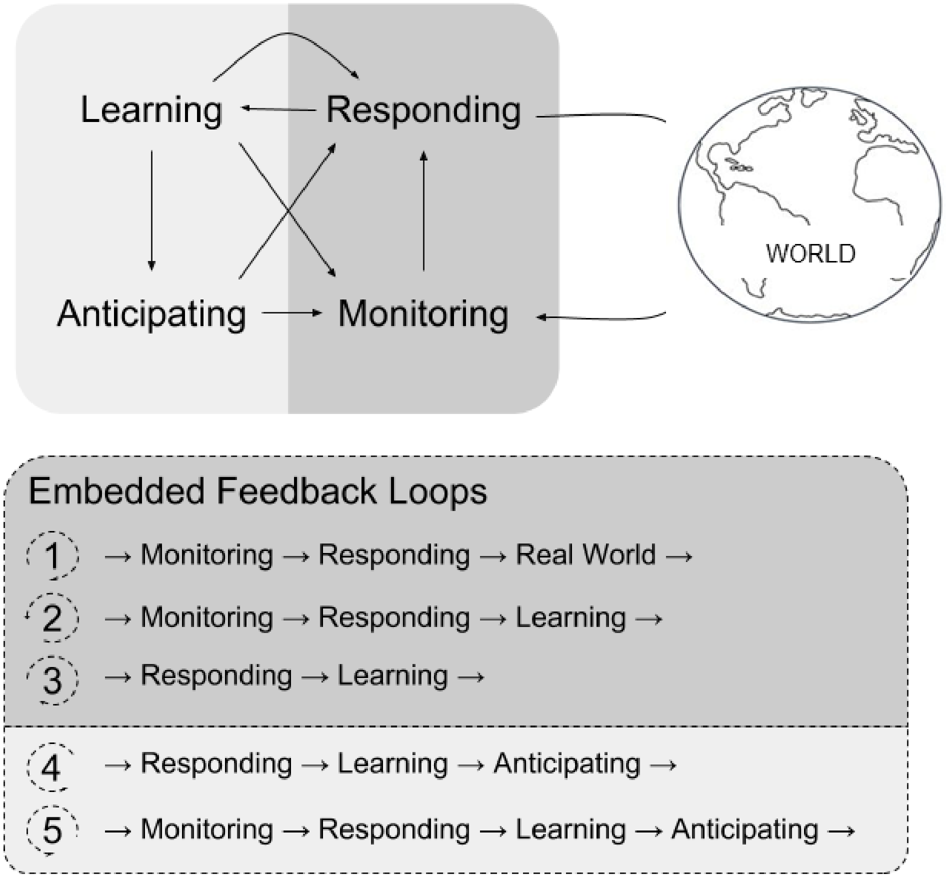

Learning
Responding
Anticipating
Monitoring
WORLD
Embedded Feedback Loops
1 → Monitoring → Responding → Real World →
2 → Monitoring → Responding → Learning →
3 → Responding → Learning →
4 → Responding → Learning → Anticipating →
5 → Monitoring → Responding → Learning → Anticipating →

Fig 10 Four Key Abilities for Resilience (based on Hollnagel).
Hollnagel [44] defines four abilities and their dependencies that dictate how CPS systems respond to disruptions. The critical ability dictating resilience to a situational or fundamental surprise is learning, i.e., the ability to change monitoring, responding, and anticipating practices. Feedback loop 1 does not engage learning, and cannot effectively respond to surprise. Feedback loops 2 and 3 engage learning to improve resilience to situational surprise by updating models for monitoring and responding. Feedback loops 4 and 5 engage learning to improve resilience to fundamental surprise by updating how disruptions are anticipated prior to updating and changing models.

- "Knowing what has happened: how to learn from experience, in particular how to learn the right lessons from the right experience – successes as well as failures."
- "Knowing what to expect: how to anticipate developments, threats, and opportunities further into the future, such as potential changes, disruptions, pressures and their consequences."

Hollnagel's taxonomy provides a characteristically different pre-analytic vision than existing literature that relies on resilience definitions from Federal agencies. First, the taxonomy focuses on the processes CPS systems do to bring about positive outcomes (monitoring disruptions) rather than the resilient outcome itself (e.g., withstanding a disruption). Moreover, monitoring, responding, learning, and anticipating are continuous, proactive abilities where withstanding, adapting, and recovering (or otherwise) occur in reaction to a surprise. Finally, Hollnagel's abilities all occur simultaneously in time with explicit dependencies across them (Fig. 10) were resilience abilities defined by Federal agencies refer to distinct stages in crisis response that are sequential in time.

The dependencies among abilities in Hollnagel's taxonomy emphasize that key ability dictating Type-1 and Type 2 feedback is learning. In their discussion of surprise, Wears and Webb [39] emphasize that situational surprise can be anticipated, but fundamental surprise cannot, and that proactive learning and responding are critical in the presence of fundamental surprise. The embedded feedback loops in Hollnagel's taxonomy show learning processes updates monitoring, responding, and anticipating abilities for resilience (see: Fig. 10). In particular, situational surprise engages Type-1 feedback in loops 2 and 3, where learning processes update existing models for monitoring and responding without modifying previous expectations. Fundamental surprise engages Type-2 feedback in loops 4 and 5 as the formation of new expectations of real world phenomena leads to changes in how disruptions are anticipated. Learning in this way leads to a new frame of reference that requires responding and monitoring to be updated with characteristically new models.

Hollnagel's taxonomy is important because it offers a simple way to categorize future analytic models - those that support Type-1 learning or Type-2 anticipating. Previous studies in resilience analytics do not consider which form or learning proposed analytic models support. According to Hollnagel's taxonomy, these studies may not consider the full extent of learning abilities available to CPS networks by overlooking anticipating as an ability influencing CPS resilience. However, Hollnagel's taxonomy makes clear the need for anticipating processes to be updated and engaged to adapt to fundamental surprises and can offer a simple way for modelers to classify their work for resilience research. This becomes relevant when positive outcomes for CPS systems require current expectations for resilience to be revised and analytic models to change.

A Path Forward

Overall, the resilience research community needs to rethink their role in developing resilience analytics for CPS networks. The limited, yet burgeoning research in resilience analytics focuses largely on establishing a pre-analytic vision for the research community that promotes the use of analytic techniques designed for high volume, velocity, and variety data. While overcoming technical challenges in analytic models is an important focus area for CPS networks, improving their resilience will require significant effort figuring out how to use them in a way that does not inhibit Type-2 feedback. In short, resilience analytics are not limited by a lack of computational tools, resilience analytics are limited by a lack of ways to adapt to fundamental surprise.

Resilience is about adaptive capacity, and the resilience research community are a part of this process. The 9/11 terrorist attacks and the near-breaching of the Oroville Dam would have benefited by having a modeler-in-the-loop to adapt established tools to unanticipated decision contexts. This means we, the research community, must be able to get outside our models. We need to find better ways to interpret a user's decision frame and translate that information into effective tools. We also need to become aware of our own values to ensure that the resilience analytics we produce have utility, rather than exacerbate problems. Finally, we need analytics that help us be explicit about forming new mental models. That is, CPS resilience analytics research cannot just be about developing and applying new statistical techniques, resilience analytics need research about forming and adapting the pre-analytic vision as well.

Unfortunately, we aren't at the point where we can apply big data analytics in a resilient way, because we still lack theory, methods, and tools to adapt models to fundamental surprise. In 9/11 and Oroville, the best response users' had available was to abandon models and improvise. We envision a future where the modeler-in-the-loop takes an active role to support CPS network resilience and adapt models when needed.

A challenge is that decision frames and pre-analytic visions are tacit values held be individuals and groups, and therefore unlikely to be amenable to analysis. Finding new ways to make a user's decision frame and a modeler's pre-analytic vision explicit is an important undertaking that should be promoted within the Risk Analysis community. Likewise, combining objective analytic models with these subjective understandings of resilience remains an important area of research for infrastructure systems. Since neither perspective is complete, the outputs from both need further reflection as more analytics are developed for CPS networks. Hollnagel's taxonomy offers one way to consider the relationship between CPS disruptions, models, and sociotechnical dynamics. A more resilient future where CPS systems are poised to adapt to surprises will require applying taxonomies like this one in the context of resilience research itself.

CHAPTER 3

ROBUSTNESS AND EXTENSIBILITY IN INFRASTRUCTURE SYSTEMS

This chapter is provisionally accepted pending revisions in the journal *Reliability Engineering & System Safety* and appears as submitted prior to review. The citation for this article is: Eisenberg, D.A., Seager, T.P., Hinrichs, M.M., Kim, Y., Wender, B.A., Markolf, S., Thomas, J.E., Chester, M.V., Alderson, D.L., Park, J., Lai, Y-C., Linkov, I., Spierre Clark, S., Woods, D. (2018) *Reliability Engineering & Systems Safety, In review.*

Introduction

Prior to Holling's 1973 [46] seminal publication, the word "resilience" was used in few scientific settings – notably, in materials science to describe elastic deformation under stress, and in psychiatry and psychology to describe the characteristics of individuals that allow them to recover from psychological trauma [47]. These understandings of the word are analogous and consistent with the etymological roots of its original verb form, to resile, meaning “to return to a former position” [47], which is sometimes interpreted as "to bounce back" (e.g., Meerow, Newell, & Stults [48]). Building upon Holling’s work, this understanding persists in the natural sciences through groups like the Resilience Alliance, which describes resilience as "the capacity of a social-ecological system to absorb or withstand perturbations and other stressors such that the system remains within the same regime, essentially maintaining its structure and functions" [46], [49]–[51]. More recently, usage of resilience has increased exponentially across various disciplines [52] with each new adoption resulting in efforts to redefine its meaning to fit the purposes of broad applications like business, sustainability, and disaster risk reduction [15]. For example, the United States National Academy of Sciences now defines disaster resilience a "the ability to plan and prepare for, absorb, recover from, and adapt to adverse events" [9], where the United Nations defines disaster resilience as "the ability of a system, community or society exposed to hazards to resist, absorb, accommodate to and recover from the effects of a hazard in a timely and efficient manner, including through the preservation and restoration of its essential basic structures and functions," [10]. Both definitions draw upon the retrospective concept of returning to a former position through a process of recovery, but also include future and present temporal perspectives that seek to minimize hazardous outcomes in the first place. Holling's work expanded "resilience" from simple (material elasticity) and individual (psychology) applications to complex systems. Accommodating these new applications, understandings of the word resilience itself were made more complex.

In ecology, resilience is a descriptive term that does not suggest one system state is better than any other. By contrast, in psychology, business, engineering, and other disciplines resilience is a normative term that largely suggests a preference for the status quo. The difference is most evident in contrasting the incorporation of recovery into the definitions of disaster resilience. To ecologists, recovery processes were dubbed “engineering resilience” [53] to segregate them from socio-ecological perspectives, despite this misnomer ignoring technological systems in the Resilience Alliance's canonical definition. Still, the distinction is of critical importance as the dominant view in design disciplines such as engineering, architecture, and urban planning is that resilience is a good thing that successful systems do, need, or have when faced with adversity [54], [55], suggesting more resilience is always better. This view is also evident in psychology, psychiatry, management, sustainability, and disaster risk reduction where resilience is the result of enacting positive coping capacities to better manage hazards and risks [48]. However, the original verb resile is not meant to evoke success. Rather, it has pejorative connotations, as in reneging on a commitment or retreating from a prior position [47]. The positive perspectives of resilience which now dominate research overlook this pejorative definition and may limit theoretical progress by also overlooking possible ways systems cope with change.

The idea that resilience might be both positive and negative is resurrected here to provide greater clarity and illustrative examples to two particular concepts of resilience important to infrastructure systems: robustness and extensibility. In particular, this paper describes how robustness and extensibility concepts guide different activities to maintain infrastructure services under stress while simultaneously being the reason infrastructure services may be lost. To establish a foundational theory of resilience that is broadly generalizable, resilience research must realize the differences between concepts that only become clear when discussing both their desirable and undesirable qualities [56]. In our view, resilience research must shift from identifying which concept is superior to identifying use of both in practice and how to facilitate switching between them when needed. In this paper, we expound upon robustness and extensibility and draw upon examples in electric power, water management, and transportation systems to illustrate their positive and negative implications for infrastructure management and crisis response.

Risk and Resilience in Infrastructure Systems

Improving the resilience of infrastructure systems is meant to protect them from unforeseen and unknown threats, yet confusion remains over what resilient infrastructure is. “Resilience” entered the civil protection lexicon through materials science, medicine, psychology, social science, and ecology and has recently become a popular word describing the ability of infrastructure components and systems to handle adversity [4], [57], [58]. In the context of infrastructure, resilience is generally associated with the design of built systems and actions that ensure the provision of services like mobility, energy, and water when faced with threats [11], [13]. Even with broad consensus on the need to maintain the structure and function of built systems, literature reviews seeking to condense the growing number of research articles into specific definitions, metrics, methods, and applications continue to produce conflicting views. Resilience is often likened to divergent concepts like risk [4], [59], reliability [60], sustainability [61], adaptive capacity [62], and transformation [32]. Confusion is further amplified as numerous research articles and policy documents from influential organizations discuss infrastructure resilience (e.g. [63]) or use resilience in their title (e.g., [64]) but fail to be informed by a mature theoretical understanding of resilience that can be broadly applied.

Part of the reason that resilience is so difficult to apply in infrastructure systems is that the word itself occupies an awkward position in the English language. Although “resilience” is used as a noun, the most popular definitions describe it as a capacity to act – which makes resilience an action or property that systems perform, like a verb, rather than a property that a system has, like a noun. Table 5 compares different forms of the words “risk” and “resilience” to further illustrate this point. While both risk and resilience work well as abstract nouns, only risk works as a quantifiable noun. This may explain some of the difficulty that researchers have coming up with quantifiable, concrete measures of resilience for infrastructure. On the other hand, the action verb form of risk is a poor choice, whereas the word resile, although obscure, is nonetheless proper and useful. Risk works well as a linking or helping verb, but resile does not. The ways in which we can use these words in English creates constraints around the ways we think about them for infrastructure design and management. We can see that both risk and resilience can be used in noun and verb forms, but that risk works better as an objective, quantifiable noun and helping verb, whereas resilience works better as an action verb. We should think of infrastructure resilience not just in the capacity to act, but in the action itself. Consequentially, the tools and methods for measuring and addressing infrastructure risks are not appropriate for resilience, as these two related concepts are fundamentally different.

Table 5 Comparison of the Noun and Verb Forms of Risk and Resilience.

Part of Speech	Risk	Resilience
Abstract Noun	What is risk?	What is resilience?
Concrete / Quantifiable Noun	What is a risk?	What is a resilience?
Action Verb	I risked.	I resiled.
Linking Verb	I risk floods.	I resile floods.
Helping Verb	I risk flooding.	I resile flooding.

Note: Green and red colors emphasize grammatically correct and incorrect sentences, respectively.

Infrastructure resilience as a verb endorses designing built systems with beneficial properties such as diversity [65] or efficiency [66] to maintain service provision, as well as systems that have the capacity to switch between these properties. Major resilience research efforts across disciplines promote the need for an array of beneficial system properties that influence infrastructure failure response (see [67] for a more comprehensive list of properties). However, designing built systems with beneficial qualities like efficient failure response systems is often in conflict with increasing the diversity of response options, as too many different technologies or decision-makers may inhibit timely crisis response [68]. In contrast, efficient systems may fail in unknown and unforeseen situations that require a diversity of failure response options to maintain service provision [66]. Neither approach is perfect nor resilient. That is, resilience would neither be found in infrastructure systems that emphasize efficiency nor diversity, but rather in systems with a capacity to deploy efficiency in some scenarios and diversity in others. We refer to the act of designing infrastructure systems to have some combination of efficient, diverse, or otherwise beneficial properties as pursuing different resilience strategies. The shift from focusing on system properties to resilience strategies is important because any single strategy can help maintain a continuity of needs in the present, but if practiced forever may eventually fail. A theory of resilience therefore cannot promise complete protection of built systems and services against all adverse events, but it could reveal the benefits and limitations of different adaptive strategies in practice. The verb resile in this context refers to need to switch between strategies when current practices are found to be impractical or dangerous, e.g., when efficiency trumps diversity, or vice versa.

Concepts of Resilience for Infrastructure Systems

We build upon work in the subdiscipline of “resilience engineering” to realize how different resilience strategies may be implemented in infrastructure systems. Resilience engineering has a large and growing body of literature with roots in system safety and organizational theory relevant to the design and management of infrastructure [5], [69]. In general, authors within the subdiscipline share consistent views of resilience as an action systems do, rather than a property they have (e.g., [44], [45], [70]). Still, the subdiscipline has more than three decades of development and debate that contrast different strategies to engineer systems to handle unknown and unforeseen events [24], [71], [72]. Recently, four concepts of resilience extant in the literature were distinguished that can form the basis for resilience strategies in infrastructure systems [5], [73]:

- Resilience as rebound – to return to normal activities after traumatic events.

- Resilience as robustness – to manage increasing stressors, complexity, and challenges with limited to no impact on normal activities.
- Resilience as graceful extensibility – to extend existing system performance when surprise events challenge current capabilities.
- Resilience as sustained adaptability – to manage trade-offs and build adaptive capacity to continuously evolving contexts.

Given this pluralistic view, each concept reflects a distinct strategy to maintain the structure and function of built systems tailored to a specific stress context. That is, no single concept is appropriate for all stress conditions, and each concept may be more or less desirable when applied in practice. Still, previous work only delineates theoretical differences between concepts rather than discussing which stress contexts they manage or how to implement them in infrastructure. Here, we demarcate the stress contexts that robustness and extensibility manage and identify the ways to implement each strategy in electric power, transportation, and water management systems. We focus on robustness and extensibility because both concepts emphasize adaptive actions to maintain service provision, rather than return systems to a previous state or evolve to changing contexts. Thus, both are comparable in practice, and their clarification can inform broad understandings of infrastructure resilience.

Robustness as a Resilience Strategy

Robustness as a resilience strategy emphasizes active buffering and dynamic reallocation of resources in response to known hazards and in accordance with explicit protocols, policies, or procedures, while accepting the inevitability that surprises may lead to catastrophic losses. For example, highway rules sometimes allow travel in shoulder lanes during periods of peak travel or inclement weather, called “hard shoulder running” [74], [75]. Under ordinary conditions travel in the roadway shoulder would be prohibited, with the space at the side of the road reserved for emergency and broken-down vehicles. However, during times expected to be peak travel periods, some rules designate the shoulders for travel, increasing the capacity of the roadway and mitigating the likelihood of traffic jams. While this policy is adaptive in the sense that it deploys the capacity of the roadway shoulder only when the normal travel lanes would be overwhelmed, this dynamic reallocation of resources also leaves the highway system vulnerable to massive congestion. Without a shoulder, crashes or breakdowns will cause even greater impacts to traffic given that response vehicles (e.g., police, tow trucks) will be delayed without a clear path by which to reach the site of the emergency.

Robustness is often the adaptive strategy employed when infrastructure designers and managers are able to correctly forecast known adverse events and establish automatic sensory and control systems to dynamically reallocate resources. The need for a continuity of services in infrastructure systems suggests that any loss of structure or function must be avoided. Robustness epitomizes fault or disruption prevention by designing well-controlled systems which avert known dangers via calculated precision, accuracy, and repeatability. We delineate robust systems from others as those that avert known "faults" or "disruptions". Robustness requires that threats must be recognized and designed for prior to their onset to ensure infrastructure services remain available. In other words, robust systems only prevent perturbations that are known a priori, and avert losses to these anticipated stressors by established IF...THEN contingencies in such a way that service users never experience a change in quality or access.

Still, pursuing robustness exclusively for infrastructure protection will never ensure a continuity of services to all hazards. It emphasizes threat identification as the first and foremost step prior to any design actions. Nonetheless, any attempt to prevent one type of failure may increase the likelihood and damages experienced from others [76]. When robustness fails, it typically is because reallocation of resources results in sudden and catastrophic collapse when system loads become overwhelming, or the system encounters unexpected stressors for which no contingency exists.

Recent controversies involving United Airlines treatment of passengers exemplified a robustness failure (April, 2017). In one instance, United was criticized for refusing to board passengers that were, in the opinion of the gate agents, improperly dressed to fly on complementary tickets reserved for company friends and family. Airline officials defended the decision of the gate agents by saying they were acting in accordance with United policies that require friends and family be held to higher dress code standards than paid passengers. However, just a few weeks later the airline found itself the target of public outcry for forcibly dragging a paid passenger from an overbooked plane [77]. Again, officials defended the actions of the flight and ground crews as consistent with airline policies and protocols. Only later did the CEO admit that the company failed to communicate to front line employees that they could exercise discretion in the enforcement of those policies, rather than resort to excessive force. These examples demonstrate that customer service policies work well for known situations, yet these same policies may exacerbate situations for which they were not developed.

Designing Robust Infrastructure Systems

One of the advantages of robustness strategies is that they lend themselves to automatic control systems. Thus, robustness might be best achieved by technologies in isolation, rather than humans in isolation. For example, at complex roadway intersections, it is becoming more common to deploy cameras and other traffic sensors that feed information to automated control algorithms and adjust signal timings to reallocate green lights to the lanes or turns that are in greatest demand. Because the stressors and remedies are pre-programmed, they can be implemented immediately without the additional cost of human intervention. However, under unusual traffic conditions such as a crash site, a temporary closure for a special event, or a special procession, it is still common to employ human police to override automated control systems.

Even when using linear models and simple equations, calculating the flow of resources like electricity, water, data, and traffic is a demanding task. The most effective robust designs consider all aspects of future hazards and system dynamics, including how system losses propagate in many different operational scenarios. Computers can complete these tasks flawlessly in fractions of time. This characteristic difference in precision and throughput between technology and people can be further expanded to suggest that technology will outperform people when completing any complex task with explicit rules such as driving [78] and games like Go [79]. Each of these systems epitomizes robustness by averting anticipated hazards through well-defined tasks and by experiencing difficulty when managing situations with ill-defined rules.

Because technologies have the throughput and precision to ensure robustness and lack the fallibility of humans in well-defined scenarios, robustness is largely a technological hazard prevention strategy,

Although computerized systems epitomize robust operations, robust approaches to resilience can also be carried out by people when conforming to prescribed responses to known threats. For example, generation-load dispatch in power grids can be optimized to reduce the probability of losses to unusual weather, rare and novel threats like geomagnetic disturbances [80], and hurricanes [81]. To realize these adaptive actions, sensor information is used to update operational protocols and reliable human responses. Robustness enhancing policies include N-k reliability standards that require operations of N interconnected infrastructures to survive k failures without reduction in service constraints. The standard for electric power grids is N-1 reliability [82], where systems are designed to continue functioning after the loss of any single infrastructure, but is not necessarily guaranteed for a larger number of failures. Similar thresholds exist in infrastructure operations, including limits on the number of system errors allowed to occur and their impact on customer access to services [83]. Thus, robustness requires explicit contingency policies that demand reliable human actions.

Tradeoffs of Pursuing Robustness in Infrastructure Systems

Robustness has limitations for managing inconceivable threats that may prove disastrous. Improving a system to handle a known threat can increase the likelihood that other threats will cause greater damages, as has been demonstrated in control theory [76].This tradeoff exists when implementing any of the adaptive robustness strategies described above in infrastructure systems – redesigning the interactions among built components, changing operational methods, and developing regulatory thresholds for ordinary operations – where tradeoffs exist even among robustness strategies themselves. In complex systems, this is referred to as the conservation of fragility [76], [84] and is most pronounced in systems highly optimized to few, specific threats. The more robustness is pursued to increase the resilience of infrastructure, the greater the risk that catastrophic failures can occur from unforeseen events.

In some cases, robust contingency plans remain underdeveloped because rare events are misunderstood as inconceivable – even when they are well within the imagination of infrastructure operators and managers. The near-breaching of the Oroville Dam in California serves an important case of imagined catastrophes being realized. In 2005, several environmental groups expressed concern that allowing high water levels to overtop a secondary (i.e., emergency) spillway may cause significant damage to the dam, surrounding power plants, fisheries, communities, and waterways [85]. Although infrastructure managers refuted this vision by claiming the safety of the dam and reservoir control would not be compromised in the event of an emergency spillway discharge [86], a surge of rain and melting snow pack in February 2017 combined with a structural failure of the main spillway overwhelmed the capacity of existing operating procedures to ensure the safety of downstream communities. The realization of events outside operational routine and thresholds demonstrate the potential drawbacks of robust infrastructure management [86].

Extensibility as a Resilience Strategy

An extensible infrastructure system seeks the same outcome as a robust system, which is to prevent loss of services by protecting the system against hazards. However, extensible infrastructure systems achieve protection in a contradictory way to robustness – by defying rules and protocols rather than shoring them up. Events like Deepwater Horizon and the Fukushima Daiichi Meltdown were exacerbated into disasters by built systems working (and failing) in known ways and people following the rules to manage them [59]. Seminal works by Perrow [87] and Hollnagel et al. [44] argue that these events are caused by characteristically different stressors from faults or disruptions, called surprises, that cannot be anticipated a priori. However, even where hazards are pre-conceived, contingencies plans will fail in the face of complexity, as a sufficient number of simultaneous disruptions, feedback loops, or maladaptive responses can result in “normal accidents” [87] that amplify consequences beyond any previous expectations. Following the rules and norms established for the operation and management of these cascading, unforeseen scenarios may only exacerbate damages [88]. In these cases, extensibility is needed to break established systems, norms, rules, or expectations to arrest failures. Thus, we define extensibility in infrastructure systems as the adaptive modification of existing system structures and functions to prevent losses resulting from surprise.

In contrast to the United Airlines example of robustness failure, the actions of Captain Sullivan in the case of US Airways 1549 after dual engine failure exemplify abandoning robustness in favor of extensibility (Jan, 2009). According to Capt. Sullivan's testimony and after action findings, it was only by departing from established procedures that the pilots were able to land the plane in the Hudson river without a single loss of life [89]. While the crew was trained in emergency procedures for engine failure, these procedures assumed cruising altitude and never anticipated total loss of engine thrust at a low altitude so soon after takeoff. The resulting checklists for dual engine failure included many more checks than the pilots had time to complete prior to emergency landing [89]. In this event, following the explicit rules prior to ditching may have led to catastrophe by slowing decision-making processes. Instead, the pilots extended response protocols by skipping several recommended tasks and improvising a safe response.

Designing Extensible Infrastructure Systems

Extensibility requires that infrastructure systems have controls that can be turned on, shut down, modified, or moved to arrest surprising threats. These controls allow human discretion. For example, modern office buildings increasingly use motion detectors to control lights and faucets, thereby avoiding the waste associated with lighting unoccupied rooms or running water into empty sinks. However, almost all modern office occupants have experienced the frustration of having the automatic light switches turn off accidentally, or the frustration of waving their hands in front of an automatic faucet in an attempt to get running water. Manual light switches and faucets are the consumer analog of circuit breakers in power systems [90], activated floodways in streamflow management systems [4], and ad hoc communication networking devices [91]. Although these systems are sometimes used for normal infrastructure operations--e.g., in power distribution systems and roadway management-- they enable humans to respond to surprises by opening and closing paths for service flow, allowing infrastructure to function beyond designed thresholds, and switching on and off backup resources.

Extensibility is engineered into various infrastructure systems through the use of human-in-the-loop systems that enable people to rearrange physical dependencies, system operation, and management processes. These systems are evident in control rooms where operators manipulate the structure and function of built systems. For example, all major factories and plants use supervisory control and data acquisition systems (SCADA) to collect and display real-time data on the function of working infrastructure (e.g., a turbine) and enable operators to modify infrastructure working conditions (e.g., is the turbine on or off). A common operator practice is to disregard information these systems display as SCADA systems are notorious for calculating and displaying unrealistic system errors [92], many of which are either benign, or if acted upon, would increase the possibility of a disruption to critical services . In response, operators must identify and ignore these errors, or in certain cases, actively generate them [83] to maintain continuous service provision. Assuming that there is no prescribed way in which SCADA errors are ignored or initiated, control room operators are practicing infrastructure extensibility by applying their own expert heuristics to unpredictable circumstances.

Infrastructure policies that promote extensibility use imprecise language in support of context-specific implementation. Designing extensible infrastructure systems requires that people associated with infrastructure operations and management have the ability to influence and redirect service provision. While policies for robust solutions assign explicit thresholds and roles for infrastructure providers, extensible policies have “strategic ambiguity” [93] to empower people to act on their own volition. For example, military doctrine has now adopted the principal of “commander’s intent” that allow for ingenuity and adaptation in the field [94]. The commander’s intent gives high level, strategic direction, but remains ambiguous in the specific tactics or pathways that may be used to achieve the intent. Similarly, standards for developing and maintaining manufacturing robots utilize ambiguous language, using the term “justifiable trust” for the necessary amount of trust the technological system is meant to display to the human operators that work with them [95]. The ambiguous nature of this term is purposeful to force a broad interpretation of trust across many manufacturing industries and foster systems with flexible approaches to sociotechnical safety. This ambiguity supports extensibility by requiring infrastructure providers to continuously manage shifting interpretations of trust across their respective industries similar to shifting international politics surrounding nuclear and cyber warfare [96].

Tradeoffs of Pursuing Extensibility in Infrastructure Systems

Extending current infrastructure systems to handle surprises may also increase the risk that known disruptions become unmanageable through inefficient and distributed decision-making practices. Embedding people in infrastructure and creating human-in-the-loop, activated, and strategically ambiguous systems supports surprising responses to surprising events by not setting explicit rules. The greater the extensibility of an infrastructure system, the greater the risk that systems experience a brittle failure (i.e., sudden and cascading) because adaptive actions exhaust routine resources. When a system draws upon shared resources to practice extensibility, communication breakdowns can result in lack of coordination, working at cross-purposes, and loss of productivity such that existing resources are insufficient to keep pace with increasing demands.

We refer to these processes collectively as “decompensation”: when a sociotechnical system exhausts its extensibility in a way that jeopardizes other hazard prevention activities [97]. An example of decompensation in infrastructure systems comes from roadway management. Deployable traffic control equipment can be used to create a detour around accidents for the safety of local drivers. While this detour exists, the use of equipment may increase the risk of a major traffic jam as other accidents and crisis situations cannot be detoured because traffic control equipment is already committed. In this example, the road system may experience a brittle failure (sudden, large traffic jam) as the routine activity (detour) is unavailable when extensible resources (traffic control equipment) are committed to other activities (working at cross purposes).

Not all extensibility is “graceful”. Where decompensation results in a degradation of performance, a system may be extended in ways that management may fail to recognize – even in the face of overwhelming evidence. For example, evidence of decompensation can be found in “near misses” [98], when catastrophic failure was narrowly avoided through some human ingenuity and adaptation. However, people may misinterpret the lesson from the near miss as evidence that they are more robust than they really are, rather than interpreting the near miss as evidence of decompensation. The ongoing water quality crisis in Flint, Michigan emphasizes the danger of overlooking near misses. In 2014, the decision for the City of Flint to change water sources from Detroit to the Flint River extended distribution systems to convey water with historically worse water quality [99]. Subsequent discovery of pathogens and corrosive chemicals in city water led to a series of boil water warnings and attempts by local residents to switch water sources again, this time away from the Flint River [100]. Attempts to change water sources were rebuked by government officials believing corrective actions taken by the Michigan Department of Environmental Quality to treat Flint River water were effective [101]. This failure to recognize decompensation exacerbated the initial extensibility of built systems to use a new water source and human actions to continually correct mounting issues. Eventually, the failure to act upon early issues regarding E coli and corrosion exposed residents to water with Legionnaires disease [99] and an unsafe concentration of lead [100].

Decompensation is only possible when systems have extensibility. As humans are best at recognizing surprises and breaking the rules, the act of extending system capabilities is shaped by the same fallibility that makes people worse than computers at robustness. The example of control room operators ignoring SCADA errors emphasizes that “graceful” extensibility requires human agency and ingenuity during times of system stress to defy norms, procedures, and faults. As the operators form heuristics for managing SCADA errors, the system that was previously extensible can become decompensated to follow specific protocols. Keeping human-in-the-loop operation ‘graceful’ requires learned heuristics to ensure operators retain the capacity to recognize and respond to surprises, even though these heuristics may be fallible. Preconditioned systems and optimization protocols do not allow for grace. Even the most sophisticated technological and artificial intelligence systems require explicit rules for making decisions that the algorithms themselves do not change.

Robustness and Graceful Extensibility in Infrastructure Systems

Revisiting the discussion of models in Ch.2, the nature of infrastructure design is to create an expectation about the future (model) that enables decisions about technological and human system structures and functions. Inevitably, robust and extensible design expectations will be challenged by surprise. Some surprises may be situational, i.e., unlikely events that do not challenge previous model expectations, or fundamental, i.e., events that do challenge previous model expectations. Moreover, we could call positive surprises, such as accidental scientific or innovative discoveries, serendipity, whereas we could call negative surprises calamity. In either case, robustness and extensibility strategies fail when they do not enable infrastructure systems to adapt to surprise and ensure serendipity or calamity lead to positive outcomes. Because robust models must be built with anticipated thresholds in mind, robustness strategies requires that decision needs must exist prior to the model, as it is impossible to predict that which cannot be conceived of a priori. This means robust design and management strategies are best at managing situational surprises. Likewise, extensible design and management strategies require extending anticipated decision needs, and are best at managing fundamental surprise.

Promoting use of either robustness or extensibility without an appreciation of its limitations overlooks an essential fact: *surprise leads to negative outcomes when decision-makers are stuck in stale models of risk management*. Whether serendipitous or calamitous, surprises challenge our current models and understandings of systems. Yet, there are no guidelines for design, operation, and adaptation of infrastructure that explicitly addresses surprise. After crisis events that fundamentally surprise robust design and management strategies, many new infrastructure designs and retrofits are still based on previous approaches to engineering that value historical tolerances. Assuming no surprises occur in the near future, designs will become stale and persist well beyond their intended lifetime. Eventually a fundamental surprise will occur, infrastructure will fail, and no one, not even the most knowledgeable, will see it coming.

A practical understanding of resilient infrastructure embraces both robustness and extensibility concepts. Although many agree that infrastructure resilience emphasizes the ability for systems to respond to crises, few agree on how to interpret and implement resilience in practice. Instead, I recommend using a new approach to thinking about resilience that emphasizes the need to switch between strategies when the other becomes stale (Fig. 11). In brief, robustness strategies are employed when planning has identified contingencies and responses ahead of time to limit the negative outcomes of situational surprise. Extensibility strategies are employed when plans, models, and algorithms become stale, or when confronted with fundamental surprise.

The need to switch between strategies is to ensure resilience models do not become state, because *neither strategy works indefinitely*. Robustness is challenged by situations that overwhelm predetermined thresholds, as seen in many disasters discussed above. Likewise, extensibility can fail and cause large-scale infrastructure disruptions when independent systems

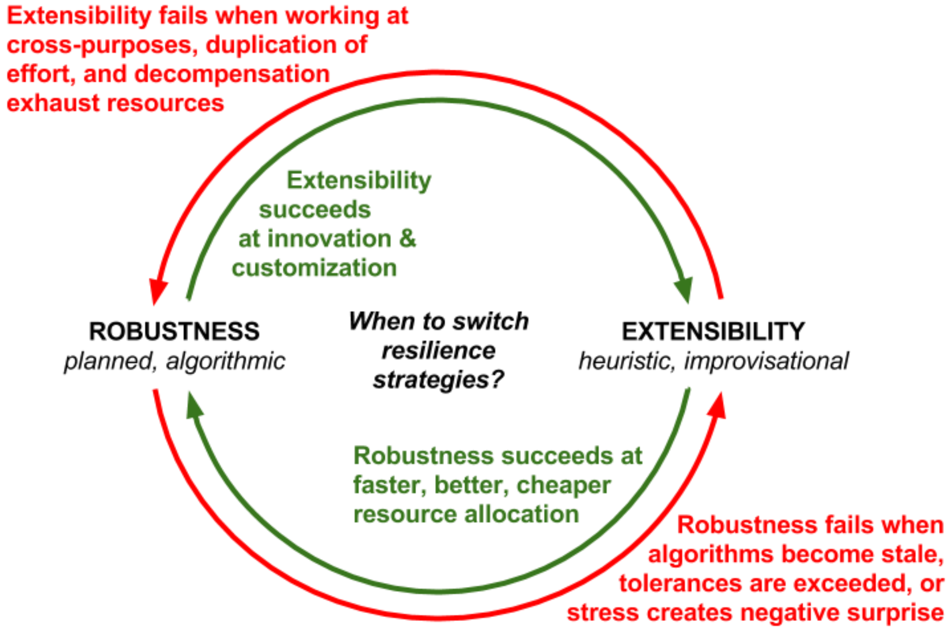

Extensibility fails when working at cross-purposes, duplication of effort, and decompensation exhaust resources
Extensibility succeeds at innovation & customization
ROBUSTNESS
planned, algorithmic
When to switch resilience strategies?
EXTENSIBILITY
heuristic, improvisational
Robustness succeeds at faster, better, cheaper resource allocation
Robustness fails when algorithms become stale, tolerances are exceeded, or stress creates negative surprise

Figure 11 Relationship Between Robustness and Extensibility Strategies. Robustness and extensibility are two strategies used to help infrastructure systems manage disruptions. Robustness strategies are best at managing situation surprises, and where they fail, improvisational strategies of extensibility are required to succeed (represented by the red circle). Likewise, there are benefits gained from switching strategies (represented by the green circle) when serendipity enables new robust and extensible capabilities. Infrastructure resilience is not one strategy or another, but the ability to change strategies in response to changing stressors and organizational state

are working at cross purposes or events require more efficient use of limited resources. True resilience is being able implement the proper strategy for a given situation, i.e., shore up resources into strict plans sometimes, and improvise to handle overwhelmed events in other situations. Failure occurs when the strategy used does not match stress conditions experienced. Infrastructure managers need guidance on when shifting between strategies is necessary to avoid large-scale disruptions.

This means resilience is not a state property, like vulnerability, which can be enhanced through careful investment in system hardening or failure response. Instead, resilience is a set of *processes*, best understood as an action (verb) a system performs, rather than a characteristic (noun) a system has. Thus, resilience is found neither in isolated, nor interdependent infrastructure systems, neither hierarchical, nor egalitarian command structures for emergency response, and neither cohesive, nor individualistic communities. Rather, resilience is the ability for built systems to reconfigure themselves between isolated and interdependent modes, for organizations to change command structures, and for communities modify relationships to match stress conditions. Similarly, there is no single systems or mental model that is superior for resilience. Rather, resilience is the capacity to change between models as circumstances warrant.

This understanding of resilience from a robustness and extensibility perspective is important to distinguish from other system design concepts that such as flexibility and agility (or otherwise). Flexibility and agility themselves are easily conflated, as only the recent work of Sherehiy et al. [102], Santos Bernardes & Hanna [103], and Alberts et al [104], [105] provide nested frameworks for understanding the distinction between flexibility and agility, and Chester & Allenby [106] describe how flexibility and agility relate to infrastructure systems. Across all authors, flexibility is treated as an inherent infrastructure system property, defined as the characteristics of system components to change status within an existing configuration. Flexibility is designed into infrastructure systems by using technologies and management protocols that function together (compatible), communicate to each other (connectable), and are easy to add, modify, or remove from the system (modular). In contrast, agility is a system-level organizing paradigm that enables an infrastructure system to rapidly reconfigure to new operating parameters. Thus, a resilient infrastructure system needs both flexibility and agility in technological and social sub-systems to adapt current designs to new configurations. While each of these capabilities may enable robust or extensible resilience strategies, neither flexibility nor agility take into account the implications of using automated or human means achieve desired outcomes, or whether design decisions handle situational or fundamental surprises. It is entirely possible to have a flexible and agile system that is fully automated and/or at full discretion of people, but each system will fail in different characteristic stress contexts. The first system will be brittle when design thresholds are exceeded, and the second will brittle when decompensation threatens service provision. Resilience supersedes these concepts to include the inherent limitations of different flexibility and agility design options, and categorizes these concepts within robustness and extensibility strategies.

In particular, resilience demands better *heuristics* for knowing when and how to change our system models and establish new parameter sets, and recent advancements in the theory of resilience have revealed some important insights in how to organize our thinking [5], [73], [107]. In particular, several processes that must be mastered by any organization that seeks to consider itself resilient. In Ch. 2, we discuss these processes as monitoring, responding, learning, and anticipating [44], [45]. Further development of these processes also consider sensing and adapting [4], [5]. Each of these process has technological and organizational functions. For example, in sensing, data may come in quantitative forms – such as the weather radar or stream elevation gauges. But it may also come in qualitative forms, such as anecdotes, images, or even body language. Similarly, adapting could come in technical forms, such as automated controls or contingency plans and in organizational forms, such as reallocation of decision rights, changes in access to information, or patterns and policies or interaction.

Robustness and Extensibility in Power, Transport, and Water Systems

We compare robustness and graceful extensibility as distinct concepts based on at least three criteria for infrastructure systems: threat perception, failure response, and implementation strategies. Pursuing robustness requires threat identification as a first step, and is most appropriate for managing frequent threats with which operators have prior experience or historical data. By contrast, graceful extensibility requires the treatment of threats as surprises and is more appropriate for unprecedented events. The strategies themselves become less and less useful when misapplied, such that robust systems fail under surprise and extensibility fails under decompensation. Although both strategies are pursued in distinct ways, by emphasizing different approaches to future threats, they may complement each other in practice.

Robust strategies defer decision-making to pre-determined contingency plans and protocols with strict rules for decision-making, information sharing, and action. Failure to have, know, and follow known protocols will quickly lead to loss of services. In contrast, extensible systems are successful in unconstrained, imagined situations that require improvisation to try new ideas. Risk of system failure increases as decompensation limits response options and available extensibility is wasted, unbeknownst to infrastructure providers. As systems become decompensated, people are forced to extend systems without regard to how improvised activities further decompensate them. Decompensation can overwhelm extensible systems, just surprises may overwhelm robust systems.

Some infrastructure designs already embrace the capacity to be robust and extensible, such as switching between manual and autopilot systems in commercial planes during flight. Autopilot is a robust solution to safe flight, making it unable to handle surprising threats. Humans can overtake automated systems at any given time, increasing the extensibility of current systems. This is standard in situations where constant training is needed or surprises are common, such as take-off and landing. Still, the moments in which the aircraft is controlled entirely by the pilot are susceptible to decompensation.

Robustness and extensibility in infrastructure systems require distinct implementation strategies. Summarized in Tables 6 and 7 is a non-exhaustive list of ways in which both strategies can be implemented in infrastructure systems with specific examples for electric power, transportation, and water systems. This list is based upon well-known approaches used by infrastructure designers, operators, and managers to maintain the structure and function of built systems and provides a new organization of these strategies based on robustness and extensibility. Rows within the tables compare robustness and extensibility strategies across different infrastructure systems. For example, manual switchgear in power systems offers equivalent control over power flow as deployable traffic equipment in roadways and activated floodways in flood control systems (Table 7). Cells across Tables 7 and 8 offer comparison between robustness and extensibility strategies in practice. For example, using automated flow regulating devices is a robustness strategy to flood management that is built directly into the water infrastructure system (Table 6). Likewise, activated floodways that must be opened or destroyed to control floodwaters could be extensible infrastructures built into the system wherever operating rules require expert judgment for their actuation. Both flood control infrastructures provide the same services, but in characteristically different ways.

Across all three infrastructure systems common methods for automating systems exist, including computer controlled services to protect infrastructure and users like self-islanding microgrids and self-driving cars. Robust human responses are supported by strict operations and maintenance expectations like vegetation management and material specifications. Moreover, policies and standards support robustness by further defining normal operations through strict reliability criteria and regulatory requirements.

Graceful extensibility can also be designed into the technological and human systems that make up infrastructure, yet appear as different kinds of human-in-the-loop design through activated systems and strategically ambiguous policies. Common activated infrastructures include circuit breakers and floodways and deployable technologies like power conditioning batteries, bridge retrofits, floodwalls, and sandbags. Assuming sensor networks and infrastructures are feeding human decisions rather than automated systems, the move to smart grid, transportation, and water infrastructure may be increasing the capacity of people to take improvisational actions and make graceful decisions. Finally, strategically ambiguous operational protocols and policies support heuristic response by giving autonomy to infrastructure providers. Some reliability indices used across infrastructure systems like SAIDI enable this form of autonomy among power providers. Similar autonomy is gained in US transportation systems through different enforcement policies across city and state lines for equivalent laws (e.g., speed limits and ticketing expectations).

None of the strategies in Table 6 for designing robust built systems, operational protocols, and/or policies preclude those in Table 7 for gracefully extensible systems. In other words, infrastructure systems can and are designed to have a redundancy of options that support both robust and extensible hazard prevention strategies. One example would be an activated infrastructure that has both automatic systems to prevent known failures and human activated systems to enable extensibility such as some microgrids in power systems that have automatic and on-site control systems. However, few infrastructure components or systems are designed for this form of optionality, making it difficult to fund redundancy among strategies. In current infrastructure operations and management environments with limited time and money, infrastructure providers will be faced with choosing to employ one strategy or the other.

Table 6 Robust Infrastructure Implementation Strategies

Implementation and Design		Electric Power[1]	Transportation[2]	Water[3]
Built System	*Automating*	• Automatic circuit reconfiguration • Self-islanding microgrids	• Intelligent transportation systems • Automated signaling systems • Self-driving cars	• Flow regulating devices • Remote water quality monitoring system
Infrastructure Operations	*Explicit Protocols*	• Operator training to follow strict protocols • Vegetation management	• Managed lanes • Infrastructure materials specifications • Maintenance and development policies	• Dam discharge and flood warning protocols • Inspection, maintenance, and enforcement programs to ensure continued function of dams and levees • Emergency water supply plans (e.g., for health care facilities)
Policies and Standards	*Operational Thresholds*	• N-1 reliability criteria • Minimum generation reserve margins • Frequency and stability limits	• Return period for infrastructure design • Insurance and tax limitations	• Hydrographs for design storms • Floodplain management ordinance (e.g., elevation certificates, flood insurance) • Fire flow rules for water distribution systems

Note: sources for table contents – [1][108], [2][63], [109], [110]*, and* [3][4], [111]–[114]

Table 7 Extensible Infrastructure Implementation Strategies

Implementation and Design		Electric Power[1]	Transportation[2]	Water[3]
Built System	*Activated Infrastructure*	• Manual switchgear and circuit breakers • Utility scale batteries for power conditioning	• Modular construction techniques • Deployable retrofits • Deployable traffic management infrastructures	• Activated floodways • Detention/retention basin parks • Dam spillways • Water shut-off/isolation valves in distribution systems • Connecting alternative water source to the building plumbing
	Human-in-the-Loop Design	• Demand response • Household distributed energy resources (solar panels and wind turbines) • Non-automated microgrids (on-site management)	• Human drivers, pilots, and captains of vehicles • Roundabouts	• Clearing garbage or sediment build-up in stormwater drains • Self-assessment guide for drinking water • Arranging with another public water supply to obtain potable water (e.g., water delivery trucks)
Infrastructure Operations	*Strategic Ambiguity*	• Operator training without explicit protocols and expectations	• Intersections and lanes managed by traffic officers	• Implementing damage reduction measures for existing buildings such as acquisition, relocation, retrofitting, and maintenance of drainage ways and retention basins
	Human-in-the-Loop Design	• Smart grid systems and software for situational awareness	• Smart traffic sensors and SCADA systems • Real-time traffic and route management	
Policies and Standards	*Strategic Ambiguity*	• System interruption and availability indices without explicit thresholds (e.g., SAIDI)	• Enforcement of speed limits and traffic laws	• Low Impact Development practices

Note: sources for table contents – [1][108][108] *,* [2][109], [115]–[117][109], [115]–[117] *, and* [3][4], [65], [112]–[114]

Conclusion

For robustness and extensibility to be different resilience concepts, there must exist different characteristic stress contexts that impact infrastructure services. We categorize these based on the stressors each resilience concept handles best – robustness prevents losses to known disruptions and faults, where graceful extensibility prevents losses to surprises. Many of the differences between resilience strategies in practice come from the initial conceptualization of system stressors, and infrastructure solutions tend to follow choice of stress context. A focus on calculated, detailed faults and disruptions emphasizes automated, robust solutions. In contrast, a focus on complex, systemic interactions that generate surprising responses will emphasize extensible solutions to embed decision-makers and ways to rearrange systems on the fly.

Following that multiple stress contexts exist, there is a need for both robust and extensible systems to manage the stressors that threaten infrastructure systems. Neither pre-defined rules nor ambiguous policies manage all stress contexts, and a blend of both approaches will be necessary to protect infrastructure systems. Pursuing resilience as a verb in infrastructure systems cannot endorse automated nor human controlled systems alone, but suggests that strategies that bridge them may handle a large number of stress contexts. Consequently, where a single concept of resilience dominates governance of infrastructure systems, more of that single concept may have counterproductive effects. Based on this work, resilient strategies must be shared between the robustness provided primarily by technologies and the extensibility provided primarily by human expert ingenuity.

CHAPTER 4

SOCIOTECHNICAL NETWORK ANALYSIS FOR POWER GRID RESILIENCE IN SOUTH KOREA

This chapter is published in the journal *Complexity* for the special issue on Energy and Complexity and appears as submitted prior to final proofs. The citation for this article is: Eisenberg, D.A., Park, J., Seager, T.P. (2017) Sociotechnical Network Analysis for Power Grid Resilience in South Korea. *Complexity*, 2017, 1-14. doi:10.1155/2017/3597010.

Introduction

The increasing frequency and costs of catastrophic events has prompted concerted international efforts to study and design more resilient power systems. In the United States, national policy is encouraging technical efforts to improve the resilience of infrastructure systems, including: energy, water, cyber security, communications, transportation, emergency management, healthcare, financial, and government systems [2], [118]. Global organizations like the United Nations [119] and Rockefeller Foundation [120] promote similar goals across partner nations to establish resilient cities to future catastrophes. In all cases, the resilience of electric power systems receive particular interest, as electricity is essential to the provision of nearly all other infrastructure services. Power grid resilience research now produces a constant stream of novel analytical techniques to predict and reduce systemic losses associated with infrastructure failures, natural disasters, and terrorist attacks [31], [121], [122]. Despite these efforts, even the most modern power grids continue to experience large-scale blackouts. Countries like the US [123], India [124], Ukraine [125], and Australia [126] suffered major brownouts and blackouts between 2011 and 2016 from a broad range of events from extreme weather to cyberattack.

We argue the lack of resilience in critical infrastructure is, in part, due to overemphasizing technological solutions that underestimate crisis decision-making and social context [127]–[130]. Currently, power system protection focuses on hardening existing system components and designing automated, redundant, smart, or otherwise technological solutions to reduce the probability of losses [128], [129]. However, reducing the probability of losses via technological solutions alone does not reduce their consequences (i.e., outcome of emergencies), which is dictated by human actions. For example, the 2003 US Northeast blackout included a combination of infrastructure, control system, and decision-making failures that exacerbated unstable conditions and led to cascading damages [131]. Since 2003, post-mortem analysis of several major blackout events continue to recommend improved communication within and across organizations to enhance crisis response [127], [132], [133]. Thus, research should expand awareness beyond technological limitations to include the diverse institutions that influence human decision-making and failure consequences, such as operations and management practices, economic constraints, organizational and industry cultures, and affected parties. We refer to the joint consideration of technological systems with these and other social institutions hereafter as “sociotechnical” analysis [134].

Network science enables one to model the components and interactions of human and infrastructure systems [135], suggesting the potential to develop a sociotechnical network analysis (STNA) for infrastructure resilience. Both electric power grids and human interactions are now studied as networks, yet isolated research does not treat engineering and social science perspectives as equals for sociotechnical guidance. The term “sociotechnical” is primarily used in network science to describe the study of human processes organized or mediated by technology, such as the formation of online social networks like Facebook and Twitter [136], traffic flows on transportation systems [137], or human interactions on communication networks [138]–[140]. Instead, we use the term STNA to describe the application of sociotechnical systems theory [19] to technological and human networks coupled by a single context. The tenets of sociotechnical systems theory can be translated into infrastructure network models by analyzing both social and technological networks together to avoid unpredictable and harmful recommendations from narrow perspectives on a single system [62], and by considering the tasks taken by social units and the expected function of technological systems alongside network structure [32]. A STNA of blackout management, thus, requires both infrastructure networks of substations, generators, transmission lines, and transformers as nodes and links [141] alongside social networks of human constructs like actors and their relational ties (e.g., who knows whom) [142], not one or the other. A STNA also requires knowledge of how power systems provide electric power services and the tasks people and organizations take to ensure services remain available. We argue that this form of STNA better supports the design of resilient power grids than those extant in the literature by integrating knowledge from engineering and social science without marginalizing either. To the best of the authors' knowledge, this form of STNA is also novel as no network studies in the literature give built and human systems equal consideration.

In this work, we develop the first STNA of a power grid to improve blackout response. We construct corresponding infrastructure and social networks and study them to identify critical components. We use results from power grid analysis in a new way by converting knowledge of critical infrastructure into demographic data of the organizations that manage their failures when lost. We further combine these results with a social network analysis of the formal institutions that dictate crisis coordination during large-scale blackouts [143]–[145]. The social network analysis reveals important organizations that fulfill coordination roles among them. Together, these analyses uncover which organizations are critical to power system protection from both engineering and administrative perspectives, and can offer ways to improve blackout management policies that either analysis is incapable of offering its own.

Due to the significant amount of context-specific data required for STNA, this work centers on a single case study location: the South Korean power grid (KPG). In 2011, the worst brownout experienced in Korea caused roughly half of Seoul to lose power and was exacerbated by slowed decision-making processes across operator and regulatory agencies [146]. In 2013, corruption among regulatory officials lead to nationwide power shortages after components in Korean nuclear power plants were found to have forged reliability documentation [147]. In 2014, the national tragedy of a ferry capsizing and killing 295 people (mostly children) [148] triggered the reorganization of the entire Korean emergency management industry to centralize crisis coordination efforts into a single agency [149]. In 2016 a city-wide blackout in Jeonggwan New City was exacerbated by a failure to deploy backup infrastructure stored on the other side of the country. Taken together, a case study of the KPG will have broad impacts on Korean society as the South Korean grid in need of social and technological guidance for blackout response.

Background on Korean Electric Power and Emergency Management Industries

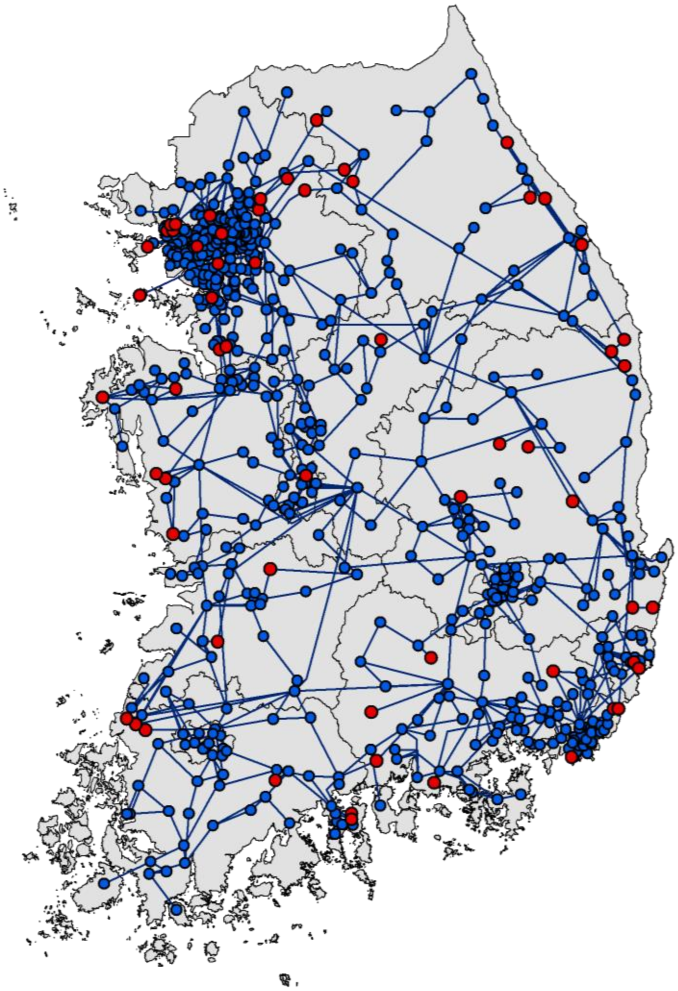


Figure 12 Map of the 2013 South Korean Power Grid. This map shows the connectivity of major power grid infrastructure in mainland Korea, i.e., power plants (red circles), high-voltage transmission substations (dark blue circles), and power lines (dark blue lines). Transformers connect buses that are too close together to be shown in this image. For security purposes data is simplified to only publicly available data from the Korean Power Exchange [204]**. Jeju Island off the southern coast of Korea is also excluded from the image because it is not considered in the current analysis.**

The KPG is an islanded power system which has two primary parts, a large mainland grid serving the majority of Korea and a smaller, self-contained grid on the island state of Jeju-Do. In this work, we focus on the mainland KPG. The mainland grid has voltage classes from 765 kV to as low as 3.3 kV, yet ~55.1% of substation and 96% of power line infrastructure is either 345 and 154 kV (Fig. 12) [150]. The 345 and 154 kV transmission infrastructure are geographically clustered in population-dense regions such as the Seoul Metropolitan Area in the Northwest. Korean power generation is dominated by coal, natural gas, and nuclear power technologies, and this power production is geographically centralized, where roughly 95% of installed capacity is located in 55 separate sites throughout the county [151].

KPG infrastructure is owned and operated by a few, key organizations (Table 8). Korean power transmission and distribution is managed by a single company, the Korea Power Exchange (KPX) and infrastructure ownership and maintenance is dominated by a separate company, the Korean Electric Power Corporation (KEPCO). During crises, KPX and KEPCO act as focal points for grid status, health, and management across the nation – KPX managing power flow and operations decisions and KEPCO managing power line and infrastructure recovery. KEPCO has 6 generation subsidiaries that independently operate and manage ~97% of Korean grid [152]. Liquid fuel, natural gas, and coal-fired power plants are owned and operated by 5 of the 6 generation subsidiaries, each with roughly the same total generation capacity – 10-15 GW. The single largest generation subsidiary (~20 GW) is Korea's sole owner and operator of all nuclear power plants, Korea Hydro Nuclear Power (KHNP). Besides nuclear and fossil fuel generation, ~7% of electricity is generated from hydroelectric and renewable sources. KHNP and other KEPCO subsidiaries operate single purpose dams (power generation) whereas the Korean Water Administration (Kwater) manages all Korean multi-purpose dams (power, water supply, and flood control).

Korean blackout response requires the coordination of electric power regulators (Table 8) and emergency managers for decision-making and crisis support (Table 9). KPX is the established hub for minor blackout incidents. Ministries and support organizations provide additional oversight in larger events depending upon the type of generation technologies involved (Table 8). For major fires, typhoons, earthquakes, and terrorist attacks, the power industry coordinates with first-responder and emergency management organizations (fire fighters, police, and crisis mangers) to mitigate and recover failed infrastructure. Federal regulatory and crisis coordination agencies also become involved in decision-making in worst case scenarios where national power availability is deemed vulnerable. The Ministry of Trade, Industry, and Energy (MOTIE) is the acting headquarters for man-made disasters including infrastructure failure due to human error or intentional attack, and works with KPX and KEPCO to respond to national

Table 8 Electric Power Industry Organizations

Operation & Management			Regulation & Decision Making	
		% Gen Capacity		
Power Transmission:	Korea Electric Power Corp Korean Power Exchange		***Industry-wide:***	Ministry of Trade, Industry, and Energy Korea Electricity Commission
Thermoelectric Power:	Korea Midland Power*	12.0%	***Sector Specific -- Nuclear:***	Nuclear Safety and Security Commission Korea Institute of Nuclear Safety
	Korea Western Power*	10.6%		
	Korea East-West Power*	10.6%		
	Korea Southern Power*	9.6%	***Sector Specific -- Hydroelectric:***	Ministry of Land, Infrastructure, and Transport Kum River Flood Control Office Youngsan River Flood Control Office Nakdong River Flood Control Office Han River Flood Control Office
	Korea Southeast Power*	9.6%		
	POSCO Power	3.1%		
	SK Energy	2.1%		
	K-Power LTD	1.2%		
	Korea District Heating Corp	1.2%		
	Meiya Power Company	1.2%		
	GS EPS	1.1%		
	Hyundai Corporation	1.1%		
Nuclear Power:	Korea Hydro Nuclear Power*	29.0%		
Hydroelectric Power:	Korea Water Administration	2.9%		
	Korea Hydro Nuclear Power*	--		

*subsidiary of Korean Electric Power Corporation. Note: only companies with >1% of total generation capacity for Korea are listed.

Table 9 Disaster Management Industry Organizations

Local Operations & Management		Federal Operations & Management	
Crisis Operations -- State:	Gyeonggi Firefighting & Disaster HQ Gangwon Fire HQ Chungcheongbuk HQ of Fire Mgmt. Chungcheongnam Fire Safety Office Jeollabuk Fire Dept. HQ Jeollanam Fire Safety HQ Gyeongsangbuk Fire Protection HQ Gyeongsangnam Fire Service HQ Jeju Fire & Disaster Mgmt. HQ*	***Crisis Coordination:***	Ministry of Trade, Industry, and Energy Ministry of Security and Public Administration National Emergency Management Agency
		Oversight:	Prime Minister's Office National Security Office
Crisis Operations - City:	Seoul Fire & Disaster HQ Busan Fire Department Incheon Fire & Safety Mgmt. Dept. Daejeon Fire Fighting Head Office Gwangju Fire Safety HQ Daegu Fire Fighting HQ Ulsan Fire & Disaster HQ	***Additional Federal Support:***	Ministry of Land, Infrastructure, and Transport Ministry of Strategy and Finance Ministry of Employment and Labor Ministry of Health and Wellness Ministry of Defense National Police Agency Ministry of Culture, Sports, and Tourism Korean Communications Commission Korean Meteorological Agency

*Jeju Island is not included in the current analysis. Note: based on 2013 data.

blackouts. MOTIE's disaster management division works with the National Emergency Management Agency (NEMA) and the Ministry of Security and Public Administration (MOSPA) to monitor and manage natural disasters. When MOTIE, NEMA, or MOSPA are involved in disaster management, MOTIE is the final decision-maker for built infrastructure and NEMA coordinates crisis support across a hierarchy of state and special city crisis headquarters to city, county, and district fire, police, and emergency management agencies.

Our description of the KPG and related crisis management organizations is based on 2013-2014 data collected from and verified by experts in formal interviews. We focus on this timeframe to ensure that power system analyses match with blackout management analyses. Since then, MOSPA and NEMA have become part of the same organization, the Ministry of Public Security and Safety (MPSS). Nonetheless, analysis of this blackout management system is a critical case relevant for many current policies and practices that remain intact, and all conclusions made in this work are applicable to the most recent organizational relationships.

Materials and Methods

Data for Network Analysis

Power Grid Networks

The KPG data was directly provided as a PSS/E (power system simulation for engineering) printout by KEPCO, and was converted into a complex network using methods similar to those described in Kim et al. [150]. We assessed the extracted KPG model with Matlab packages for optimal power flow [153] and complex network analysis [154], [155]. We use the Direct Current (DC) power flow approximation for all analyses [153]. Power flow analysis was calculated with the summer-time generation and demand dispatch for peak system load used by KEPCO for power system planning.

Korean Power Grid Emergency Networks

Primary data for the interorganizational blackout management social network was collected through semi-structured interviews with Korean electric power industry experts. 14 expert interviews ranging from 30 minutes to 2 hours in length were held in South Korea over two 3 month periods in 2014 and 2015. A total of 12.7 hours of interviews were held. Experts interviewed include industry and academic experts from the following organizations: KEPCO, KPX, KHNP, NEMA, KMA, Kwater, Seoul National University, and Ulsan National Institute of Science and Technology. In these interviews experts provided researchers with 208 pages of primary documents outlining various power system emergency protocols that were verified among interviewees. These primary documents were coded to determine the specific roles of different power system organizations identified in Tables 1 and 2. Additional interviews were then held to clarify roles and explicit information sharing and decision-making relationships among power grid and emergency management organizations.

Together, the interviews and coded documents resulted in social network models of the formal institutions for blackout management in South Korea, where nodes represent organizations in Tables 1 and 2 and links represent bi-directional information sharing and decision-making relationships. These networks are detailed representations of real policies and protocols to the best of the authors' knowledge and incorporate additional expert input for their accuracy of relationships.

The shifting context of power grid operations and decision-making changes with power system health, defined by system reserve margin, and requires the creation and analysis of six blackout management social networks. Six reserve margin thresholds are defined in Korean policies, one for normal operations, one for minor events that do not reduce reserve margin past set thresholds, and four for increasing blackout risks as backup power becomes less available and the system becomes more unstable. We label these thresholds by associated titles denoted within the protocols themselves, with increasing risk of blackout from prevention activities to Alarm Red.

- **Normal Operations:** State/city emergency management agencies coordinate infrastructure failure response directly with power infrastructure owners and operators. This network applies when infrastructure losses do not affect power grid reserve margin.
- **No Alarm – Prevention:** KPX provides blackout coordination to protect the power grid and some coordination still exists between state/city emergency managers and infrastructure owner/operators

- **Alarm Blue – Concern:** KPX serves primary blackout coordination role between electric power and emergency management industries. Industry-specific regulators like the MOTIE provide industry oversight.
- **Alarm Yellow – Caution:** Additional oversight ministries involved in coordination efforts and first responder decision-making shifts from emergency management agencies to city/state governor offices.
- **Alarm Orange – Alert:** Crisis coordination and decision-making switches from electric power industry organizations to the MOSPA and the NEMA.
- **Alarm Red – Serious:** All communication and decision-making between industries mediated by Korean Federal Ministries with increasing Ministerial participation (e.g., inclusion of military support).

Network Analysis Methods

Betweenness of Infrastructure Networks

The resilience of a power grid must be understood with respect to the service it provides [62] – the delivery of electricity from generation to distribution substations that then serve point of use. This generation-demand relationship corresponds to social network theory via “package”-based flow processes [156]. Unlike other social process such as gossip that transfers information among actors in an unregulated, probabilistic way, packages are assumed to have explicit destinations. Information sharing and decision-making among blackout crisis managers follow a similar package delivery relationship due to the regulated nature of the industry.

The “package delivery” structure and function of the KPG indicates that betweenness, which measures the flow contribution of network elements, can be used to identify critical components in both infrastructure and social networks. Betweenness in abstract graphs is based on the “geodesic path (or shortest path)” from node i to j. The set of all geodesic paths between any two nodes i and j is referred to as the “minimum cut set” of i and j. Following this definition, the “betweenness” of a node or link (B_v) is the total number of geodesic paths the network element v resides on (σ_{ij}^{v}) normalized by the total number of geodesic paths (σ_{ij}) in a network [135], following:

$$B_v = \sum_{i \neq v \neq j \in N} \frac{\sigma_{ij}^{v}}{\sigma_{ij}} \qquad (1)$$

When used in power grid networks, betweenness identifies critical infrastructure whose loss may initiate cascading failures [157]. The same measure in crisis management networks identifies authoritative actors that broker emergency information and decision-making rights among disconnected groups [143], [145], [158]. Thus, betweenness analysis should identify infrastructures that have the greatest influence on power delivery and partnerships that dictate crisis coordination activities.

Additional Power Grid Betweenness Measures

B_v in Eq. 1 assumes that all links and nodes are equivalent (unweighted and homogeneous), which is not true of real power grids. Within the KPG, different characteristic infrastructures extract electricity from the network, constraining the total number of origin-destination flow paths within the resulting graph. Moreover, power system infrastructure (e.g., power lines) have electrical properties that impede and limit electricity from travelling along paths, further constraining potential flow. Thus, Eq. 1may produce an unrealistic ranking of critical network elements by ignoring relevant power system characteristics.

In response to the perceived impracticality of Eq. 1 for power grids, researchers have developed betweenness measures that include relevant power system data for assessing flow contribution. At least two novel electrical betweenness metrics (EB_v^1 and EB_v^2) are proposed in literature to build upon the formation and purpose of Eq. 1. The method developed by Nasiruzzaman et al. [159] combines network science and power system engineering by using geodesic paths weighted based on the amount of power flowing through them.

$$EB_v^1 = \sum_{i \neq v \neq j \in N} \frac{P_{ij}^{v}}{P_{ij}} \qquad (2)$$

where P_{ij} is the maximum power flowing in the shortest path between nodes *i* and *j*, and P_{ij}^{v} is the maximum of inflow and outflow of power at bus v on this shortest path. The feasibility of Eq. 2 for ranking nodes has been studied on numerous IEEE test power systems using both AC [160], [161] and DC [159], [162], [163] power flow models.

Another method developed by Arianos et al. [164]–[166] does not calculate shortest paths, and instead uses simplified power grid vulnerability methods [167] and combines their output to recreate a measure comparable to betweenness. This method measures the sensitivity of nodes and links to the changes in generation and load throughout the system to assess their potential contribution to power flow. First, links are considered to be power lines and transformers ($|\boldsymbol{L}| = M_{lines}$) and nodes are power system buses organized into three sets: generation ($|\boldsymbol{G}| = N_{Gen}$), transmission ($|\boldsymbol{T}| = N_{Trans}$), and distribution ($|\boldsymbol{D}| = N_{Dist}$). Then, power transfer distribution factors [168], f_i^{gd}, are calculated for each power line, $l \in \boldsymbol{L}$, for a unit injection of electricity at a given generation bus, $g \in \boldsymbol{G}$, and a comparable increase in load at distribution bus, $d \in \boldsymbol{D}$. This value is used to determine how the structure of the KPG influences power transmission capacity across all g to d relationships. In addition, it is used to calculate a total transfer capability factor, C_g^d, to ensure all power lines remain within maximum power flow limits for each generation-demand relationship:

$$C_g^d = \min_{l \in \boldsymbol{L}} \left(\frac{P_1^{max}}{f_1^{gd}} \cdots \frac{P_l^{max}}{f_l^{gd}} \cdots \frac{P_M^{max}}{f_M^{gd}} \right) \qquad (3)$$

The bus betweenness of bus *v* combines these two elements – the sensitivity of power lines connected to it and total transfer capability of the grid – and is defined as:

$$EB_v^2 = \frac{1}{2} \sum_{g \in \boldsymbol{G}} \sum_{d \in \boldsymbol{D}} C_g^d \sum_{l \in \boldsymbol{L}^v} \left| f_l^{gd} \right|, \; g \neq v \neq d \qquad (4)$$

where $\boldsymbol{L}^v$ is the set of power lines connected to bus *v* and the factor of $\frac{1}{2}$ deals with double counting flow into and out of nodes. As $\frac{1}{2} C_g^d \sum_{l \in \boldsymbol{L}^v} \left| f_l^{gd} \right|$ can be interpreted as the security constrained contribution to power flow of node *v* for a single generation – load pair, Eq. 4 calculates the total power flowing through *v* relative to all generation – distribution pairs within the system. Thus, Eq. 4 directly measures the contribution of node *v* to flow without determining geodesic paths or minimum cut sets, which is computationally difficult for large networks. The feasibility of Eq. 4 for ranking nodes has been studied on numerous IEEE test power systems and the Italian high voltage transmission grid [164]–[166], [169], [170].

Converting Infrastructure Network Results into Demographic Results

We use all three betweenness measures to find critical power grid infrastructure in the KPG because there is no established “best” option among power grid betweenness measures. Then we aggregate results into demographic data useful to blackout management organizations. We treat each betweenness score as the relative importance of each power grid bus within the KPG characterizing its criticality. Then, we sum normalized scores based on demographic information of where each node is located in South Korea (longitude / latitude location) and ownership information. These two pieces of information aggregate individual node betweenness values into the infrastructure companies that own and operate them (Table 9) and the state or special city run emergency management agency (Table 10).

Additional Social Network Measures

We use general social network analysis measures outlined below to characterize the six blackout management networks and Eq. 1 to identify the critical organizations that broker information for blackout coordination. Social network visualization and analysis was completed using ORA-LITE social network analysis software [171] developed by the Carnegie Mellon Center for Computational Analysis of Social and Organizational Systems.

To compare and contrast blackout management contexts, additional measures are used to characterize network-level properties of all six social networks, including [172]:

- **Network Size:** the number of organizations (nodes) in each network and the number of interactions (links) among organizations.
- **Network Density:** Density is calculated as ratio of network interactions to the total number of possible interactions. Density is a normalized measure ranging from 0 to 1, where 0 indicates an unconnected network and 1 indicates a completely connected network.

- **Network centralization (degree and betweenness):** Network centralization measures the relative importance of highest ranking node for a single network measure to rest of the network. This is expressed as a ratio of the sum of the differences between the highest ranking node and the rest of the nodes in the network to the maximum possible sum of the differences. Freeman [173] defines standard ways to calculate degree and betweenness centralization with the following equations:

$$Network\ Centralization, Degree = \frac{\sum_{i=1}^{n} Deg_{max} - Deg_i}{(n-1)(n-2)} \qquad (5)$$

$$Network\ Centralization, Betweenness = \frac{\sum_{i=1}^{n} Bet_{max} - Bet_i}{(n-1)(n-2)(n-3)} \qquad (6)$$

  where Deg_i is the number of links connected to node *i* (referred to as the degree of *i*), and Deg_{max} is the degree of the node with the most links. Likewise, Bet_i is the betweenness of node *i*, and Bet_{max} is the highest betweenness in the network. All centralization values are between 0 and 1, where 0 indicates no centralization (all nodes equal) and 1 indicates complete centralization (one node dominates the measure).

Results

Aggregated Power Grid Criticality Results

Linking the Korean blackout management industry organizations and infrastructure criticality analysis results implicates the involvement of different power system and emergency management organizations in protecting infrastructure for future blackout events. Table 10 presents the aggregated and normalized criticality scores for the infrastructures owned by power system organizations. All measures implicate KEPCO as owning and operating the majority of critical KPG infrastructure. In particular, B_v and EB_v^1 only identify power generation companies owning and operating fractions of a percent of the critical infrastructure. In contrast, EB_v^2 identifies a much larger participation of power companies in owning and operating critical infrastructure, suggesting that KEPCO and KPX only operate ~50% of the critical infrastructure within the KPG.

The differences between power organizations become more apparent when excluding transmission infrastructure and only comparing the critical generation buses. Even though few power plants are identified as critical, it is important to pinpoint these infrastructures to identify the importance of generation assets to the KPG. We present the relative importance of just these infrastructures to determine which organizations may operate these few, central plants. Here, B_v identifies only a single generation company, Korea Midland Power, as owning and operating critical infrastructure. EB_v^1 and EB_v^2 each identify multiple generation companies, but with varying importance of generation technologies. EB_v^1 implicates thermoelectric power companies as more important than nuclear, and, in contrast, EB_v^2 implicates the exact opposite. Moreover, EB_v^2 produces results quantitatively similar to the percent total installed generation capacity, and is the only measure to suggest power producers not affiliated with KEPCO to own and operate critical buses.

Table 10 Criticality of KPG Buses Aggregated by Power Industry Organizations

	Generation and Transmission			Generation Only			
Power Industry Organizations	**B_v**	**EB_v^1**	**EB_v^2**	**% of Installed Gen Capacity**	**B_v**	**EB_v^1**	**EB_v^2**
KEPCO	100.0%	99.9%	49.9%	--	--	--	--
KHNP	0.0%	0.0%	12.7%	29.0%	0.0%	5.6%	25.3%
KOSEPO	0.0%	0.0%	5.4%	9.6%	0.0%	0.0%	10.8%
KOSPO	0.0%	0.0%	5.1%	9.6%	0.0%	16.9%	10.1%
EWP	0.0%	0.0%	7.0%	10.7%	0.0%	8.5%	13.9%
KOWEPO	0.0%	0.0%	4.5%	10.3%	0.0%	22.6%	8.9%
KOMIPO	0.0%	0.1%	6.3%	12.0%	100.0%	46.4%	12.5%
Kwater	0.0%	0.0%	0.4%	2.9%	0.0%	0.0%	0.7%
Posco Power	0.0%	0.0%	1.7%	3.1%	0.0%	0.0%	3.3%
GS Power Co	0.0%	0.0%	0.3%	0.9%	0.0%	0.0%	0.7%
K-power LTD	0.0%	0.0%	0.5%	1.2%	0.0%	0.0%	0.9%
Korea District Heating	0.0%	0.0%	0.2%	1.2%	0.0%	0.0%	0.5%
Posco E&C LTD	0.0%	0.0%	1.0%	0.8%	0.0%	0.0%	2.0%
GS EPS	0.0%	0.0%	0.6%	1.1%	0.0%	0.0%	1.2%
Meiya Power Co	0.0%	0.0%	0.5%	1.2%	0.0%	0.0%	1.0%
STX Energy	0.0%	0.0%	0.0%	0.1%	0.0%	0.0%	0.0%
Korea Energy Mgmt Corp	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
Daelim Mitsubishi	0.0%	0.0%	1.5%	1.2%	0.0%	0.0%	3.0%
S-Power	0.0%	0.0%	0.1%	0.7%	0.0%	0.0%	0.2%
SK Energy	0.0%	0.0%	2.4%	2.2%	0.0%	0.0%	4.7%
Hyundai Corp	0.0%	0.0%	0.0%	1.1%	0.0%	0.0%	0.0%

We combine infrastructure scores for geographic regions to predict which emergency management headquarters may be involved in crisis response. Fig. 13 presents the aggregated infrastructure results including a frequency plot of power generation and transmission infrastructure in South Korea compared and normalized criticality scores for infrastructure in each state and city region. Although more power system infrastructure is located in the Northwest region surrounding the Seoul Metropolitan Area and the Southern coast (Fig. 13A), the measures indicate that critical infrastructure may be located elsewhere. Method B_v suggests that the vast majority of critical infrastructure is located in the state Gyeonggi-Do (GGD) surrounding Seoul and to a lesser extent the three states making up the center of the country: Chungcheongnam-Do (CCND), Chungcheongbuk-Do (CCBD), and Gyeongsangbuk-Do (GSBD), from east to west, respectively (Fig. 13B). Method EB_v^1 produces results similar to the physical location of infrastructure with greater emphasis on the central and northwest regions of the country instead of Seoul and Incheon cities (Fig. 13C). Method EB_v^2 suggests that Gyeonggi-Do (GGD) is not the most important region, but rather Chungcheongnam-Do (CCND) and Gyeongsangnam-Do (GSND), together, contain nearly 50% of all critical infrastructure (Fig. 13D). Across all methods, the top ranked infrastructures are more often located in three states of Chungcheongnam-Do (CCND), Gyeongsangnam-Do (GSND), and Jeollabuk-Do (JBD).

Blackout Management Social Network Results

Fig. 14 presents general results of network analysis for the six blackout management social networks. Results show that formal policies produce social networks that have increasing organizational inclusion with blackout risk. Formal institutions assume that less risky scenarios require less regulated interactions among electric power and emergency management sectors, and vulnerable situations with lower reserve margins and greater grid instability require more oversight and Federal involvement. This is represented in the network size (Fig. 14A) as the number of organizations connected to the network almost doubles from 43 organizations in Normal Operations to 79 in Alarm Red. The majority of these new nodes represent either emergency managers or federal ministries not involved in minor blackouts, such as governor-level crisis management HQs and the Ministry of Defense.

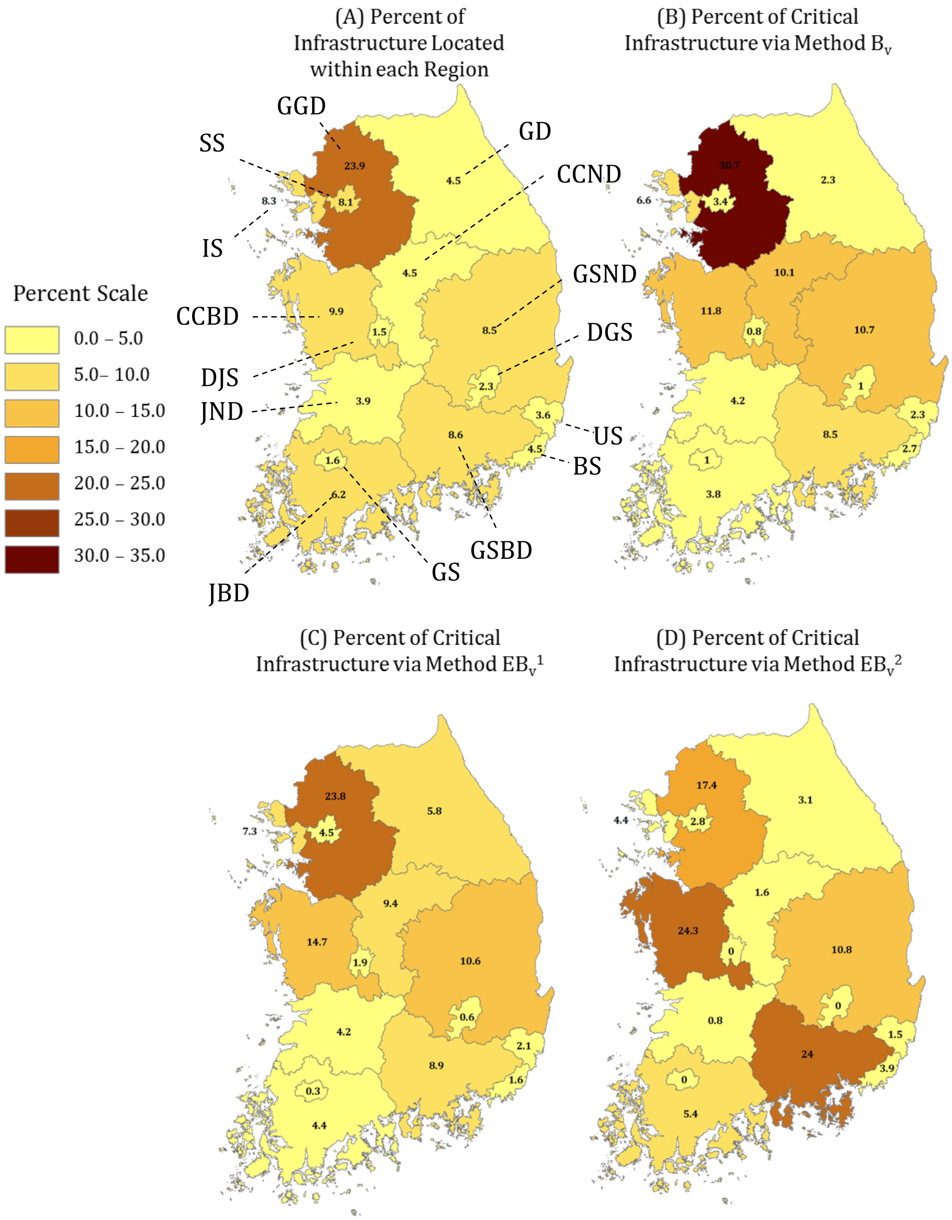


Figure 13 Aggregate Criticality Scores for Korean Power Grid Infrastructure by Emergency Management Region.
The top left image of Korea presents the amount of generation and substation buses located in each region (A), where all other images show the normalized total criticality score for each region (B, C, and D). Thus, percent scale refers to quantity of infrastructure (A) and aggregated criticality score (B, C, and D). Regions are labelled in (A) with abbreviations: Gyeonggi-Do (GGD), Gangwon-Do (GD), Chungcheongnam-Do (CCND), Chungcheongbuk-Do (CCBD), Gyeongsangnam-Do (GSND), Gyeongsangbuk-Do (GSBD), Jeollanam-Do (JND), Jeollabuk-Do (JBD), Seoul-Si (SS), Incheon-Si (IS), Daejeon-Si (DJS), Gwangju-Si (GS), Daegu-Si (DGS), Ulsan-Si (US), and Busan-Si (BS).

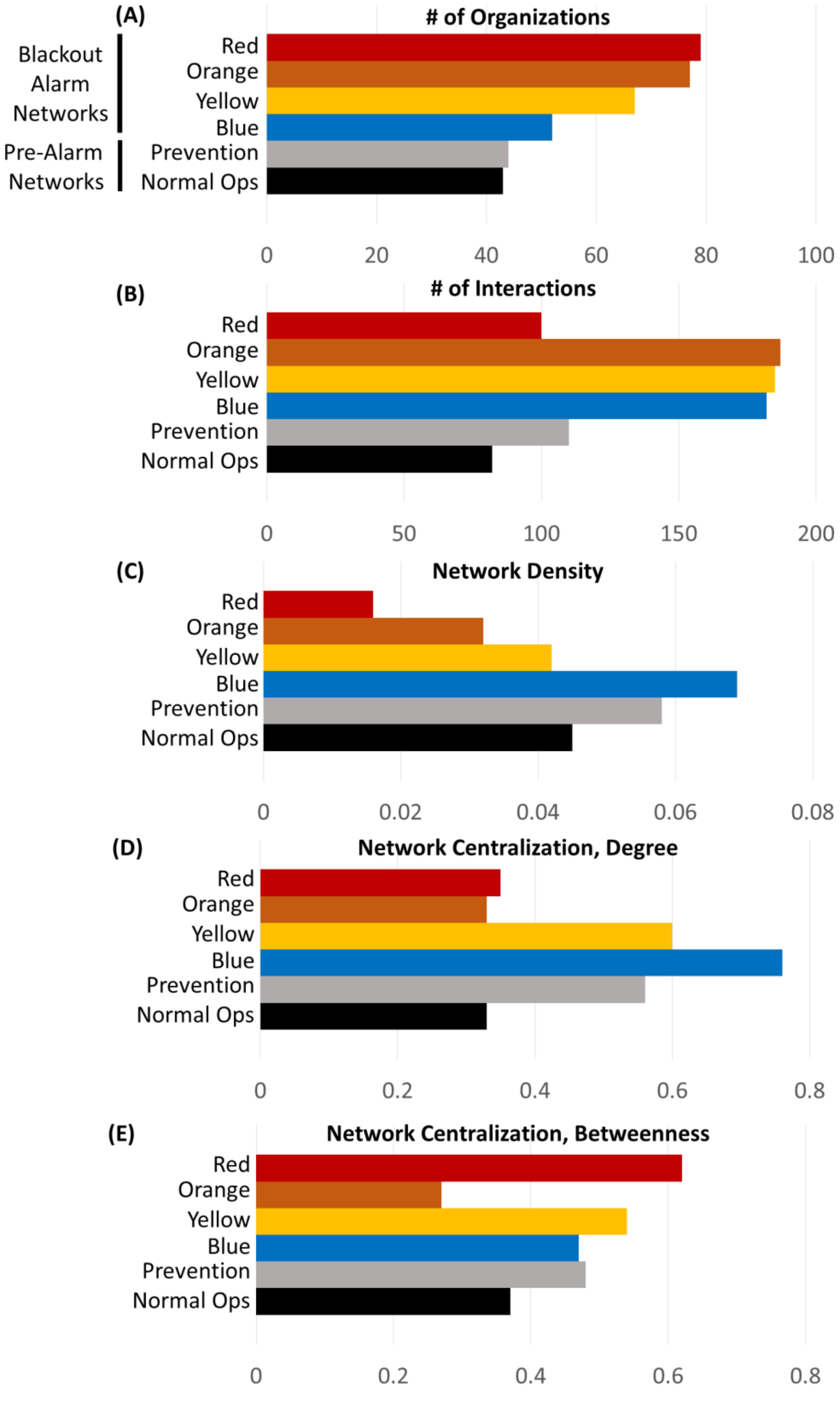


Figure 14 Network-Level Results for Korean Blackout Management Social Networks. We characterize the 6 blackout management social networks (y-axes) with five characteristic network-level measures (x-axes). (A-B) Social network size is measured by the total number of organizations and interactions (i.e., links). (C) Network density, (D) centralization of degree, and (E) centralization of betweenness are normalized values ranging from 0 to 1 (see Methods).

The decision-making authority of the electric power industry peaks when the first blackout alarm is activated (Alarm Blue) and then shifts to the emergency management industry, as represented by the number of links (Fig. 14B), network density (Fig. 14C), and centralization of node degree (Fig. 14D). All three measures show peaking trends as blackout alarms increase in severity. Even though the number of nodes among networks steadily increase with crisis risk level, the number of links peak around ~180 links and then decreases to 100 at Alarm Red. This sudden drop in links corresponds with the transition of decision-making and information-sharing authority from the electric power to the emergency management industry. Moreover, the network density and centralization of degree peak at Alarm Blue and decrease across all four alarms, corresponding with the initial centralization of authority among the electric power industry and its diffusion into emergency management organizations as they join to the network.

Fig. 14E also demonstrates variability in the centralization of blackout coordination activities among sectors with the centralization of betweenness. The centralization of betweenness increases across the first four networks, drops to its minimum at Alarm Orange, and is at its maximum in Alarm Red. The low centralization of betweenness of Alarm Orange when compared to Alarm Yellow or Red corresponds to the electric power and emergency management industries sharing information brokerage activities almost equally for that interorganizational configuration. All other instances with high centralization of betweenness will have a single organization as the most central crisis coordinator.

Nodal betweenness identifies that organizations with fewer decision-making roles than others tend to broker information during blackouts. Betweenness results presented in Fig. 15 identify the specific organizations that act as information hubs for blackout response. KEPCO and Gyeonggi-Do Fire Mgmt. HQ share central crisis coordination roles for Normal Operations, KPX is the most central organization for Prevention, Alarm Blue, and Alarm Yellow, NEMA and KPX share coordination for Alarm Orange, and NEMA is the central coordinator for Alarm Red. These results correspond to general perspectives held by blackout management experts that either KPX or NEMA is the crisis management HQ for blackouts. Still, KPX and NEMA have fewer decision-making roles as outlined in formal protocols and may not be best suited for being the central information broker. The number of roles assigned to each organization (labelled next to its name) reveal that MOTIE (33), KEPCO (19), and MOSPA (19) have far more blackout management roles to fulfil than KPX (6) and NEMA (6). This result indicates that decisions made by authoritative organizations must travel through intermediary organizations before reaching their final destination.

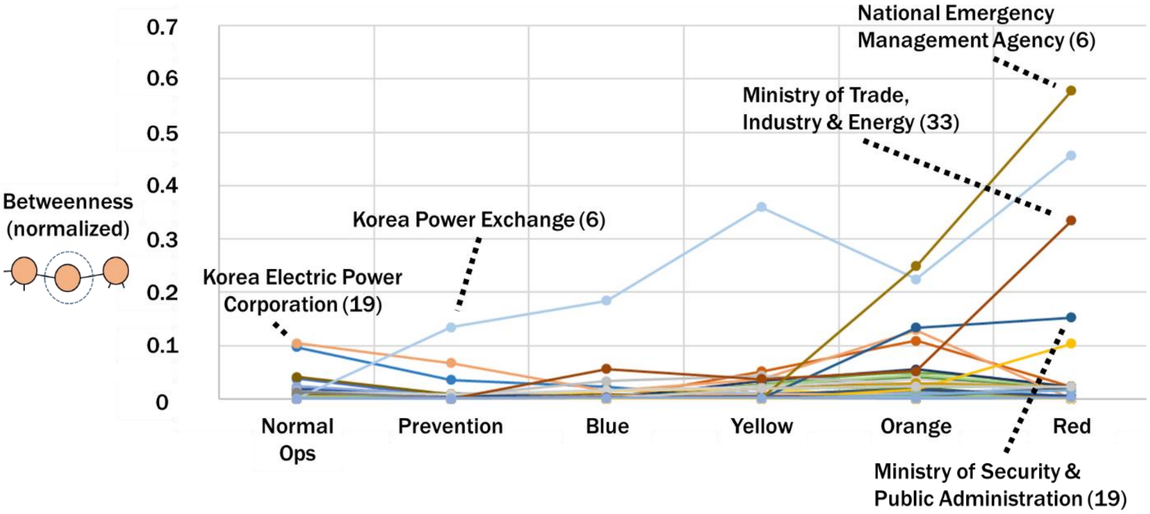


Figure 15 Betweenness and Number of Roles for Korean Blackout Management Organizations.
Each line represents a different organization. As the majority of organizations are periphery actors, they have low betweenness compared to few central, coordinating organizations. These central and important organizations are labelled: name (number of crisis management roles). Results demonstrate that few organizations from both electric power and emergency management sectors are the key crisis coordinator for different blackout risks, specifically: KEPCO, KPX, and NEMA. In contrast, MOTIE and MOSPA are key decision-making organizations, yet remain periphery to information brokerage.

Discussion

Implications for Blackout Management Protocols from the Infrastructure Perspective

Results suggest that certain generation companies may be more involved in future blackout scenarios. Current blackout management policies make limited differentiation between organizational roles between generation companies, which may be inappropriate when each company owns and operates different amounts of critical infrastructure. For example, both B_v and

EB_v^1 would recommend increased protection and recovery capacity be located at generation facilities owned and operated by Korea Midland Power, where EB_v^2 results emphasize nuclear power plants managed by KHNP and relatively equivalent treatment of other KEPCO subsidiaries. Moreover, EB_v^2 highlights differences among private power producers that manage an appreciable amount of critical infrastructure like SK Energy, Posco Power, and Daelim Mitsubishi that are not reflected in crisis management protocols. Based on these results, we recommend crisis management policies make more explicit roles for the KEPCO subsidiaries and private power companies that operate these critical infrastructures to emphasize their potential involvement in blackout response.

Specific state and city headquarters have a greater chance of being the crisis management authority in large-scale blackout support activities than others. Combining results across measures, Chungcheongnam-Do (CCND), Gyeongsangnam-Do (GSND), and Jeollabuk-Do (JBD) house the more critical power grid infrastructure than other regions. Moreover, aggregate scores for regions consistently score states higher than cities, with Gyeonggi-Do (GGD), Chungcheongnam-Do (CCND), Gyeongsangbuk-Do (GSBD), and Gyeongsangnam-Do (GSND) receiving top ranks across multiple methods. Whereas existing national blackout management policies treat emergency management HQs equivalently, more focused policies may highlight power system protection and response in these regions. For example, the most recent blackout in Korea which occurred in the Southeastern region of Gyeongsangnam-Do (GSND) was exacerbated as backup infrastructure was only housed in Seoul. Reorienting crisis response resources to match these results would have led to a shorter blackout duration by maintaining backup transformers near more critical substations.

Implications for Blackout Management from the Social Network Perspective

This analysis is the first to take a system-wide perspective on blackout management and identify when decision-making and information-sharing authority shifts between industries. Policies and protocols outline explicit decision-making and information-sharing roles, and experts are aware of the interactions among multiple sectors. However, explicit transitions in authority are not outlined in formal institutions making it difficult for actors to predict which electric power or emergency management organization will be the central coordinating body when alarms are activated. Network-level analysis demonstrates a transition in authority between the electric power and emergency management industries associated with a drop in number of links, network density, average degree, and centralization of degree and an increase in centralization of betweenness. Decision-making is most centralized in the power industry for Alarm Blue and makes a transition to the emergency management industry between Alarms Orange and Red. Experts can use this information to determine if current reserve margin and power system stability measures are effective for creating the wanted decision-making context to handle blackout risk.

Betweenness results indicate that there may be a mismatch between blackout decision-making authority and information brokerage in South Korea, suggesting a need to restructure current policies. Although KPX and NEMA are identified as central hubs for power grid and emergency management information, they are not the central decision-makers. Having central actors be involved in information-sharing is vital for successful blackout response, as effective coordination avoids the duplication of work, hindrance of first responders, delays due to misunderstanding, and inappropriate allocation of resources [174]. Crises including the 2011 Seoul Brownout, 2013 Corruption Scandal, 2014 Ferry Tragedy, and 2016 Blackout were exacerbated by hindrances like the infeasibility to centrally manage, role ambiguity, and unbalanced workload distribution. Restructuring blackout response policies to centralize actors with greater decision-making authority may alleviate this issue. MOTIE, in particular, is identified through interviews as an important organization for decision-making and oversight, yet remains a periphery node within all networks for information brokerage. Making MOTIE a central node is a possible way to improve coordination activities. We recommend doing this for intermediary networks that transition authority between sectors like Alarm Yellow and Orange as MOTIE has equal authority to other Federal organizations where KPX does not. Thus, we recommend that future policies restructure policies to centralize MOTIE for Alarms Yellow and Orange to support decision-making and shifting authority among industries.

Combined Guidance

Completing infrastructure and interorganizational network analyses side-by-side offers combined recommendations to improve blackout management in South Korea. The results from both network analysis are complementary as infrastructure analysis identifies which periphery organizations own, operate, and respond to critical infrastructure failures and social network analysis identifies which organizations coordinate decision-making and information-sharing among them. Betweenness results for the social network further indicate that there is a mismatch between organizational authority and information brokerage that may require updating protocols to restructure the network. While above recommendations for improving formal policies may be helpful, they remain superficial by not specifying how improvements are to be made. For example, social network analysis can offer the recommendation to restructure the social network to centralize MOTIE for Alarms Yellow and Orange, but cannot specify which paths or organizations should be involved in restructuring. Instead, the results from infrastructure network analysis identifies critical organizations that should be involved in these heightened blackout risk scenarios. Our combined recommendation is then to restructure formal institutions to increase information flow among the power companies Korea Midland Power, SK Energy, Posco Power, and Daelim Mitsubishi the emergency management agencies in Chungcheongnam-Do, Gyeongsangnam-Do, and Jeollabuk-Do and MOTIE.

Conclusion

Blackouts continue to occur across the globe due to failed blackout coordination activities, and power grid resilience depends upon effective formal policies and protocols to handle emergency response. We identify critical cases in which blackout coordination does not match infrastructure failure needs in South Korea by conducting STNA with matching data from 2013 for KPG infrastructure and blackout management policies. In the KPG, separate analysis of infrastructure and interorganizational networks provide insight into the cause of recent, exacerbated events. Power grid criticality analysis shows that some infrastructures and organizations may be disproportionately involved in large-scale events, yet formal policies do not distinguish between them. Social network analysis characterizes the transition of authority among sectors and organizations to help guide more precise use of policies to manage future events.

Still, each analysis on its own can only provide broad recommendations for improving institutions rather than specific changes to policy. Combined results instead pinpoint the specific social networks and organizations that needed to be changed when updating future policies.

This work demonstrates that the growing number of studies comparing criticality measures for other real-world power systems [169], [175]–[177] or developing social networks around infrastructure systems [137] would benefit from linking technological analyses to social context. Since the majority of academic literature does not bridge infrastructure and social contexts, power grid protection and resilience may be undermined by overlooking the social consequences of technical recommendations. The inclusion of ownership and jurisdictional boundaries in this work revealed Korean organizations whose actions may have greater influence on power grid protection than others. In interconnected grids, a similar analysis may highlight local decision-makers that have disproportionate authority over power system security that crosses utility, state, and country borders. The same is true for social network analysis of actors that manage infrastructure systems. Taking a public administration perspective while ignoring the interconnected and complex infrastructure system it surrounds may overlook salient interactions that connect social entities but exist in the technology. Crisis management protocols made without reference to the physical limitations of existing infrastructure creates latent weaknesses embedded in policy which may exacerbate damages in future emergencies. The sociotechnical network analysis presented herein offers one way to overcome these issues.

CHAPTER 5

ADVANCING CASCADING FAILURE MODELS FOR IMPROVED BLACKOUT MANAGEMENT IN SOUTH KOREA

This chapter is in preparation for the journal *Nature Energy* and appears as is prior to submission. The citation for this article is: Eisenberg, D.A., Seager, T.P., Park, J. (2018) Advancing Cascading Failure Models for Improved Blackout Management. *Nature Energy*, in review

Introduction

One of most important research innovations for measuring cascading failure vulnerability in power systems is the cascading failure model [178]–[181]. The 2003 blackout across the US and Canada was one of the first well-documented cascading failure events, where small losses caused by trees touching power lines, demand imbalances, and out of date operational models eventually led to the biggest blackout in North American history [132]. Since 2003, numerous large-scale blackouts occurred across the world initiated by diverse events like natural disasters and cyber attack [124]. Even with a growing number of documented cascading failure events, there is limited information to form a generalizable understanding of cascading failures in power grids. Instead, researchers turn to cascading failure models as a means to simulate cascades, study different failure mechanisms, and predict expected losses. There are three general types of models, each relating power grid vulnerability to a different aspect of power grids: network-based models that relate vulnerability to system structure and connectivity, dynamics-based models that relate vulnerability to electric power flow redistribution, and component-based models that relate vulnerability to joint probabilities and stochastic losses [181], [182]. Prominent models in literature include CLM [183], Motter-Lai [184], Oak Ridge–Pserc– Alaska (OPA) [185], [186], Hidden Failure [187], the Manchester Model [179], Branching Process [181], and CASCADE [181]. Several reviews summarize model development, applications, validation in power grids [178]–[181], [188]. Taken together, cascading failure models represent an important means to improve power grid resilience by estimating total losses expected when cascades occur and guide decision-making by revealing critical infrastructures whose failure may cause cascades.

With a growing library of tools for predicting and controlling cascading failures, the question remains: do these models make people more prepared for cascading failures? In their current form, guidance is limited because essentially all studies focus on predicting the consequences of cascades without considering the complex decision-making situations during cascades. While predating consequences helps identify critical infrastructure components and offers solutions to reduce the probability that they fail, it does little to support human response when failures eventually happen. Some power grid cascades occur on a sub-second timescale faster than humans can respond where these hardening activities are essential. Still, the majority of large-scale failures happen on the minute and hour timescales and elicit human response [181]. Power grid system operators are not complacent when infrastructure fails, they act according to reliability standards and protocols [33]. Common actions taken include remedial efforts to adjust power flows, protect vulnerable infrastructures, prepare backup resources, and coordinate with relevant owner and regulator organizations. Operators and managers are also trained in a number of worst-case scenarios and develop heuristics for managing known instabilities within their own systems. Current cascading failure models to do not consider these human actions and assume that cascading failure processes are captured entirely by in the built components of power grids. In other words, existing cascading failure models assume that cascading failure operations are equivalent to normal grid operations.

However, cascading failures are not normal, and are precisely when current decision-making practices stretch to their limits. Cascades often occur because power system failures originate from risks never experienced before. For example, massive losses caused by a few downed power lines touching trees seemed impossible prior to the 2003 North American blackout. More recent cascades during Superstorm Sandy [31] and Hurricane Irma [189] have little resemblance to the 2003 event, as losses were caused by excessive storm surge and winds that stretched the imagination of seasonal weather conditions. This shifting pattern of risk is a common factor across many large-scale blackouts, and cascading failure models should be oriented to study what people do during unimaginable events that lack prior knowledge. Representing the human-in-the-loop during cascades is important as adaptive human actions are often the reason systems are saved or lost during crisis. In best-case scenarios, human actions may manage cascades in new and inventive ways never done before. In worst-case scenarios, remedial actions taken by grid operators and managers may exacerbate cascading losses beyond the scope any failure model would predict. In both situations, it is the adaptive actions taken by people that change the outcome cascades, neither of which are considered in existing failure models. Thus, cascading failure models should be refocused to inform how grid operators and managers extend systems when faced with the unknown, rather than and ignore human actions entirely.

We define extensibility as the way people leverage new information and past experience to come up with novel solutions to unforeseen and unknown surprises. Extensibility in power grids is not random, it is based on both situational awareness held by infrastructure operators and managers as events occur and existing training, guidelines, and partnerships. Improving future extensibility requires knowledge of the social context surrounding crisis decision-making alongside sociotechnical processes of sensing, anticipating, adapting and learning as crises occur. Only very recently are studies trying to embed “humans-in-the-cascading failure-loop” to understand how human factors for information collection and use improve or exacerbate losses [124]. Still, there is essentially no knowledge of the social context influencing crisis decision-making when cascades occur, yet a diversity of social factors like utility customer contracts, local operational and management practices, economic constraints, regulations, and organizational culture influence how decisions are made.

In this work, we reimagine the purpose of cascading failure models from measuring consequences to providing a heuristic way to study extensibility in power grids. Each cascading failure model embeds a series of sub-models, including a model to represent the power grid, estimate power flow, initiate cascading failures, iterate to measure additional overloads and failures, and reach a stopping point. We shift the output of these models from total losses, e.g., load shed, to outputs relevant for social context such backup reserve margin, ownership, and the location of losses. This approach links system stress during N-1 failure situations in South Korea to a blackout management social network model for interorganizational coordination (Methods). The resulting social network is comprised of nodes representing organizations and links representing information sharing and coordination partnerships weighted by the frequency and intensity of system stress. Taken together, the social network model is an idealized representation of the interorganizational coordination context expected in South Korea prior to the onset of a large-scale failure and provides a basic structure to understand how organizations may extend coordination activities when faced with surprise.

Generating Cascading Failure Context

South Korean blackout management involves the coordination of several distinct organizational entities to respond to failures, namely infrastructure owners and operators, emergency management offices, and federal agencies involved in regulation and coordination across sectors. Fig. 16 presents the unweighted social network of partnerships among Korean power and emergency management organizations established prior to national emergencies. Fig. 16 is comprised of 43 companies, including transmission infrastructure owners, major power producers each with greater than 10% of national generation capacity, smaller private power companies, and state-level emergency management headquarters for organizing first responder support to power losses.

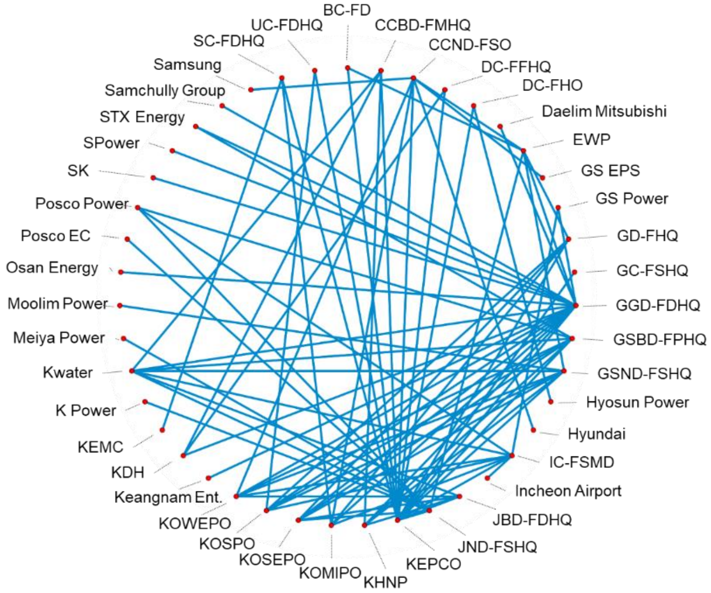


Figure 16 Unweighted Social Network for Korean Blackout Management Organizations. Infrastructure owners, operators, and emergency responders coordinate to manage power grid failures across South Korea. Blue links represent information sharing partnerships that link organizations when problems occur as defined in national blackout management protocols harmonized across the power industry. We use this social network model as a basis for studying blackout management contexts during cascades. *Note:* Based on data from [191]**. See Box 1 for full list of acronyms**

Box 1 List of Acronyms: Korea Electric Power Corp (KEPCO), Korea Hydro-Nuclear Power (KHNP), Korea South East Power (KOSEPO), Korea Southern Power (KOSPO), Korea Western Power (KOWEPO), Korea District Heating (KGH), Korea Energy Mgmt. Corp (KEMC), Seoul City Fire Disaster HQ (SC-FDHQ), Ulsan City Fire Disaster HQ (UC_FDHQ), Busan City Fire Department (BC-FD), Chungcheongbuk-Do Fire Mgmt. HQ (CCBD-FMHQ), Chungcheongnam-Do Fire Safety Office (CCND-FSO), Daegu City Fire Fighting HQ (DC-FFHQ), Daejeon City Fire Head Office (DC-FHO), East West Power (EWP), Gangwon-Do Fire HQ (GD-FHQ), Gwangju City Fire Safety HQ (GC-FSHQ), Gyeonggi-Do Fire Disaster HQ (GGD-FDHQ), Gyeongsangbuk-Do Fire Protection HQ (GSBD-FPHQ), Gyeongsangnam-Do Fire Safety HQ (GSND-FSHQ), Incheon City Fire Safety Mgmt. Department (IC-FSMD), Jeollabuk-Do Fire Dept. HQ (JBD-FDHQ), Jeollanam-Do Fire Service HQ (JND-FSHQ).

Results from our cascading failure model show that N-1 failures only involve partnerships presented in Fig. 16 because they do not cause significant disruptions in national reserve margin (measured as a percentage of available power transfers across the KPG) (Fig. 17). Korean blackout management policies use a series of reserve margin thresholds to establish which organizations serve decision-making and coordination roles, and each threshold relates to a different social network [33]. The KPG is N-1 reliable, and at no point does any N-1 failure lead to the activation of national crisis management thresholds that require the inclusion of organizations or partnerships outside of Fig. 16. This is an expected result as power is dispatched to be N-1 reliable during normal KPG operations.

N-1 losses do lead to a re-weighting of the social network in Fig. 16 based on which organizations are involved after infrastructure is lost (Fig. 17). Our model estimates the redistribution of electricity that forces some power infrastructure to be overloaded or near overload post failure. In most cascading failure models, these overloaded assets are then assumed to fail and cause additional damages. In our model, we assume human action manages the additional cascading losses and allow for the system to correct these imbalances. We initially weight the “pre-failure” social network based on the amount of infrastructure each organization is involved in managing during blackouts and their position within the social network. Then, we use the shifting blackout risk during corrective actions to estimate the subset of blackout coordination partnerships that would be active prior to additional N-2 or N-3 failures. Each individual model run is averaged, and Fig. 17 presents the mean weighting across all links for each phase in the propagation of power grid congestion. These weighted social networks estimate the likely strength of social ties among organizations by embedding the frequency each partnership is used for crisis coordination and the relative system congestion when infrastructure losses occurred.

Guiding Interorganizational Coordination during Blackouts

The combination of social and power grid data leads to changes in the link weights that reveal salient differences in the importance of each organization for blackout management. These differences are captured by the betweenness of each organization (Fig. 18). An organization with high betweenness in social network theory is assumed to be a gatekeeper of information by brokering indirect connections among power companies and emergency management organizations. These gatekeeper organizations act as information sharing hubs, and can support coordination across the Korean power industry.

Fig. 18 presents normalized unweighted betweenness, B_v, and weighted betweenness, B_v^1, for the KPG social network before, during, and after infrastructure failures. Prior to a failure, the weighted social network reveals a significant change in the relative importance of KEPCO and GGD-FDHQ and a rearrangement of importance among emergency management headquarters, e.g., an increase of betweenness of GSBD-FPHQ. During cascades, the importance of KEPCO and GGD-FDHQ remains stable, yet the importance of regional crisis management hubs shifts to reveal the Northwestern emergency management organization, IC-FSMD, as more central during stressed power grid states than those in central and southern regions (CCND-FSO and JND-FSHQ, respectively). GGD-FDHQ and IC-FSMD coordinate response in Gyeonggi-Do and Incheon City, the most populous regions in Korea and surrounding Seoul City, suggesting that N-1 losses are most likely to impact the Northwestern Seoul Metropolitan Area irrespective of where the infrastructure failures occur. This information would be masked without considering the cascading failure context, as the betweenness rank of IC-FSMD both drops and increases across cascading failure iterations.

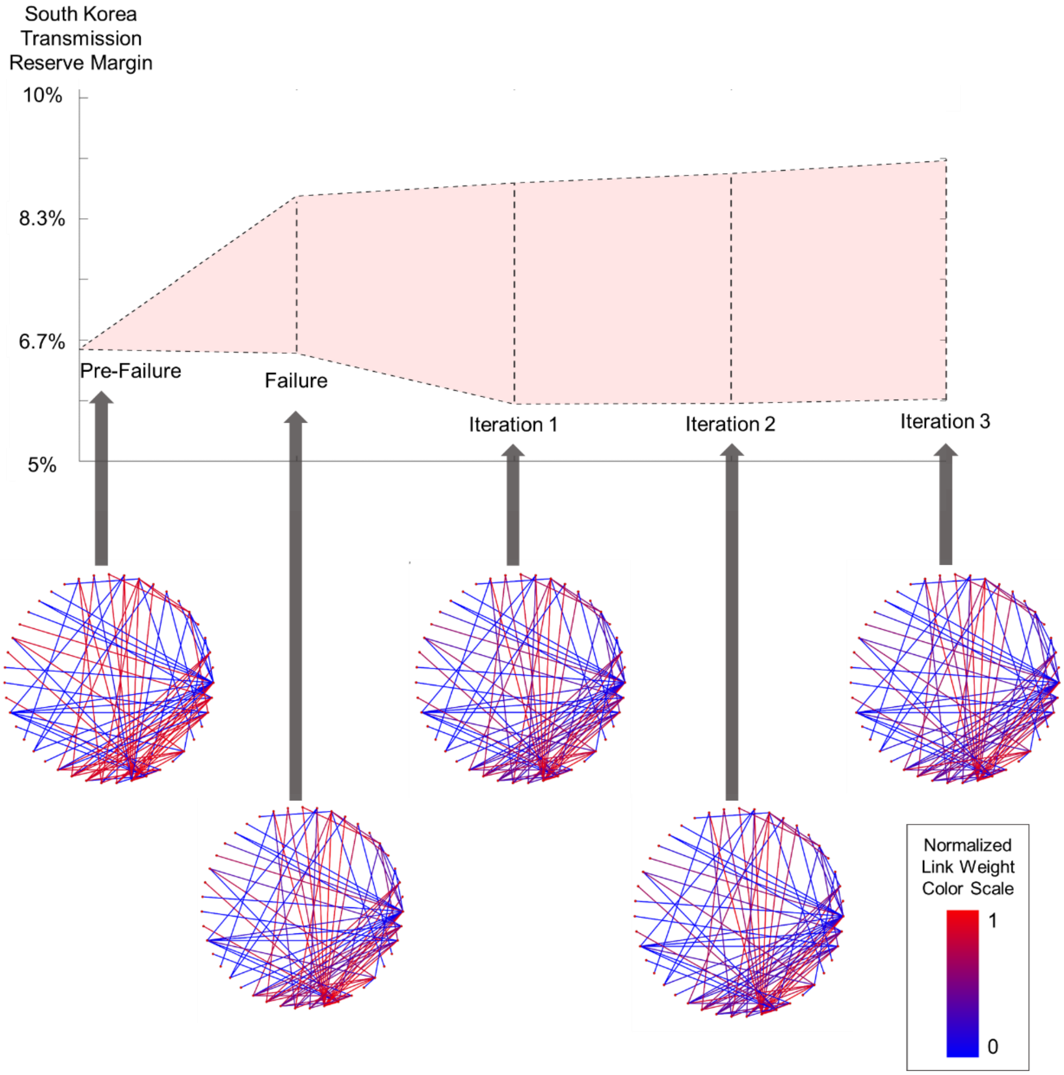


Figure 17 Cascading Failure Results for South Korea and Associated Weighted Blackout Management Social Networks.
When a single substation or generation bus fails, electricity redistributes across the grid and total dispatchable reserve margin changes. The light red region in the above graph encompasses all reserve margin gains and losses from N-1 failures in the South Korean power grid, where top and bottom dashed lines are the largest gains and losses, respectively. Social network links form based on which organization owns and operates stressed infrastructures, where stressed infrastructures are located, and how stressed they are (see Methods). The weight of each social network link is the mean weight across all N-1 failure scenarios with a normalized, maximum partnership strength of 1. Strong and weak partnerships are shown across the cascading process as red and blue links, respectively.

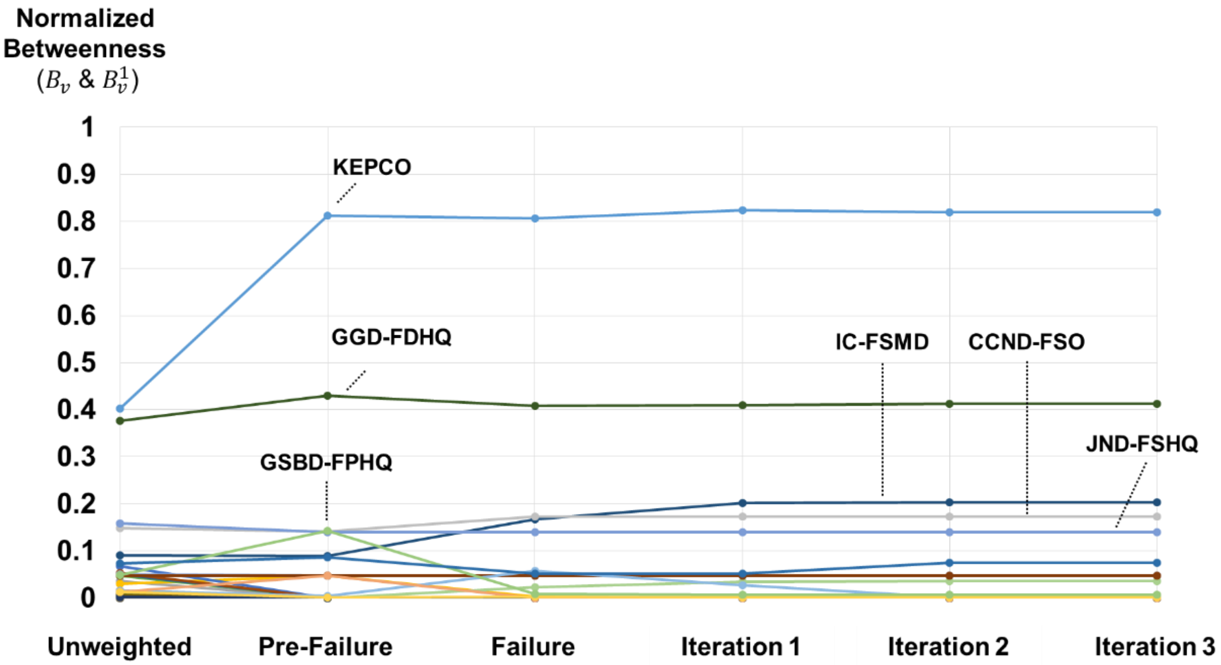


Figure 18 Critical Korean organizations for crisis coordination during cascading failures.
Weighted social networks across each N-1 cascading failure iterations lead to shifting importance of emergency management organizations to supporting blackout response. In particular, IC-FSMD is revealed as a one of the most central organizations for corrective blackout response during N-1 operations. The combination of models reveals the shifting of blackout risk from central and southern regions to the northeastern states that surround Seoul during stressed system states.

We use social network analysis to reveal potential ways for organizations can extend operations within the current framework of national blackout management policies. B_v^1 results are based on strong (frequent) partnerships and represent coordination activities when all organizations serve idealized coordination roles. In surprising situations there is no guarantee that KEPCO, GGD-FDHQ, or IC-FSMD will fulfill its information sharing activities. Instead, B_v^2 identifies which organizations have feasible partnerships to be information sharing hubs, yet are unlikely to fulfill this role in normal situations because partnerships are weak on average. Results presented in Fig. 19 via B_v^2 reveal which organizations that can serve coordination activities in parallel to those identified in B_v^1. By focusing on weak ties, B_v^2 offers a heuristic way to determine which organizations should relinquish or take on coordination activities during surprising situations when KEPCO, GGD-FDHQ, and IC-FSMD need additional support. In particular, B_v^2 suggests that dam and flood control managers (Kwater), emergency management coordinators in southern states (GSBD-FPHQ), and power companies (STX Energy and East West Power) can support extended, cascading failure situations.

Discussion

Combining the structure and function of the KPG with interorganizational demographic information and social network data reveals the interorganizational coordination context of the Korean power grid during crisis. Cascading failures as surprises, by nature, will be unpredictable and will require extensibility by Korean power organizations to fulfill roles they normally would not. Still, it is difficult to pinpoint which organizations support extended and surprising situations in practice, because large-scale failures are infrequent and blackout management protocols treat all power companies and state and city-level emergency management coordinators considered in this study equally. Combining a cascading failure model in the power grid with social network analysis reveals ways to extend coordination prior to the onset of large-scale, surprising failures. Specifically, organizations like KEPCO and IC-FSMD can be supported by extended, parallel coordination efforts in Kwater, GSBD-FPHQ, STX Energy, and EWP. Moreover, GGD-FDHQ and JND-FSHQ remain central across both B_v^1 and B_v^2 measures suggesting that if either organization stopped fulfilling is information sharing role, many parts of the power grid would lack a means to coordinate. In both cases, our model reveals the web of complex social relationships that will change the course of cascades as they occur. This web should be considered in future, more detailed studies that try and predict the total losses expected when failures cascade beyond N-1 scenarios.

Our study can advance national emergency management policies in South Korea to support new, important ways for organizations to manage blackouts. Several Korean infrastructure emergencies demonstrate that centralized emergency management protocols may exacerbate problems. For example, the largest Korean brownout in 2011 was exacerbated from a contained situation outside of Seoul to a cascading loss of electricity across Seoul because of slowed coordination and information sharing activities among power organizations and regulators

[33], [146]. Based on our results, the partnerships among specific Korean organizations make them more effective at supporting emergency management when coordination breaks down. We recommend that additional coordination roles be created among central organizations found across social network measures, e.g., creating new coordination partnerships between KEPCO and GGD-FDHQ with Kwater and STX Energy.

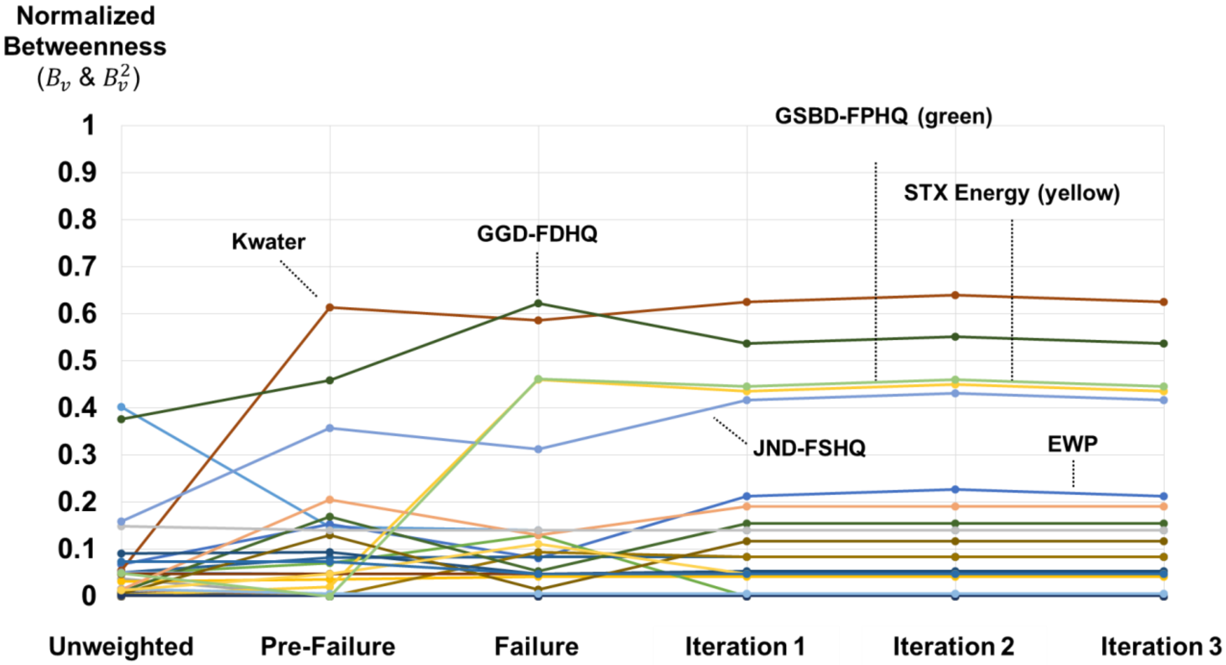


Figure 19 Critical Korean Organizations that can Serve Crisis Coordination during Cascading Failures via Weak Ties.
Weighted social networks reveal unlikely organizations that are central to serve information sharing and coordination roles. In stressed and surprising situations where central organizations identified in Fig. 3 fail to fulfill information sharing activities, Kwater, GSBD-FDPH, STX Energy, and EWP can support coordinated blackout response. Organizations with high ranks in both measures, i.e., GGD-FDHQ and JND-FSHQ, are the most critical to the Korean power grid coordination because they will be relevant to information sharing in both normal and surprising situations.

We feel confident that these minor changes in blackout management protocols will lead to significant changes in the management of future blackouts based on similar changes made recently in earthquake preparedness. In 2016, earthquake response in Gyeongju, South Korea was exacerbated by slowed national response and information sharing to the public [189]. The slowed response was caused by strict, hierarchical decision-making processes policies that were removed post-event to speed up coordination. The recent 2017 earthquake of similar size and velocity near Pohang, South Korea had a much faster response due to these minor policy changes. Since our study is identifying similar ways to avoid bottlenecks in blackout management coordination, we anticipate that the small changes to national crisis management policies we recommend offer a proactive way to ensure better blackout response in the future.

Conclusion

Current use of cascading failure models do little to question the existing blackout management practices that dictate the real outcomes of surprising infrastructure failures. Outside this study, the current use of cascading failure models is as a predictive tool for losses rather than a descriptive tool to support blackout management. Ignoring the human factors and social contexts that influence crisis decision-making in studies may erode the resilience of global power grids by leaving organizations surprised. This study on South Korea finds ways to overcome surprise, by showing the shifting importance of Korean organizations during cascades and pinpointing organizations that can support information sharing and coordination activities. By linking knowledge of social and technological systems together, we overcome limitations of current modeling efforts.

Methods

Data and Software

Data is based on a well-studied model of the South Korean power grid (KPG) [33], [150] and social network models for Korean power organizations studied in [33]. KPG data was provided directly by KEPCO as a PSS/E (power system simulation for engineering) file, and the model consists of 2083 power system buses and 4167 power lines and transformer links. All power flow analysis was conducted in Matlab with the Matpower package [153] and the GLPK optimization solver [190]. Social networks were generated using matlab at analyzed using ORA-LITE social network analysis software [191]. Data for both models relates to the years of 2013-2014. Refer to Eisenberg et al. [33] for more detailed descriptions of social network models and general metrics characterizing their structure.

Power Grid Betweenness

Betweenness is a generic measure used in both power grid and social network theory to identify critical components of systems [156]. The generic form of betweennes that applies to any network is based on geodesic paths (or shortest paths) from nodes *i* to *j.* The set of all geodesic paths between nodes *i* and *j* is called the “minimum cut set,” σ_{ij}. The betweenness of any given node v is then defined as the total number of geodesic paths that node v lies on normaled by he size of each minimum cut set [192]:

$$B_v = \sum_{i \neq v \neq j} \frac{\sigma_{ij}^{v}}{\sigma_{ij}} \qquad (1)$$

Where σ_{ij}^{v} is the size of the cut set between nodes *i* and *j* that node v is on, summed over all node pairs within a network.

The generic form of this equation is often inappropriate for power systems. In particular, electric power does not flow based on geodesic path, it flows based on power line impedence. To address this discrepency, several authors developed power grid specific betweennes measures that incorporate measures of power flow. Here, we use the electrical betweenness measure developed Arianos et al. [164]–[166] that uses standard measures of power grid vulnerability to determine “electrically between” nodes that influence power flow. To calculate electrical betweenness, first the power grid infrastructure is separated into four groups, power lines and transformers ($|\mathbf{L}|=M_{\text{lines}}$), buses that produce electricity ($|\mathbf{G}|=N_{\text{Gen}}$), buses that demand power ($|\mathbf{D}|=N_{\text{Demand}}$), and transmission buses that direct power flow ($|\mathbf{T}|=N_{\text{Trans}}$), where the total number of power grid nodes N = $N_{\text{Gen}} + N_{\text{Demand}} + N_{\text{Trans}}$. Then, linear shift factors (also called power transfer distribution factors), f_i^{gd}, are calculated for each power line, $l \in$ **L**, for a unit injection at generation bus, $g \in$ **G**, and an equal increase in load at demand bus, $d \in$ **D**. These linear shift factors determine the relationship between KPG structure and shifts in power flow over all power lines. The linear shift factors are then used to estimate a total transfer capability for a single power line, TTC_g^d, by assessing the power transfer for a given g and *d* relationship:

$$TTC_g^d = min\left\{\frac{P_1^{max}}{f_1^{gd}}, \dots, \frac{P_l^{max}}{f_l^{gd}}, \dots, \frac{P_M^{max}}{f_M^{gd}}\right\} \qquad (2)$$

The electrical betweenness of a given power system bus v, is then define as:

$$EB_v = \frac{1}{2}\sum_{g\in\boldsymbol{G}}\sum_{d\in\boldsymbol{D}} TTC_g^d \sum_{l\in\boldsymbol{L}^v}\left|f_l^{gd}\right|,\ g \neq v \neq d \qquad (3)$$

where **L**^{v} is the set of power lines attached to bus v and the factor of 1/2 accounts for power flow into and out of buses. $(1/2)\ TTC_g^d \sum_{l\in L^v}\left|f_l^{gd}\right|$ is interpreted as the security constrained contribution of power flow of bus v for a single *g* and *d* pair. Thus, (3) measures the contriubtion of each bus to power flow without considering geodesic paths.

Power Grid Cascading Failure Model

We use (2) and (3) to advance a well-strudied cascading failure model, the Crucitti-Latora-Marchi (CLM) model [150], [183], [193], [194], to assess shifting congestion wihin electric power systems. The CLM model has unique properties that are useful for understanding shifting crisis coordination activities during N-1 failures rather than measure the propogation of failures to their final cascaded state. The CLM model focuses on understanding how congestion within a system is shifted around relative to overloaded nodes. Thus, it is not a cascading failure model per se, because it does not depend upon additional failed infrastructure to estimate if overloads are occuring. Instead, it focuses on shifting congestion throughout the power grid until a stable state is found. The CLM model was originally developed using structural network mesures B_v and link efficiency, e_{ij}, which is considered the inverse of the distance between two nodes at a given time interval, t. Together, these measures are used in a simple algorithm to determine how losses within a generic network may cascade across connections. First, the capaity of each node is estimated as its inial betweenness at time, $B_v(t = 0)$, tuned by a capacity parameter, α:

$$C_v = B_v(t = 0) * (1 + \alpha) \qquad (4)$$

Assuming initial effiency, $e_{ij}(t=0) = 1/d_{ij}(0) = 1$, a node is removed from the network and link efficienices are recalcualted with each iteration based on the following equation:

$$e_{ij}(t) = \begin{cases} min\left(\frac{C_i}{B_i(t)}, \frac{C_j}{B_j(t)}\right); if B_i(t) > C_i \; or \; B_j(t) > C_j \\ e_{ij}(t=0); otherwise \end{cases} \quad (5)$$

We build upon this model by for studying congestion-based cascades in power grids using the following procedure and substitutions in eqs. 4 and 5. First, we replace B_v with EB_v. We then calcualte eq. 4 assuming the power flow limits found in current KPG data are sufficient where $\alpha = 0$. We then relate link efficiency to power line impedence prior to initating cascades. For all calculations, we use the DC power flow approxiamtion which simplifies efficiency to be power line reactance, x_{ij}, such that, $x_{ij}(t) = x_{ij}(t=0)/e_{ij}(t)$. With the modified version of Eq. 5, we remove a single bus from the KPG model and start the CLM cascading procedure [194]. These modifcations change the original CLM model from a network-based model assessing congestion caused by network connectivity, to a dynamics-based model that assesses congestion based on power flow analysis.

Transmission Reserve Margin Estimation

Relating cascading failure results to social network generation requires we estimate the national reserve margin for South Korea. The reserve margin for the national grid determines the crisis management level and resulting organizations involved in blackout response [33]. Reserve margin is a function of both the available generation capacity and the capability to transmit this electricity to customers. To estimate reserve margin, we first estimate the total transfer capability [195]–[197] of the KPG, TTC_{net}, summing over all *g* and *d* pairs from equation (2),

$$TTC_{net} = \frac{1}{N_{Gen}N_{Demand}} \sum_{g \in \boldsymbol{G}} \sum_{d(g \neq d) \in \boldsymbol{D}} TTC_g^d \quad (6)$$

We then calculate the active transfer capability, $ATC_{net}(t)$, for each timestep which is qualitatively similar toTTC_{net} but also considers active congestion within the power grid estimated as active power injections,

$$ATC_g^d(t) = min\left\{\frac{P_1^{max} - P_1(t)}{f_1^{gd}}, \dots, \frac{P_l^{max} - P_l(t)}{f_l^{gd}}, \dots, \frac{P_M^{max} - P_M(t)}{f_M^{gd}}\right\} \quad (7)$$

$$ATC_{net}(t) = \frac{1}{N_{Gen}N_{Demand}} \sum_{g \in \boldsymbol{G}} \sum_{d(g \neq d) \in \boldsymbol{D}} ATC_g^d(t) \quad (8)$$

where $P_l(t)$ is the real power flow over line *l* at time *t*. We then estimate the transmission reserve margin , $TRM(t)$, as reductions in available generation due to system congestion that may inhibit the dispatch of additional generation resources in Korea. First, we relate reserve margin to transfer capability using the standard equation for power system planning [195], [196],

$$ATC = TTC - TRM \quad (9)$$

and rearrange this equation to relate reductions in generation capacity to system congestion with the folowing equations:

$$AGC = IC - D \quad (10)$$

$$UGC(t) = AGC\left(1 - \frac{ATC_{net}(t)}{TTC_{net}}\right) \quad (11)$$

$$TRM(t) = AGC - UGC(t) \quad (12)$$

where AGC is available generation capacity, IC is installed generation capacity, D is the total demand, $UGC(t)$ is the unavailable generation capacity due to system congestion at cascade iteration *t* (eq. 9-12 are all in units of GW).

This measure of TRM assumes that the dominating factor preventing power dispatch are the thermal limits on power lines, which is reasonable for DC power flow, but limited using AC power flow equations. Eq. 6 – 12 also assume that demand, D, remains constant throughout a cascading failure event, which is a common assumption across all cascading failure models [178].

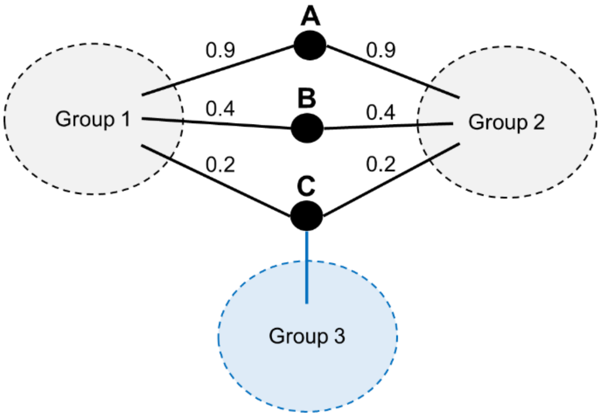
Social Network Generation and Weighting

We use the set of nodes (|**O**|= $N_{orgs} = N_{pc} + N_{em}$) and links (|**P**|= M_{orgs}) to distinguish blackout management social networks from power grid networks. We use the basic network structure presented in Fig. 1 and cascading failure model described above to generate sub-networks for each cascade based on system stress, ownership and locatoin. During each N-1 cascading failure procedure, we generate a subset of “active” power organzations, $N_{orgs}^{active} \in N_{orgs}$, organizations by finding which power grid buses are stressed and likely to cause cascading failures if lost. The stress at power system bus *v*, S_v, is measured by,

$$S_v(t) = \begin{cases} \frac{EB_v(t)}{EB_v(t=0)}, if\ EB_v(t=0) \leq EB_v(t); \\ 0, otherwise \end{cases} \qquad (13)$$

Each bus at a given cascade iteration *t* with $S_v(t) \geq 1$ is considered “active” and put in set $N_{bus}^{active} \in (N_{Gen} \cup N_{Demand} \cup N_{Trans})$. These active buses are then related to the power industry by establishing the subset of power companies that own and operate stressed infrastructure, $N_{pc}^{active} \in N_{pc}$, and the subset of emergency management agencies that will support infrastructure response and recovery based on the geographic region stressed infrastructure is located in, $N_{em}^{active} \in N_{em}$. Then, all partnerships among active organizations, $M_{orgs}^{active} \in M_{orgs}$, are added to the social network and given equal weight, $w_{ij} = 1$. The final, weighted scocial networks are generated by taking the mean of each active link across all N-1 failure scenarios. Thus, all link weights are $0 \leq\ w_{ij}^{avg}\ \leq 1$, where a partnership with $w_{ij}^{avg}\ = 0$ means the partnership was never relevant to N-1 blackout management, and $w_{ij}^{avg}\ = 1$ means the partnership was active across all failure scenarios.

Social Network Betweenness



Considering Groups 1 and 2 only

$$B_A = \frac{1}{3}; B_B = \frac{1}{3}; B_C = \frac{1}{3}$$

$$B_A^1 = 1;\ B_B^1 = 0;\ B_C^1 = 0$$

$$B_A^2 = 0;\ B_B^2 = 0;\ B_C^2 = 1$$

Considering Groups 1, 2 and 3

$$B_A = \frac{1}{3}; B_B = \frac{1}{3}; B_C = 2\frac{1}{3}$$

$$B_A^1 \geq 1;\ B_B^1 = 0;\ B_C^1 = 2$$

$$B_A^2 = 0;\ B_B^2 = 0;\ B_C^2 = 3$$

Figure 20 Practical Differences among Social Network Betweenness Measures. Consider groups 1 and 2 linked by nodes A, B, and C (ignoring group 3). B_v is a purely structural measure, and nodes A, B, and C receive equal values. When measures include the link weights shown, B_v^1 denotes node A as the most between and B_v^2 denotes node C as the most between. With only two connected groups, B_v^1 and B_v^2 are inverse measures of each other. However, in more complex systems where group 3 does exist, B_v^1 and B_v^2 will reveal characteristically different information about the social network independent of the weight of link C to group 3. In this work, B_v^1 captures optimal information sharing across strong ties, where B_v^2 captures least optimal, yet feasible information sharing across weak ties.

The unweighted measure of betweenness, B_v, does not measure organizational importance in a weighted social network [192]. Large line weights, $w_{ij}^{avg} \sim 1$, in our model means strong social ties across partnerships that frequently used for blackout management. Thus, we use the inverse weighted betweenness of each organization to determine which is most imporant to blackout coordination. This measure, B_v^1has the same mathematical form as B_v, but new cut sets for shortest paths between any pair of nodes *i* and *j* are found using link distances based on weights, $d_{ij}^{avg} = 1/w_{ij}^{avg}$**.** We also are interseted in finding all feasible shortest paths througohut the social network that are unlikely to be used for blackout management. These paths offer a heuristic way to determine which organizations can extend their current operations to support blackout coordination. In this case, we use weighted betweenness, B_v^2, which has the same mathematical form to B_v, but new cut sets for shortest paths between any pair of nodes *i* and *j* are found using link distances based on weights, $d_{ij}^{avg} = w_{ij}^{avg}$. The practical differences between the ouputs of these two weighted betweenness measures for blackout coordination is demonstrated in Fig. 20.

CHAPTER 6

CONCLUSION

This dissertation advances a new way to *think* about resilient infrastructure systems. The Majority of existing resilient infrastructure research is based on canonical, yet flawed definitions and models of resilience. In an attempt to change the canon, each chapter in this dissertation identifies misconceptions about four fundamental building blocks – data, goals, systems, and failures – that encourage flawed thinking. The results from each chapter help clarify how to overcome each misconception in the following ways:

- **Summary of Ch. 2:** Thinking that better data analytics will improve resilience misunderstands how data analytics serve infrastructure systems. More descriptive, predictive, and prescriptive analytics that obviate the need for a molder-in-the-loop or a user-in-the-loop can only reinforce existing pre-analytic visions and leave infrastructure systems vulnerable to fundamental surprise. Resilience is not gained through a stronger commitment to current pre-analytic visions, but through better ways to change visions when current models become stale.

- **Summary of Ch. 3:** Thinking that resilience is a "good" thing that successful systems "have" ignores the inherent limitations of resilience strategies. Pursuing a resilience strategy like robustness or extensibility is a worthwhile activity only until rigid thresholds or decompensation reveal latent, systemic deficiencies to manage surprising events. Resilience is neither robustness nor extensibility, but a capacity to switch between them to match given stress conditions. This fact is problematic in a world of limited resources, where a commitment to any single strategy potentially means the rejection of another. In an uncertain future, the robust and extensible infrastructure systems built today will resile between strategies not because they want to, but because they must.

- **Summary of Ch. 4:** Thinking that resilience is improved via technological solutions that reduce the probability of losses ignores the sociotechnical nature of infrastructure systems. First, researchers take for granted that the network model they are using to study an infrastructure system is ground truth, when conflicting system models exist that change results and recommendations. Developing more nuanced decisions that integrate conflicting models overcomes probabilistic thinking on failure likelihood with possibilisitic, "what-if" thinking necessary for resilience. Furthermore, possibilisitic perspectives on technological models in isolation only offer limited recommendations to the human actions that dictate failure consequences. Expanding analysis to include both technological and social models offers explicit recommendations for infrastructure crisis response that neither approach could offer on its own.

- **Summary of Ch. 5:** Thinking that infrastructure losses can be estimated via cascading failure models also ignores the sociotechnical nature of infrastructure failures. The amount of damages that infrastructure endures during surprise is dictated by human actions *during* cascading failures. Assuming normal operations during surprises overlooks the shifting social contexts that eventually dictate coordination activities, human response, and failure consequences. By focusing on the social context of cascading failures while they happen, new recommendations for emergency coordination can be developed that would otherwise be overlooked.

Through the clarification of how data, goals, systems, and failures influence resilience research, this dissertation advances new ways to think about three of the SAAL processes of sensing, adapting, and anticipating (Fig. 18). Based on the simple control loop model presented in the Introduction (see Ch. 1, Fig. 2), system models developed by researchers for to study resilience embed sensing, adapting, and anticipating processes. Current resilience thinking tends to produce research that only considers sensing via analytic models, adapting via robustness, and anticipating via engineering. Based on this dissertation, sensing processes are expanded to consider human-in-the-loop to reveal latent issues with analytic designs and overcome stale models with imaginative new descriptions, predictions, and prescriptions of infrastructure systems. New approaches to sensing enable contextual information regarding the beliefs and training of users to be shared with modelers and guide decision-making in unforeseen and unknown futures. Adapting processes are expanded to include both robustness and extensibility strategies for managing unforeseen and unknown failures. Clarification for when one strategy is preferred over another depends on how benefits and drawbacks match stress conditions.

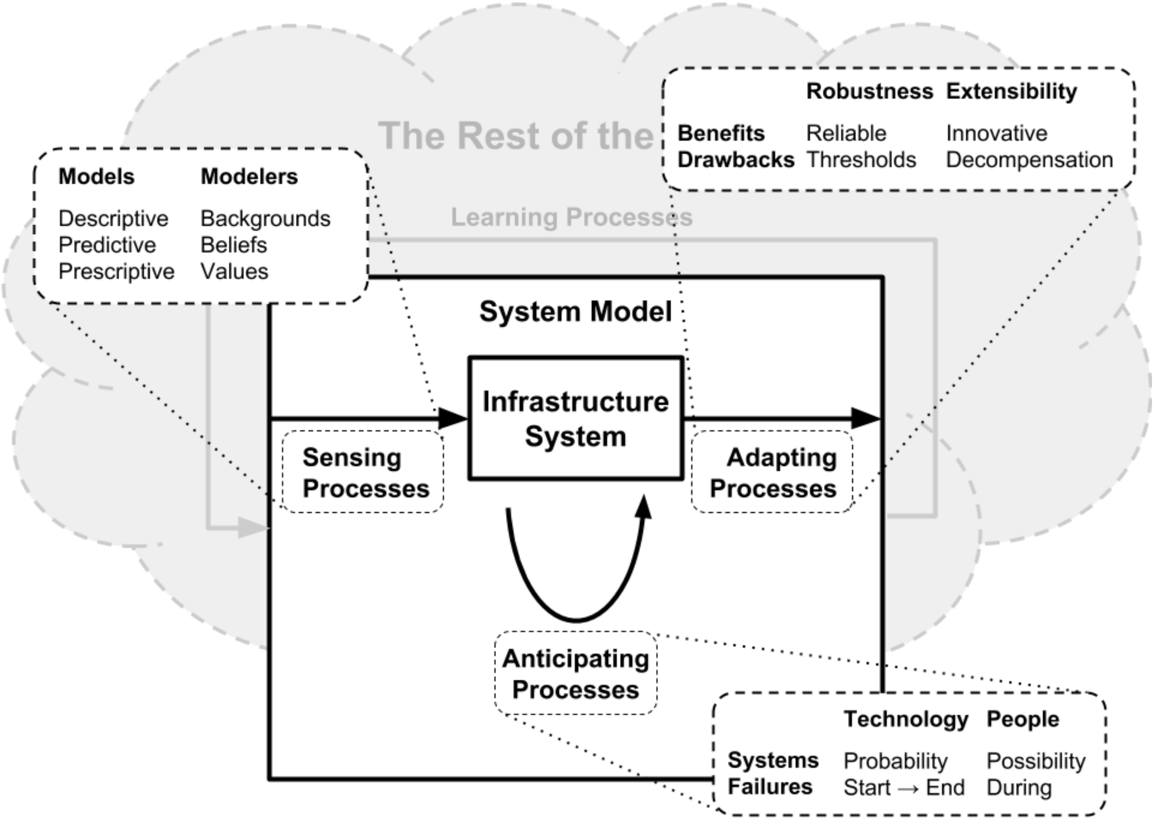


Figure 18 Dissertation contribution to SAAL Processes.
This dissertation expands current notions of the three processes that comprise the system model portion of the SAAL framework (refer to Ch.1, Fig. 2). Prevalent understandings of SAAL processes only consider sensing with analytics, adapting with robustness, and anticipating via technological models. This dissertation presents new, competing options for performing these processes: sensing via analytic models and modelers, adapting via robustness and extensibility strategies, and anticipating via people-centered systems and failure models.

Finally, anticipating processes for systems and failures are expanded from a technology-centric perspective to a sociotechnical perspective. Unlike sensing and adapting processes, advancing anticipating processes requires the act of anticipating itself by discovering the biases and beliefs embedded in specific models for a critical infrastructure system. Interrogating models and their embedded biases is necessary, because each infrastructure system has a characteristic architecture [198]–[201] that is has both generalizable and idiosyncratic elements. Complexity in infrastructure systems arises from the need to represent system architecture with a simplified model to understand infrastructure structure and function [84], [202], [203]. Since no single model is capable of including all embedded characteristics of infrastructure systems, anticipating design and management of infrastructure failures from multiple perspectives helps reveal embedded biases and can produce mutually beneficial results that resolve issues of complexity. This dissertation work advances anticipating processes specifically for electric power systems by studying the South Korean power grid using established network science measures of betweenness. Both engineering and social science literature use different models when applying betweenness measures to emphasize some aspects of power systems over others. The majority of this work focused on interpreting the results from engineering network models with social science solutions, and vice versa. Together, this dissertation advances anticipating processes by considering the structure of social systems dictate infrastructure failure response and expanding probabilistic thinking about failure likelihood to possibilisitic thinking about what will be done when failures occur. Likewise, technological anticipation emphasizes what initiates failures and the total losses, where a human perspective anticipates the actions taken during events.

This new understanding of the SAAL processes is significant for resilient infrastructure systems writ large because it advances a way to think about resilience as a verb. Overall, this dissertation centers on what resilience means when treated as a verb. Results from all chapters indicate that risk-based thinking focuses on the properties or objects that systems have, rather than the actions systems do. This is why risk lends itself to quantifiable measures where attempts to measure resilience remain conceptual or impracticable. This is because resilience is not like risk – resilience is not a property an infrastructure system has, it is an *action* an infrastructure system *does*. This way of thinking about resilience is the foundation of this dissertation.

Treating resilience as a verb means the future of resilience research may look very different than the current literature. Resilience as a verb means resilient infrastructure research should examine of ways infrastructure systems take action to manage surprising events. By revealing misconceptions about data, goals, systems, and failures, each chapter in this dissertation reveals multiple ways to perform SAAL. Each way, e.g., robustness or extensibility, brings with it different benefits and drawbacks that must be managed. Associated resilience analyses would then examine how infrastructure systems perform the SAAL processes and measure how difficult it would be to change current strategies to meet a new stress context. A resilient system is one that has the capability to match sensing, adapting, and anticipating processes to surprise.

In conclusion, there is now a new way to think about resilience that may bring radical changes to the future development of a resilience theory. Where current definitions and models fail to change risk-based failure management practices, this new way of thinking rejects the current canon for one unavailable in the literature. For example, the National Academies of Science definition of resilience as, “the ability to plan and prepare for, absorb, recover from, and adapt to adverse events,” would be discarded for verb forms of resilience such as:

> **to resile (verb): to adjust current models to meet surprising stress conditions.**

New, provocative models will also replace the critical functionality curve to shift from the retrospective measures of system damages to the prospective measures of system processes.

Whether or not this way to think about resilience is correct, it is important because it has the power to change the failure management paradigm away from risk. Disasters today and into the future will continue to remind society that risk-based thinking does not protect infrastructures from crisis. Hopefully, with the change put forth in this work, infrastructure systems and the people that depend on them will be better at managing future disasters.

REFERENCES

[1] S. Kaplan and B. J. Garrick, “On The Quantitative Definition of Risk,” Risk Anal., vol. 1, no. 1, pp. 11–27, 1981.

[2] Department of Homeland Security (DHS), “National Infrastructure Protection Plan (NIPP): Partnering for critical infrastructure security and resilience,” 2013.

[3] J. Bergstrom, R. van Winsen, and E. Henriqson, “On the rationale of resilience in the domain of safety: A literature review,” Reliab. Eng. Syst. Saf., vol. 141, pp. 131–141, 2015.

[4] J. Park, T. P. Seager, P. S. C. Rao, M. Convertino, and I. Linkov, “Integrating risk and resilience approaches to catastrophe management in engineering systems.,” Risk Anal., vol. 33, no. 3, pp. 356–67, Mar. 2013.

[5] T. P. Seager, S. Spierre-Clark, D. A. Eisenberg, J. E. Thomas, M. M. Hinrichs, R. Kofron, C. Jensen, L. R. McBurnett, M. Snell, and D. L. Alderson, “Redesigning Resilient Infrastructure Research,” in Resilience and Risk: Methods and Application in Environment, Cyber and Social Domains, I. Linkov and J. Palma-Olivera, Eds. Springer, 2017.

[6] J. Park, T. P. Seager, and P. S. C. Rao, “Lessons in risk- versus resilience-based design and management.,” Integr. Environ. Assess. Manag., vol. 7, no. 3, pp. 396–399, Jul. 2011.

[7] Office of the President of the United States, “Executive Order 13636: Improving Critical Infrastructure Cybersecurity,” 2013.

[8] Office of the President of the United States, “Presidential Policy Directive 21: Critical Infrastructure Security Resilience,” 2013.

[9] Committee on Increasing National Resilience to Hazards and Disasters, Disaster Resilience: A National Imperative. The National Academies Press, 2012.

[10] United Nations International Strategy for Disaster Reduction and World Meteorological Organization, “Disaster Risk and Resilience,” 2012.

[11] R. Francis and B. Bekera, “A metric and frameworks for resilience analysis of engineered and infrastructure systems,” Reliab. Eng. Syst. Saf., vol. 121, pp. 90–103, 2013.

[12] M. Bruneau and A. Reinhorn, “Exploring the Concept of Seismic Resilience for Acute Care Facilities,” Earthq. Spectra, vol. 23, no. 1, pp. 41–62, Feb. 2007.

[13] M. Bruneau, S. E. Chang, R. T. Eguchi, G. C. Lee, T. D. O'Rourke, A. M. Reinhorn, M. Shinozuka, K. Tierney, W. A. Wallace, and D. Von Winterfeldt, "A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities," Earthq. Spectra, vol. 19, no. 4, pp. 733–752, 2003.

[14] I. Linkov, T. Bridges, F. Creutzig, J. Decker, C. Fox-Lent, W. Kröger, J. H. Lambert, A. Levermann, B. Montreuil, J. Nathwani, R. Nyer, O. Renn, B. Scharte, A. Scheffler, M. Schreurs, and T. Thiel-Clemen, "Changing the resilience paradigm," Nat. Clim. Chang., vol. 4, no. 6, pp. 407–409, May 2014.

[15] S. Hosseini, K. Barker, and J. E. Ramirez-Marquez, "A Review of Definitions and Measures of System Resilience," Reliab. Eng. Syst. Saf., vol. 145, pp. 47–61, 2016.

[16] Presidential Commission on Critical Infrastructure Protection, "Critical foundations: Protecting America's infrastructure," 1997.

[17] "Deadly Wildfires Devastate Northern California," The Weather Channel, Oct 11, 2017.

[18] "London fire: What happened at Grenfell Tower?," BBC, 2017.

[19] M. Park and E. C. McLaughlin, "Evacuations ordered over concerns at California dam system," CNN, 2017.

[20] CNN Library, "2017 Atlantic Hurricane Season Fast Facts," CNN.

[21] A. Rankin, J. Lundberg, R. Woltjer, C. Rollenhagen, and E. Hollnagel, "Resilience in Everyday Operations: A framework for analyzing adaptations in high-risk work," J. Cogn. Eng. Decis. Mak., vol. 8, no. 1, pp. 78–97, 2014.

[22] D. D. Woods, "How the theory of graceful extensibility addresses the mystery of sustained adaptability." Environ. Sys. & Decisions. *In review*

[23] J. Park, "Complex Coupled Engineered Systems: Balancing Resilience and Efficiency in Design and Management," Purdue University, 2012.

[24] A. W. Righi, T. A. Saurin, and P. Wachs, "A systematic literature review of resilience engineering: Research areas and a research agenda proposal," Reliab. Eng. Syst. Saf., vol. 141, pp. 142–152, 2015.

[25] M. L. Snell, D. A. Eisenberg, T. P. Seager, S. S. Clark, Y. J. Oh, J. E. Thomas, and L. R. McBurnett, "A Multidimensional Review of Resilience: Resources, Processes, and Outcomes," in International Risk Governance Council Resource Guide on Resilience,

2016, pp. 1–7.

[26] United States Government Accountability Office, “Data Analytics to Address Fraud and Improper Payments,” 2017.

[27] “The Digital Analytics Program.” [Online]. Available: https://www.digitalgov.gov/.

[28] M. Eckstein, “Navy Digital Warfare Office Proving Data Analytics Can Help Address Nagging Operational Problems,” US Naval Institute News, 2017.

[29] K. Barker, J. H. Lambert, C. W. Zobel, A. H. Tapia, J. E. Ramirez-Marquez, L. Albert, C. D. Nicholson, and C. Caragea, “Defining resilience analytics for interdependent cyber-physical-social networks,” Sustain. Resilient Infrastruct., vol. 2, no. 2, pp. 59–67, 2017.

[30] G. G. Brown, “Model Building”, INFORMS Analytics Body of Knowledge (ABOK), Wiley, 2018.

[31] Quadrennial Energy Review Task Force and The Department of Energy (DOE), “Quadrennial Energy Review: Transforming the Nation’s Electricity System: The Second Installment of the Quadrennial Energy Review,” 2017.

[32] S. Amir and V. Kant, “Sociotechnical Resilience: A Preliminary Concept,” Risk Anal., vol. 0, no. 0, 2017.

[33] D. A. Eisenberg, J. Park, and T. P. Seager, “Sociotechnical Network Analysis for Power Grid Resilience in South Korea,” Complexity, vol. 2017, 2017.

[34] G. H. Walker, N. a. Stanton, P. M. Salmon, and D. P. Jenkins, “A review of sociotechnical systems theory: a classic concept for new command and control paradigms,” Theor. Issues Ergon. Sci., vol. 9, no. 6, pp. 479–499, 2008.

[35] National Institute of Standards and Technology, “NIST Special Publication 1190: Community Resilience Planning Guide for Buildings and Infrastructure Systems, Volume I,” vol. II, p. 260, 2015.

[36] J. A. Schumpter, History of economic analysis. Psychology Press, 1954.

[37] R. Costanza, “Visions, values, valuation, and the need for an ecological economics,” Bioscience, vol. 51, no. 6, pp. 459–468, 2001.

[38] SNAFUcatchers Workshop, “STELLA: Report from the SNAFUcatchers Workshop on

Coping With Complexity,” pp. 1–44, 2017.

[39] R. L. Wears and L. K. Webb, “Fundamental on Situational Surprise: a Case Study with Implications for Resilience,” in Resilience engineering in practice. Volume 2, Becoming resilient, CRC Press, 2016, pp. 61–74.

[40] R. W. Quinn and M. C. Worline, “Enabling Courageous Collective Action: Conversations from United Airlines Flight 93,” Organ. Sci., vol. 19, no. 4, pp. 497–516, 2008.

[41] T. McMillan, Flight 93: The story, the aftermath, and the legacy of American courage on 9/11. Rowman & Littlefield, 2014.

[42] California Department of Water Resources, “Lake Oroville Spillway Incident: Timeline of Major Events February 4-25,” p. 500, 2017.

[43] California Department of Water Resources “Independent forensic team report Oroville dam spillway incident,” 2018.

[44] E. Hollnagel, D. D. Woods, and N. Leveson, Resilience engineering: Concepts and precepts. Ashgate Publishing Ltd., 2007.

[45] E. Hollnagel, “Resilience engineering and the built environment,” Build. Res. Inf., vol. 42, no. 2, pp. 221–228, Mar. 2014.

[46] C. S. Holling, “Resilience and Stability of Ecological Systems,” Annu. Rev. Ecol. Syst., vol. 4, pp. 1–23, 1973.

[47] D. E. Alexander, “Resilience and disaster risk reduction: an etymological journey,” Nat. Hazards Earth Syst. Sci., vol. 13, no. 11, pp. 2707–2716, Nov. 2013.

[48] S. Meerow, J. P. Newell, and M. Stults, “Defining urban resilience: A review,” Landsc. Urban Plan., vol. 147, pp. 38–49, 2016.

[49] C. S. Holling and L. H. Gunderson, “Resilience and adaptive cycles,” in Panarchy: Understanding Transformations in Human and Natural Systems, Island Press, 2002, pp.25–62.

[50] B. Walker, C. S. Holling, S. R. Carpenter, and A. Kinzig, “Resilience, Adaptability and Transformability in Social – ecological Systems,” Ecol. Soc., vol. 9, no. 2, 2004.

[51] Resilience Alliance, “Resilience,” 2017. [Online]. Available:

https://www.resalliance.org/resilience. [Accessed: 07-Jul-2017].

[52] A. Rose, “Defining Resilience Across Disciplines,” in Defining and Measuring Economic Resilience from a Societal, Environmental and Security Perspective. Integrated DisasterRisk Management., Springer Singapore, 2017, pp. 19–27.

[53] G. C. Gallopín, “Linkages between vulnerability, resilience, and adaptive capacity,” Glob. Environ. Chang., vol. 16, no. 3, pp. 293–303, 2006.

[54] Y. Y. Haimes, “On the complex definition of risk: A systems-based approach,” Risk Anal., vol. 29, no. 12, pp. 1647–1654, 2009.

[55] Y. Y. Haimes, “On the definition of resilience in systems,” Risk Anal., vol. 29, no. 4, pp. 498–501, 2009.

[56] J. Mochizuki, A. Keating, W. Liu, S. Hochrainer-Stigler, and R. Mechler, “An overdue alignment of risk and resilience? A conceptual contribution to community resilience,” Disasters, 2017.

[57] D. A. Eisenberg, J. Park, M. E. Bates, C. Fox-lent, T. P. Seager, and I. Linkov, “Resilience Metrics: Lessons from Military Doctrines,” Solut. J., 2014.

[58] I. Linkov, T. Bridges, F. Creutzig, J. Decker, C. Fox-Lent, W. Kröger, J. H. Lambert, A. Levermann, B. Montreuil, J. Nathwani, R. Nyer, O. Renn, B. Scharte, A. Scheffler, M. Schreurs, and T. Thiel-Clemen, “Changing the resilience paradigm,” Nat. Clim. Chang., vol. 4, no. 6, pp. 407–409, May 2014.

[59] J. Park, T. P. Seager, and P. S. C. Rao, “Lessons in risk- versus resilience-based design and management,” Integr. Environ. Assess. Manag., vol. 7, no. 3, pp. 396–399, Jul. 2011.

[60] K. A. Pettersen and P. R. Schulman, “Drift, adaptation, resilience and reliability: Toward an empirical clarification,” Saf. Sci., 2015.

[61] T. P. Seager, “The Sustainability Spectrum and the Sciences of Sustainability,” Bus. Strateg. Environ., vol. 453, no. September, pp. 444–453, 2008.

[62] D. A. Eisenberg, J. Park, D. Kim, and T. P. Seager, “RESILIENCE ANALYSIS OF CRITICAL INFRASTRUCTURE SYSTEMS REQUIRES INTEGRATION OF MULTIPLE ANALYTICAL TECHNIQUES,” in Urban Sustainability and Resilience, 2014.

[63] S. T. F. on C. C. and Energy, “Adapting Transportation to the Impacts of Climate Change: State of Practice 2011,” Washington, DC, 2011.

[64] Y. Wang, S. Member, C. Chen, J. Wang, S. Member, and R. Baldick, “Research on Resilience of Power Systems Under Natural Disasters — A Review,” vol. 31, no. 2, pp. 1–10, 2015.

[65] J. Ahern, “From fail-safe to safe-to-fail: Sustainability and resilience in the new urban world,” Landsc. Urban Plan., vol. 100, no. 4, pp. 341–343, 2011.

[66] J. Fiksel, “Designing resilient, sustainable systems.,” Environ. Sci. Technol., vol. 37, no. 23, pp. 5330–5339, 2003.

[67] Yeowon Kim, D. A. Eisenberg, E. N. Bondank, M. V. Chester, G. Mascaro, and B. S. Underwood, “Fail-Safe and Safe-to-Fail Adaptation: Decision-making for Urban Flooding under Climate Change,” Clim. Change, vol. in review, pp. 1–16, 2017.

[68] P. E. Roege, Z. a. Collier, J. Mancillas, J. a. McDonagh, and I. Linkov, “Metrics for energy resilience,” Energy Policy, vol. 72, pp. 249–256, Sep. 2014.

[69] S. Jackson and T. L. J. Ferris, “Resilience Principles for Engineered Systems,” Syst. Eng., vol. 16, no. 2, pp. 152–164, 2012.

[70] A. M. Madni and S. Jackson, “Towards a Conceptual Framework for Resilience Engineering,” IEEE Syst. J., vol. 3, no. 2, pp. 181–191, Jun. 2009.

[71] J. C. Le Coze, “Vive la diversite! High Reliability Organisation (HRO) and Resilience Engineering (RE),” Saf. Sci., 2015.

[72] T. K. Haavik, S. Antonsen, R. Rosness, and A. Hale, “HRO and RE: A pragmatic perspective,” Saf. Sci., 2016.

[73] D. D. Woods, “Four concepts for resilience and the implications for the future of resilience engineering,” Reliab. Eng. Syst. Saf., vol. 141, pp. 5–9, 2015.

[74] K. R. Buckeye, “Innovations on Managed Lanes in Minnesota,” Public Work. Manag. Policy , vol. 17, no. 2, pp. 152–169, 2012.

[75] P. J. Chun and M. D. Fontaine, “Evaluation of the Impact of the I-66 Active Traffic Management System,” 2016.

[76] D. L. Alderson and J. C. Doyle, “Contrasting Views of Complexity and Their Implications For Network-Centric Infrastructures,” IEEE Trans. Syst. Man, Cybern. - Part A Syst. Humans, vol. 40, no. 4, pp. 839–852, Jul. 2010.

[77] A. Pizam, “The practice of overbooking: Lessons learned from United Airlines flight 3411,” Int. J. Hosp. Manag., vol. 64, pp. 94–95, 2017.

[78] D. J. Fagnant and K. Kockelman, “Preparing a nation for autonomous vehicles: Opportunities, barriers and policy recommendations,” Transp. Res. Part A Policy Pract., vol. 77, pp. 167–181, 2015.

[79] C. S. Lee, M. H. Wang, S. J. Yen, T. H. Wei, I. C. Wu, P. C. Chou, C. H. Chou, M. W. Wang, and T. H. Yan, “Human vs. Computer Go: Review and Prospect,” IEEE Comput. Intell. Mag., vol. 11, no. 3, pp. 67–72, 2016.

[80] M. Lu, H. Nagarajan, E. Yamangil, R. Bent, and S. Backhaus, “Optimal Transmission Line Switching under Geomagnetic Disturbances,” pp. 1–8, 2017.

[81] D. Pasqualini, “Resilient Grid Operational Strategies,” 2017.

[82] North American Electric Reliaility Corporation, “Standard TPL-001-4 — Transmission System Planning Performance Requirements,” 2014.

[83] E. Roe and P. R. Schulman, “Toward a Comparative Framework for Measuring Resilience in Critical Infrastructure Systems,” J. Comp. Policy Anal. Res. Pract., vol. 14,no. 2, pp. 114–125, 2012.

[84] J. C. Doyle, D. L. Alderson, L. Li, S. Low, M. Roughan, S. Shalunov, R. Tanaka, and W. Willinger, “The ‘robust yet fragile’ nature of the Internet.,” Proc. Natl. Acad. Sci. U. S. A., vol. 102, no. 41, pp. 14497–502, Oct. 2005.

[85] FRIENDS OF THE RIVER SIERRA CLUB SOUTH YUBA RIVER CITIZENS LEAGUE, “MOTION TO INTERVENE,” 2005.

[86] Federal Energy Regulatory Commission, “Office of Energy Projects Emergency Spillway Re-Evaluation,” 2006.

[87] C. Perrow, “Normal Accidents: Living With High-Risk Technologies.” Princeton University Press, 1984.

[88] E. Hollnagel and Ö. Goteman, “The Functional Resonance Accident Model,” Proc. Cogn. Syst. Eng. Process plant, pp. 155–161, 2004.

[89] National Transportation Safety Board, “Loss of Thrust in Both Engines After Encountering a Flock of Birds and Subsequent Ditching on the Hudson River US Airways Flight 1549 Airbus A320-214, N106US,” 2010.

[90] C. Chen, J. Wang, and D. ton, “Modernizing Distribution System Restoration to Achieve Grid Resiliency Against Extreme Weather Events: An Integrated Solution,” Proc. IEEE, vol. 105, no. 7, 2017.

[91] J. Loo, J. L. Mauri, and J. H. Ortiz, Mobile Ad Hoc Networks: Current and Future Trends. CRC Press, 2012.

[92] P. Schulman, E. Roe, M. Van Eeten, and M. De Bruijne, “High Reliability and the Management of Critical Infrastructures,” J. Contingencies Cris. Manag., vol. 12, no. 1, pp. 14–28, 2004.

[93] S. Davenport and S. Leitch, “Circuits of power in practice: Strategic ambiguity as delegation of authority,” Organ. Stud., vol. 26, no. 11, pp. 1603–1623, 2005.

[94] L. G. Shattuck and D. D. Woods, “Communication of intent in military command and control systems,” in The human in command: Exploring the modern military experience, Springer, 2000, pp. 279–292.

[95] K. Eder, C. Harper, and U. Leonards, “Towards the safety of human-in-the-loop robotics: Challenges and opportunities for safety assurance of robotic co-workers’,” Proc. - IEEE Int. Work. Robot Hum. Interact. Commun., vol. 2014–Octob, no. October, pp. 660–665, 2014.

[96] M. C. Libicki, “The Strategic Uses of Ambiguity in Cyberspace,” Mil. Strateg. Aff., vol. 3, no. 3, pp. 3–10, 2011.

[97] D. D. Woods and M. Branlat, “Basic Patterns in How Adaptive Systems Fail,” in Resilience Engineering in Practice: A Guidebook, Ashgate, 2011, pp. 127–144.

[98] D. D. Woods, “Incidents - Markers of Resilience or Brittleness?,” Resil. Eng. concepts precepts, pp. 69–75, 2006.

[99] S. J. Masten, S. H. Davies, and S. P. McElmurry, “Flint Water Crisis: What Happened and Why?,” J. - Am. Water Words Assoc., vol. 108, no. 12, pp. 21–34, 2016.

[100] S. Zahran, S. P. McElmurry, and R. C. Sadler, “Four phases of the Flint Water Crisis: Evidence from blood lead levels in children,” Environ. Res., vol. 157, no. February, pp. 160–172, 2017.

[101] L. Pulido, “Flint, Environmental Racism, and Racial Capitalism,” Capital. Nat. Social., vol. 27, no. 3, p. 16, 2016.

[102] B. Sherehiy, W. Karwowski, and J. K. Layer, “A review of enterprise agility: Concepts, frameworks, and attributes,” Int. J. Ind. Ergon., vol. 37, no. 5, pp. 445–460, 2007.

[103] E. Santos Bernardes and M. D. Hanna, “A theoretical review of flexibility, agility and responsiveness in the operations management literature,” Int. J. Oper. Prod. Manag., vol.29, no. 1, pp. 30–53, 2009.

[104] D. Alberts, R. K. Huber, and J. Moffat, NATO NEC C2 Maturity Model. 2010.

[105] D. S. Alberts, The Agility Advantage: A Survival Guide for Complex Enterprises and Endeavors. 2011.

[106] M. Chester and B. Allenby, “Towards Adaptive Infrastructure: Flexibility and Agility in a Non-Stationarity Age,” Sustain. Resilient Infrastruct., pp. 1–24.

[107] D. A. Eisenberg, T. P. Seager, M. M. Hinrichs, Y. Kim, B. A. Wender, S. Markolf, J. E. Thomas, M. V. Chester, D. L. Alderson, J. Park, Y.-5 C. Lai, I. Linkov, S. Spierre Clark, and D. Woods, “Robustness and Extensibility in Infrastructure Systems,” Reliab. Eng. Syst. Saf.

[108] Committee on Enhancing the Resilience of the Nation’s Electric Power Transmission and Distribution System, Enhancing the Resilience of the Nation’s Electricity System. 2017.

[109] S. A. Markolf, C. Hoehne, A. Fraser, M. V. Chester, and B. S. Underwood, “Transportation Resilience to Climate Change and Extreme Weather Events – Beyond Risk and Robustness,” Transp. Policy, vol. in review, 2017.

[110] M. D. Meyer and B. Weigel, “Climate Change and Transportation Engineering: Preparing for a Sustainable Future,” J. Transp. Eng., vol. 137, no. 6, pp. 393–403, 2011.

[111] Federal Emergency Management Agency, “Mitigation Ideas: A Resource for Reducing Risk to Natural Hazards,” 2013.

[112] C. Balcazar, “Resilient Infrastructure for Sustainable Services. Latin America: Mainstreaming of Disaster Risk Management in the Water Supply and Sanitation Sector,” 2012.

[113] T. Le Dinh, W. Hu, P. Sikka, P. Corke, L. Overs, and S. Brosnan, “Design and deployment of a remote robust sensor network: Experiences from an outdoor water quality monitoring network,” Proc. - Conf. Local Comput. Networks, LCN, pp. 799–806, 2007.

[114] R. J. Dawson, T. Ball, J. Werritty, A. Werritty, J. W. Hall, and N. Roche, “Assessing the effectiveness of non-structural flood management measures in the Thames Estuary under conditions of socio-economic and environmental change,” Glob. Environ. Chang., vol. 21, no. 2, pp. 628–646, 2011.

[115] W. Fawcett, I. R. Urquijo, H. Krieg, M. Hughes, L. Mikalsen, and Ó. R. R. Gutiérrez, “Cost and Environmental Evaluation of Flexible Strategies for a Highway Construction Project under Traffic Growth Uncertainty,” J. Infrastruct. Syst., vol. 21, no. 3, p. 5014006, 2015.

[116] “HDR predicts an adaptable and flexible future for roadways,” ITS International, 2017. [Online]. Available: http://www.itsinternational.com/categories/charging-tolling/features/hdr-predicts-an-adaptable-and-flexible-future-for-roadways/.

[117] “What is SMART?,” SMART Motorway Tunnel, 2017. [Online]. Available: http://smarttunnel.com.my/smart/what-is-smart/.

[118] R. L. Wilby and R. Keenan, “Adapting to flood risk under climate change,” Prog. Phys. Geogr., vol. 36, no. 3, pp. 348–378, 2012.

[119] United National International Strategy for Disaster Reduction, “Hyogo Framework For Action 2005-2015: Building the resilience of nations and communities to disasters,” 2007.

[120] The Rockefeller Foundation and ARUP, “City Resilience Index,” p. 16, 2015.

[121] Committee on Determinants of Market Adoption of Advanced Energy Efficiency and Clean Energy Technologies, The Power of Change: Innovation for Development and Deployment of Increasingly Clean Electric Power Technologies. The National Academies Press, 2016.

[122] Committee on Analytical Research Foundations for the Next-Generation Electric Grid, Analytic Research Foundations for the Next-Generation Electric Grid, Analytic Research Foundations for the Next-Generation Electric Grid. The National Academies Press, 2016.

[123] North American Electric Reliability Coporation, “September 2011 Southwest Blackout Event,” 2011.

[124] O. P. Veloza and F. Santamaria, “Analysis of major blackouts from 2003 to 2015: Classification of incidents and review of main causes,” Electr. J., vol. 29, no. 7, pp. 42–49, 2016.

[125] C.-C. Sun, C.-C. Liu, and J. Xie, “Cyber-Physical System Security of a Power Grid: State-of-the-Art,” Electronics, vol. 5, no. 3, p. 40, 2016.

[126] Australian Energy Market Operator (AEMO), “PRELIMINARY REPORT 3rd Oct – BLACK SYSTEM EVENT IN SOUTH AUSTRALIA ON 28 SEPTEMBER 2016,” no. SEPTEMBER, 2016.

[127] M. M. Adibi and L. H. Fink, “Restoration from cascading failures,” IEEE Power Energy Mag., vol. 4, no. 5, pp. 68–77, 2006.

[128] M. Panteli and P. Mancarella, “The grid: Stronger, bigger, smarter?: Presenting a conceptual framework of power system resilience,” IEEE Power Energy Mag., vol. 13, no. 3, pp. 58–66, 2015.

[129] M. Panteli and P. Mancarella, “Influence of extreme weather and climate change on the resilience of power systems: Impacts and possible mitigation strategies,” Electr. Power Syst. Res., vol. 127, pp. 259–270, 2015.

[130] M. Panteli and P. Mancarella, “Modeling and Evaluating the Resilience of Critical Electrical Power Infrastructure to Extreme Weather Events,” IEEE Syst. J., pp. 1–10, 2015.

[131] P. Pourbeik, P. S. Kundur, and C. W. Taylor, “The Anatomy of a Power Grid Blackout,” IEEE power & energy magazine, no. september/october, 2006.

[132] G. Andersson, P. Donalek, R. Farmer, N. Hatziargyriou, I. Kamwa, P. Kundur, N. Martins, J. Paserba, P. Pourbeik, J. Sanchez-Gasca, R. Schulz, a. Stankovic, C. Taylor, and V. Vittal, “Causes of the 2003 Major Grid Blackouts in North America and Europe, and Recommended Means to Improve System Dynamic Performance,” IEEE Trans. Power Syst., vol. 20, no. 4, pp. 1922–1928, 2005.

[133] D. Kirschen and F. Bouffard, “Keeping the lights on and the information flowing,” IEEE Power Energy Mag., vol. 7, no. 1, pp. 50–60, 2009.

[134] G. Walker, “Come back sociotechnical systems theory, all is forgiven …,” Civ. Eng. Environ. Syst., vol. 32, no. 1–2, pp. 170–179, 2015.

[135] M. E. J. Newman, Networks: An Introduction. Oxford: Oxford University Press, 2010.

[136] F. Hu, A. Mostashari, and J. Xie, Socio-Technical Networks: Science and Engineering Design. CRC Press, 2011.

[137] A. Vespignani, “Modelling dynamical processes in complex socio-technical systems,” Nat. Phys., vol. 8, no. 1, pp. 32–39, Dec. 2011.

[138] P. M. Salmon, N. a Stanton, G. H. Walker, D. Jenkins, C. Baber, and R. McMaster, “Representing situation awareness in collaborative systems: a case study in the energy distribution domain.,” Ergonomics, vol. 51, no. 3, pp. 367–384, 2008.

[139] N. A. Stanton, “Representing distributed cognition in complex systems: how a submarine returns to periscope depth.,” Ergonomics, vol. 57, no. 3. Taylor & Francis, pp. 403–18, 2014.

[140] N. A. Stanton and C. Harvey, “Beyond human error taxonomies in assessment of risk in sociotechnical systems: a new paradigm with the EAST ‘broken-links’ approach,” Ergonomics, vol. 139, no. October, pp. 1–13, 2016.

[141] P. H. J. Nardelli, N. Rubido, C. Wang, M. S. Baptista, C. Pomalaza-Raez, P. Cardieri, and M. Latva-aho, “Models for the modern power grid,” Eur. Phys. J. Spec. Top., vol. 2437, no. Resilient Power Grids and Extreme Events, pp. 1–15, 2014.

[142] K. M. Carley, “Computational organizational science and organizational engineering,” Simul. Model. Pract. Theory, vol. 10, no. 5–7, pp. 253–269, 2002.

[143] K. Jung and M. Song, “Linking emergency management networks to disaster resilience: bonding and bridging strategy in hierarchical or horizontal collaboration networks,” Qual. Quant., vol. 49, no. 4, pp. 1465–1483, 2015.

[144] N. Kapucu and V. Garayev, “Designing, Managing, and Sustaining Functionally Collaborative Emergency Management Networks,” Am. Rev. Public Adm., 2012.

[145] N. Kapucu and V. Garayev, “Structure and Network Performance: Horizontal and Vertical Networks in Emergency Management,” Adm. Soc., p. 0095399714541270-, 2014.

[146] T. Kim, “Blackouts Hit Korea Nationwide,” The Korea Times, 2011.

[147] C. Sang-Hun, “Scandal in South Korea over nuclear revelations,” New York Times, 2013.

[148] T. Kim, S. Nazir, and K. I. Øvergård, “A STAMP-based causal analysis of the Korean Sewol ferry accident,” Saf. Sci., vol. 83, pp. 93–101, 2016.

[149] Y. Kim and H. Kim, “Improving Korea’s Societal Security by Preparing for Unforeseen Disasters: Focused on the Horizontal Collaboration Approach,” Int. J. Secur. Its Appl., vol. 10, no. 3, pp. 11–20, 2016.

[150] D. H. Kim, D. A. Eisenberg, Y. H. Chun, and J. Park, “Network topology and resilience analysis of South Korean power grid,” Phys. A Stat. Mech. its Appl., vol. 465, pp. 13–24,

2017.

[151] Korea Power Exchange. (KPX), “Electric Power Statistics Information System,” 2016. [Online]. Available: http://epsis.kpx.or.kr/epsis/ekesStaticMain.do;jsessionid=Y0JXXWdKvpwzznLpXTn5fy0Z4sLvbZzlQytHgtwF2kN2phJJQjsR!241999982?cmd=001001&flag=&locale=EN. [Accessed: 01-Sep-2016].

[152] D. Ngar-yin Mah, J. M. van der Vleuten, J. Chi-man Ip, and P. Ronald Hills, “Governing the transition of socio-technical systems: A case study of the development of smart grids in Korea,” Energy Policy, vol. 45, pp. 133–141, Jun. 2012.

[153] R. D. Zimmerman, C. E. Murillo Sánchez, and R. J. Thomas, “MATPOWER: Steady-State Operations, Planning, and Analysis Tools for Power Systems Research and Education,” Power Syst. IEEE Trans., vol. 26, no. 1, pp. 12–19, 2011.

[154] “Matlab Tools for Network Analysis (2006-2011),” 2011. [Online]. Available: http://strategic.mit.edu/downloads.php?page=matlab_networks. [Accessed: 01-Sep-2016].

[155] D. Gleich, “MatlabBGL,” 2008. [Online]. Available: https://www.mathworks.com/matlabcentral/fileexchange/10922-matlabbgl?requestedDomain=www.mathworks.com. [Accessed: 01-Sep-2016].

[156] S. P. Borgatti, “Centrality and network flow,” Soc. Networks, vol. 27, no. 1, pp. 55–71, 2005.

[157] M. Rosas-Casals, S. Bologna, E. F. Bompard, G. D’Agostino, W. Ellens, G. A. Pagani, A. Scala, and T. Verma, “Knowing power grids and understanding complexity science,” Int. J. Crit. Infrastructures, vol. 11, no. 1, pp. 4–14, 2015.

[158] N. Kapucu, “Interorganizational Coordination in Dynamic Context: Networks in Emergency Response Management,” Connections, vol. 26, no. 2, pp. 33–48, 2005.

[159] A. B. M. Nasiruzzaman, H. R. Pota, and M. A. Mahmud, “Application of centrality measures of complex network framework in power grid,” IECON 2011 - 37th Annu. Conf. IEEE Ind. Electron. Soc., pp. 4660–4665, 2011.

[160] A. B. M. Nasiruzzaman, H. R. Pota, A. Anwar, and S. Member, “Comparative Study of Power Grid Centrality Measures using Complex Network Framework,” in Power Engineering and Optimization Conference (PEDCO), 2012, no. June, pp. 6–7.

[161] A. B. M. Nasiruzzaman, H. R. Pota, A. Anwar, and F. R. Islam, “Modified centrality

measure based on bidirectional power flow for smart and bulk power transmission grid," 2012 IEEE Int. Power Eng. Optim. Conf. PEOCO 2012 - Conf. Proc., no. June, pp. 159–164, 2012.

[162] A. B. M. Nasiruzzaman and H. R. Pota, "Transient Stability Assessment of Smart Power System using Complex Networks Framework," in IEEE Power and Energy Society General Meeting, 2011, pp. 1–7.

[163] A. B. M. Nasiruzzaman and H. R. Pota, "Complex Network Framework Based Comparative Study of Power Grid Centrality Measures," Int. J. Electr. Comput. Eng., vol. 3, no. 4, 2013.

[164] S. Arianos, E. Bompard, a Carbone, and F. Xue, "Power grid vulnerability: a complex network approach.," Chaos, vol. 19, no. 1, p. 13119, Mar. 2009.

[165] E. Bompard, R. Napoli, and F. Xue, "Extended topological approach for the assessment of structural vulnerability in transmission networks," IET Gener. Transm. Distrib., vol. 4, no. 6, p. 716, 2010.

[166] E. Bompard, D. Wu, and F. Xue, "Structural vulnerability of power systems: A topological approach," Electr. Power Syst. Res., vol. 81, no. 7, pp. 1334–1340, Jul. 2011.

[167] G. C. Ejebe, J. Tong, J. G. Waight, J. G. Frame, X. Wang, and W. F. Tinney, "Available transfer capability calculations," IEEE Trans. Power Syst., vol. 13, no. 4, pp. 1521–1527, 1998.

[168] A. J. Wood, B. F. Wollenberg, and G. B. Sheble, Power Generation, Operation, and Control. John Wiley & Sons, 2014.

[169] E. Bompard, E. Pons, L. Luo, and M. Rosas Casals, "A Perspective overview of topological approaches for vulnerability analysis of power transmission grids," Int. J. Crit. Infrastructures, vol. 11, no. JANUARY, 2015.

[170] E. Bompard, E. Pons, and D. Wu, "Extended Topological Metrics for the Analysis of Power Grid Vulnerability," IEEE Syst. J., vol. 6, no. 3, pp. 481–487, 2012.

[171] K. M. Carley, J. Pfeffer, J. Reminga, J. Storrick, and D. Columbus, "ORA User's Guide 2013," no. CMU-ISR-13-108, 2013.

[172] A. Abbasi and N. Kapucu, "A longitudinal study of evolving networks in response to natural disaster," Comput. Math. Organ. Theory, 2015.

[173] L. C. Freeman, “Centrality in social networks conceptual clarification,” Soc. Networks, vol. 1, no. 3, pp. 215–239, 1978.

[174] B. Petrenj, E. Lettieri, and P. Trucco, “Towards enhanced collaboration and information sharing for critical infrastructure resilience: current barriers and emerging capabilities,” Int. J. Crit. Infrastructures, vol. 8, p. 107, 2012.

[175] E. P. R. Coelho, J. C. Thomazelli, M. H. M. Paiva, and M. E. V Segatto, “A Complex Network Analysis of the Brazilian Power Test System,” pp. 113–118, 2015.

[176] Z. Wang, A. Scaglione, and R. J. Thomas, “Electrical centrality measures for electric power grid vulnerability analysis,” Proc. IEEE Conf. Decis. Control, no. 2009, pp. 5792–5797, 2010.

[177] H. Bai and S. Miao, “Hybrid flow betweenness approach for identification of vulnerable line in power system,” IET Gener. Transm. Distrib., vol. 9, no. 12, pp. 1324–1331, 2015.

[178] P. D. H. Hines and P. Rezaei, “Cascading Failures in Power Systems,” in Smart Grid Handbook, C.-C. Liu, S. McArthur, and S.-J. Lee, Eds. John Wiley & Sons, 2016, pp. 215–234.

[179] H. Guo, C. Zheng, H. H.-C. Iu, and T. Fernando, “A critical review of cascading failure analysis and modeling of power system,” Renew. Sustain. Energy Rev., vol. 80, no. March, pp. 9–22, 2017.

[180] R. Baldick, B. Chowdhury, I. Dobson, Z. Dong, B. Gou, D. Hawkins, H. Huang, M. Joung, D. Kirschen, F. Li, J. Li, Z. Li, C. C. Liu, L. Mili, S. Miller, R. Podmore, K. Schneider, K. Sun, D. Wang, Z. Wu, P. Zhang, W. Zhang, and X. Zhang, “Initial review of methods for cascading failure analysis in electric power transmission systems,” IEEE Power Eng. Soc. Gen. Meet., pp. 1–8, 2008.

[181] M. Vaiman, K. Bell, Y. Chen, B. Chowdhury, I. Dobson, P. Hines, M. Papic, S. Miller, and P. Zhang, “Risk assessment of cascading outages: Methodologies and challenges,” IEEE Trans. Power Syst., vol. 27, no. 2, pp. 631–641, 2012.

[182] P. F. Petersen, H. Jóhannsson, and A. H. Nielsen, “Investigation of Suitability of Cascading Outage Assessment Methods for Real-Time Assessment,” in PowerTech, 2015 IEEE Eindhoven, 2015, pp. 1–5.

[183] R. Kinney, P. Crucitti, R. Albert, and V. Latora, “Modeling cascading failures in the North American power grid,” Eur. Phys. J. B, vol. 46, no. 1, pp. 101–107, 2005.

[184] A. E. Motter and Y. C. Lai, “Cascade-based attacks on complex networks,” Phys. Rev. E,

vol. 66, no. 6, pp. 2–5, 2002.

[185] B. A. Carreras, D. E. Newman, I. Dobson, and N. S. Degala, “Validating OPA with WECC data,” Proc. Annu. Hawaii Int. Conf. Syst. Sci., pp. 2197–2204, 2013.

[186] I. Dobson, B. A. Carreras, and V. E. Lynch, “An initial model for complex dynamics in electric power system blackouts,” in Hawaii International Conference on System Sciences, 2001, no. January.

[187] J. Chen, J. S. Thorp, and I. Dobson, “Cascading dynamics and mitigation assessment in power system disturbances via a hidden failure model,” Int. J. Electr. Power Energy Syst., vol. 27, no. 4, pp. 318–326, 2005.

[188] L. Cuadra, S. Salcedo-Sanz, J. Del Ser, S. Jiménez-Fernández, and Z. Geem, “A Critical Review of Robustness in Power Grids Using Complex Networks Concepts,” Energies, vol. 8, no. 9, pp. 9211–9265, 2015.

[189] C. D. Zorrilla, “The View from Puerto Rico - Hurricane Maria and Its Aftermath,” N. Engl. J. Med., vol. 377, no. 19, pp. 1801–1803, 2017.

[190] A. Makhorin, “GLPK (GNU linear programming kit).” .

[191] N. Altman, K. M. Carley, and J. Reminga, “ORA User’s Guide 2017,” pp. 11–1, 2017.

[192] U. Brandes, “A faster algorithm for betweenness centrality,” J. Math. Sociol., vol. 25, no. 2, pp. 163–177, 2001.

[193] R. Kinney, P. Crucitti, and V. Latora, “Modeling Cascading Failures in the North American Power Grid,” no. 1, pp. 1–6, 2003.

[194] V. Cupac, J. T. Lizier, and M. Prokopenko, “Comparing dynamics of cascading failures between network-centric and power flow models,” Int. J. Electr. Power Energy Syst., vol. 49, pp. 369–379, Jul. 2013.

[195] North American Electric Reliability Corporation, “Transmission Capability Margins and Their Use in ATC Determination,” 1999.

[196] North American Electric Reliability Corporation, “Standard MOD-001-0 — Documentation of TTC and ATC Calculation Methodologies Introduction,” 2005.

[197] P. W. Sauer, “Alternatives for calculating transmission reliability margin (TRM) in

available transfer capability (ATC),” Proc. Thirty-First Hawaii Int. Conf. Syst. Sci., vol. 3, no. February 1998, 1998.

[198] J. Doyle and M. Csete, “Motifs, control, and stability,” PLoS Biol., vol. 3, no. 11, pp. 1868–1872, 2005.

[199] M. Csete and J. Doyle, “Bow ties, metabolism and disease,” Trends Biotechnol., vol. 22, no. 9, pp. 446–450, 2004.

[200] J. C. Doyle and M. Csete, “Architecture, constraints, and behavior,” 2011.

[201] M. Chiang, S. H. Low, A. R. Calderbank, and J. C. Doyle, “Layering as optimization decomposition: A mathematical theory of network architectures,” Proc. IEEE, vol. 95, no. 1, pp. 255–312, 2007.

[202] D. L. Alderson, G. G. Brown, M. W. Carlyle, and L. Anthony Cox, “Sometimes There Is No Most-Vital’’ Arc: Assessing and Improving the Operational Resilience of Systems,” Mil. Oper. Res., vol. 18, no. 1, pp. 21–37, 2013.

[203] D. L. Alderson, G. G. Brown, and W. M. Carlyle, “Operational Models of Infrastructure Resilience,” Risk Anal., p. n/a-n/a, 2015.

[204] Korea Power Exchange (KPX), “Korea Power Exchange Transmission Map,” 2016. [Online]. Available: https://www.kpx.or.kr/eng/contents.do?key=333. [Accessed: 01-Sep-2016].

APPENDIX A

A. CO-AUTHOR AUTHOR PERMISSION FOR PUBLISHED MATERIAL

Each chapter based on published, in review, or in preparation material lists the order of co-authors and proper citation. For Ch. 2, both Alderson and Eisenberg are co-first authors. Ch. 3-5, Eisenberg is the first author. All co-authors have granted permission for use the material in this disseration.