ASSESSING RESILIENCE IN POWER GRIDS AS A PARTICULAR CASE OF SUPPLY CHAIN MANAGEMENT

THESIS

Gabriel Alejandro Montoya, Lt. Col. Argentine Air Force

AFIT/LSCM/ENS/10-08

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

The views expressed in this thesis are those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense or the United States Government.

AFIT/LSCM/ENS/10-08

ASSESSING RESILIENCE IN POWER GRIDS AS A PARTICULAR CASE OF SUPPLY CHAIN MANAGEMENT

THESIS

Presented to the Faculty

Department of Operational Sciences

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science in Logistics and Supply Chain Management

Gabriel Alejandro Montoya

Lt. Col., Argentine Air Force

March 2010

AFIT/LSCM/ENS/10-08

ASSESSING RESILIENCE IN POWER GRIDS AS A PARTICULAR CASE OF SUPPLY CHAIN MANAGEMENT

Gabriel Alejandro Montoya

Lt. Col., Argentine Air Force

Approved:

//SIGNED//

_____ 12-MAR-10

Daniel D. Mattioda, Major, USAF, PhD. (Chairman) date

//SIGNED//

_____ 12-MAR-10

Timothy J. Pettit, Lt. Col., USAF, PhD. (Member) date

//SIGNED//

_____ 12-MAR-10

Doral E. Sandlin, Lt. Col., USAF, PhD. (Member) date

Abstract

Electrical power grids represent a critical infrastructure for a nation as well as strategically important. Literature review identified that power grids share basic characteristics with Supply Chain Management.

This thesis presents a linear programming model to assess power grid resilience as a particular case of Supply Chain Management.

Since resilient behavior is not an individual or specific system's attribute but a holistic phenomenon based on the synergic interaction within complex systems, resilience drivers in power grids were identified. Resilience is a function of Reliability, Recovery Capability, Vulnerability and Pipeline Capacity. In order to embed heterogeneous variables into the model, parameterization of resilience drivers were developed. A principle of improving resilience through redundancy was applied in the model by using a virtual redundancy in each link which allows reliability improvement throughout the entire network. Vulnerability was addressed through a quantitative standard (MIL-STD 882D) and mitigated through security allocation. A unique index (R) integrates the resilience complexity to facilitate alternate scenarios analysis toward strategic decision making. Decision makers are enabled to improve overall power grid performance through reliability development as well as security allocation at the more strategic links identified by the optimal solutions. Moreover, this tool lets decision makers fix grid variables such as reliability, reduced pipeline capacity, or vulnerabilities within the model in order to find optimal solutions that withstand disruptions.

The model constitutes an effective tool not only for efficient reliability improvement but also for rational security allocation in the most critical links within the network. Finally, this work contributes to the federal government mandates accomplishment, intended to address electrical power-related risks and vulnerabilities.

To my wife and my daughters, for supporting my effort in this endeavor. Their love and patience enabled me to successfully overtake this challenge. Likewise, to my parents, who always trusted me

Acknowledgments

I would like to express my sincere appreciation to my faculty advisor, Major Daniel D. Mattioda, for his outstanding guidance and support throughout the course of this thesis effort. Likewise, my sincere thanks and recognition to the members of my thesis committee, Lt. Col. Thimothy J. Pettit and, Lt. Col. Doral E. Sandlin for their outstanding guidance, encouragement and expertise.

Gabriel Alejandro Montoya

Table of Contents

Page

List of Figures

Figure **Page**

Page

List of Tables

Table **Page**

List of Appendices

Appendix **Page**

ASSESSING RESILIENCE IN POWER GRIDS AS A PARTICULAR CASE OF SUPPLY CHAIN MANAGEMENT

I. Introduction

Background

In the last decades, energy has become one of the most critical sustainability issues of economies around the world. Statistics reveal that nationwide electricity consumption in the US doubled from 8% to 16%, from 1970 to 2000, as percentage of overall energy consumption (USPGS&U, 2009). United States net import of crude oil is expected to increase from about 10 million barrels per day to over 13 million barrels per day by 2030 (EIA, 2009).

In 2006, the US Department of Defense (DoD) was responsible for 80% of the energy used by the US Government and almost 1% of the nation's total energy use. In personnel, budget, and energy use, the DoD can be considered equivalent to a small nation (Ryan, 2008).

On the other hand, technology development, quality of life improvements and military operations have required the US to use more energy than expected. The current trend is a 2% annual increment in US electricity consumption. This trend demands strategic decisions in order to be able to reach goals in a more sustainable and secure environment (Peltier, 2006:70).

Additionally, privately and publicly operated commercial distribution systems like the national electric grids have been identified in United States as vulnerable to a loss of service from natural disasters, aging infrastructure, human error, or a physical or cyber attack from inside or outside the system (USAF, 2208:4).

Since energy consumption is a US concern, this work is focused on American power grids performance. This involves not only military installations but also those installations that ensure the availability of essential utilities and services in both, tactical (deployed) and fixed installations. Concepts and conclusions are presented which are relevant for all networked utilities, involving energy demand as strategic resource.

The relevance of this work is not only about commercial grids but electricity supply as a whole. Current geopolitical environment has changed traditional beliefs. DoD has traditionally assumed that commercial electrical power grids are highly reliable and subject to only infrequent (generally weather-related), short-term disruptions. For backup supplies of electricity, DoD has depended primarily on diesel generators with short-term fuel supplies. This represents just a tactic backup with limited capability to support short-term operations. However, current threats are complex, long lasting and dangerous as well (GAO, 2009:1-2).

The Presidential Decision Directive/NSC-63 (1998) has been found as a valuable source to identify Critical Infrastructure capabilities:

1. To perform essential national security missions and to ensure the general public health and safety.
2. To maintain state and local governments order and to deliver minimum essential public services.
3. To ensure (the private sector) the orderly functioning of the economy and the delivery of essential telecommunications, energy, financial and transportation services.

The same document, also states: “any potential interruption or manipulation of these critical functions must be brief, infrequent, manageable, geographically isolated and minimally detrimental to the welfare” (US Presidential Decision Directive/NSC-63, 1998:3). This is the first illustration of resilient behavior in this work.

On the other hand, in 1999, President Clinton signed the Executive Order 13123 with the following preamble “The Federal Government, as the Nation’s largest energy consumer shall significantly improve its energy management in order to save taxpayer dollars and reduce emissions that contribute to air pollution and global climate change” (US President, 1998:30851). The main issues addressed are those related to sustainability, money saving and environment protection. Since we cannot manage what we cannot measure, the expression “energy management” implies the need of assessment, a basic tool for decision makers.

Since the 9-11 attack, energy use was conceived as related to the following risks and challenges (DoD, 2008):

1. ***Mobility:*** Risk to operational forces due to a large and growing fuel demand coupled with limited fuel distribution networks in some theaters. Estimates for the true cost of fuel in the field range from 10 times greater than the purchase price (for air tanker delivered fuel) to over 100 times greater than the purchase price (for fuel delivered to deep forward operating bases).
2. ***Sustainability:*** Ability to sustain critical missions at fixed and tactical installations due to an interruption of energy (both fuel and electricity) availability. Fixed installations are currently almost completely dependent on

the commercial power grid; tactical installations must either tap into indigenous energy sources or bring their own power generators.

3. ***Cost Instability:*** Another energy challenge comes from price instability. High fuel and electricity demand coupled with volatile commodity prices can create budget problems. A $10 a barrel change in oil pricing results in about a $1.3 billion change in cost to the DoD.
4. ***Geo-political Considerations:*** Global warming is predicted to present serious international security issues, because of its adverse effects on food and fresh water availability. The US is also under increasing pressure from their closest allies to take a stronger leadership role in reducing greenhouse gas emissions. Besides, because the global oil market is not publically held but is largely controlled by governments, it can easily be exploited and controlled. As prices rise due to demand increases, suppliers do not increase their supply, driving prices even higher.

The DoD recognizes that the most critical assets are vulnerable to electrical power disruptions, but it lacks sufficient information to determine the full extent of their vulnerability. At least 24 of the 34 most critical assets experienced some electrical power disruptions lasting up to 7 days during the 3-year period from January 2006 through December 2008 (GAO, 2009:22).

A critical root cause of DoD energy risks is that currently energy supply processes do not systematically recognize risks inherent in delivering fuel and energy to operational forces or risks that have potential to disable the commercial power grid. Both seriously degrade critical national security capabilities (DoD, 2008).

The US electricity market (and the energy industry itself) is strongly influenced by the availability and price of nonrenewable resources. New challenges range from lack of enough resources to produce energy and reduce cost, to an adequate transmission infrastructure which ensures availability and continuity of electricity utility where it is needed (DoD, 2008).

On the other hand, the Department of Homeland Security (DHS) is the principal federal entity responsible for leading, integrating, and coordinating the overall national effort to protect the nation's critical infrastructure and key resources. DHS led the development of the National Infrastructure Protection Plan, which provides a framework for managing risks to US critical infrastructure (US GAO, 2009). From the 37 target capabilities listed by DHS (Appendix A), at least 26 are directly or indirectly related (dependency relationship) to energy (power) concerns (McGill and Ayyub, 2009).

Within the framework of the National Infrastructure Protection Plan of 2009, DoD has to collaborate with the Department of Homeland Security and the Department of Energy to address risks and vulnerabilities associated with electrical power infrastructure (GAO, 2009:3).

Moreover, DoD establishes the following four strategic goals to support a path to future sustainable energy:

1. Maintain or enhance operational effectiveness by reducing total force energy demands.
2. Increase energy security through strategic resilience by increasing the availability and use of alternative or assured energy sources.

3. Enhance operational and business effectiveness by institutionalizing energy considerations and solutions in DoD planning & business processes.
4. Establish and monitor Department-wide energy metrics.

Collectively, these goals address the DoD's primary energy challenges. Also, DoD states that these goals, to be effective, will likely require increased investment or policy emphasis in the following areas:

1. Science and Technology to explore and test energy efficiency technologies and alternative sources of energy.
2. Installation energy initiatives and policies to reduce energy demand and enhance energy self-sufficiency at both tactical and fixed sites.
3. Improved capability to model energy impacts on acquisition and operations.

Although energy concerns have been presented without distinguishing among the different kind of resources, this work will focus on electrical networks that are highly dependent on no-renewable resources such as petroleum.

Strategic Resilience, as referred by DoD in the Energy Security Strategic Plan (DOD, 2008:8), carries out a broad meaning and must be specified in measurable terms if we want to manage such a strategic resource (electricity). Given that resilience concept has been brought to the Supply Chain Management arena from different fields; this work will develop a theoretical research about resilience's scope in different fields. Then, considering power grids as a particular case of supply chain-network, a resilience assessment model will be proposed as a decision tool to assess actual power grids' performances.

The results from this work will contribute to strategic energy management by developing a model based on resilience assessment in order to improve the strategic decision making process.

The Problem and the Research Questions Statement

Since energy concerns involve several different aspects that need to be addressed, the present work will focus on power grids' performance assessment as a way to contribute to the following goals:

1. Enhance *effectiveness of power grids management*.
2. Increase energy security through *strategic resilience* measurement.
3. Develop energy performance (resilience) *metric*.
4. Model *power grid resilience* as a representative performance to assess.
5. Explore *potential contributions of SmartGrid design* to overall resilience.
6. Develop performance in a *sustainable framework.*

From the aforementioned concepts, the problem to be addressed in this thesis is stated as follows:

- What attributes define resilience in power grids, and what metrics will enable effective strategic management?

Taking into account such a complex problem, this thesis seeks to answer the following research questions:

- How can be *resilience* defined for power grids?
- What attributes are relevant to a resilient power grid behavior? Are they quantifiable?

- How should attributes involved in power grids performance be embedded within a resilience assessment model, in order to have a quantitative (objective) and comparable measurement?
- Does a Linear Programming Model provide quantifiable (useful) information to support decision making processes with respect to resilience in power grids?
- What is the necessary data to solve a model of the problem under study?

Answering these questions will help to address the purpose of this thesis in a manageable and systematic way.

Consequently, this thesis attempts to develop a mathematical model that allows decision makers (e.g. DoE, DoD, USAF, etc) to conduct quantifiable assessments about resilience in power grids in order to contribute to strategic decision process regarding the power network management.

Assumptions

Although specific assumptions will be given in further chapters for scenario analysis, the reader is presented with the overall framework regarding to the problem on hand.

One of the most important aspects of all problem solving strategies is to establish assumptions as an integral part of the problem.

Models are simplified versions of the system or decision problem they represent, and consequently less expensive and complex than dealing with actual systems. Since developing Linear Programming Models implies the use of a large amount of data, this data is classified and analyzed in an appropriate form to reach positive results.

Disruptions affecting more than 50,000 customers or 300 megawatts (MW) of load are required to be reported to the US Department of Energy (DoE). So, we assume the proper data is available for model use. The data is provided by the US Department of Energy (DoE), Electric Power Research Institute (EPRI) and the Energy Information Administration (EIA) to allow greater fidelity in modeling power grids.

Second, we assume that the current state of power grids will not change in the short term. In fact, current power transformers in US are about 40 years old, and most power grids are based on 1950s technology with sketchy communications and antiquated control systems (Economist, 2004:19). Consequently, assessing resilience in actual power grids will result in significant benefits for decision makers.

The third assumption simplifies the analysis of flow networked problems, where demand nodes tend to represent aggregations of customers (users) in a local region.

Finally, further assumptions for model development are needed. These assumptions are described in future chapters in order to explain in depth the research methodology.

Scope

The scope of this work is focused on power grids's performance assessment in terms of resilience. This means that any other attribute or specific characteristic will not be assessed.

Since resilience engineering is a relatively new concept (Hollnagel and others. 2008), this thesis will develop a *resilience assessment tool* to be applied to power grids as a particular case of supply chain management.

Summary

Current threats to critical infrastructure range from natural disasters and accidents to intentional attacks on electrical power grids. Accidents include failures related to material, hardware and software systems as well as unintentional human-being errors. These networks are particularly relevant in supplying energy to accomplish the overall critical infrastructure's missions.

This work will develop a theoretical research about resilience's scope in different fields in order to look for common attributes shared by resilient systems. Power grids are considered as a particular case of supply chain management. Therefore, a resilience model is proposed in order to develop a decision tool to assess power grid resilience to contribute to the strategic energy management. To make the results valid, assumptions and limitations were presented. However, in further chapters others will be presented for specific scenario analysis.

This chapter has developed the relevant background that present the strategic energy management importance and the role that critical infrastructure plays for nation's security.

The remaining chapters are as follows. Chapter II presents a review of the existing literature of the topics under study. Chapters III and IV cover the methodology used for model development and the results from the models are discussed. Finally, conclusions, possible model applications, study limitations, as well as managerial implications and challenges in the subject matter are included in Chapter V.

II. Literature Review

Introduction

In this chapter the reader is presented with several background and literature topics related to the resilience concept as well as design and assessment methodology. First, relevant federal mandates, including Executive Order (EO) 13123, as well as applicable DoD, DHS and Air Force Guidance, are presented. Then, different approaches to resilience concept are presented for different fields. This is particularly relevant in that different disciplines have explored resilient behavior as a way to assess performance capability when systems, organizations and people are exposed to stress.

Likewise, since the research objective is to develop a decision model, this chapter will focus on methodological matters, including a brief summary of several model types and a thorough discussion of Linear Programming and parameterization as a method for quantitative resilience assessment in power grids.

Finally, a brief summary of the main topics developed is presented as well as the necessary theory needed for modelization, including the parameterization of the interest.

Federal Mandated and Agency Guidance

US government has been conducting specific efforts toward energy efficiency as well as sustainability, since energy use is a growing concern with critical implications for the present and the near future. The US president's Executive Order # 13123 (1999) stated that the Federal Government, as the nation's largest energy consumer, shall significantly improve its energy management in order to save taxpayer dollars and reduce emissions that contribute to air pollution and global climate change.

These issues are addressed in a subsequent Executive Order:

> In implementing the policy, the head of each agency shall: (a) improve energy efficiency and reduce greenhouse gas emissions of the agency, through reduction of energy intensity by (i) 3 percent annually through the end of FY 2015, or (ii) 30 percent by the end of FY 2015, relative to the baseline of the agency's energy use in FY 2003; (b) ensure that (i) at least half of the statutorily required renewable energy consumed by the agency in a fiscal year comes from new renewable sources, and (ii) to the extent feasible, the agency implements renewable energy generation projects on agency property for agency use. (EO 13423, 2007:sec. 2)

Consequently, since energy concern is a critical issue for the nation survivability, let's refer to the presidential definition about Critical Infrastructure:

> Critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government. They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private. (Presidential Decision Directive/NSC-63, 1998)

Other approaches refer to critical infrastructure as a term used by governments to describe assets that are essential for the functioning of a society and economy. Facilities commonly associated with the critical infrastructure are (Moteff and Parfomak, 2004):

1. Electricity generation and transmission infrastructure.
2. Gas production, transport and distribution.
3. Oil and oil products production, transport and distribution.
4. Telecommunication.
5. Water supply (drinking water, waste water/sewage).
6. Public health (hospitals, ambulances).
7. Transportation systems (fuel supply, railway network, airports, harbors, inland shipping).
8. Financial services (banking, clearing).

9. Security services (police, military).

In 2006, the Homeland Security Advisory Council presented its final report responding to a recommendations requirement in order to advance on national infrastructure policy. One of the recommendations showed that critical infrastructure is shared by both public as well private sectors; in fact the private sector owns and operate 85% of the US critical infrastructure. For that reason critical infrastructure resilience (CIR) is promulgated as a top level strategic objective to drive national policy. Likewise, the taskforce realized that critical infrastructure has been treated in a reactive way in a sense that the planning efforts (preparedness) have been focused, almost exclusively, on structural protection against terrorist threats. Experience shows that terrorist threats have to be treaded from holistic perspective, assuming terrorism is permanently learning and changing. Therefore, no protection would be enough for critical infrastructure, and resilience appears as a way to mitigate and recover from unavoidable damages (CITF, 2006).

For instance, after the 9-11 attack, energy issues became more critical for the nation's survivability and specific concerns arose. The Department of Defense (DoD) developed the Energy Security Strategic Plan (ESSP) in order to address the two primary forms of energy that concern the DoD: fuel for transportation and electricity for installations and weapons systems. The US is able to generate sufficient electricity to meet the country's needs, but distributing electricity to where it is needed is still considered as a critical challenge (DoD, 2008:12). A relevant real-world example of such a concern is the major power grid failure that struck the northeastern United States and Canada in the summer of 2003, where approximately 50 million people lost power

for hours to days in parts of the Northeastern and Midwestern United States and Ontario Canada. Over 100 power stations failed at a cost estimated between $6 to $10 billion dollars (ICF Consulting, 2003).

Two approaches for reducing risk to critical missions are also presented by the DoD: reducing electrical demand, and improving the security of energy supplied. So, security allocation appears as an effective strategy to deal with power grid's risks. Additionally, the Energy Security Strategic Plan recognizes the need of DoD-wide energy metrics, and requires improved maintenance procedures focused on maintaining high efficiency performance as an option for improving resilience against extended grid outage (DoD, 2008:22-23).

On the other hand, the United States Air Force (USAF) Infrastructure Energy Strategic Plan includes several major statutory and policy mandates toward a more resilient electrical, water and logistics fuel systems at Air Force installations. They include:

1. Reduce base water use by 2 percent per annum.
2. Increase use of renewable energy at annual targets.
3. Reduce ground vehicle fossil fuel use by 2 percent per annum.
4. Increase alternative fuel use by 10 percent per annum.

In particular, energy must be included in Air Force Critical Infrastructure Program plans, studied during Vulnerability Assessments and exercised during base response activities (USAF, 2008:11). This strategic plan' Vision include specific efforts to effectively reduce dependence on commercial energy supply and delivery systems, and enhance energy security for the Air Force (USAF, 2008:3).

As stated earlier, energy use reduction is a strategic goal. However, facility energy intensity reduction by over 30 percent from 2005-2015 is considered a hard goal to achieve.

Finally, since energy use and availability constitute a relevant concern with critical implications for the present and the near future in US, identifying disruption factors that affect energy distribution and availability, is considered as a critical point in this work.

Understanding Disruptions

Although traditional systems engineering practices usually try to anticipate and resist disruptions, they are still vulnerable to unforeseen threats as evidenced by the Columbia shuttle disaster and the Northeast electrical blackout of 2003. This is because engineered systems cannot be designed to anticipate all future possibilities. Complex systems are adaptive but also unpredictable (Fiksel, 2003:5330).

A research conducted by the Institute of Electrical and Electronics Engineers (IEEE) found that the complexity and vulnerability of modern power grids makes periodic and disastrous failures to be inevitable. Moreover, the measure typically embraced by utility regulators and managers following a major blackout is to “protect” the system from a repeat of the disaster. These renewed protection measures actually tend to be ineffective and even make future blackouts bigger and more likely. This is considered a consequence of making stronger and over protecting the failed points, allowing new and weaker vulnerabilities through the networked infrastructure (Peter Fairley, 2004).

However, since protection is a key aspect of resilience, security always is an option that has to be considered in the resilience environment. Table 1 lists a number of criteria by which the appropriateness of protection measures versus resilience measures could be assessed. Just as a linear or a complex system is not better or worse but different, the corresponding measure is not better or worse, but appropriate or inappropriate. In other words, depending on the context, resilience is not necessarily the only option for infrastructure security. The key is recognizing how the nature of the system, the budget needs, or the subject in question, would point to a differentiated approach.

Table 1. Protection and Resilience Relationship (George Mason University, 2007:16)

	Protection	**Resilience**
Activity planned	hardening structures	redesigning processes
Subject focus	asset-driven	services-driven
Desired metrics	absolute (0/1)	conditional (0-1)
Value proposition	cost-centered	benefit-centered
Security stance	reactive approach	proactive approach
Type of disturbance	(sudden) disruption	(graceful) degradation
Budget needs	short-term investments	long-term investments
Network character	insulated	interdependent
System interaction	linear	complex
System coupling	loose	tight

In order to illustrate how protection and resilience are not absolute categories, but depend on the type of system and problem at hand, power generation provides a good example. For instance, if an electric power plant did not have a perimeter fence, the activity associated with that would be hardening the structure – a protection measure.

The same company might identify the need to have a contingency staffing plan that assigns and trains substitutes for critical functions – a resilience measure. If it is a conventional plant, it is loosely coupled in terms of its energy supply, meaning it is possible to switch to another fuel (e.g. oil to coal) if the primary source is disrupted (George Mason University, 2007).

On the other hand, protection is often associated with the set of actions to harden assets to withstand identified contingencies, mitigate the damage, or make them an unattractive target. The focus is to maintain the assets' core function and ward off harm. Resilience, approaches the issue by taking reasonable protective actions, but also having alternative capabilities as needed, and the ability to withstand the disruption (George Mason University, 2007:100).

Moreover, Fiksel states that since decision makers need to embrace uncertainty (risk), strategic adaptation is more important than strategic planning in order to reach resilience in today environment (Fiksel, 2003:5338).

The national system for transmitting electricity from central generating stations to users throughout the United States and Canada is becoming increasingly fragile and susceptible to disruptions from physical attack by saboteurs or outages from natural events. Its digital control systems are susceptible to cyber attack, and are constantly probed by foreign governments (DoD, 2008:23). Extreme weather events have demonstrated how large segments of the national grid can be taken down. The 2003 blackout showed how energy infrastructures are prone to disasters. Recently a particular threat was highlighted when hackers demonstrated the ability to cause physical damage to critical components of the US electrical generation infrastructure using a laptop computer

and a wireless internet connection (DoD, 2008:23). Consequently, a relatively knowledgeable but determined saboteur has the potential to inflict significant physical damage, either by physical or cyber attack, which could require an extended period of time to restore. One of the most critical challenges that power grids face is how to predict these sorts of attacks.

On the other hand, natural disasters such as hurricanes, earthquakes, and forest fires damage and destroy energy infrastructure- sometimes on a very wide scale. These disasters are just one of the many threats that challenge power grids survivability. Existing literature agree that disruptions can be divided into three main categories in order to facilitate their likelihood analysis: natural disasters, accidents or manmade, and intentional attacks. Natural, man made, and foreign events have a high likelihood to disrupt the energy network system; it is just a matter of when. These three categories differ in the relative roles that human beings and random factors play in their cause, the methods to address their likelihood also differ (Sheffi, 2005:45).

Natural Disasters

Because natural disasters are relatively frequent, statistical models can be used to estimate the probability of their occurrence as well as their severity. In fact, insurance companies have well-developed models to predict the risk of earthquakes, floods, or lighting strikes for different areas of interest. Consequently, insurance premiums reflect the likelihood of relevant risk. For instance, the US Geological Survey (USGS) estimates that the areas most susceptible to earthquakes in the Unites States include the West Coast, the New Madrid zone in Missouri, and a few isolated locations on the US east coast. Likewise, the US National Oceanic and Atmospheric Administration (NOAA) publishes

statistics about severe weather. Climatological models define likely rainfall patterns, suggesting the probability of floods in wetter-than-expected regions.

Figure 1 shows the damage pattern within United States of whether related disasters in the period 1980-2006.

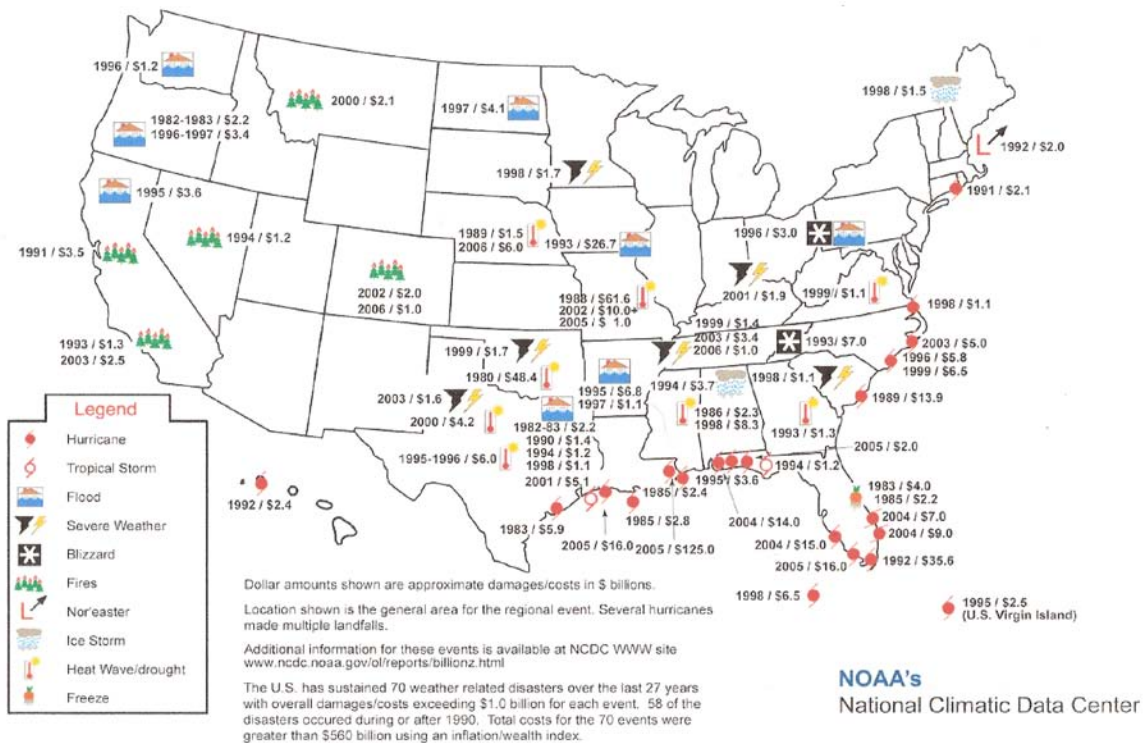


Figure 1. Billion Dollar Weather Disasters 1980-2006. (Hoffman, 20008:22)

The following definitions have been extracted from the USGS webpage in order to introduce the natural disasters phenomena:

- Earthquakes: Ground shaking caused by the sudden release of accumulated strain by an abrupt shift of rock along a fracture in the Earth or by volcanic or magmatic activity, or other sudden stress changes in the Earth.

- Hurricanes: Severe cyclones, or revolving storms, originating over the equatorial regions of the Earth, accompanied by torrential rain, lightning, and winds with a speed greater than 74 miles per hour.
- Tsunamis: Large destructive sea waves generated by earthquakes, volcanic eruptions, or large landslides.
- Floods: Relatively high streamflow that overflows the natural or artificial banks of a stream or that submerges land not normally below water level.
- Landslides: Downslope movement of rock, soil, or artificial fill under the influences of gravity.
- Volcanoes: Vents in the surface of the Earth through which magma and associated gases erupt; also, the forms of structures, usually conical, that are produced by the erupted material.
- Wildfires: Combustion, marked by flames or intense heat, in natural settings, often ignited by lightning or human activities. For fires set as part of natural resource management, use controlled fires.

These concepts give an idea of the extent and magnitude of natural phenomena that can affect power grids. However, they are within the realm of predictability.

Accidents

Although most safety literature is concerned with prevention, the first step in any safety (or secure) process should be an assessment of the likelihood of an accident (or attack).

As a system, power grids are aggregation of components from units to parts to subsystems and systems. Accordingly, accidents are also distinguished in ascending

order from incidents to accidents, from component failure to system accidents or disruptions.

To ensure safety, systems must avoid failures and losses, as well as responding appropriately when safety conditions have been violated. Major accidents are usually preceded by periods where the organization drifts toward states of increasing risk until the event leading to losses or disruptions occurs.

The 2003 blackout started as a natural event failure (trees falling on power lines have been recognized as a direct or contributing factor in cascading power failures (Hoffman, 2008:33). But a domino effect was a consequence of procedural errors in addressing the power grids's stress after trees started falling on power lines after the emergency started (Hollnagel and others, 2008:95).

Stresses of increased demand for electrical power contributed to the 2003 Northeast Blackout, which was an extended cascading power outage that affected about 50 million people living in a 9,300 square mile area in US and Canada. More than 500 generating units at 265 power plants shut down during the outage. It took over 2 weeks for power plants to regain full capacity (USG.A.O, 2009).

Networked systems have pervaded in all traditional infrastructures, rendering them more intelligent but more vulnerable at the same time. Physical infrastructure's efficiency often depends on monitoring and control by E-Networks, which usually have high levels of automation and remote controlled functionalities. Additionally, at a higher level, many complex networks are managed by man, and their performance finally depends on man's organizational performance, which is the most susceptible to failure. Moreover, networks are generally linked together and the services offered to or requested

from a single network are dependent on other interdependent networks. As a consequence we do not have to deal with single isolated systems but with systems of systems. This characteristic increases the likelihood not only of accidents but also of intentional attacks (Ulieru, 2007).

Intentional Attacks

Whereas natural disasters are forecasted based on statistical Power Law curves, and the likelihood of large accidents can be estimated from small mishaps, intentional disruptions follow a different logic. Intentional disruptions constitute an adaptive process, where saboteurs seek both to ensure the success of the attack and to maximize the damage inflicted. Here, the problem is an adaptive threat. Consequently, "hardening" one potential target against a given mode of attack may increase the likelihood that another target will be attacked or there will be a different type of attack. Since the enemy (threat) has his own learning process, attacks are likely to take place at the worst place and at the worst time, when the organization (system) is most unprepared and vulnerable (Sheffi, 2005:50).

Intentional attacks are conducted by both, internal operators as well as external operators. Because of their high frequency, labor strikes provide many examples in which an intelligent adversary will inflict damage using methods and timing that the company may not anticipate. Consequently, since intentional attacks (sabotage and terrorist) are adaptive processes, they are non-random events and require special attention as well as specific contingency plans.

When thinking of reducing an organization's vulnerabilities that eventually lead to disruptions, managers should look at increasing both security (in order to reduce the

likelihood of disruptions) and resilience (building in capabilities for bouncing back just after stress is released) (Sheffi, 2005:12-14).

In his book, Sheffi refers to security improvement as a "process based on the creation of layered defenses, tracking and responding to near misses, increasing participation of all constituents in security efforts, and collaboration with government agencies, trading partners, and even competitors" (Sheffi, 2005:14). Similarly, when thinking in resilience, instead of being worried about underlying reasons for disruptions, a resilient focus should be on the most effective way to overcome an eventual damage to the system or organization in order to rebound quickly. This is the way to design and improve resilient systems. However a major challenge is to get a quantitative measurement of such a capability in order to improve decision making process as well as resources (equipment and security) allocation.

Environmental Issues

Although environmental issues are not intentional acts but unwanted consequences from main system operations, they should not be treated as accidental issues. However, growing concerns are arising toward even greater environment protection.

The energy industry has a huge environmental impact as a consequence of the sources used to produce electricity.

While the US transportation sector emits 20% of all the carbon dioxide, the generation of electricity emits 40% of all carbon dioxide for which the US is responsible. This presents an enormous challenge for the electric power industry in terms of global climate change (DoE, 2008:20).

Likewise, the United States accounts for only 4% of the world's population and produces 25% of its greenhouse gases (Figure 2).

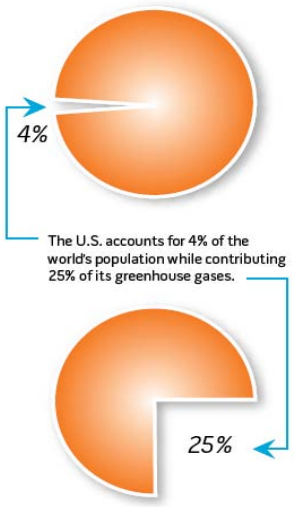


Figure 2. US Share of World Population Compared to its Production of Greenhouse Gases. (DoE, 2008:9)

Half of US's electricity is produced by burning coal, a rich domestic resource but a major contributor to global warming. Carbon footprint reduction requires that clean as well as renewable sources of energy like solar, wind and geothermal must be integrated into the nation's grid. However, without appropriate enabling technologies linking them to the grid, their potential will not be fully realized (DoE, 2008:9).

Figure 3 shows the carbon dioxide emissions by sector in the period 1990-2007. The electric power sector leads the emission ranking with an increasing trend. This explains why any solution DoD puts in place to mitigate its energy risks must comply with national laws, regulations and national policies on environmental performance, including greenhouse gas emissions (DoD, 2008:6).

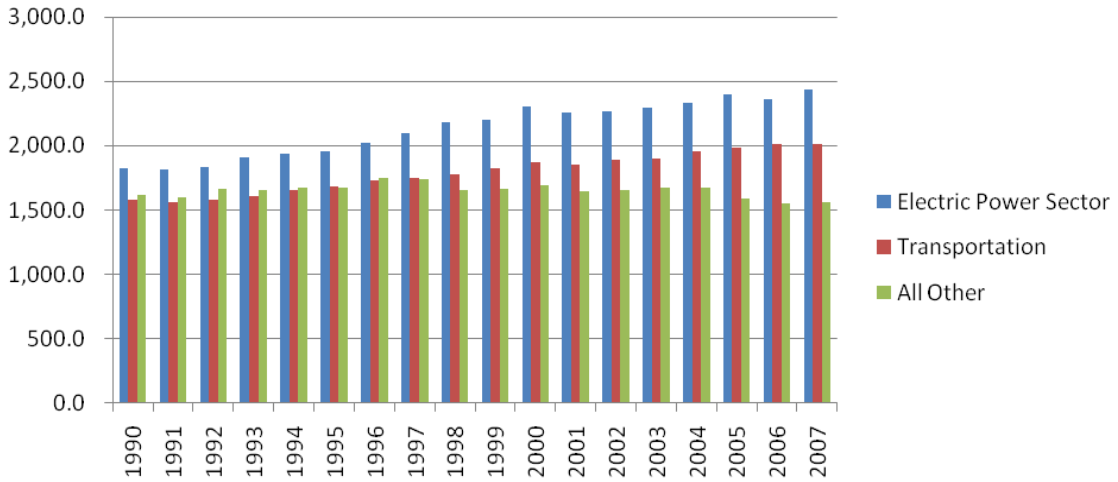


Figure 3. US Energy-related Carbon Dioxide. Emissions by Sector in Millions Metrics Tons; 1990-2007. (EIA, 2009)

Figure 4 shows the percentage of electricity generated by different sources. Coal, one of the most polluting sources of electricity production represents the major source for electricity production (48.5%).

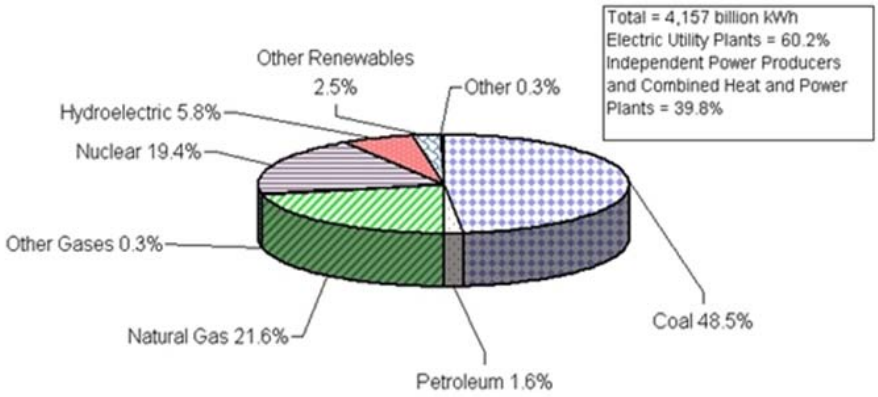


Figure 4. US Electric Power Industry Net Generation, 2007. (EIA; Report 2009)

Fiksel considers resilience as ability to resist disorder, what in turn become in the essence of sustainability. Likewise, for system design purposes he also considers that a product or service contributes to sustainability if it constrains environmental resource consumption and waste generation to an acceptable level (Fiksel, 2003:5330, 5332).

Consequently, resilience and environmental considerations are presented as fundamental components of sustainability in systems and organizations (Fiskel, 2003:5334). Therefore, further research can be conducted to identify correlation between resilience and environmental concerns as related to systems' survivability.

Smart Grids: Hope of the Future

The smart grid is a growing digital information network and modernized power generation, transmission and consumption system. Drawing upon lessons from the development of security best practices from the internet and telecom networks, smart grid technology tracks the thinking on how to best secure the emerging electricity networks of the future. In short, smart grid design is intended to deliver electricity from suppliers to consumers using digital technology to save energy and cost, as well as in a more reliable basis (Blochman, 2009).

DOE lists five fundamental technologies as drivers of the Smart Grids (DoE, 2008:24, 29):

1. Integrated communications, connecting components to open architecture for real-time information and control, allowing every part of the grid to both ‘talk’ and ‘listen’
2. Sensing and measurement technologies, to support faster and more accurate response such as remote monitoring and management
3. Advanced components, to apply the latest research in superconductivity and storage.
4. Advanced control methods to monitor essential components, enabling rapid diagnosis and precise solutions appropriate to any event.

5. Improved interfaces and decision support, to amplify human decision-making, transforming grid operators and managers quite literally into visionaries when it come to seeing into their systems

Additionally, smart grid deployment is considered as a key tool in addressing the challenges of climate change, ultimately and significantly reducing greenhouse gases. However, although the agendas of utilities and regulators are aligning and movement toward identifying and adopting Smart Grid standards, this is a still emerging technology that cannot cope with critical infrastructure's challenges in the short run. In fact, states such as Texas, California, Ohio, New Jersey, Illinois, New York and others are currently exploring ways to increase the use of tools and technologies toward the realization of a smarter grid (DoE, 2008:24, 28, 32).

Corollary of Power Grids Concerns

Statistics and forecasting processes represent a very important source for predicting natural disasters as well as human being accidents. However there is a need to develop a dynamic and smart approach to identify intentional attacks, in particular terrorist attacks that involve learning processes. This approach is needed due to the dynamic (smart) threats challenge the safety and secure status of power grids.

Supply chain intelligence describes the process of using knowledge generated and shared by partners in the supply chain. This concept, coined in the logistics field, constitutes a baseline to reach not only this strategic information sharing but also actual knowledge for strategic power grids management. The type of knowledge that can create supply chain resilience pertains to the identification of sources of risk and uncertainty at

each node and link in the supply chain. Supply chain knowledge can also be categorized as: Strategic, tactical and operational (Christopher and Peck, 2004: 9).

Similarly, environmental issues need to be considered when developing more reliable and sustainable solutions for energy development. Resilience and environmental protection was identified by Fiksel as key components for long term system survivability. This is why the energy industry and the US government have started to look at the resilience of such systems in the face of disruptive events.

However, since resilience is a concept used to identify behaviors as well as characteristics in different fields, theoretical research has been conducted in order to identify the most relevant characteristics or attributes of a resilient power grid as a particular case of supply chain.

The focus of this research is on quantitative assessment of resilience. Therefore, it is important to understand what this concept means when applied to power grids, what in turn will be the cornerstone for further performance improvements.

Defining Resilience

Resilience is defined as a desired characteristic for energy capabilities referenced by US government in several documents. However, specific concepts and attributes were not developed in order to be able to measure such desired performance in power grids. Expressions like "Increase energy security through strategic resilience" (DoD, 2008) and

> A number of steps are required to ensure more resilient electrical and logistics fuel systems support at Air Force installations: Energy must be included in Air Force Critical Infrastructure Program plans, studied during Vulnerability Assessments, exercised during base response activities, and, ultimately, incorporated into full-spectrum operational planning to fully observe and consider the potential deleterious effects. (USAF, 2008:11)

are considered not clear enough to operationalize such “resilience” throughout a quantifiable tool.

Resilience is understood as a system’s ability to absorb a significant negative change or stress and return to an acceptable performance after stress (Hoffman, 2008:37). Systems designed with the ability to adapt to changes under conditions of uncertainty are resilient and, in order to design those systems, a clear need to understand a system’s threats and potential consequences if those threats are consummate. This thesis looks at the concept of resilience and what it means for energy infrastructure performance, several approaches are presented in order to construct a more accurate concept for power grids.

Resilience means the ability to recover from (or to resist being affected by) some shock, or disturbance. However, this concept is currently used quite differently, according to the considered field.

A research focused on resilience assessment in internet networks defined resilience as the ability of the system to both absorb shock as well to recover rapidly from a disruption, so that it can return back to its original service delivery levels or close to it. In the same document, resilience is also presented as closely related to vulnerabilities that exist in the system and also the amount of adaptive capacity that the system has in the face of major shocks (Omer, 2009).

In their paper, authors recognize the necessity of being able to absorb damage but they also stress the importance of recovering capability. Besides, when they state “return back to its original service delivery levels or close to it”, they are aware of difficulties and limitations related to the recovering performance process.

Next, several approaches to resilience are presented, based on definitions in the website (Bookrags, 2009).

In physics and engineering, resilience is defined as "the property of a material to absorb energy when it is deformed elastically and then, upon unloading to have this energy recovered" (Keyofmetals. 2009). In other words, it is the maximum energy per volume that can be elastically stored. It is represented by the area under the curve in the elastic region in the Stress-Strain diagram. In Figure 5, resilience performances for two different materials are presented. In physics, larger areas represent higher resilient behavior.

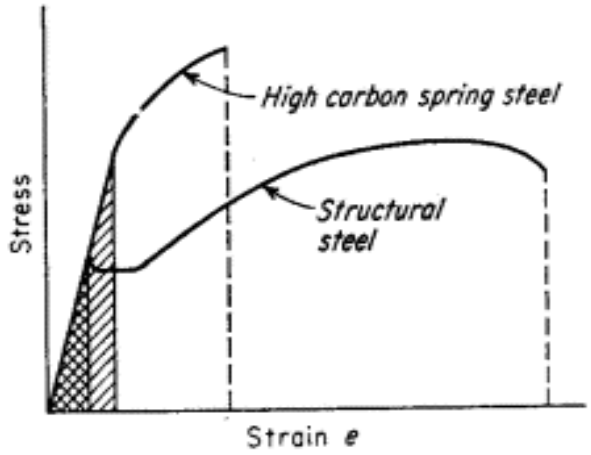


Figure 5. Stress-strain Diagram Showing Resilience Area in 2 Materials (Keyofmetals, 2009)

From Figure 5, it is possible to identify the larger area of resilience for the high carbon spring steel. This means that this material is able to absorb more energy (stress) than the structural steel without experimenting permanent deformations (consequences) after the stress releases. The distinctive characteristic in physics is that the material

(system) returns exactly to the original situation (position, performance) when it is stressed within the elastic field.

Another concept of relevance in this case is toughness. The toughness of a material is its ability to absorb energy in the plastic range (Jiles, 2008:13). In other words, it is the capability of absorbing energy or stress beyond the elastic range. In this case, the material (system) will return to a new equilibrium after the stress is released. The ability to withstand occasional stresses above the yield stress without fracturing is particularly desirable in critical systems where a collapse would be catastrophic. This approach recognizes the physical limitations that every system has in terms of resistance. One way of looking at toughness is to consider that it is the total area under the stress-strain curve, including elastic and plastic deformation as well. This area is an indication of the amount of work per unit volume, which can be done on the material (system) without causing it to rupture. Another important concept is the yield strength which is, by convention, the stress at which the residual plastic (permanent) deformation is 0.2% (Jiles, 2008:14-16, 99).

In Figure 6, the particular case of brittle materials is presented, where all deformation (strain) occurs in the elastic range. Consequently, if the system (material) is stressed beyond the elastic limit, there will be not plastic deformation but ultimate strength of the material is reached and system collapse is immediate. There is not an alternate equilibrium different than the original. This behavior is shown by brittle materials, and represents specific materials like carbon fiber. This can be considered as a very robust material but it is not capable to find different equilibrium points after being stressed (Invsee, 2009).

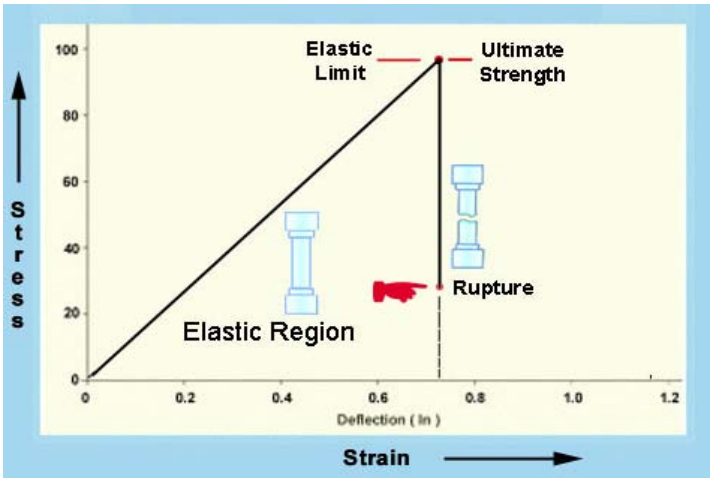


Figure 6. Stress-Strain Curve for Brittle Materials (Invsee, 2009)

Four relevant concepts need to be mentioned at this point. First, in mechanics, resilience refers to the property of a material to absorb energy when it is deformed elastically and then, upon unloading to have this energy recovered. In other words, it is the maximum energy per unit volume that can be elastically stored. If the material is stresses beyond its elastic limit (0.2% of permanent deformation), the area under the curve will include not only the energy from elastic range (resilience) but also the energy related to permanent (plastic) deformation (beyond the 0.2% deformation). This means that the material (system) will reach a new equilibrium (within the plastic field) after the stress is released. In this case the stress exceeds the actual resilient capacity, higher amount of energy is absorbed by the material and, after the stress is released, the material (system) returns to a new and different equilibrium. Second, when analyzing resilient behavior in materials, the time to recover is not considered as resilience's component. Third, physics systems do not collapse by working within the elastic field (resilient field), but collapse occurs by cumulating enough cycles (fatigue). Finally, materials are able to

absorb more energy than that related exclusively to resilient disturbance, but a new equilibrium is reached (Hertzberg, 1996:16-33).

On the other hand, in networked systems, resilience has been defined as the ability to provide and maintain an acceptable level of service that is, not necessarily optimal or normal, in the face of various faults and challenges to normal operation. Resilient networks aim to provide acceptable service to applications (CISCO, 2008). This definition fails to explain what does acceptable level or acceptable service means either in terms of performance or recovery capability. In industrial and organizational safety, the term resilience has come into use to emphasize that safety must be proactive as well as reactive. However conventional risk management approaches are based on hindsight and emphasize error tabulation and calculation of failure probabilities. Resilience engineering looks for ways to enhance the ability of systems to enable processes that are robust yet flexible, to monitor and revise risk models, and to use resources proactively in the face of disruptions or ongoing production and economic pressures. Resilience engineering failures do not stand for a breakdown or malfunctioning of normal system functions, but rather represent the adaptations necessary to cope with the real world complexity.

Nancy Levenson criticizes the frequent resilience definition, “ability to continue operations or recover a stable state after a major mishap or event”, considering that it focuses on the reactive nature of resilience. Then, she presents a more proper definition: “resilience is the ability of systems to prevent or adapt to changing conditions in order to maintain (control over) a system property” (Wood, 2008:95). Although this definition is better in that it considers resilience as a proactive behavior (preventing and adapting to

events), it does not mention the importance about the time to recover which represents a major challenge for critical infrastructures.

Ulieru also stresses the importance of being proactive rather reactive based on the volatility of today's socio-economic and political dynamics that renders obsolete the practice of "post-attack" approaches to critical supply network security (Ulieru, 2007). The same critical factors are considered to be essential not only for sustainability of organizations but also for resilient performance.

In ecology, resilience means the capacity of an ecosystem to tolerate disturbance without collapsing into a qualitatively different state that is controlled by a different set of processes. A resilient ecosystem can withstand shocks and rebuild itself when necessary (Bookrags, 2009).

Resilience in social systems has the added capacity of humans to anticipate and plan for the future. Resilience is identified in human and ecological systems as an adaptive capacity. In this definition the adaptive capacity challenges the traditional concept of resilience. Such adaptive capacity is a way to express the idea of learning and growing as defined by Fiksel in his work: "Resilience is defined as the capacity of a system to survive, adapt and grow in the face of change and uncertainty" (Fiksel, 2006).

Resilience was also defined as a productive tension between stability and change. So, the notion of adaptation to requirements of the operational environment implies the capacity to adapt and change in order to survive in a changing environment. However, understanding processes of adaptation and change is considered not an easy job but a challenge (Hollnagel and others, 2008:179).

In psychology resilience (or "psychological resilience") is a term that refers to an ability to cope with adversity. Whether outcomes are successful or not is determined by the presence (and balance) of both, risk factors and protective factors over time. This defines the term “risk”, as a way of quantifying the stress, and the capacity to withstand such risks- protective factors. (Bookrags, 2009)

On the other hand, resilience applied to the critical infrastructure is the ability to avoid, minimize, withstand, and recover from the effects of adversity, whether natural or manmade, under all circumstances of use. Likewise, resilience applied to the nation’s critical infrastructure is reliability under stress and spans high availability, continuous operations, and disaster recovery (Bookrags, 2009). This concept, gives precise capabilities related to resilient behavior. However, there is no reference to the time to recover from the effects of adversity.

A similar situation was found in Christopher and Peck definition of resilience: “ability of a system to return to its original state or move to a new, more desirable state after being disturbed” (Christopher and Peck, 2004:2). However this definition highlights the implication of the notion of flexibility; and given that the desired state may be different from the original, “adaptability” also earns a place in such definition. A final term to deal with is presented as the most problematic challenge: the risk defined as the “variation in the distribution of possible outcomes, their likelihoods and their subjective values”. Finally, these authors conclude that formalized procedures for supply chain risk management within and between organizations are needed (Christopher and Peck, 2004).

On the other hand, the document Critical Thinking: Moving from Infrastructure Protection to Infrastructure Resilience states that a difference is made between protection

and resilience (George Mason University, 2007: 90). Unlike protection, resilience is not a specific, easily definable term across all infrastructures, nor is it easily measurable. Commonly defined as the ability of a system to recover from adversity, either back to its original state or an adjusted state based on new requirements, building resilience requires a long-term effort involving reengineering fundamental processes, both technical and social. Protection is defined as follows:

> Protection includes 'protective measures', which refer to actions, procedures, or physical impediments used to mitigate vulnerabilities, minimize consequence, and reduce risk. Simply put, protective measures are implemented to defend against harm to property, personnel, or mission execution. Examples of protective measures include, but are certainly not limited to: surveillance cameras, security patrols and response capabilities, fencing, employee and visitor credentialing, and intrusion detection systems. (George Mason University, 2007: 7)

This concept is consistent with security concerns, so infrastructure protection refers to its security.

This same document presents a multidiscipline view of resilience:

> Resilience focuses on the functions that a system is designed to fulfill—clearing financial transactions, managing airspace, controlling power grids—not the individual components of the system or network. *Physics and engineering* disciplines define resilience as a physical property of materials: the capacity of a material to absorb energy when it is deformed elastically, and then upon unloading, return this energy. *Ecologists* have a more complex view of resilience in natural systems, and thus two completing definitions have emerged, each emphasizing a different aspect of resilience. Other view of resilience, specifically *ecological resilience*, focuses on state changes in complex systems: resilience is measured by the magnitude of disturbance that can be absorbed before the system changes its structure by changing the variables and processes that control behavior within the system. From a human perspective, resilience can be thought of as how well an organization can absorb unexpected challenges. (George Mason University, 2007:90)

On the other hand, Fiksel's research found that neither, protection nor profitability ensures long-term survival of any organization. In his research, resilience has been

correlated to a firm's survivability. His work found what drives corporate longevity (Fiksel, 2003:5332):

1. Sensitivity and adaptability to the business environment.
2. Cohesion and sense of identity.
3. Tolerance of diversity (decentralization).
4. Conservative use of capital.

From this study emerged the notion that the real purpose of a corporation is to learn, grow, and survive in the long run and that a corporation is best understood as a living organism. He also argues that perhaps, the essence of sustainability is resilience what in turn is a function of diversity, efficiency, adaptability, cohesion and simplicity (Fiksel, 2003:5332).

Another study addressed by Hollnagel, presents several characteristics as indicating lack of resilience in organizations:

1. Defense erosion under production pressure (organizational stress).
2. Past good performance is taken as a reason for future confidence about risk control.
3. Fragmented problem-solving clouds the big picture.
4. Failure to revise risk assessments as new evidence accumulates.
5. Lack of communication.
6. The organization cannot respond flexibly to changing demands or unexpected situations.
7. Lack of redundancy.
8. There is not "enough" devotion to safety alongside other system goals.

In their document, Hollnagel et al states the close relationship between resilience and safety as a clue to be considered in order to improve organization performance (Hollnagel and others, 2008:136-137).

Bush and Grayson of the National Infrastructure Advisory Council (NIAC) lead the Critical Infrastructure Resilience Study Working Group. They defined infrastructure resilience as the "ability to reduce the magnitude and/or duration of disruptive events. It is the ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event" (Bush & Grayson, 2009:3). They also highlighted three key features:

1. Robustness: Ability to maintain critical operations and functions in the face of crisis.
2. Resourcefulness: Ability to prepare for, respond to, and manage a crisis or disruption as it unfolds.
3. Rapid recovery: Ability to return to and/or reconstitute normal operations as quickly and efficiently as possible after a disruption

Another approach to resilience conceptualization can be found in the document *Complex Infrastructure Systems Resilience and Sustainability* as an "inherent ability of a system to sustain or rapidly recover its core value delivery in the face of change." System resilience is presented as a function of a system's vulnerabilities and its adaptive capacity (SSE, 2009).

How vulnerable a system is depends on its organizational and physical infrastructure as well as the risk culture governing its management and design. The adaptive capacity depends heavily on the organizational infrastructure and the physical infrastructures, but it can also depend on the degree of proactive or reactive focus on risk

management practices. Adaptive capacity is presented as the capacity to apply existing responses to problems or to generate and apply innovative responses to new problems. Consequently, we can synthesize these concepts as two major strategies to improve resilience:

1. Reducing system vulnerabilities.
2. Increasing system's adaptive capacity.

The Multidisciplinary Center for Earthquake Engineering Research (MCEER) has introduced the disaster resilience concept as the ability of social units to mitigate hazards, contain the effects of disasters when they occur and carry out recover activities in ways that minimize social disruption, and mitigate the effects of future disasters" (Hoffman, 2008:41). Consequently, resilient systems reduce the probabilities of failure, the effects of failures and the time to recovery.

Likewise, resilience can be measured by the functionality of the system after a disruptive event, and the time it takes to return to normal operation. Four common attributes of disaster resilience are defined by MCEER (Hoffman, 2008):

1. Robustness: ability of a system to withstand a disruptive event without significant loss of functionality or performance.
2. Redundancy: the extent to which other systems can replace functionality or performance of another system without significant loss of functionality or performance.
3. Resourcefulness: the ability to identify and prioritize problems and to initiate solutions.

4. Rapidity: the ability to restore functionality or performance in a timely manner, while avoiding disruptions.

MCEER also presented the characteristics related to resilience that make it more tangible and measurable (Hoffman, 2008:8). Specifically, disaster resilience is characterized by:

1. Reduced failure probabilities (i.e., the reduced likelihood of damage & failures to critical infrastructure, systems and components).
2. Reduced consequences from failures (in terms of injuries, lives lost, damage and negative economic and social impacts).
3. Reduced time to recovery (the time required to restore a specific system or set of systems to normal or pre-disaster level of functionality).

These three characteristics together balance the actual resilient behavior. It is important to point out that the time to recover is specifically mentioned as integral component of resilience (Hoffman, 2008:8).

Sheffi proposes redundancy as an alternative to improve resilience, where the basic form of redundancy used in business is safety stock. In the same way, instead of using inventory for redundancy, author states that some enterprises use redundant capacity for mission-critical business units. However, he also recognizes that high levels of redundancy may be too expensive (Sheffi, 2005:171-180).

Bruneau and Tierney have found in their research, that there is a consistent cross-disciplinary treatment in which resilience was viewed as both, inherent strength and the ability to be flexible and adaptable after environmental shocks and disruptive events. This finding matches with the concept of robustness and flexibility as two characteristics

of a resilient system (Bruenau and Tierney, 2007:1). Their work is based on MCEER's Resilience Framework, and attributes and determinants of resilience are presented: Robustness, redundancy, resourcefulness and rapidity (Bruenau and Tierney, 2007:2).

Fiksel refers to the concept of "resilience" as borrowed from the field of ecology that enables sustainability to be viewed as an inherent system property rather than an abstract goal. By the laws of thermodynamics, closed systems will gradually decay from order into chaos, tending toward maximum entropy. However, living systems are "open" in the sense that they continually draw upon external sources of energy and maintain a stable state of low entropy that is far from thermodynamic equilibrium. Fiksel concludes that the essence of sustainability is resilience, the ability to resist disorder (Fiksel, 2003:5332).

Figure 7 provides a simplified illustration of thermodynamic changes that characterize different types of behaviors.

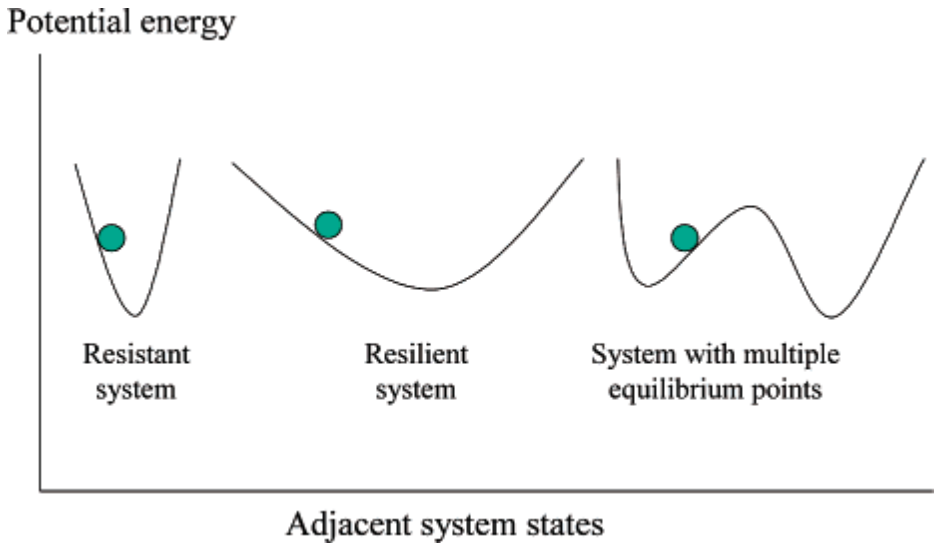


Figure 7. Examples of System Behavior. (Fiskel, 2003:5332)

.

Resistant systems are typical of engineered, highly controlled systems. They operate within a narrow band of possible states and are designed to resist perturbations from its equilibrium state. It recovers rapidly from small perturbations, but they may not survive a large perturbation.

Resilient systems are also typical of social and ecological systems. They can function across a broad spectrum of possible states and gradually tends to return to its equilibrium state. However, through adaptation and evolution, they are capable of surviving large perturbations.

Finally, systems with multiple equilibrium points can tolerate larger perturbations. Under certain conditions they may shift to a different equilibrium state, representing a fundamental change in its structure and/or function.

According to Fiksel, it is possible to identify similarities between each explanation and interpretation of resilient behaviors and the aforementioned concepts regarding physical and engineering systems. Brittle behavior is found where systems are able to absorb energy but is not able to move to a new equilibrium after stress has released. This is a robust or resistant behavior. The major power grid failure that struck the northeastern United States in the summer of 2003 is a relevant real world example of the brittleness dilemma. It was found that while several university teams that analyzed the disaster disputed some technical issues, they all gravitated toward the same broad policy lessons: That the sheer scale and complexity of modern power grids makes periodic, disastrous failures inevitable. Moreover, the measures typically embraced following a major blackout to protect the system from a repeat of the disaster, tend to make future blackouts bigger and more likely. (George Mason University, 2007)

This concept also matches to the human organizations that are learning systems with the capability of survive by reaching new equilibriums different than the previous one.

Robustness, a term developed in engineering, refers to the maintenance of system performance either when subjected to external, unpredictable perturbations, or when there is uncertainty about the values of internal design parameters. Resilient designs often involve a trade-off between maximum system performance and robustness. A robust system will typically not perform as efficiently with respect to a chosen set of criteria as its non-robust counterpart (Anderies, 2004). In the same document, Anderies states that the robust system's performance will not drop off as rapidly as its non-robust counterpart when confronted with external disturbance or internal stresses.

This concept seems to be consistent with most of the literature related to system's performances, where robust systems can absorb a huge amount of energy (stress, damage). However, issues arise when the maximum capacity is exceeded and the system collapses. Although more stress can be absorbed, the equilibrium is quite instable. Meanwhile, resilience leads to a more stable equilibrium by learning before, during and after stresses or disruptions.

Jan Husdal recognizes that Supply Chain Risk Management (SCRM) has been linked to robustness, flexibility, agility and resilience in such a way, that these concepts are often confused (Husdal, 2004:3). This author has published several articles which show an evolution in completeness in defining resilience, robustness and flexibility.

Figure 8 shows the basic difference proposed by Husdal, between robust and flexible behavior. Robustness means the ability to stay on course and to accommodate

unforeseen contingent events. Flexibility means the ability to accommodate unforeseen external events by changing tracks and being open to deviate from the initial course. In practice, no strategy should be built on pure robustness or pure flexibility, but should be a merger of both.

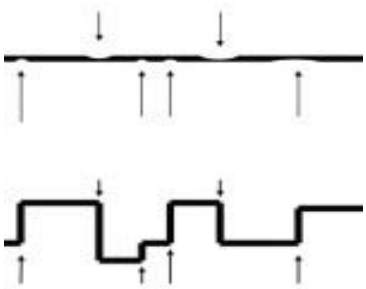


Figure 8. Difference between Robustness (above) and Flexibility (below). (Husdal, 2004)

Robustness (above) means the ability to stay on course and to accommodate unforeseen external events (indicated by arrows). Flexibility (below) means the ability to accommodate unforeseen external events by changing tracks while being open to deviate from the initial course (Husdal, 2004). The same author later brings several definitions in order to reach better understanding about Supply Chain Risk Management. He presents his own definition with a graph. The difference between robustness, flexibility, agility and resilience is illustrated in the Figure 9, taken from Husdal (2009). Note that there is a distinct notion of different severity in each of these definitions. The ability to survive (resilience) is presented as being more important (in a business setting) than the ability to quickly regain stability (robustness) or the ability to change course (flexibility or agility) (Husdal, 2009).

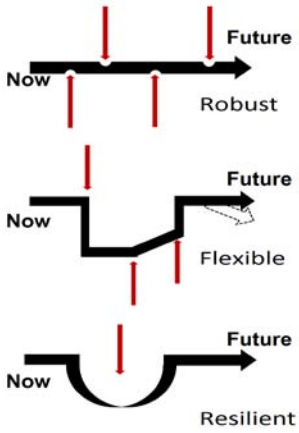


Figure 9. Robust, Flexible or Agile and Resilient Behaviors. (Husdal, 2009)

Resilient behavior differs from flexible or agile in that a resilient system regains the desired path (e.g. performance level) after deviation, while a flexible system does not ensure the follow up behavior (performance) after unforeseen external events (disruptions).

On the other hand, an important distinction between flexibility and redundancy is presented by Rice and Caniato when they present redundancy as involving capacity that may or may not be used. This additional (redundant) capacity would be used to replace the lost capacity caused by a disruption. Flexibility, on the other hand, would entail redeploying the remaining previously committed capacity (Rice and Caniato, 2008). Such issues would explain the difference between flexible and resilient behavior presented by Jan Husdal (Figure 9**)**.

In addition, Fiksel's definition of resilience is presented: 'capacity of a system to survive, adapt and grow in the face of change and uncertainty." Fiksel considers that systems evolve through cycles of growth, accumulation, crisis and renewal, and even self-organize into new, more desirable configurations. Consequently systems under such

circumstances are capable of learning in order to survive by reaching more desirable equilibriums (Pettit, 2008:21).

Hamel and Välikangas state that "any company that can make sense of its environment, generate strategic options, and realign its resources faster than its rivals will enjoy a decisive advantage (Hamel and Välikangas, 2003:12). This is considered a clear reference not only to recovery capability and resourcefulness but also the environment awareness capability.

On other hand, Cook and Woods highlight the importance of learning capability as a critical component of resilience. Resilient systems (or organizations) should be able to learn from events like "near miss" incidents and accidents. This is because such events provide information about the resilience or brittleness of the system in the face of disruptions (Hollnagel and others, 2008:342). Consequently, a resilient organization must, not only be able to change from one state to a more appropriate when stressed (flexibility), but also it should be able to return to normal functioning when such unusual conditions are over. However, normal position does not mean to go back to the same conditions before events, since the world may have changed (Hollnagel and others, 2008:344). From the latest concepts, it is possible to construct a more encompassing and complete understanding of resilient behavior. To do so, we propose to merge the normal functioning conditions proposed by Hollnagel and the system with multiple equilibrium points presented by Fiksel (Figure 7) with the additional requisite that the potential multiple equilibrium points met the desirable performance (output, service, etc) levels.

However, although a more complete conceptualization of resilient performance has been presented, based on Fiksel and Hollnagel's works, there is a missing attribute

that has not been mentioned: time to recover as a critical component of resilient organizations.

On the other hand, Cook and Nemeth define resilience as a "feature of some systems that allows them to respond to sudden, unanticipated demands for performance and then to return to their normal operation condition quickly and with a minimum decrement in their performances" (Hollnagel and others, 2008: 205). In this case there is an explicit reference to the timely recovering after stress, but this definition fails in that the authors consider only "unanticipated demands" as stressors, and forget actual threats to the entire network like natural disasters and sabotages. They also propose that resilient performance is evidence of resilient systems: "Although systems can be resilient we can fail in detecting such resilience just from the direct observation because resilient performances occur in the face of sudden, unanticipated challenges." They conclude that "the only strong evidence of resilience that we can identify is the presence of such resilient performances" (Hollnagel and others, 2008: 216). So, the question is how do we identify resilience performance? For this goal, scenario analysis seems to be a useful tool.

Cooks and Woods state that a critical component of a high resilience in organizations is continuous learning from events, incidents and accidents, so incidents as well as failures provide information about the resilience or brittleness of the system in the face of various disruptions (Hollnagel and others, 2008: 329). These concepts together bring about the resilience assessment needed in the strategic management environment.

Meanwhile, Homeland Security Advisory Council, states that Critical Infrastructure Resilience (CIR) is not a replacement for Critical Infrastructure Protection

(CIP), but rather an integrating objective designed to foster systems-level investment strategies. CIR as a goal is considered as a readily quantifiable objective, identifying the time required to restore full functionality (CITF, 2006). For that, enough background is needed regarding recovery capability in order to be embedded into a resilient model. Once a probability distribution has been identified (goodness of fit), based on actual recovery performance, it will be possible to identify the optimal time to recover for a given level of probability, if a quantitative assessment tool is available.

Hoffman and Nilchiani define Resilience as an "inherent ability of a system to absorb a significant negative change and then to return to an acceptable state". Resilience is presented in their work as a function of a system's vulnerabilities and its ability to adapt. At the same time, "acceptable state" does not mean to return exactly to the same previous equilibrium, but one compatible with the expected performance (Hoffman, 2008:7).

The Role of Quality Management in Improving Resilience

In order to be resilient, operational systems have to be capable of change, but what is the origin of that change? Nick Mc Donald states that quality as well as safety management are about maintaining stability, and since stability has to balance the change in a resilient environment, a standard performance is assured in the long run (Wooden, 2008:179).

Thomas Foster, specialist in Quality Management, stated that "one major objective of Quality Management is to enhance organizational learning." At the same time his experience has shown that organizational learning is not only about training but the sum of the change in knowledge within the system or organization (Foster, 2001).

On the other hand, Bruenau and Tierney as well as MCEER's Resilience Framework present resilience as a function of quality over the time. However, although we consider that quality is not enough to completely define resilient behavior; certainly it is a critical component for resilient systems.

The traditional way of ensuring quality in many organizations has been through direct inspection (vertical dimension). However, outstanding performances are achieved "horizontally" (cross-functional). Therefore, cross-functionality is not only a quality management characteristic but also a supply chain management characteristic, which is implemented throughout processes.

We typically think of process in the context of production: the collection of activities and operations involved in transforming inputs, which are the physical facilities, materials, capital equipment, people and energy, into outputs, or the products and services. A process perspective links all necessary activities together and increases one's understanding of the entire system, rather than focusing on only a small part (Evans and Lindsays, 2001).

Continuous Improvement

This expression refers to both incremental improvements that are small and gradual and breakthrough, or large and rapid, improvement. Improvements may take one of several forms:

1. Enhancing value.
2. Reducing errors, defects, waste, and their related costs.
3. Increasing productivity and effectiveness.
4. Improving responsiveness and cycle time performance for processes.

Major improvements may require significant simplification of work processes and often drive simultaneous improvement in system's performances. A process-focus supports continuous improvements efforts by helping to understand synergies within the systems and potential problems sources. This is a holistic consideration about networked systems, like supply chain management or power grids, where attributes composition improves outcomes.

The process-focus as seen from quality standpoint (Figure 10) has three main components linked as a chain: Supplier – Organization – Customer. This chain is reproduced also at any level within the organization and can be represented as follows:

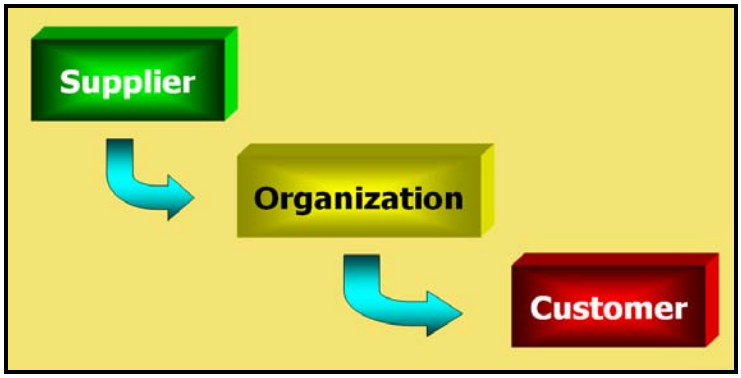


Figure 10. Quality Process (ISO 9001:2008)

This process shares the main characteristics with the supply chain, which is represented as follows in Figure 11.

Figure 11. Supply Chain Process

Christopher and Peck refer explicitly to such process in their categorization of risk. They state that there are three categories of risk that can be further subdivided to produce a total of five categories; one of them is the *process* defined as the "sequence of value adding and managerial activities undertaken by the firm" (Chistopher and Peck, 2004).

On the other hand, real improvement depends on learning that is understanding why changes are successful through feedback between practices and results, which leads to new goals and approaches (Evans and Lindsays, 2001:20).

A learning cycle, as presented by Evans and Lindsays, has four stages:

1. Planning
2. Execution of plans.
3. Assessing of progress
4. Revision of plans based upon assessment findings.

These stages are represented in the "Deming cycle" (Figure 12), what is a simple methodology for improvement. It was originally called Shewchart cycle after its founder, Walter Shewhart, but it was renamed the Deming cycle by the Japanese in 1950. The Figure 12 shows such cycle, which is basically based on learning (Evans and Lindsay, 2001:90-91):

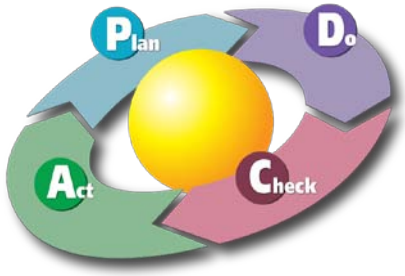


Figure 12. Deming Cycle (PDCA). (Evans and Lindsay, 2001:90-91)

PLAN. Establish the objectives and processes necessary to deliver results in accordance with the expected output. By making the expected output the focus, it differs from other techniques in that the completeness and accuracy of the specification is also part of the improvement.

DO. Implement the new processes. Often on a small scale if possible.

CHECK. Measure the new processes and compare the results against the expected results to ascertain any differences.

ACT. Analyze the differences to determine their cause. Each will be part of either one or more of the P-D-C-A steps. Determine where to apply changes that will include improvement. When a pass through these four steps does not result in the need to improve, refine the scope to which PDCA is applied until there is a plan that involves improvement.

Deming cycle is based on the premise that improvement comes from the application of knowledge. This knowledge may be related to engineering, management or how process operates.

Based on this cycle, the present work focuses on the third stage (Check) as a critical step to learn and then be able to grow as resilient system. This work highlights two major characteristics:

1. Learning process requires performance feedback in order to identify deviations from goals and implement improvements.
2. Management requires measures (assessment) that guide to decision making in order to reach goals.

Additionally, resilience is commonly embedded in processes, rather than individual physical assets (the main focus of protective measures and robustness) explicitly addressed in homeland security strategic plans, infrastructure protection programs, and the like. As an important long-term concept for homeland security, resilience should not be blurred to such a degree that its development and importance becomes diluted. Rather, in an effort to reach the larger objective of building full confidence in the security of resilient processes in general and infrastructure in particular, resilience needs to be studied further as a standalone concept (Critical Thinking, 2007:2).

The Department of Homeland Security states the need for resilient critical infrastructures as: "Any interruptions or manipulations of these critical functions must be brief, infrequent, manageable, geographically isolated and minimally detrimental to the welfare of the United States" (CITF, 2006:7). This DHS's requirement is the same as the included in the Presidential Decision Directive/NSC-63 (1998).

On the other hand, the US Government Accountability Office (GAO), in its Report to Congressional Committees (GAO, 2009:39), has recommended an executive action to develop a mechanism to systematically track the implementation of future Defense Critical Infrastructure Program (DCIP) risk management decisions and responses intended to address electrical power–related risks and vulnerabilities to DoD's most critical assets. This recommendation fits with the Continuous Improvement Process developed by Deming, where organizations work toward excellence by the following sequence: Plan- Do- Check- Act (PDCA process). Consequently, the third step is "Check" that is evaluating the actual performance in order to give a feedback that leads to

the improvements (Act). Continuous PDCA is adaption and hence, continuous adaption (improvement) will create resilience.

In the same way, such recommendation included that the DoD develop a mechanism to systematically track the implementation of future risk management decisions and responses intended to address electrical power–related risks and vulnerabilities to DoD's most critical assets.

Finally, GAO encourages DoD to provide explicit guidance on tracking the implementation of DCIP risk management decisions and responses resulting from DCIP vulnerability assessments of DoD's most critical assets.

Consequently within this framework, this thesis aims to develop an instrument as a way to assess how power networks are performing in terms of resilience as a way to enable strategic decisions toward resilient behavior and long term success.

In the document *Towards a Decision Engine for Self-remediating Resilient Networks*, Schafer presents the importance and difficulty of selecting from a set of available remediation mechanisms, a suitable subset that can be used to form an effective response to address a challenge in resilient networks. Here, he focuses on a decision engine with four main entities that are considered as necessary to effectively deduce an appropriate remediation strategy: monitoring & diagnosing, decision engine, learning & knowledge and reconfiguration & measurement. Figure 13 shows the diagram with such "entities". From the four main entities, two of them are directly related to measurement (or monitoring). This shows the importance and the need of developing a reliable tool to conduct such assessment. This is the third step in the Deming cycle: "check" (Schafer and others, 2007).

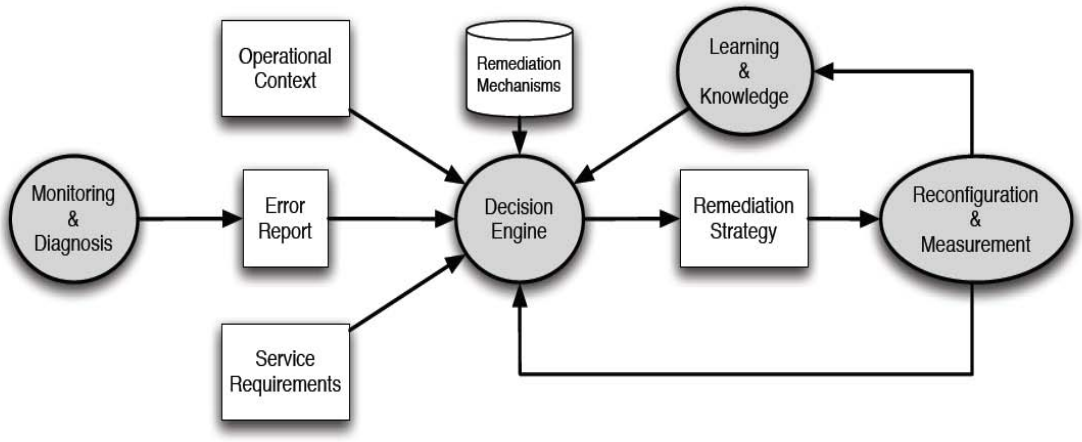


Figure 13. Entities in a Self-remediating Resilient Network. (Schafer & others, 2009)

Likewise, the United States Air Force Infrastructure Energy Strategic Plan presents the following figure as a way to explain how strategic goals are supported by four main columns: improve current infrastructure, improve future infrastructure, expand renewable, and manage costs. The cornerstone that supports this challenge includes decision management that needs effective data as well as performance measurement (Figure 14).

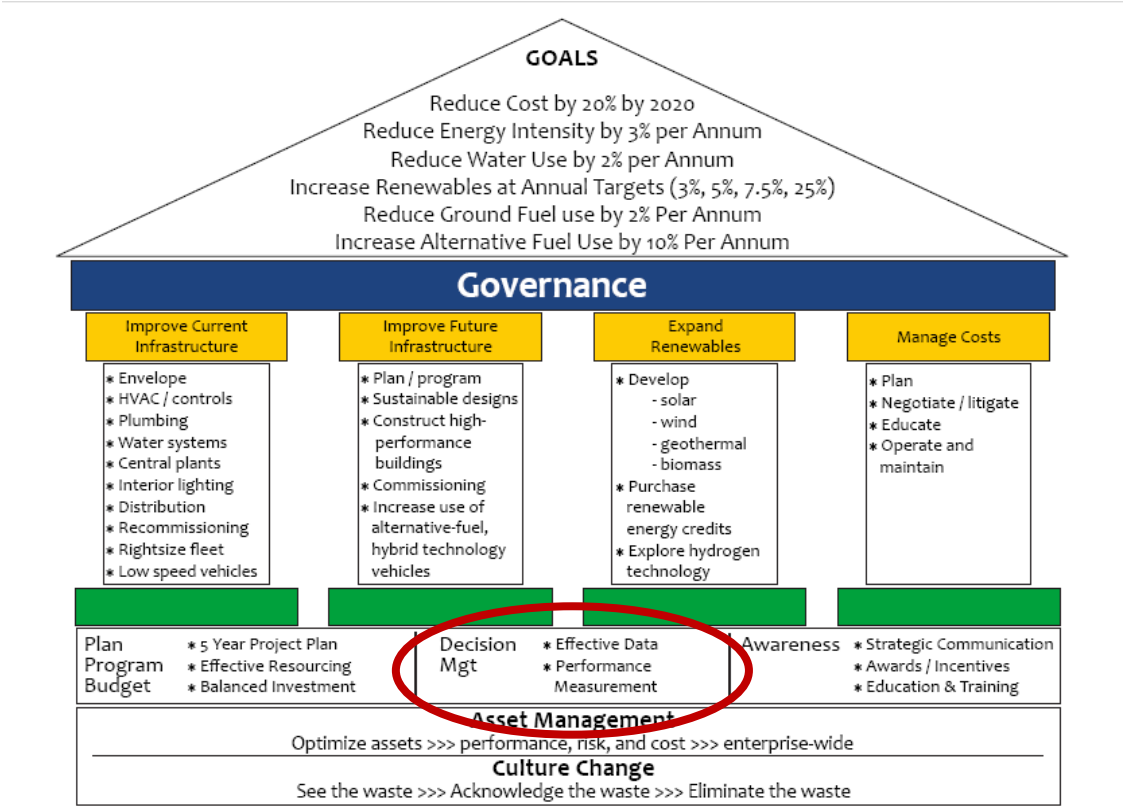


Figure 14. Pillars of the Infrastructure Energy Strategic Plan. (USAF, 2008)

Resilience Measurement

Is There a Uniform Measure of Resilience?

Some authors state that there cannot be uniform measures or expectations of resilience because levels of resilience are a direct result of investment and business decisions made by organizations that are consistent with their individual constraints and interests. Two similar organizations or systems can meet their organization's goals through resilience and different objectives. By analogy, a small sailboat is not as resilient in a heavy storm as is a battleship, but if the intent and need is to sail on the lake on

sunny days, the sailboat meets resilience expectations (George Mason University, 2007). This lets systems to be effective while saving resources, what in turn improve survivability.

On the other hand, it is impossible to prevent natural forces from affecting power lines. So, when disruptions happen, the real test of any network's resilience is how quickly and intelligently it can handle such disruptions. Think, for example, of the internet's ability to re-route packets of data swiftly and efficiently when a network link fails (The Economist, 2004).

Bruenau and Tierney present a resilience measurement approach when they state that resilience can be measured by the functionality or quality of an infrastructure system after a disaster and also by the time it takes for a system to return to pre-disaster levels of performance (Figure 15). They differentiate functionality from quality. The question is what functionality means and how it can be quantified? The same questions can be addressed for quality (Bruenau and Tierney, 2007).

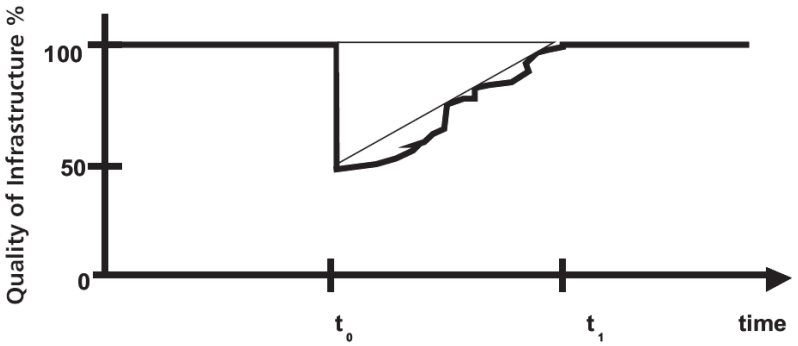


Figure 15. The Resilience Triangle. (Bruneau and Tierney, 2007)

At this point, there still are difficulties in defining resilient performance in such a way that it can be quantitatively assessed.

Since there is no unique way to measure resilience across different kind of systems and organizations, different approaches toward resilience assessment are addressed in order to look for common patterns or attributes that can be quantified in supply chain networks (SCN). Once identified, they will be used in a particular SCN, the power grids.

Resilience Measurement: Different Approaches

One approach to resilience assessment is given by Cook and Nemeth. They conclude that "resilient performance is empirical evidence of resilience" (Hollnagel and others, 2008:220). The question now is what does it define a resilient performance? Answering this question is the first step toward resilience assessment.

Although resilience concepts were broadly presented in this chapter, several approaches to resilience definition in networked structures are presented. The challenge is to identify those attributes that if measured will give a quantitative estimation about system's resilience.

Benchmarking for Home Gateways

Ramanathan and Lac (2009) have conducted a resilience research in Home Gateways (HG) which connect residential network with services like internet and VoIP access. They proposed that HG's sensitivity to faults and the increasing failure challenges are often perceived by users, giving rise to a lack of trustworthiness in the HG. In order to tackle this kind of problems, an improvement of HG's resilience was proposed. To do so, they conducted an assessment of the dependability and security of the manufacturer's prototypes through benchmark. They analyzed the effective metrics

for measuring and assessing the various HG responses under different situations with respect to the resilience properties (Ramanathan and Lac, 2009).

Table 2 shows their proposed synopsis of HG resilience with two main components: Dependability and Security, with dependability as a function of: availability, reliability, safety, interoperability and maintainability.

Table 2. Resilience Metrics in Communication. (Ramanathan and Lac, 2009)

Availability/Reliability metrics	**Security metrics**
Failure rate: Number of failures reported during a period of time.	*Login procedure:* Authorized users authenticated by the HG.
Boundary violation: Application not performing as desired, e.g., results falling outside the specified window.	*Data protection:* Personal documents to be kept safe (confidentiality, integrity).
Readiness: Likelihood that an application is available for use.	*Secure communication:* Messages reaching the correct destination and kept secret (if necessary).
MTBF: Average amount of time the HG operates between failures.	*Rights management:* Access to local resources determined by local security policies.

They define the units for each resilience property, thus resulting in a performance evaluation. Some examples are the following:

1. Outage time: how long a service has been unavailable,
2. Average number of call attempts: how many times, on average, a user must call to establish a connection,
3. Dropped calls: number of times a call is dropped in the midst of a conversation,
4. Audio delay: once a call is established, the average lags between utterances.

Results are displayed in Figure 16. Different components of resilient performance are compared between prototypes (models).

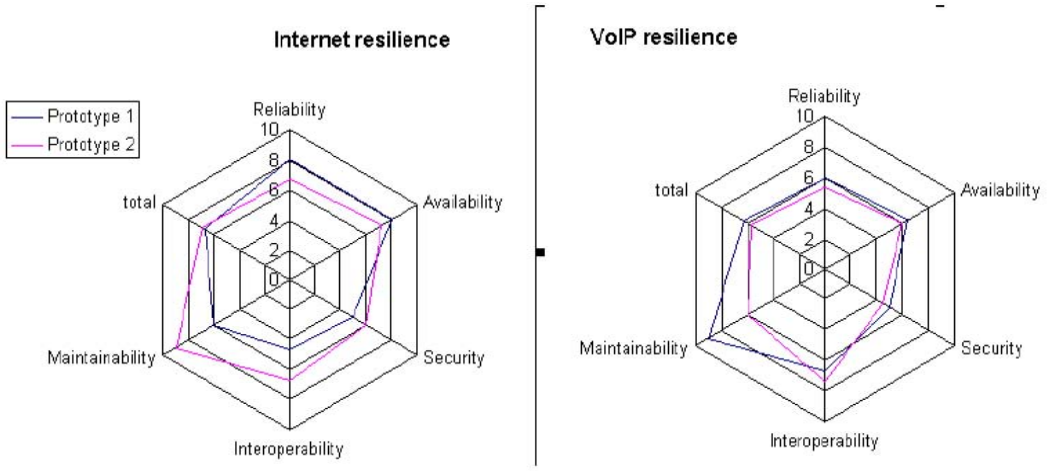


Figure 16. Resilience Benchmarking. (Ramanathan and Lac, 2009)

Authors conclude that through prototypes comparison, resilience benchmarking offers solutions to improve performance under failed components, and to satisfy Quality of Service (QoS) demands in case of fluctuating and/or insufficient resources. Resilience was found to be function of reliability, availability, security, interoperability and maintainability. In this work, authors assess resilience by comparing specific attributes at end-point (home-gateways), ignoring potential issues within the networked system.

Applying the R4 Framework of Resilience (Risk Management at Northrop Grumman – A case study)

Northrop Grumman Corporation is a Fortune 100 company that is diversified across several high technology markets. The company is the world's largest ship builder and the third largest defense contractor. The specific business unit that is presented is Sperry Marine which operates in Northrop Grumman's electronic sector. In late September 2003, Sperry Marine faced the task of preparing for the landfall of Hurricane

Isabel, with a projected storm track passing directly over Charlottesville. For approximately ten days the hurricane traveled over the open Atlantic waters periodically changing strengths between a category three and category five hurricanes. Eventually, by 6 p.m. September 18, 2003, the full force of Hurricane Isabel had reached the city limits of Charlottesville, Virginia and a citywide power loss soon followed. The auxiliary power unit (diesel generator) immediately engaged and all emergency circuits at Sperry Marine became active. However, there was one major problem that the information technology engineers and operations staff had not planned for: a complete loss the data center air conditioning system. This essential system was necessary in order to maintain the core Ethernet core working. Finally, a fan was placed beside the core Ethernet switch to keep it cooled enough to operate until normal power was restored. Although, after analyzing this case, King and Zobel conclude that the enterprise showed a resilient behavior, they were worried about resilience measurement in order to assess how resilient the company was? They identified the following four factors, as presented by MCEER's Resilience Framework:

1. Robustness: The company conducted a continuous redesign of information technology architecture with the objective of predictability and reliability.

2. Redundancy: There was an identical hardware configuration including two servers and a complete user documentation.

3. Resourcefulness: Use of regular fans for improvised cooling.

4. Rapidity: After power disruption auxiliary power unit (diesel generator) design started almost immediately to power the system.

Finally, they presented the classic availability equation as a measurement instrument for resilience:

$$Availability = \frac{MTBF}{MTBF + MTTR} \qquad (1)$$

where MTBF is mean time between failure usually provided by the equipment manufacture and MTTR is mean time to repair. This function focuses on the component level within specific information technology architecture (King and Zobel, 2008).

Based on the case on hand, authors reduced the goal related to resilience assessment to an availability assessment. Authors present this availability equation as a valid resilience measurement tool. However, according to Ebeling definition of availability ("probability that a system is performing its required function at a given point in time when used under stated operating conditions") this method for resilience assessment seems to be quite limited in that it cannot drill down within the complexity of systems and ignores the risky environment (exogenous factors) (Ebelin, 2005:6).

Measuring Resilience in Internet Infrastructure System

Omer (2009) defines resilience as the "ability of the system to both absorb shock as well to recover rapidly from a disruption so that it can return back to its original service delivery levels or close to it" (Omer, 2009:1). The global submarine fiber optics cable network that serves as the backbone of the internet is a particularly critical infrastructure system that is vulnerable to both natural and man-made disasters. In this paper, the authors propose a model to measure the base resilience of this global network, and explore the node to node and global resilience of the network using existing data

demand, capacity and flow information. The base resilience of the system is considered as a measurement of the value delivery of the system after a disruption to the value deliver of the system before a disruption. The work demonstrates how the resilience of the global internet infrastructure can be enhanced through reducing the network vulnerability and increasing its adaptive capacity. In order to model the resilience of the global submarine fiber optics cable network, authors address it as a logical network made up of nodes (geographic regions) connected by links (the fiber optic cables). The network used for the model development is shown in Figure 17, which shows the physical connections between the world continents (Omer, 2009:3).

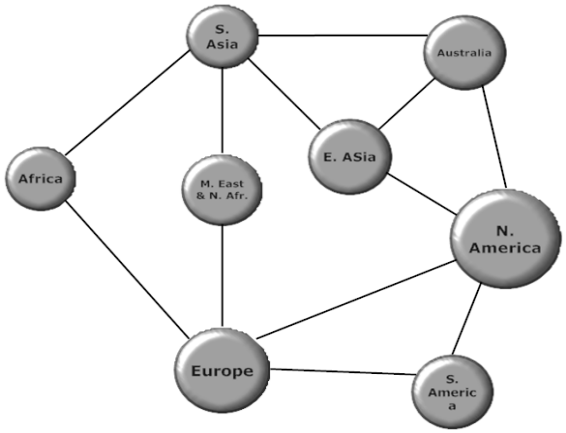


Figure 17. Logical Network of the Global Submarine Cable System. (Omer, 2009)

Resilience Calculation: Base resilience is defined for the network as the ratio of the value delivery of the network after a disruption to the value delivery of the network before a disruption, as shown in equation (2):

$$R_{network} = \frac{V_{init} - V_{loss}}{V_{init}} \qquad (2)$$

The initial value delivery of the internet network V_{init} is the total amount of information that needs to be carried through the network. The loss in value delivery V_{loss} is the information loss as a result of cable damages.

The node to node resilience is the ratio of the value delivery between the two nodes after a disruption to the value delivery between the two nodes before a disruption. The node to node resilience measured as shown in equation 3.

$$R_{node} = \frac{V_{init\_node} - V_{loss\_node}}{V_{init\_node}} \qquad (3)$$

Where V_{init_node} is the total demand of the node and V_{loss_node} is the total information loss taking into consideration the information routed by the extra network capacities.

Using these resilience measures, authors evaluate the damage when a link or a node is partially or completely down. Then different resilience strategies can be addressed in order to minimize the losses caused by potential disruptions.

In order to quantify the network, three parameters were taken into consideration; the node demand, link capacity and traffic flow of the network. The demand is the information in mega bytes per second that has to be transported from source to destination. The total demand of a node is the total information that needs to be carried through the network to the node.

The capacity of the link is the collective capacity of the fiber optic cables that are between the two nodes. In the real network, there may be more than one fiber optic cable systems between two nodes. The traffic flow is determined by the demand and the link

capacities. The flow through the links from node $_i$ to node $_j$ is x_{ij}, it is determined by the demand of any one node from the rest of the nodes. In order to quantify resilience values, the problem was formulated as a network optimization problem, where flow disruptions change the link flows limited by link capacities (pipeline capacity). Following equations show the formulation of the network optimization using linear programming:

Objective Function: Maximize V_{init} (4)

Subject to the constraints:

$$\sum_{i=1}^{n} x_{ij} + s_i \leq D_i \quad (5)$$

$$x_{ij} + x_{ji} \leq \alpha_{ij} c_{ij} \quad (6)$$

Where V_{init} is the total information through the network, x_{ij} is the flow going into node i from the node j, x_{ji} is the flow going out of node $_i$ to other nodes, n is the number of nodes connected to node i and D_i is the demand of node i and s_i is a parameter used to measure the amount of information lost when the capacity c_{ij} of any link is reduced. The capacity degradation is controlled by the coefficient α_{ij}. Equation (5) is the node demand constraint, the sum of the flow into one node is made equal to the demand of that node, and therefore any information that could not reach the destination due a capacity reduction of the link is captured by the coefficient S_i. Equation (6) ensures that the flow through the link in both directions, that is, from node i to node j and vice versa, does not exceed the capacity of the link c_{ij}. The value delivery between two nodes is the total

amount of information that flow in the link connecting the two nodes. Using the resilience metric authors measure the resilience when a link or a node is partially or completely down. With these considerations, network resilience is measured (Equation 2) as the total information flow in the network.

Critical Link Identification is also proposed as the vulnerability of the network, which is evaluated by identifying the links in the network that would lead to greater damage than others when disrupted (Omer, 2009:4).

In their work, authors measured resilience based on availability. Although, vulnerability issues are identified as critical component in resilient infrastructures, they are not included into resilience assessment model.

Assessing Resilience in the US National Energy Infrastructure

Assessing Resilience in the US National Energy Infrastructure is a document developed by Hoffman and Nilchiani that includes a resilience assessment of the United States national energy infrastructure when faced with natural and man-made disasters (Hoffman, 2008).

By using event tree analysis, the authors studied cascading power failures affecting the national electrical grid either initiated or propagated by man-made errors. To do so, they propose that resilience can be measured by the functionality of the system after a disruptive event, and the time it takes to return to normal operation.

They also make reference to the MCEER's resilience triangle. The pre-condition assumes the system is running at 100% of its desired functionality and performance. By improving a system's resilience, the aim is to reduce the decline in functionality and performance and also shorten the time it takes to recover.

However, at the moment of assessing resilience in power grids, they refer to a NERC's report, concluding that major disruptions and cascade effect are related to Right of Way (ROW) maintenance (Falling trees).

Deficiencies in vegetation management along power ROW have been found as a key factor in the Northeast Blackout of 2003 and other major cascading blackouts as well (Hoffman and Nilchiani, 2008:40-42). They propose to remove or trim trees by using growth retardant. Vegetation maintenance is considered as expensive to undertake, especially outside of dry, arid, or very cold climates.

Finally, the workshop came up with a number of vegetation management best practices with the top 5 listed here:

1. State law giving utility right to trim/remove (vegetation).
2. Adequate financial resources to maintain vegetation management cycles.
3. City partnership to work with homeowner association.
4. Use of herbicides to control growth on vegetation and in ground.
5. Directional pruning.

Although important finding and measures to control ROW are presented, we consider that actual resilience needs more strategic (effective and preventive) actions than just to trim trees.

Resilience Overview

In order to drill down through the different approaches to resilience definition and conceptualization, bar graphics were developed showing the frequency distributions of attributes and management challenges (like measurement needs), that have been associated to resilient behavior in systems and organizations. As a result critical attributes to be considered in the model development were identified. Figures 18a and 18b show the percentage frequency distribution found through chapter I and chapter II. They spot attributes considered as actual drivers (positively or negatively related) to resilience performance in different fields of the expertise. During the literature review process, 207 references as well as managerial challenges related to resilience driving have been found and processed from 38 different literature references.

Figure 18a shows the broad spectrum of attributes identified. They were grouped in 45 classes as presented through the literature review.

While class is a way to classify qualitative data, class frequency is the number of observations in the data set falling into a particular class. In order to gain insight within the data set, class percentage (class relative frequency multiplied by 100) was used to drill down and find the most relevant attributes involved in resilience.

Consequently, analyzing the data set (class percentages) arranged in a Pareto diagram, it was found that while the last 20 classes represent only 13.52% of the total references, the first 20 classes account for the 79.23% of the total frequency.

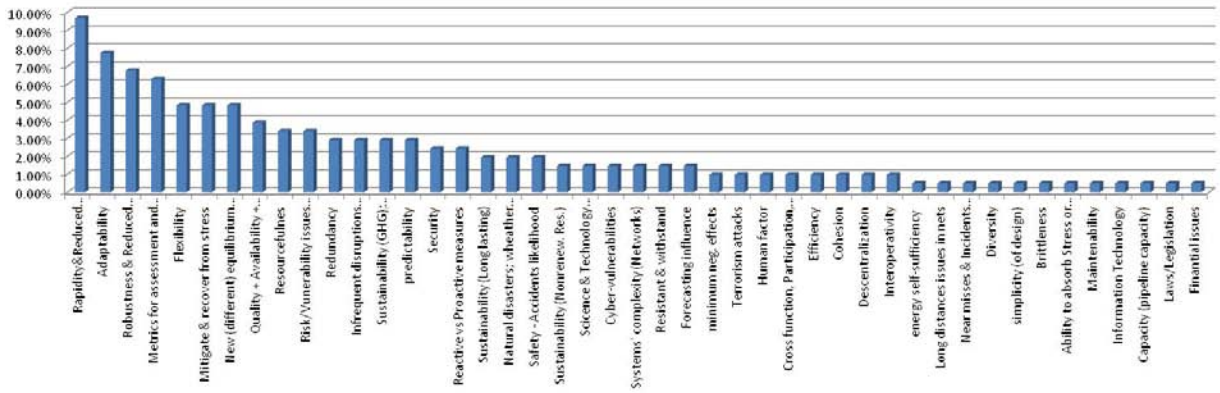


Figure 18a. Class Percentage (%) Distribution of Resilience Drivers Found Through the Literature Review. All 45 attributes (classes) from the literature review.

Figure 18b shows the 20 most relevant classes (attributes) found through the literature review. Some of these attributes show similarities that let us to aggregate them in a lower number of classes.

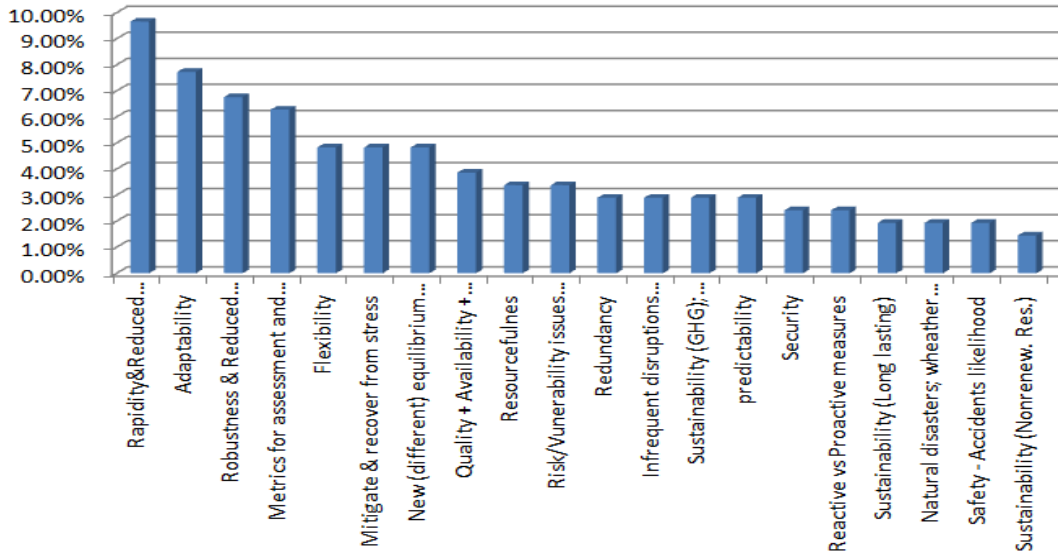


Figure 18b. Class Percentage (%) Distribution of Resilience Drivers Found Through the Literature Review (20 most referenced attributes).

Figures 19a and 19b show aggregated values of similar or related attributes (reduced number of classes) in order to identify the most relevant resilience drivers shared through different fields of expertise, ranging from psychology and ecology through logistic management. This information was useful for the following 2 main objectives:

1. Resilience definition approach for power grids as a particular case of Supply Chain Management.
2. Model design development to be conducted in chapter 3.

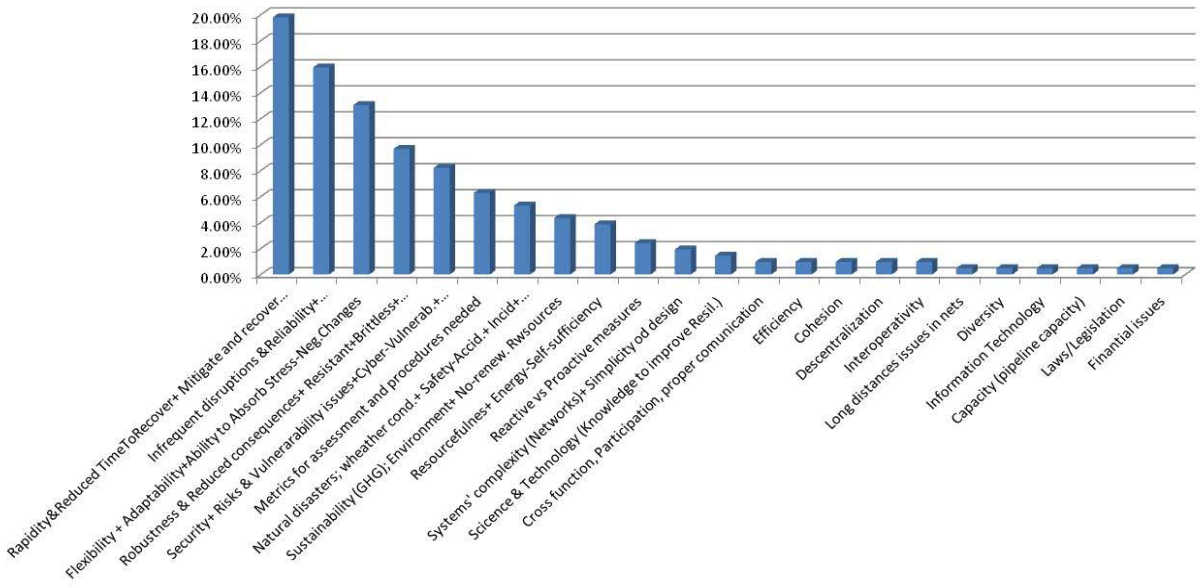


Figure 19a. Frequency Distribution (%) of Aggregated Resilience Drivers, Found Through the Literature

In the Figure 19b, the 14 most relevant classes (attributes and managerial challenges related to resilience driving) are shown. The aggregation process was conducted according to the theory developed throughout Ebeling (2005), Leenders and other authors (2006), and Lambert (2008).

Table 3 shows the aggregation criterion assumed to identify the critical resilience drivers in the literature review. It is possible to verify that those 14 categories encompass the 94.17 % of the original 207 references found through related literature.

Table 3. Aggregated Criterion for the 14 Attributes and Managerial Challenges Extracted from the Literature Review Process.

Number	Aggregated Factors (Classes)	Aggregated values	Aggregated values as %
1	Reduced TTR, Maintainability	**41**	**19.81%**
2	Reliability, infrequent disruptions	**33**	**15.94%**
3	Flexibility + Adaptability	**27**	**13.04%**
4	Robustness+ Resistant	**20**	**9.66%**
5	Security/Vulnerarability issues	**17**	**8.21%**
6	Metrics & procedures	**13**	**6.28%**
7	Natural disasters & Accid (HF)	**11**	**5.31%**
8	Sustainability (Envir. issues)	**9**	**4.35%**
9	Resourcefulness&Selfsufficiency	**8**	**3.86%**
10	Reactive vs Proactive measures	**5**	**2.42%**
11	Systems' complexity (Networks)	**4**	**1.93%**
12	Scicence & Tech.(Knowledge)	**3**	**1.45%**
13	Cross function, comunic.	**2**	**0.97%**
14	Efficiency	**2**	**0.97%**
TOTAL		**195**	**94.17%**

From Figure 19b it is possible to identify recover capability (rapidity, timely recover), reliability and vulnerability issues among the most relevant drivers of resilience performance. Appendix B and Appendix C have the content used to develop Figures 18a, 18b, 19a and 19b.

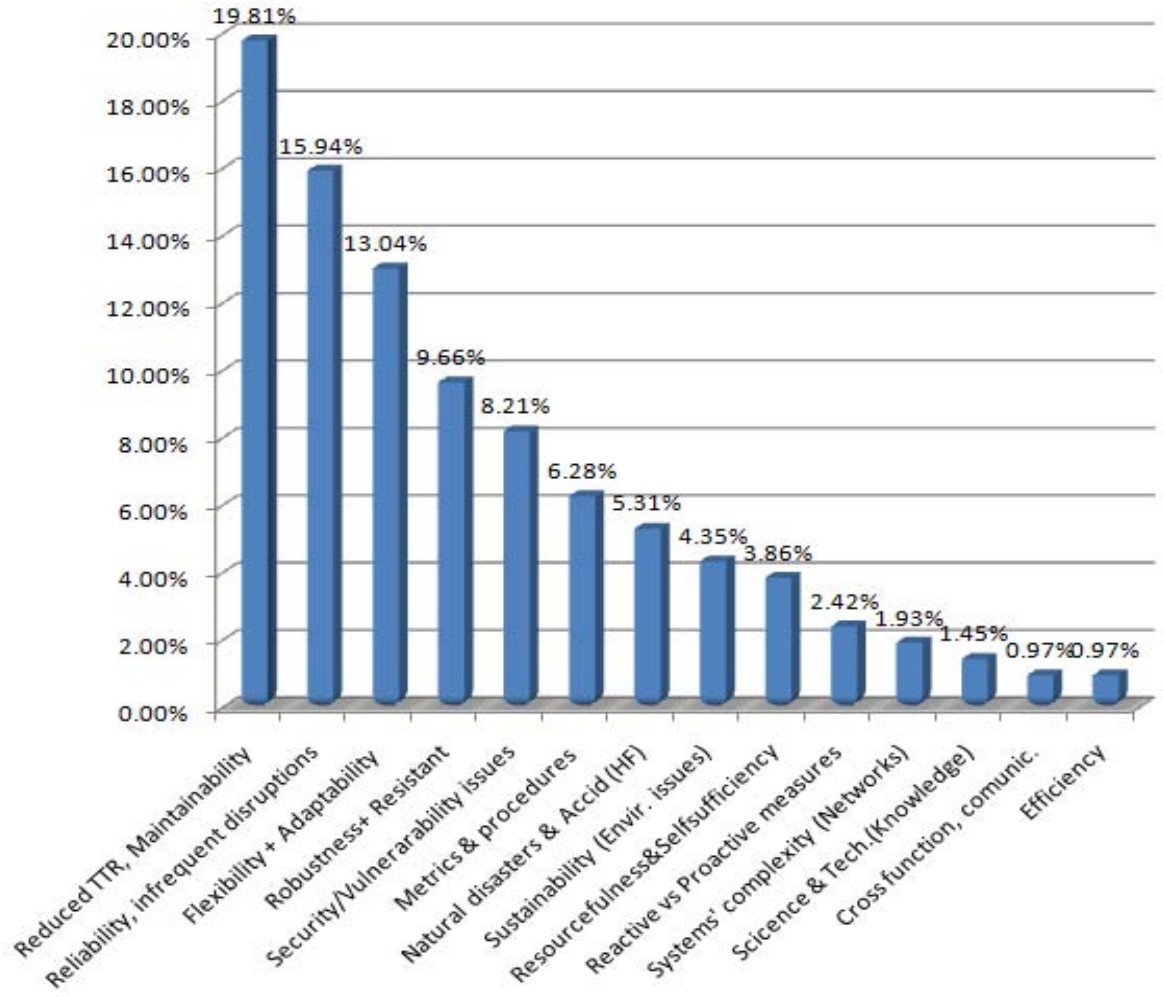


Figure 19b. Frequency Distribution (%) of Aggregated Resilience Drivers, Found Through the Literature (The 14 most relevant).

Vulnerability Assessment

Although vulnerability and risk issues were mentioned systematically through the chapter, no useful information was found about how to manage such a resilience driver.

The use of Reliability Centered Maintenance has been routinely applied to mechanical and electrical systems and their use has been also extended to other fields where hazard risk analysis is needed. The successful integration of reliability centered maintenance with a structural integrity program conducted for the F-15 risk assessment and maintenance program, found the usefulness of the standard MIL-STD 882D for risk classification. It combines a description of the severity with a frequency of occurrence into a hazard matrix (Figure 20). Numeric and color coding is used for group rankings and show pictorially the potential risk. Then, based on the risk grouping, mitigation actions are decided as a managerial tool (Hinkle and others, 2009:2-3).

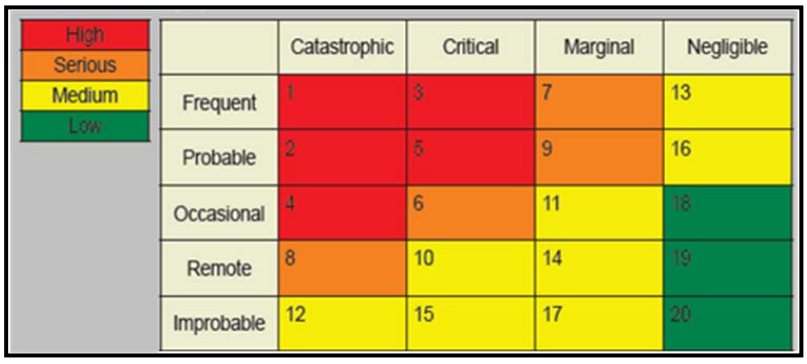


Figure 20. Hazard Risk Matrix. (Hinkle and others, 2009:2-3)

This standard addresses a useful approach in the management of environmental, safety, and health mishap risks encountered in the development, test, production, use, and disposal of DoD systems, subsystems, equipment, and facilities. The approach described herein provides a consistent means of dealing with vulnerabilities that must be identified,

evaluated, and mitigated to a level acceptable to the appropriate authority, and compliant with federal laws and regulations.

When properly applied, these requirements should ensure the identification and understanding of hazards and their associated risks; and mishap risk eliminated or reduced to acceptable levels. The objective of this system is to provide requirements for developing and implementing a program to identify hazards within systems and to improve design requirements. It constitutes a tool for managing activity in order to achieve acceptable mishap risk through a systematic approach of hazard analysis, risk assessment, and risk management. Additionally, this standard provides a mean to identify the most rational way to protect power sources and critical components (DoD, 2000).

Resilience in Power Grids

In defining resilience, we need to focus on the functions or performances that a system is designed to fulfill, and not the individual components of the system or network under study (George Mason University, 2007:90). Therefore, the following definition is presented for resilience in power grids:

> **Resilience in power grids is defined as their capability to cope with adversity arising from intentional and unintentional threats, and to recover in a timely manner to an acceptable level (new equilibrium) of performance after have been stressed.**

Additionally, since power grids constitute critical infrastructure, vulnerability is function of intentional attacks and minimized through security allocation.

This definition implies inherent learning process from previous experiences, so after a disruption new considerations are included to withstand in a more efficient way further stresses.

Power Grids and Supply Chain Management

Sheffi defines the term "Supply Chain" as a simplification of the Supply Web or Networks of Suppliers, manufacturing plants, retailers, and the numerous supporting companies involved in design, procurement, manufacturing, storing, shipping, selling and servicing goods (Sheffi, 2005:82).

Lambert, defines Supply Chain Management as the "integration of key business processes from end-user through original suppliers that provides, products, services, and information that add value for customers and other stakeholders." (Lambert, 2008:287). This logistician recognizes the supply chain management to be, in fact, a network of business and relationships that offers the opportunity to capture the synergy of managing such a networked structure (Lambert, 2008:2).

Consequently, since a supply chain is a network connecting suppliers and customers through networks, power grids can be thought as a particular case of supply chain as presented in Table 4.

Table 4. Proposed Analogy between Supply Chain and Power grids. Based on Yossi Sheffi and Lambert's concepts.

Order	Networks	
	Supply Chain	**Power grids**
1	• Inbound (Supply process), suppliers	• Supply, original suppliers, fuel supply, generation plants
2	• Conversion (production: internal process)	• Generation – Operation
3	• Warehouse	• No available today (smart-stores)
4	• Transportation (Shipment)	• Transportation (networks)
5	• Outbound (Distribution process and Customers)	• Delivery to customers
6	• Postponement	• Postponement
7	• End-users	• Customers, Demand nodes
8	• Products, services, information	• Electricity (utility), information

One limitation of current power grids is that unlike water or gas, electricity cannot be stored in mass quantities. So, it must be generated and then consumed within seconds of being generated (NERC, 2010). This means that supply needs to roughly equal demand and unused capacity cannot be stored for later usage. Any under load or over load on an electrical system can cause significant damage. Electrical power is setup as a highly interconnected grid as shown in Figure 21, but with little overall oversight. This supports the supply and demand need but can also create vulnerability if a part of the grid experiences a problem (Hoffman, 2008:31).

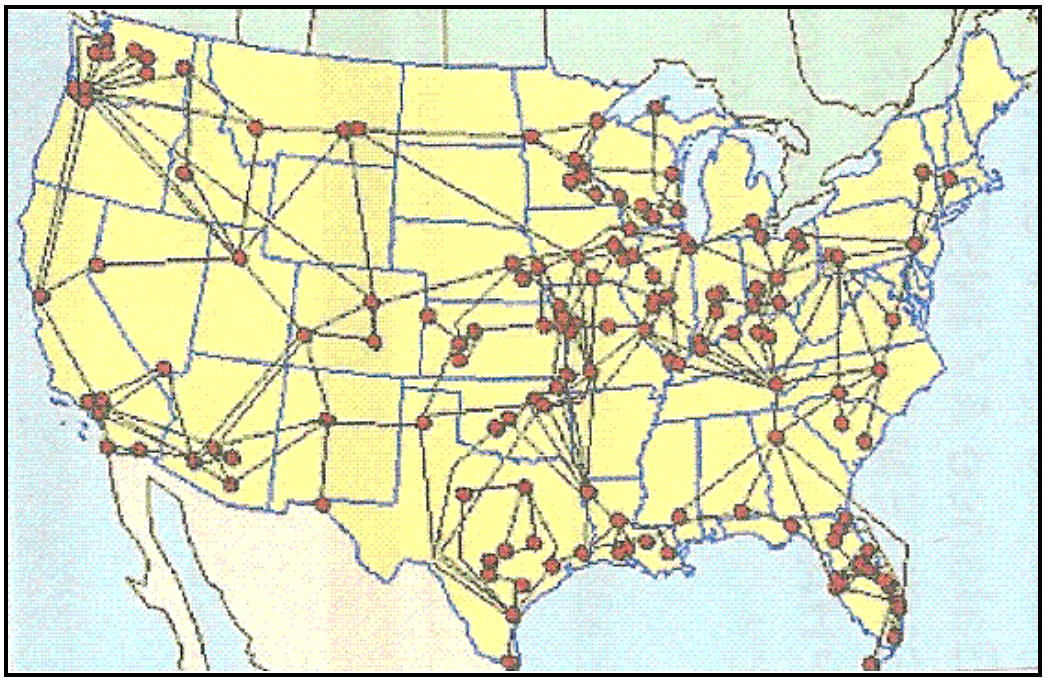


***Figure 21: United States Power Grid Interconnections (*Hoffman, 2008)**

Ulieru proposed the following three types of interdependent networks (Ulieru, 2007):

1. ***Supply networks:*** transportation grids for electrical power, oil and gas; water distribution networks; transport/road tunnel systems; production flow supply chains; health care systems.
2. ***Cyber-networks***: tele-control and SCADA (Supervisory Control and Data Acquisition) networks, e-banking/finance networks, etc.
3. ***Managerial/organization networks*** where human resources supervise and/or utilize.

Since power grids play a critical role within a nation's survivability (critical infrastructure), it is possible to state that power networks share characteristics from the

three networks presented above. However, electrical powers are specifically mentioned as supply networks.

Considerations Related to Power Networks

Since one of the characteristics that limit supply chains' capability is their pipeline capacity, specific considerations regarding power networks are presented. Energy transmission through the power grid is measured in megawatts (MW), a unit of power.

While the power grid operates as a complex network with the power flow on individual lines governed by the laws of physics, conceptual studies to examine node to node transmission are often performed using typical transmission line capacities that are a function of the line voltage, number and size of the wires in each of the three phases, and the distance (link's length) over which the power is being transmitted. In order to show how these variables are related to the line load (pipeline capacity expressed as Surge Impedance Loading Curve- SIL), Figure 22 is included. Here it is possible to verify how the pipeline capacity is inversely related to distance- link length (AEP, 2010).

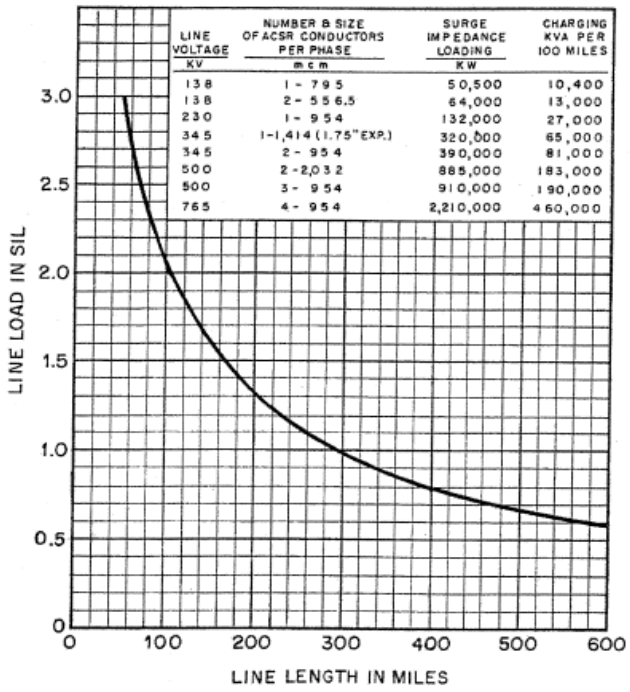


Figure 22. Transmission Line Capacity as a Function of Surge Impedance Loading (SIL). (IEEE, 1979)

Power networks are prone to be affected by several types of threats. Although those damages related to natural disasters and human errors could be forecasted, the risks related to security issues (intentional attacks) are almost impossible to be predicted. Therefore, while assessment of multiple contingencies is a regular part of the planning and operation of the electrical grids, there are a nearly infinite number of combinations of multiple contingencies, making analysis toward protection against all possible events impossible. This situation shows the need for the electrical grid to become more resilient (addressing the consequences of a failure) since it is practically impossible to protect the system from all possible causes that can lead to a failure (Hoffman, 2008:33). Consequently, recovery capability is a crucial component for scenarios assessment in terms of resilience.

However, as a networked system, a percentage of transmission line outages in power grids do not result in loss of service to customers because the transmission system is designed with redundant paths. This means that end point's assessment (output) is prone to disregard actual issues embedded within the network, considering that network's performance is correct (apparently).

Model Development

The idea of using models in problem solving and decision making analysis has lead to useful achievements across many different fields. From mental model to complex computerized models are based on assessment and decision making needs.

It is almost trivial to say that a model is needed to understand issues related to resilience networks as well as to think about how it can be secured, maintained and improved. A model will be useful to identify what information to look for and to provide a mean to explain relationships among variables. To do so, two requirements should be accomplished. First, the model needs to provide an explanation or understanding of the phenomenon under study. Second, it should be able to be used with reasonable investment of resources and effort. Consequently, the goal should be develop a model that is simple enough that it can be used without engendering problems or requiring excessive specialized knowledge, but at the same time powerful enough in order to reach successful outcomes (Hollnagel and others, 2008:252-254).

However, although a model should be a simplified representation of reality, it is only useful as long it is valid. A valid model is one that accurately represents the relevant characteristics of the object or decision problem under study (Ragsdale, 2008).

Benefits of using modelization in system's assessment are presented by Ragsdale as follows:

1. It is often less expensive to analyze decision problems using models than actual systems.
2. Models, often deliver needed information on a more timely basis, what is critical for timely decisions making.
3. Actual system's complexity usually turn impossible to exanimate their behavior in the reality.
4. Models allow decision makers to gain insight and understanding about the object or decision problem under investigation. The ultimate purpose of using models is to improve decision making.

Scenario Analysis

Since making decisions when facing uncertainties is a difficult task, scenario analysis has been proposed as a useful tool to assess actual as well as potential performances toward efficient and proactive decisions (Husdal, 2004).

Scenario analysis, also known as 'What-if?' analysis, is a systematic method of studying and articulating probable future events that may affect the systems or its operating environment. This turns stochastic variables into deterministic parameters enabling managers to gain insight into how sensitive the performance measure is to changes to the input variables (Ragsdale, 2008:562).

One clear advantage of this method is that the future outcome of a large number of possible inputs or decisions can be analyzed before resources are committed. Using scenario analysis, the supposedly most likely, or most expected, future can be

determined, and initial decisions made accordingly. However, the downside of scenario analysis is its inability to handle contingent decisions that arise within the scenario. So, once the scenario is determined, and decisions made, and the future starts running, there is practically no way of returning and making a different decision. Since the most likely scenario may not be the optimal solution, several alternatives can be analyzed in a timely manner in order to have a networked big picture and hence to take the best possible decision. It is important to say that scenarios analysis is not intended to foresee the future. Forecasting is a challenge that is not always possible when managing critical infrastructure that are menaced not only by unpredictable risks but also by smart risks like terrorist attacks (Husdal, 2004).

Summary

Relevant federal mandates, as well as different approaches to the resilience concept and its assessment were presented from different fields standpoints, as a way to assess performance capability when systems, organizations and people exposed to stress.

Common attributes that drive resilience have been found ranging from resilience in ecology and psychology to supply chain environments. Among the more than 200 individual references to resilience drivers and management issues that have been found, most of them share common concepts. Consequently, the original 45 attributes extracted from the 38 different publications were grouped into a relative few classes in such a way they showed consistent meaning in actual resilience drivers.

Therefore, these classes (attributes) enable strategic decision makers to successfully address resilience in systems and organizations, where Supply Chain Management represents a particular environment of challenge.

It was shown that power grids are, in essence, a supply network where essential components can be identified: suppliers, customers, commodity to be delivered and infrastructure to conduct the transportation (shipment). Therefore a specific definition of resilience was proposed for power grids to be implemented in the model process.

Although it was found that some of the literature disregards reduced time to recover after disruption or stress as critical resilient behavior, "rapidity" was also presented by practitioners as necessary to enable efficient systems to reduce unnecessary and expensive robustness as well as physical redundancy. Moreover, desirable recovery processes take resilient systems to an acceptable level of performance rather than to the same situation existing before the stress or disruption. This is a consequence of the learning process that capitalizes previous experiences in order to improve resilience toward future new and more complex challenges. This attribute was presented as desirable rather of overprotecting (securing) systems that makes them more fragile and hence less flexible to withstand unexpected stress.

While resilience is proactive in positioning a system to survive and thrive given known and unknown challenges, security, as generally practiced, provides specific protection against identified or projected risks or circumstances (George Mason University, 2007:105). As a result, excess of security can become a disadvantage.

Since power grids operate as a complex network with the power flow on individual lines that are a function of the line voltage, number and size of the wires in each phase, and the distance (link's length) over which the power is being transmitted, pipeline capacity was identified as a physical constraint for power grids resilience.

On the other hand, the standard MIL-STD 882D was also presented as a quantitative tool for vulnerability classification. It combines a description of the severity with a frequency of occurrence into a hazard matrix. So, based on the risk grouping, quantitative resilience assessment is enabled to take account of vulnerabilities issues.

In methodological matters, lineal programming models have been used for performance assessment, including availability in networked systems. Meanwhile, resilient behavior was identified as related to several variables or attributes, where the highest frequencies were found for reduced time to recover, reliability, pipeline capacity and vulnerability.

Meanwhile, smart grid designs have been presented as a still emerging digital technology that is capable not only to contribute to costs saving and reliability improvement, but also to bring threats of cyber-attacks.

Finally, environmental concerns are arising as a strategic issue to be considered within sustainability goals, where smart grids are predicted to play a relevant role.

Chapter 3 discusses the methodology and model development used in this research.

III. Methodology

Introduction

This chapter presents the model development and the concepts needed to support the decision making process. Although decision makers are usually interested in costs, savings and payback risks, money is not always the unique element in the strategic decision making environment. In Chapter II, we showed how US leaders have emphasized other factors that should influence and guide strategic decisions involving critical infrastructure. For example, the Department of Homeland Security (DHS) presented the need for scenarios that test the resilience of critical infrastructures in the face of both, direct and indirect effects of an event (CITF, 2006:9).

In the same way, model development is able to serve as a useful tool to conduct exercises like those recommended by the DHS/CITF as part of a critical infrastructure exercise program. At DHS, CITF defines these exercises as an ongoing series of scenario-driven tabletop events that bring together different stakeholder communities and emphasize learning versus demonstration (CITF, 2006:9).

In Chapter II Husdal's definition of robustness was presented as the ability to stay on course and to accommodate unforeseen contingent events without the need of change, and flexibility as the ability to change. That is, to accommodate unforeseen external events by changing tracks and being open to deviate from the initial course. Likewise, he proposed that resilient strategy should be built on both robustness as well as flexibility (Husdal, 2004). If we merge these two concepts into a system, as two faces of the same coin and then, develop a timely recovery capability when such unforeseen events occur,

we will be developing not only a synergic behavior but also a smart system that learns and reaches a more reliable equilibrium (resilient).

MCEER's concepts have been found as summarizing the main components embedded in resilient systems: disaster resilience is characterized by reduced failures, reduced consequences from failures, and reduced time to recovery (Hoffman, 2008:8). These three attributes or characteristics together are considered to constitute actual resilient behavior. Consequently, the model is developed including these attributes in such a way that minimizing the Objective Function (OF) value of the Linear Program Model will result in an optimal solution by minimizing vulnerabilities, as well as failure probabilities for energy delivery. In addition, since the time to recover is specifically mentioned as an integral component of resilience, the model also addresses time to recover between nodes as actual resilient behavior: the faster the recovery, the more resilient is the power network. This specific attribute has been linked to the power grid's timely recovery capacity when a disruption happens. Timely recovery capacity has been chosen to feed the model from two potential sources:

1. Time elapsed from disruption until the service was recovered to a desirable level to satisfy demands without neither security nor safety issues (Empirical distribution from actual data set provided by DoE).
2. Assumed probability from Maintainability Theory for Maintenance Time: Lognormal distribution. The objective of maintainability is to reduce system down time by facilitating the repair effort (Ebeling, 2005:218).

The compliance requirements against potential threats are coming from many angles: privacy, security, corporate governance, environmental, labor, trade and financial

reporting. Since 100% protection against such threats is impossible in practice, organizations (systems) must learn to be resilient to withstand threat's effects. Resilience requirements need to be specific to each scenario for some time before standards merge or any mandates are levied by governmental or regulatory agencies. Although information technology and security management is governed by international standards, none of the existing standards are broad enough in scope to address resilience, and it is doubtful that any will emerge in the near future. Consequently, experienced organizations best practices can be presented as the backbone of resilience requirements (George Mason University, 2007:104). Resilience design is not an easy matter, and there is not one recipe that fits all organizations or systems. Therefore, this research assesses performance under alternative scenarios in order to get valuable information to feed the strategic decision making process. This "what-if" analysis will be useful to assess not only actual power network's resilience but also to identify and prioritize strategic allocation of both, reliability and security.

This research presents a parameterized model for resilience assessment in order to develop a quantitative tool that embed heterogeneous variables (e.g. reliability, pipeline capacity, failure probability, vulnerability) into a specific model in order to enable comparison among alternate scenarios in the strategic management environments.

Thus, a unique resilience value, between zero and one ($0 \sim 1$) is used to standardize the resilience assessment process over a wide range of possible organizations and systems. Each system should meet a specific value of such "Resilience" (goal) in order to meet the system's desired goals.

In other words, first, this work develops a model that lets managers to identify the minimum value of performance needed through the net in order to reach the system's goal in terms of resilience. Then, current values for critical system's attributes are embedded into the model in order to identify the most efficient way to allocate resources between nodes and within the whole network.

Assumptions for the Model

The following assumptions complement those presented in Chapter I, in order to reach consistency in the model development process:

1. Electric power cannot be stored for an extended time. Electricity is consumed within seconds of being generated.
2. Total supply roughly equals Total demand within the network.
3. Electrical power distribution is setup as a highly interconnected grid as shown in Figure 21, but with little oversight. This situation can create vulnerability if a part of the grid experiences a problem (Hoffman, 2008:31).
4. There is a high likelihood of blackout that will affect multiple links within grids. So, the model is able to identify the weakest links, where such an outage could begin (Hoffman, 2008:34).
5. In an event of disruption, a reliability of 0.955 is assumed for timely and proper recover, reaching the power network's availability goals (Rr).
6. Problem to be modeled can be described using equations and inequalities that are linear.

The modeled power networks represent actual energy grids. Historical disaster statistics are used to develop potential scenarios which in turn are assessed by the model.

Their potential consequences are identified in terms of lack of pipeline capacity, priorities for security (to reduce vulnerability), and reliability (to reduce failure probability) allocation.

Model

Reliability and Vulnerability Assessment

Determining probabilities related to reliability as well as vulnerabilities are out of the main scope of this methodology. Reliability and vulnerability data by themselves do not guarantee successful outcomes when the decision makers face broad and complex scenarios. Reliability and vulnerability related to critical power networks is embedded throughout the model development process. Therefore, an accurate assessment of these data is critical for managerial decisions.

The model analyzes different reliability and vulnerability configurations (alternate paths within the grid) in order to select the optimal solution that minimizes the total path's vulnerability and maximizes the overall reliability.

The model weighs the aforementioned attributes as directly proportional to the amount of energy to be delivered through each link within the network as follows:

1. ***Reliability*** is defined as the *probability that a component or system will perform a required function for a given period of time when used under stated operating conditions (Ebeling, 2005:5).* Reliability design includes a virtual redundant system. While physical infrastructure is installed as a networked system, reliability of recovery capability is a virtual component designed through Time To Recover (TTR) analysis from actual data or modeled as a lognormal distributed phenomenon according to Maintainability theory. The main

advantage of this design is that more resilient parallel systems (virtual redundancy) are designed without actual physical redundancy. Moreover, while physical infrastructure in power networks need to be replicated for each alternate electricity flow direction (one way versus two ways flow), recovery capability (Rr) design works as a two way component as shown in Appendix D. Since model design minimizes the objective function value, reliability is calculated through the following Failure Probability equation (7):

Failure Probability = 1 - Reliability (7)

2. ***Vulnerability***. Since system's vulnerability eventually leads to disruptions, identification of sources of risk and uncertainty at each node and link in the supply chain needs to be indentified and assessed (Christopher and Peck, 2004: 9). Managers need to look at increasing security in order to reduce the likelihood and severity of disruptions (Sheffi, 2005:14). As presented in Chapter II, critical infrastructure vulnerabilities assessment is required to be included as a cornerstone component in DoD and USAF's strategic plans. Military Standard for System Safety Program Requirements (MIL-STD-882D) is used for vulnerability assessment in power grids as input in order to feed the model. This standard lets users customize its content to specific situations. The following criteria (Table 5) for vulnerability measurement has been adapted from the aforementioned standard to allow the model to minimize the Objective Function, and hence to find the optimal solution:

Table 5. Vulnerability Index Criteria (Adapted from MIL-STD 882D)

VULNERABILITY INDEX	CRITERIA	Color code
1 - 3	Acceptable without review	***(Green)***
4 - 11	Acceptable with review by System Manager	***(Yellow)***
12- 15	Undesirable (Decision Maker acceptance needed)	***(Orange)***
16 - 20	Unacceptable	***(Red)***

Consequently, the following vulnerability matrix (Table 6) has been obtained to be applied to power grids:

Table 6. Vulnerability Matrix for Power Grids (Adapted from MIL-STD 882D)

SEVERITY CATEGORY / FREQUENCY	CATASTROPHIC	CRITICAL	MARGINAL	NEGLIGIBLE
FREQUENT	**20**	**18**	**14**	**8**
PROBABLE	**19**	**16**	**12**	**5**
OCASIONAL	**17**	**15**	**10**	**3**
REMOTE	**13**	**11**	**7**	**2**
IMPROBABLE	**9**	**6**	**4**	**1**

DoE and DHS define the severity categories according to the specific power network's risks and potential consequences. Although frequency related to natural disasters and accidental disruptions background can be used in this process, terrorist attacks and other man-made threats (intentional attacks) require specific treatment to determine their likelihood and security allocation needs.

Pipeline Capacity

Although this physical restriction is included in the model as constraints for feasibility purposes, this resilience component is also parameterized within the overall resilience assessment. Reducing pipeline capacity means more and longer routes, which in turn increases the risks. Pipeline capacity issues are simulated through efficiency coefficients (α_i) that let decision makers simulate actual capacity reduction through the links.

This variable (α_i) can also emulate potential outages (when coefficient α_i is equal to zero) within power grid.

Path Length

Although time-based or distance-based network problems tend to use the shortest path to measure resilience, analyzing critical infrastructures like power grids and water distributions networks, shorter paths are not always the best alternative. Security allocation as well as threats characteristics can transform an apparent best alternative into a high risk endeavor. Consequently, although vulnerability assessment process should include path's lengths a sensitive path's attribute, the model accounts for the partials lengths (links) as well as total length (sum of all used links within the grid) related to the optimal solution.

Information about link's length is given by the model in order to,

1. Compare among similar solutions in terms of reliability and vulnerability, or
2. Estimate potential costs (e.g. to build) when investment is needed to lengthen specific arc in the network or to evaluate the potential creation of an alternative arc in the decision making process.

The Model Statement

This research develops a model in order to emulate actual power grid's performance under alternate scenarios toward a resilience assessment. Linear Programming models have shown to be useful to assess critical attributes that constitute actual resilient behavior within the power grids.

Based on previous researches and criteria found in Chapter II, the selected attributes that drive resilience in networked systems are:

1. Reliability.
2. Timely recover capability (Also defined as "rapidity", means the ability to restore functionality or performance in a timely manner, while avoiding disruptions (Hoffman, 2008:8).
3. Vulnerability.
4. Pipeline capacity.

Particular man-made stressors such as terrorist attacks and sabotages (intentional attacks) can be addressed as particular vulnerability issues. These attributes are embedded in the model in such a way that the model's behavior is representative of actual power networks.

Linear Programming for model development is selected not only because of its usefulness but also its simplicity that facilitates further implementation of findings. This thesis focuses on a mathematical model implemented through computers via spreadsheets (SOLVER®). The model uses mathematics to describe a decision problem. Mathematics is used in a broad sense, encompassing not only elements of math, but also the related topics of logic.

Mathematical Model Category

As it was stated earlier, the model tends to represent alternative scenarios in terms of resilience characteristics which are strongly related to reliability, vulnerability, pipeline capacity and a timely recovery capability. Two main alternatives are faced regarding data availability although modelization process is based on actual literature and power grids characteristics:

1. Actual data is available to feed the independent variables of the model that are under decision making's control.
2. Values of independent variables are unknown or uncertain.

A *Prescriptive Model* is the first case, where the functional relationship between the independent variables and the dependent variables is known and well-defined. The independent variables are known or under decision maker's control.

In the second case, although a functional relationship between the independent variables and the dependent variables is known and well-defined, values of independent variables are unknown or uncertain. This category of mathematical model is known as a *Descriptive Model*.

Consequently, this thesis develops a prescriptive model to represent the actual behavior of network energy through alternative scenarios. Functional relationship between variables is established based on the literature review and the values of the independent variables are known or under a decision maker's control.

Problem-Solving Process

The modeling technique used is an important part of the total problem-solving process since the ultimate goal in building models is to help managers make good decisions that lead to good outcomes. Figure 23 summarizes the key elements in the process.

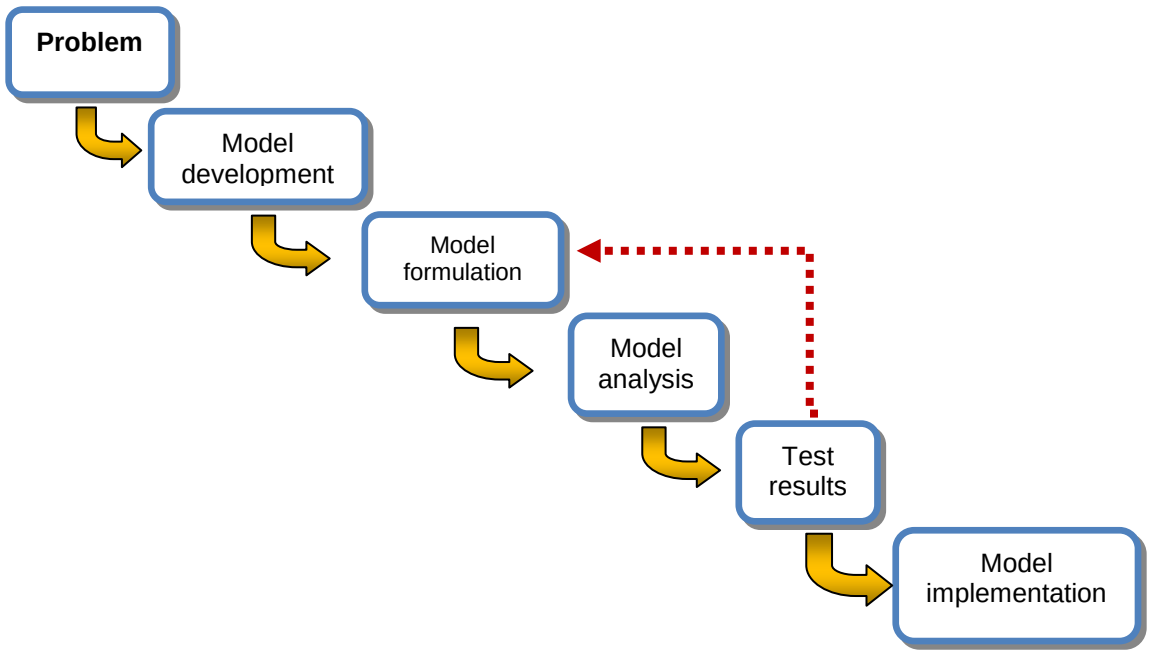


Figure 23. Visual Model of the Problem-Solving Process. (Adapted from Ragsdale, 2008:8)

Figure 23 shows the logical process that starts when the problem has been identified and concludes when the Model has been verified and validated and is ready to be implemented. The process is not merely a one way process but a two way process where a feedback is required upstream to get a more accurate model representing actual system behaviour. Eventually, the best model is found as the simplest one that accurately

reflects the relevant characteristics of the power grid performance in terms of the study matter (resilience).

Problem Formulation in Linear Programming

As a optimization problem, three elements are considered:

1. Decision variables: Represented by the amount of energy to be delivered through each link for the optimal solution.
2. Constraints: These are restrictions in each scenario on the alternatives available to the decision maker. The constraints represent potential network restrictions that are represented in each scenario. There are three possible ways of expressing the constraints relationships:
   a. A "less than or equal to" constraint ➔ f(X1,X2, …, Xn) ≤ b
   b. A "greater than or equal to" constraint ➔ f(X1,X2, …, Xn) ≥ b
   c. A "equal to" constraint ➔ f(X1,X2, …, Xn) = b
3. Objective: The objective in an optimization problem is represented by an Objective Function which identifies the decision variables that the decision maker wants to either maximize or minimize. The objective function general format is:
   a. MAX (or MIN) f (X1, X2, …, Xn)

A network flow problem can be described or displayed in a graphical form known as a network. Power grids assessment is implemented through network modeling, which is a particular case of linear programing (Ragsdale, 2008).

All network flow problems are represented as a collection of nodes connected by arcs. The circles in Figure 24 represent nodes and the lines connecting the nodes are called arcs. The arcs indicate valid paths or connections between nodes in the network.

Lines connecting nodes are arrows, that indicates the energy flow direction. When the connectivity beteween two nodes inlcudes two way energy flows, then two arcs are implemented, showing the flowe direction. This constitutes a key compoenent for the optimal soution.

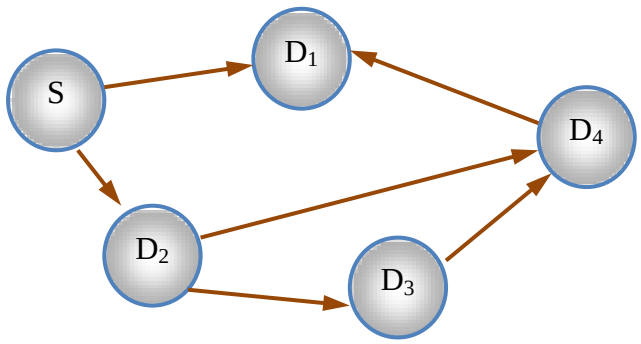


Figure 24. Example of Network Representation

Power grids assessment is modeled as a “Generalized Network Flow Problem”. For model development purposes, LINK is defined as the budle of “Source node”, “Arc” and “Destination node”. This definition prevents confusions between bundles of a connected elements and arcs. Although each link has been defined as the bundle including source node and destination node, some nodes work also as “transhipment” nodes (Figure 24, nodes D_2, D_3 and D_4) when energy arrives to them in order to continue toward the final demand nodes (Figure 24, node D_1).

Model formulation

Fiksel emphasizes the importance of the assessment not only of actual performance (output), but also of the intrinsic characteristics (resilience drivers) that constibute to the system resilience (Fiksel, 2003:5337).

In order to solve the research questions stated in Chapter I, and hence the problem, the following steps are accomplished:

1. Research statement.
2. Decision variables.
3. Objective Function as a linear combination of the decision variables.
4. Constraints.
5. Upper and lower bounds on the decision variables.

To make the model feasible, the amount of energy available to deliver needs to be equal to the total demand within the power network. Hence, when the energy available is not enough to satisfy such feasibility requirement, an artificial variable (dummy node) will supply the difference to run the model properly (node #5 in the model in Appendix E). Conversely, if the amount of energy to be delivered exceeds actual overall (networked) demand, the same artificial variable (dummy node #5) will "demand" the excess of energy in order to ensure the feasibility of the model, and an optimal solution will be reached. Node #5 represents the artificial variable in the network model.

Research Statement

This research *develops a mathematical model that allows Decision Makers (e.g. DoE, DoD, USAF, etc) to make a more quantifiable assessment about resilience in power grids, in order to contribute to Strategic Energy Management.*

Decision Variables

Since the model is intended to assess power grid's performance under alternative scenarios, the decision variables are the amount of energy to be delivered through the links ($Q_{ij,}$ $Q_{ji,}$).

Objective Function (OF) as a Linear Combination of the Decision Variables.

In order to take advantage of the more reliable and less vulnerable paths within the network, the Objective Function statement is set as the minimum value possible of the following product:

$$\text{OF;} \quad \text{(MIN);} \quad \sum (Q_{[ij]} \text{ x } P(\text{failure})_{[ij]} \text{ x } \text{Vulnerability}_{[ij]} + Q_{[j,i]} \text{ x } P(\text{failure})_{[j,i]} \text{ x } \text{Vulnerability}_{[j,i]}); \quad \text{for all i, j} \qquad (8)$$

Since the OF value is minimized, the optimal solution, what is directly proportional to the amount of energy to be delivered, minimizes vulnerability as well as failure probability within the power network. Consequently, the optimal solution is the one that satisfies the demands at each node in the most resilient way ($R \rightarrow 1$), while accomplishing the model constraints and feasibility requirements.

Constraints

Constraints in the model are as follows:

1. The amount of energy delivered through each link has to be less or equal to the capacity at each link. There are two values for link capacity:
    a. The designed or theoretical capacity (Highest possible value) and
    b. Actual capacity which is given by the designed or theoretical capacity at each link multiplied by a coeficient ($\alpha \leq 1$) in order to adjust (reduce) the design capacity to the scenario on hand.
2. All demands must be satisfied. This constraint ensures feasibility of the model. Additionally, this constraint is used to test overall network resilience when optimal solution is found.

The constraints formulation is as follows:

$$Q_{ij} \leq C_{ij} ; \qquad \text{for all i, j} \qquad (9)$$

$$Q_{ji} \leq C_{ji} ; \qquad \text{for all i, j} \qquad (10)$$

$$\sum Qd = \sum Qs \qquad (11)$$

Upper and Lower Bounds on the Decision Variables.

The upper bound for the decision variables are set in the constraints module (SOLVER®), while the lower bound is given by the nonnegativity condition.

Nonnegativity condition can be set in two ways in the SOLVER® configuration table :

1. As a constraint or
2. in the software configuration box "***Options***" as "***assume Non-Negative***". The non-negativity formulation is presented in equation (12):

$$\mathbf{Q_{ij}\ ,\ Q_{ji} \geq 0\ ;} \qquad \text{for all i, j} \qquad (12)$$

Model Implementation

The model is composed of the following seven main modules:

1. Module: Nodes connectivity within the grid: This model relates nodes to each other through links in order to feed the optimal solution process. Besides, it relates each node to its supply or demand
2. Module "Reliability and Recovery Capability": This module accounts for the infrastructure's reliability and the recovery capability currently available within the network as well as the design values (goals). Optimal solution is based on design (theoretical) values compared to current values. Information about lack of reliability at each link (for the optimal solution configuration) is given to the decision maker. Reliability allocation is decided after optimal path is found. The following explanation presents the characteristics of the components, as represented in Figure 25:

a. Link Reliability (Rs): Probability that a LINK will perform a required function for a given period of time when used under stated operating conditions (serial configuration of the product of reliabilities of each component in the link).

b. Recovery capability probability (Rr): As a resilient system, timely recovery after disruption is evaluated through a virtual parallel component at each link. This value represents actual resilient behavior which can be improved. This virtual design (Appendix D) combines the advantages of parallel systems (redundancy) with the redundancy on demand (network component performs only when disruption happens). In the Model, "Rr" is Reliability related to "timely recovery" probability. This information comes from two possible sources:

    i. Actual distribution of time elapsed from disruption until the service is recovered to a desirable level to satisfy demands without neither security nor safety issues (Empirical distribution from actual data set).

    ii. Assumed probability for Maintainability. Time involved in recovery process after a disruption: Lognormal distribution (Ebeling, 2005). Lognormal distribution applies to tasks and repair actions comprised of several subsidiary tasks of unequal frequency and time duration; the more complex tasks cause a skew to the right (Jackes, 2009).

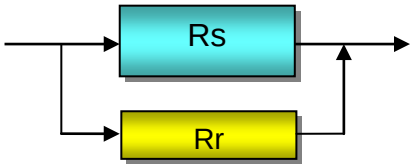


Figure 25. Reliability Configuration at Each Link

3. Module "Pipeline capacity" (constraint- Upper Limit): Contains the link capacity within the network as a constraint. Since actual power networks suffer from capacity degradation (outdated technology, aging transformers, etc), a coefficient ($\alpha < 1$) is added to adjust such theoretical or design value (goal) to actual pipeline capacity availability for energy delivery. When optimal solution is given based on theoretical capacity (goal), the decision maker is given the information to identify those links that need improvement (Only those that have been selected in the optimal solution). Consequently, it will be possible to concentrate the effort on those links that are identified as needing an overall vulnerability reduction (through security allocation). An alternative decision is the elimination of the most vulnerable link/s from the network by setting $\alpha = 0$. This new network configuration model will avoid selecting those undesired links for the optimal solution. Additionally, actual values for pipeline capacity can be set as actual constraint instead of theoretical or design values. In this case, the optimal solution will not require pipeline capacity improvement. This alternative can be used when pipeline capacity is not feasible or desired. However, latest alternative can induce model feasibility issues if pipeline capacity is excessively reduced.

4. Module "Vulnerability configuration": Based on MIL-STD 882D, this module works with both, actual and desired (goal) values of vulnerability in order to identify the vulnerability reduction needed at a specific link, when included in the optimal solution. The model uses:
    a. Vulnerability design (Theoretical value): Is the desired (theoretical) value of vulnerability at each link.
    b. Actual vulnerability value: Related to each link, this information is used to find the vulnerability improvement needed at each link when an optimal solution is found for energy delivery. This set of values needs to be assessed in regards to intentional threats.
5. Module "Pipeline length and number of used links" (optimal solution): Although this information is not used by the Objective Function, link lengths are provided in order to find and to compare total path length (within the power grid) among optimal solutions for alternate scenarios. This is considered as critical information for managerial purposes.
6. Module "Network demand accomplishment" (constraint): This module guaranties that all node demands are satisfied from supply. This is a feasibility requirement performed by the dummy node (Node #5 in Appendix E).
7. Network resilience assessment (index): This module is the model's cornerstone, which synthesizes overall performances assessed within the network in a simple value (between 0~1) for each link and for the entire power grid. This module integrates disaggregated information from network performances (reliability, vulnerability, pipeline capacity and timely recovery probability) into a unique

value of resilience for each of the links (R_i) and other for the entire network (R), for a given scenario. Finally, power network resilience is obtained as the average of all link's resilience. Model integrates resilience index through the whole network with same weight (W=1) for all links (no weighted average).

The referred modules are shown in Appendixes F, G and H

All these modules are identifyied in the Figure 26:

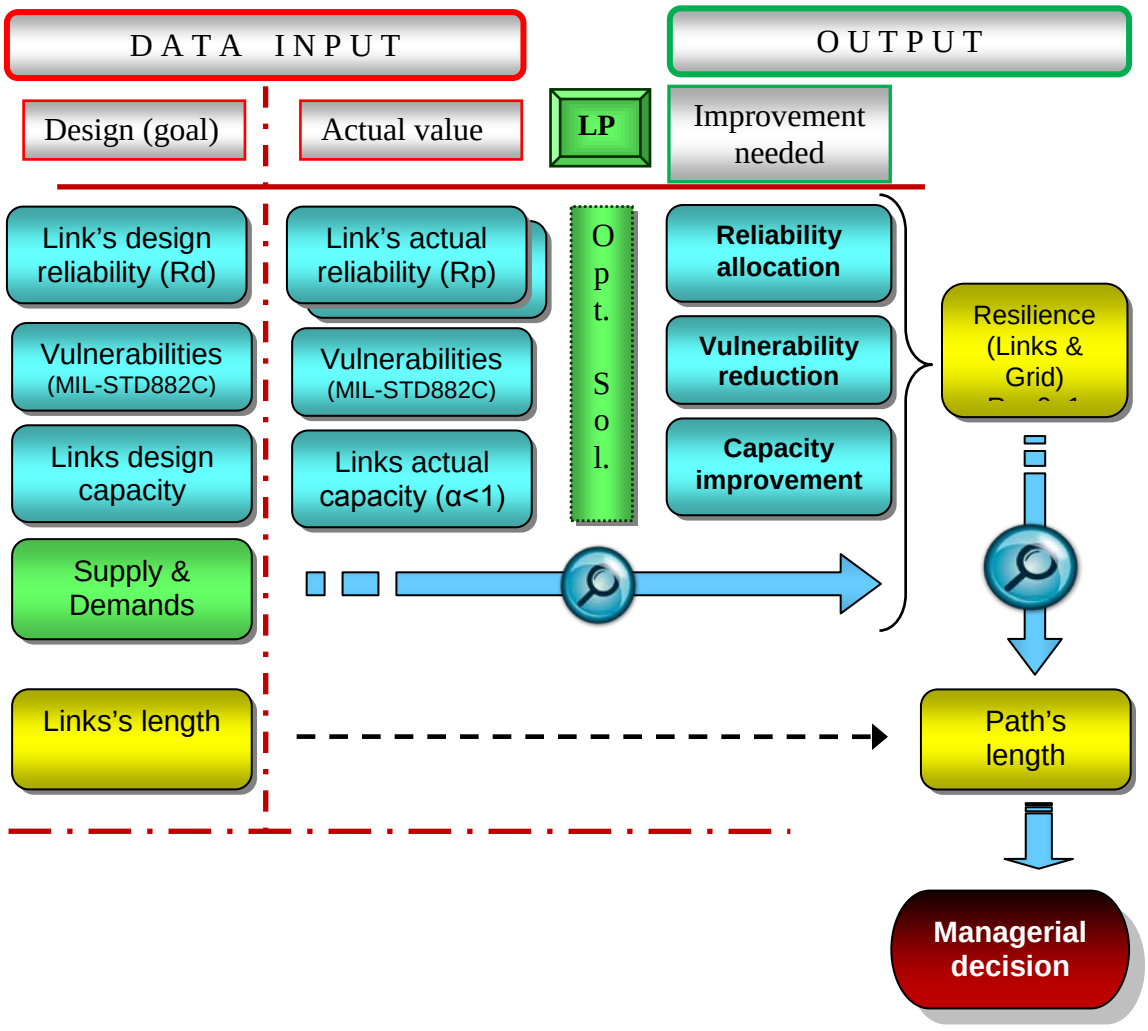


Figure 26. Power Grids's Resilience Assessment Model (Flowchart)

As a corollary, this model provides alternate scenarios in order to let decision makers improve overall performance through reliability increment as well as through security allocation at the more strategic links involved in the optimal solutions. Moreover, the model lets decision makers to fix grid variables such reliability, reduced pipeline capacity or vulnerabilities within the model in order to find optimal solutions that withstand with this kind of issues. Under these circumstances, optimal solution will include the referred restrictions as constraints, and improvement requirements will be focused on those variables or characteristics that decision makers are willing or able to address.

Verification

The purpose of verification is to identify how well the actual model represents the conceptual model on hand.

So, one mean of verification is through addressing changes in the scenario (modeled) in such a way that different outcomes will present alternate ways to improve actual network through for instance, reliability as well as security allocation within the analyzed network. Two basic models were developed for verification purposes:

1. The first model had only 4 nodes (1 supply and 3 demands) and 7 arcs. It was developed and tested for several conditions of reliability.
2. The second model included 7 nodes (1 supply, 1 dummy node and 5 demands) and 13 arcs. This model was also developed and tested for several conditions.

Both basic models were coded in a spreadsheet (Solver®). Same results were obtained through two different procedures (with computer and manually).

Once the basic models were properly verified, their complexities were increased with more nodes and arcs until reach final design of 13 nodes and 27 arcs. Eventually, all resilience drivers were introduced into the model in order to get the final network model.

Once the power network has been assessed and the most critical components identified and ranked, a failure of each component was simulated. Such process was conducted through the six different scenarios where resilience values showed to be consistent with the issues introduced within the networks. Basically, all solutions selected the shorter path available as well as those links that minimizes not only failure probabilities but also vulnerabilities.

Validation

Validation process is conducted against model assumptions and real system behavior. A model validation process including the validation of the assumptions and comparison between model results and real system behavior are considered valuable. Therefore, the purpose of validation is to determine how well the model represents the real system.

Although actual data was required in order to enhance the validity of the model, they were not available. Data required to conduct final validation process of the model was considered restricted information by governmental entities, and hence they were not disclosed. However, model's behavior was consistent with the related theory about networked system, and the resilient performances were identified.

Conclusion

Based on the theory presented in Chapter II, a power network model was developed in order to conduct a quantitative assessment of resilience in power grids.

Critical attributes embedded into the model were: inherent reliability within each link (Rs) calculated as a serial system (source node- arc-destination node), virtual reliability represented by the timely recovery capability (Rr), pipeline capacity constraints, and vulnerability assessment based on the MIL-STD 882D.

Different alternatives were analyzed by running the Model for alternate scenarios and conditions related to network's reliability, vulnerability and pipeline capacity.

A parameterized model for resilience assessment was developed in order to get a quantitative tool that let decision makers to compare among alternate scenarios in strategic management environment. An algorithm embedded within the model can give optimal solutions based on the theoretical or design values for reliability, time to recover, vulnerability and pipe line capacity. In such cases, optimal solutions consider the maximum performance possible, based on theoretical values (design). Likewise, network's attributes can be sequentially fixed in the model when decision maker is not able or willing to address changes on specific variables like reliability, vulnerability or pipeline capacity (for the optimal solution).

Then, the model excludes those links deemed as unnecessary by the optimal solution (labeled as "Unused-Link") and highlights the necessary improvements within the selected path (links configuration). This leads not only to a more feasible decision, but also to a more rational allocation of physical resources as well as security on those links included in the optimal solution for a given scenario.

Finally, path length regarding the optimal solution is given to support managerial decisions in the scenarios comparison process. Thus, a unique resilience value (index), between zero and one (0: not resilient system; 1: full resilient) is used to standardize the resilience assessment process over a wide range of possible scenarios in a more efficient way.

Values of resilience equal to 1 (R=1) do not mean fragility nor robustness. Such values mean that theoretical or desired values (goals) for system's performances have been reached.

The following chapter presents the results and conclusions from the 6 assessed scenarios, the limitations of the developed model, and answers to the research questions what in turn constitute a respond the research's problem.

IV. Results and Analysis

Introduction

This chapter analyses model results under alternate scenarios with different combinations of power network performances. To do so, real world data was used when possible for necessary inputs. The modeled network includes 13 nodes and 27 arcs as shown in Appendix E.

The first scenario was intentionally designed without issues in order to get a baseline to analyze model behaviors against such reference. Likewise, conclusions are given by using the modeling process as a decision making tool.

Supply – Demand Configuration

In order to run the model presented in Chapter III, available information from the DoE was chosen to define generation capacity (Supply) and demand. The parameters are shown in Table 7.

Table 7. Summary Statistics for the United States Electricity Market, 2005 through 2007. (EIA, 2007)

Description	Years		
Demand, Capacity Resources, and Capacity Margins – Summer	**2007**	**2006**	**2005**
Net Internal Demand (megawatts)	764,476	760,108	746,470
Capacity Resources (megawatts)	915,292	906,155	882,125

Based on the DoE's information (Table 7), an annual supply capacity of 915,000 Megawatts is assumed. Demand configuration is presented in the first scenario and needed changes for alternate scenarios are presented for each case. While supply was set based on actual energy capacity, demand was split among the *demand nodes* in the

model. Since the model is "transparent" in terms of units, model design allows for use of different criteria for supply and demand units (model's flexibility).

With supply-demand configurations defined, different scenarios were assessed by making changes in the resilience drivers (reliability, recovery capability, pipeline capacity, and vulnerability).

Since no actual data was obtained to run the alternate scenarios, goals or theoretical performances values were set according to potential situations and kept fixed through all scenarios. Values, referred as "current" were assumed for the first scenario (baseline) and changes were introduced in order to conduct resilient behavior assessment.

Link Pipeline Capacity

Changes in network pipeline capacity were addressed in order to analyze alternate solutions. Pipeline capacity restrictions showed to have important influence on model's feasibility through different scenarios.

Serial Reliability at Each Link (Rs)

As explained in Chapter III, each link is considered as a bundle of ***Source-node***, ***Linking-arc*** and ***Destination-node***. These three elements together form a link as a serial system. Consequently, link reliability is estimated as a serial system of three reliabilities. Therefore, the resulting reliability is lower than the lowest of the component. This work refers to this reliability value as inherent reliability (Rs) within the links.

Link Recovery Capability (Rr)

The Lognormal function representing network performance was selected from reliability theory (Ebeling, 2005:73-77). The arguments are a mean time to recover (mean time to repair) after a disruption and standard deviation. The recovery capability

(Rr) is considered an actual resilient behavior with a probability assumed to be 95.5%. This means that an eventual disruption will be solved within a specific amount of time after a disruption, with a probability of 95.5%.

Designed Reliability at Each Link (Rd)

These values represent the overall reliability goal at each link in order to measure how far each link's performance is from the design or goal value (theoretical value). This value is given for each link as a goal (theoretical value) within the network.

Scenario 1

The first scenario was designed in such a way, that no issues were involved for the optimal solution calculation. Theoretical values (goals) and current values were set as equal. Consequently ideal values of resilience were obtained in all links (R_i=1), and hence in the overall power network (R=1). This first scenario is the baseline. Following values were used:

1. Supply-demand configuration: Total supply was set as equal to total demand in order to met feasibility requirements ➔915,000 Megawatts.
2. Links characteristics:
    a. Inherent reliability (Rs): Equal value for all links ➔ 0.9703.
    b. Recovery capability (Rr) at each link: Equal value for all links ➔ 0.955.
    c. Reliability at each link (Rp): Obtained as a parallel system (Rs, Rr). Solving such parallel system gave Rp = 0.998663 for all links.

d. Designed Reliability (Rd: goal): Set as equal to Rp (Rd=Rp=0.998663).

3. Vulnerability in the power network was considered separately for the trunk (principal) links (1-2, 1-3 and 1-4) and secondary links. Secondary links are all others except the links that connect the Supply node (Node # 1) to the dummy or virtual node (Node #5):
    a. Current vulnerability values (Vc) were set as equal to Designed (Vd=goal). Vc=Vd=3 (acceptable without review, according to MIL-STD 883D).
4. Pipeline capacity was separately considered for the trunk (principal) links (1-2, 1-3, and 1-4) and for secondary links. Secondary links are all others except the links that connect the supply node (Node # 1) to the dummy or virtual node (Node #5):
    a. Capacity at the Trunk links ➔ 500,000 Megawatts (MW).
    b. Capacity at the secondary links ➔ 500,000 Megawatts (MW).
5. Distance between nodes or link's lengths. Although these values are critical for vulnerability assessment, this work takes into account these values in order to include the total path length for the decision making environment. All distance values were set to 100 miles.

Results

Since all design (goal) values for inherent reliability (Rs), recovery capability (Rr) and vulnerability (Vc) were set as equal to current values (specifically for this model), no issues affecting resilience were found. This result supports the model verification, and a unit value for resilience was obtained. Numerical results are summarized as follows:

1. Total network resilience → 1; (R=1)
2. Objective function value (OF) → 9.064
3. Number of used links → 11
4. Total pipeline length → 1100 Miles.

The unit value for Resilience (R=1) is a consequence of no restrictions or issues in the model (baseline model). The baseline model is used in order to assess model's behavior by progressive changes of inherent reliability, recovery capability, vulnerability and pipeline capacity. The result presents the shortest path to satisfy all demands within the power network. Table 8 presents the resilience values for all links selected in the optimal solution.

Table 8. Resilience Values Throughout the Network for Scenario 1

Links		Resilience components (Sc.1)		
#	(i - j)	$R_{(Capacity)}$	$R_{(Reliability)}$	$R_{(Vulnerability)}$
1	(1-2)	1	1	1
2	(1-3)	1	1	1
3	(1-4)	1	1	1
4	(2-6)	1	1	1
5	(3-10)	1	1	1
6	(4-11)	1	1	1
7	(6-7)	1	1	1
8	(7-8)	1	1	1
9	(9-12)	1	1	1
10	(10-9)	1	1	1
11	(12-13)	1	1	1

Figure 27 shows the results, where all resilient attributes are equal to 1. Consequently, power network resilience value was also 1 (the maximum possible value). This makes sense because the goals were reached for all performances that make the system resilient. No values higher than 1 can be obtained for resilience assessment. However, if resilience values greater than 1 are obtained, they would imply wasting of resources.

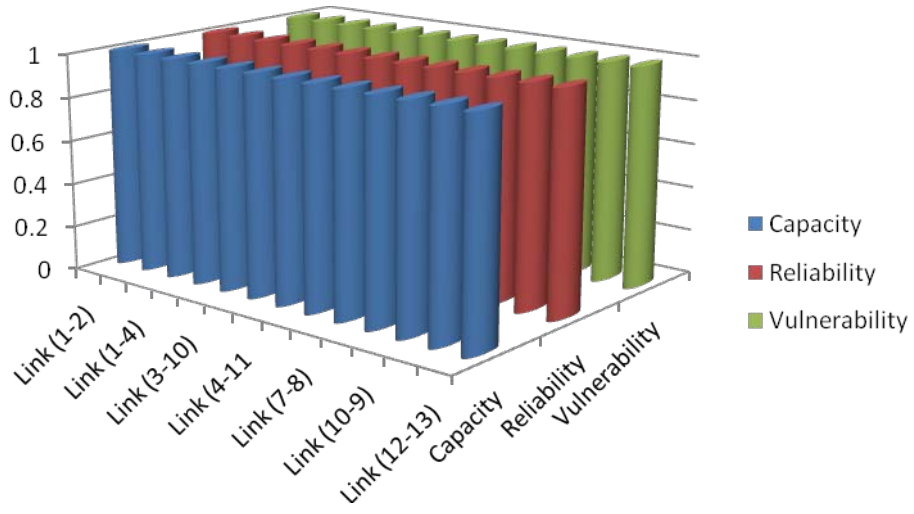


Figure 27. Graphic Representation (bars) of Resilience Components in Scenario 1

Likewise, Figure 28 shows an alternative graphic representation (radar) of resilient behavior within the network. This graph shows the superposition of the three curves that represent resiliencies (all values equal to 1).

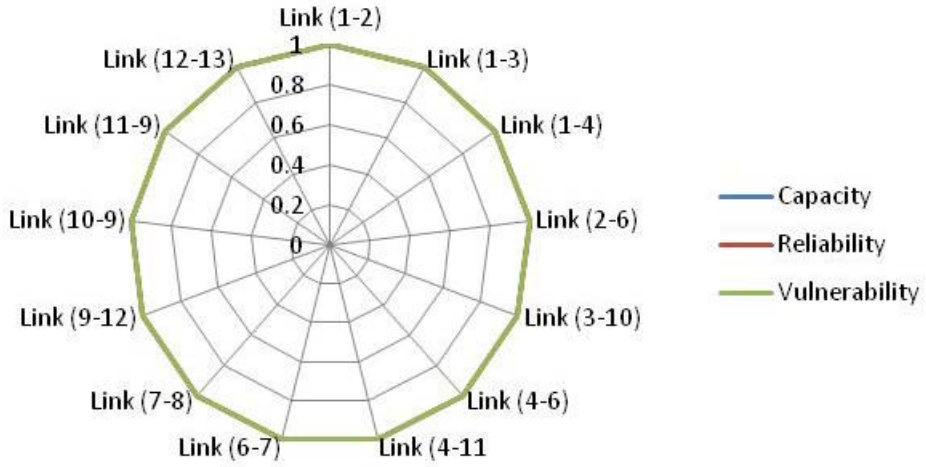


Figure 28. Graphic Representation (radar) of Resilience Configuration in Scenario # 1

Scenario 2

The second scenario incorporates restrictions addressed by the model in order to find an optimal solution. Consequently more realistic values of resilience were obtained for the links, and hence in the overall power network. Following values were used:

1. Supply-demand configuration: Total supply was set as equal to total demand in order to met feasibility requirements ➔915,000 MW.
2. Link's characteristics:
    a. Inherent reliability (Rs): Equal for all links ➔ 0.9703
    b. Recovery capability (Rr) at each link: Equal for all links ➔ 0.955
    c. Reliability at each link: Obtained as a parallel system (Rs, Rr). Rp = 0.998663 for all links.
    d. Designed reliability (Rd: goal): Set as equal to Rp (Rp=Rd=0.998663).

3. Vulnerability in the power network was considered separately for the trunk (principal) links (1-2, 1-3 and 1-4) and for secondary links. Secondary links are all others except the links that connect the supply node (Node 1) to the dummy or artificial node (Node 5):
    a. Current Vulnerability values (Vc) equaled designed vulnerability (Vd: goal). Vc=Vd=3 (acceptable without review, according to MIL-STD 883D) for all links within the power network.
4. For this scenario, ***actual*** pipeline capacities were reduced by applying an efficiency coefficient ($\alpha<1$), reducing the capacity available for the optimal solution:
    a. Capacity at the Trunk links ➔ 350,000 x 0.9 = 315,000 MW.
    b. Capacity at the secondary links ➔ 200,000 x 0.9 =180,000 MW.
5. Distance between nodes or link's length. All distance values equaled to 100 miles.

Results

For the second model, the optimal solution included a longer path (more links were used). Numerical results are summarized as follows:

1. Total network resilience → R = 0.992
2. Objective function value (OF) → 9.064
3. Number of used links → 13
4. Total pipeline length → 1300 miles.

The resilience value below 1 is a consequence of pipeline capacity restrictions in the model. Although this model is still a simple one, Figures 29 and 30 show how power

network resilience is composed from inherent reliability (Rs), recover capability (Rr) and pipeline capacity. Restrictions in pipeline capacity result in a longer path, compared to scenario 1. Table 9 presents the resilience values for all links selected in the optimal solution.

Table 9. Resilience Values Throughout the Network for Scenario 2

Links		Resilience components (Sc.2)		
#	(i - j)	$R_{(Capacity)}$	$R_{(Reliability)}$	$R_{(Vulnerability)}$
1	(1-2)	1	1	1
2	(1-3)	1	1	1
3	(1-4)	0.940	1	1
4	(2-6)	0.900	1	1
5	(3-10)	0.900	1	1
6	(4-6)	1	1	1
7	(4-11)	0.947	1	1
8	(6-7)	1	1	1
9	(7-8)	1	1	1
10	(9-12)	1	1	1
11	(10-9)	1	1	1
12	(11-9)	1	1	1
13	(12-13)	1	1	1

Figure 29 shows how pipeline capacity restrictions affect overall grid resilience.

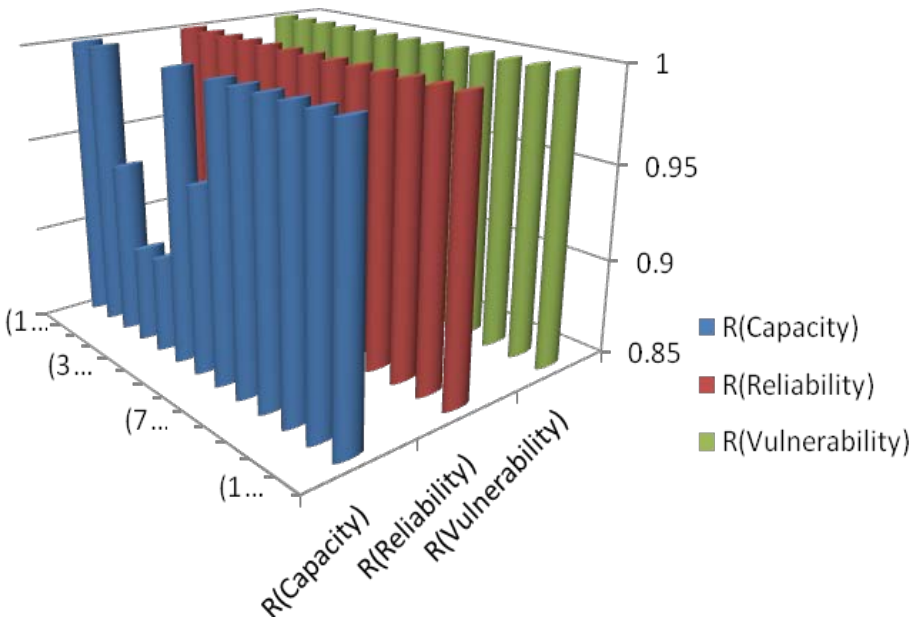


Figure 29. Resilience Components in Scenario 2

Figure 30 shows how each resilience issues affect grid resilience. Reduced pipeline capacity configuration forces the use of an alternate path to supply the energy at all nodes. This graph shows where capacity improvement is needed in order to reach higher resilience value (Links: 1-4, 2-6, 3-10 and 4-11). If no pipeline capacity improvements are addressed, such physical restrictions in capacity could prevent proper energy delivery from the source-node (node 1) to all demand-nodes.

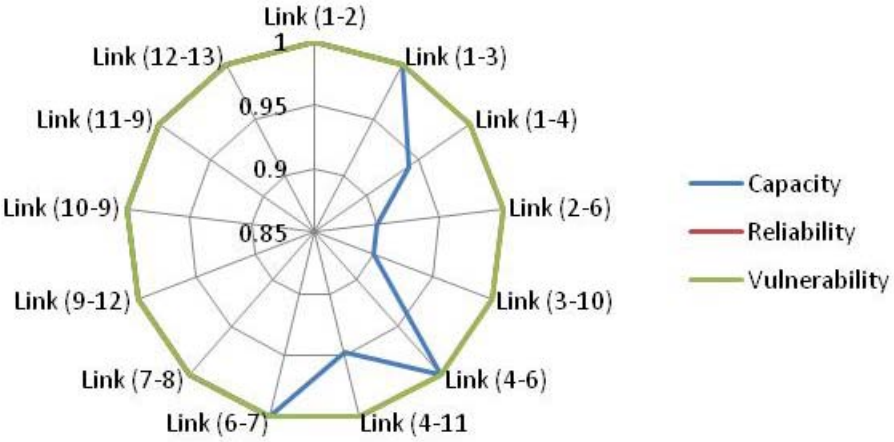


Figure 30. Resilience Configuration in Scenario 2

Neither reliability nor recovery capability issues were found. This scenario still meets theoretical performances in such areas and hence a maximum value of resilience was reached.

Scenario 3

The third scenario investigates increased number of restrictions to the model. Consequently more realistic values of resilience are obtained in all links and overall power network. Following values were used:

1. Supply-demand configuration: Total supply was set at 915,000 Megawatts (MW) while total demand was set at 930,000 Megawatts (MW). The demand in node 13 was increased by 15,000 MW with respect to the Scenario 2. Consequently $\sum S < \sum D$.
2. Links characteristics:
    a. Inherent reliability (Rs): Equal for all links ➔ 0.9703
    b. Recovery capability (Rr) at each link: Equal for all links ➔ 0.955

c. Reliability at each link: Obtained as a parallel system (Rs, Rr). Solving these two values gave Rp = 0.998663 for all links.

d. Designed Reliability (Rd: goal): Set as equal to Rp (Rp=Rd=0.998663).

3. Vulnerability in the power network configuration was considered the same as Scenario 1:

    a. Current Vulnerability values (Vc) were set as follows:

        i. Vc=3 for Links 1-2; 1-3 and 1-4 (trunk links).

        ii. Vc=15 for Link 2-6 (longer link).

        iii. Vc=5 for all others links in the network.

    b. Designed vulnerability (Vd=goal) was set as Vd=3 (acceptable without review, according to MIL-STD 883D).

4. Pipeline capacity. Like in Scenario 2, pipeline capacity configuration was reduced by the use of an efficiency coefficient (α= 0.9), reducing the design capacity as follows:

    a. Capacity at the trunk links ➔ 350,000 x 0.9 = 315,000 MW.

    b. Capacity at the secondary links ➔ 200,000 x 0.9 = 180,000 MW.

5. Distance between nodes or link's length. All distance values were set equal to 100 miles, except link 2-6 (200 miles). This value is justifies its vulnerability.

Results

Optimal solution included a longer path than in Scenario 2 (more links were used) and the resilience value was lower than the previous scenario for the optimal solution. Numerical results are summarized as follows:

1. Total network resilience → R = 0.8762
2. Objective function value (OF) → 9.38485
3. Number of used links → 14
4. Total pipeline length → 1500 Miles.

This lower resilience value is a consequence of the pipeline capacity restrictions as well as the vulnerability increment. Table 10 shows how reliability and capacity restriction have direct impact in overall resilience performance.

Table 10. Resilience Values Throughout the Network for Scenario 3

Links		Resilience components (Sc.3)		
#	(i - j)	$R_{(Capacity)}$	$R_{(Reliability)}$	$R_{(Vulnerability)}$
1	(1-2)	1	1	1
2	(1-3)	1	1	1
3	(1-4)	0.9	1	1
4	(2-6)	0.9	1	0.2
5	(3-10)	0.9	1	0.6
6	(4-6)	1	1	0.6
7	(4-11	0.9	1	0.6
8	(6-7)	1	1	0.6
9	(7-8)	1	1	0.6
10	(8-12)	1	1	0.6
11	(9-12)	1	1	0.6
12	(10-9)	1	1	0.6
13	(11-9)	1	1	0.6
14	(12-13)	1	1	0.6

Additionally, Figures 31 and 32 show how pipeline capacity and vulnerability's increment, impact the overall power network resilience. Since no issues related to either inherent reliability (Rs) or recovery capability (Rr) were added to this scenario, power network resilience was not affected by such performances. Higher vulnerabilities values made the total path's length to be longer (1500 miles) compared to scenarios 1 and 2.

Restrictions in pipeline capacity and vulnerabilities issues resulted in a lower resilience value for this scenario compared to scenarios 1 and 2.

Figure 31 shows how the vulnerability growth in link 2-6 as well as capacity restrictions affect the power network resilience.

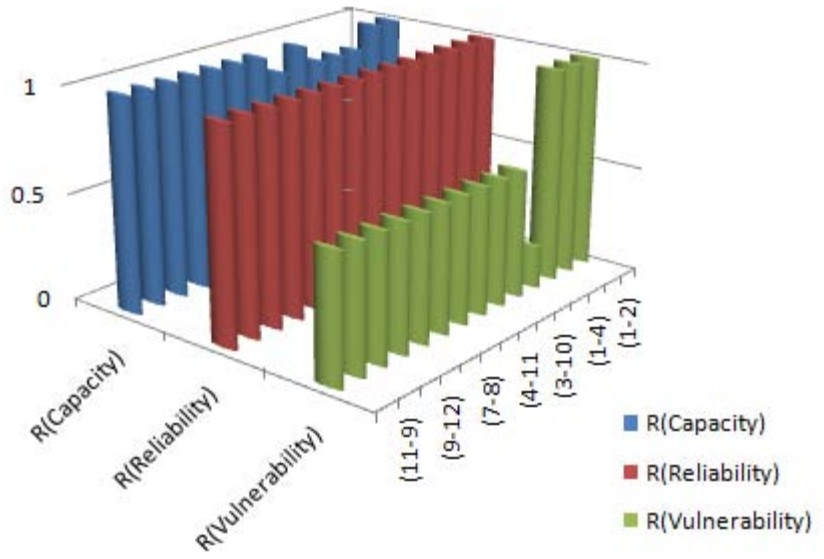


Figure 31. Resilience Components in Scenario 3

On the other hand, Figure 32 shows how each resilience issues affect grid's resilience. Reduced pipeline capacity forces the use of alternate path to supply the energy at all nodes. These graphs indicate where capacity improvement is needed in order to reach higher resilience value (Links: 1-4, 2-6, 3-10 and 4-11). If no pipeline capacity improvements are addressed, resilience value will be the one that was estimated for this scenario. However, physical restrictions in pipeline capacity could prevent proper energy delivery from source-node (node 1) to all demand-nodes.

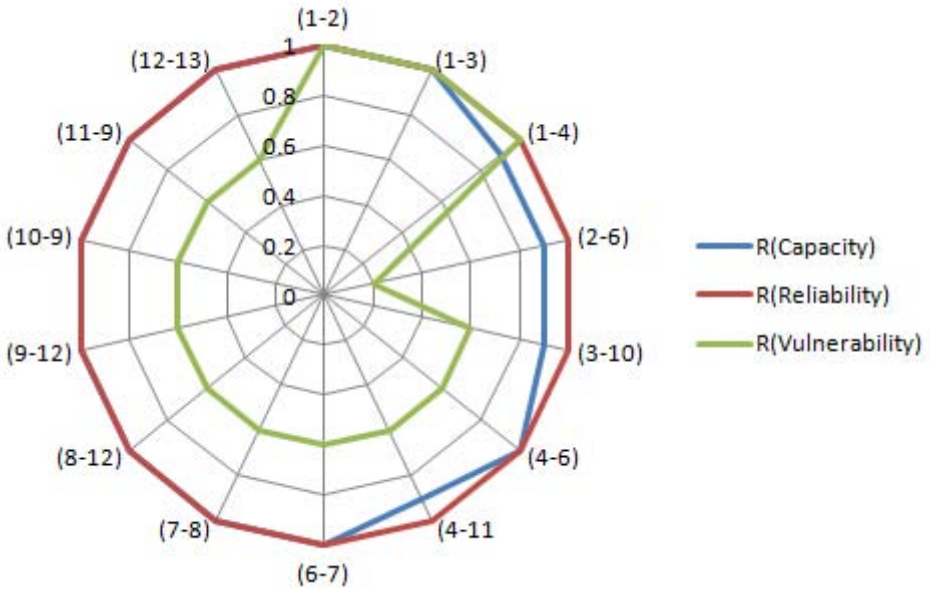


Figure 32. Resilience Configuration in Scenario 3

Since no issues were found regarding reliability or recovery capability (red line in Figure 32), this model still meets theoretical performances in such areas and hence maximum value of resilience was reached for such scenario's attributes. However vulnerability reduction is required in eleven links. Since Vd=Vc for the trunk links, no vulnerability issues were found in these links. Pipeline capacity improvement is needed in four links (1-4; 2-6; 3-10 and 4-11).

Scenario 4

The fourth scenario was modeled as a particular case of the scenario 3. Basically, the same network's characteristics were incorporated in this model. Additional restrictions related to pipeline capacity configuration were introduced for the optimal solution calculation process . The main distinctive characteristic in this scenario is related to pipeline capacity constraint. For this scenario, flow through each link should

be less or equal to "actual" pipeline capacity at each link (theoretical value reduced by α=0.8). This scenario attempted to look for optimal solution without addressing improvements in pipeline capacity.

Results

Since the pipeline capacity configuration limited the physical possibility to deliver the needed energy through all links, this scenario resulted in an unfeasible solution.

The conclusion for this scenario is that improvement in pipeline capacity is required before assessing other network's attributes. Such improvement can be introduced (simulated) into the model, through progressive increments in efficiency's values (α).

Scenario 5

The fifth scenario introduces an increased number of restrictions to be addressed by the model (for the optimal solution calculation). Consequently even more realistic values of resilience were obtained in all links, and hence in the overall power network. Values for network inherent reliability configuration (Rs) were reduced, while recovery capability (Rr) remained unchanged. Likewise, energy supply has been increased causing an excess of supply to appear within the model. Following values were used:

1. Supply-demand configuration: Total supply was set at 1,100,000 MW, while total demand was set 915,000 MW. Consequently $\sum S > \sum D$.
2. Link's characteristics:
    a. Inherent reliability (Rs) was reduced from 0.9703 (0.95 x 0.95 x 0.95 = 0.9703) to 0.8574 (0.95 x 0.95 x 0.95 = 0.8574) for all links.

b. Recovery capability (Rr) at each link is the same value (Rr=0.955) for design as well as for actual values in the model. So, there were no issues regarding this performance.

c. Resulting resilience value at each link (Rp) was obtained as a parallel system (Rs, Rr). Solving this parallel system in each link, gave Rp = 0.99358 for all links.

d. Designed Reliability (Rd: goal) was set as Rd=0.998663. Hence, Rd>Rp for this scenario.

3. Vulnerability in the power network is the same as Scenario 3:

    a. Current vulnerability values (Vc) were set as follows:

        i. Vc=3 for Links 1-2; 1-3 and 1-4 (trunk links).

        ii. Vc=15 for Link 2-6 (longer link and highest vulnerability).

        iii. Vc=5 for all others links in the network.

    b. Designed vulnerability (Vd=goal) was set as Vd=3 (acceptable without review, according to MIL-STD 883D).

4. Pipeline capacity. Same as scenario 2. An efficiency coefficient (α= 0.9) was applied to the pipeline capacity configuration, reducing the design capacity:

    a. Capacity at the trunk links ➔ 350.000 x 0.9 = 315.0.00 MW.

    b. Capacity at the secondary links ➔ 200.000 x 0.9 = 180.000 MW.

5. Distance between nodes or link's length. All distance values were set equal to 100 miles, except link 2-6 (200 miles).

Results

For this scenario, the optimal solution included 13 links. Numerical results are summarized as follows:

1. Total network resilience → R = 0.8775
2. Objective function value (OF) → 9.064
3. Number of used links → 13
4. Total pipeline length → 1400 miles.

This lower resilience value (compared to the first scenario) is a consequence of pipeline capacity restrictions as well as vulnerabilities and reliabilities issues that were introduced in this scenario. Table 11 shows resilience components values.

Table 11. Resilience Values Throughout the Network for Scenario 5

Links		Resilience components (Sc.5)		
#	(i - j)	$R_{(Capacity)}$	$R_{(Reliability)}$	$R_{(Vulnerability)}$
1	(1-2)	1	0.99491	1
2	(1-3)	1	0.99491	1
3	(1-4)	0.9403	0.99491	1
4	(2-6)	0.9	0.99491	0.2
5	(3-10)	0.9	0.99491	0.6
6	(4-6)	1	0.99491	0.6
7	(4-11)	0.94737	0.99491	0.6
8	(6-7)	1	0.99491	0.6
9	(7-8)	1	0.99491	0.6
10	(9-12)	1	0.99491	0.6
11	(10-9)	1	0.99491	0.6
12	(11-9)	1	0.99491	0.6
13	(12-13)	1	0.99491	0.6

Figures 33 and 34 show how pipeline capacity and vulnerability increment impact in the overall power network's resilience. Additionally, although reliability improvements are needed in those links that were selected for the optimal solution path,

the impact is almost imperceptible (Figure 34). This is because the recovery capability (Rr) in parallel with link's inherent reliability (Rs) let the overall reliability (Rp) within each link to be still high. This complex scenario results in a length path of 1500 miles. Likewise, impacts of high value of vulnerability in the link 2-6, as well as capacity restrictions affect the power network resilience.

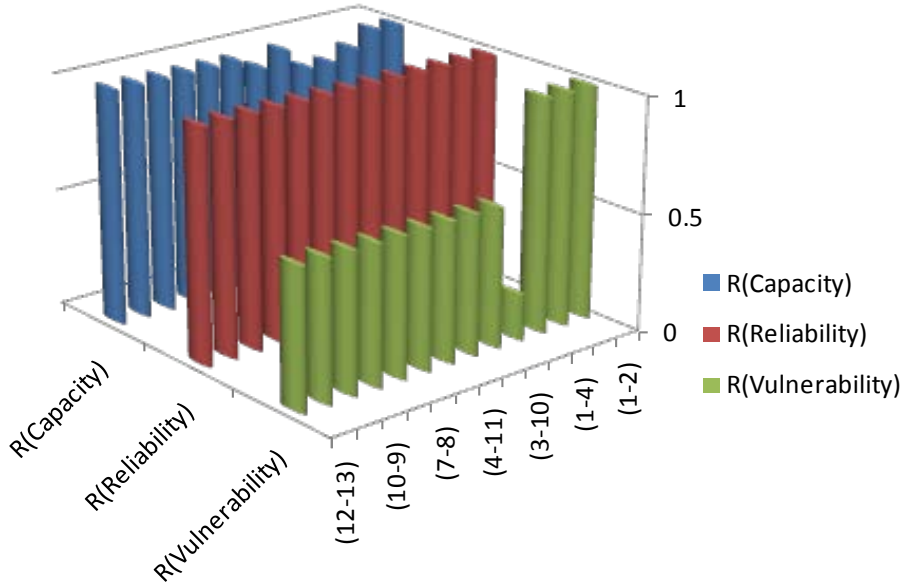


Figure 33. Resilience Components in Scenario 5

Figure 34 shows how each resilience issue (pipeline capacity, vulnerability and link's inherent reliability) affect grid resilience. Reduced pipeline capacity and the high vulnerability value in link 2-6 force the use of an alternate path to supply the energy at all nodes producing the path to be longer. Although reliability improvement is needed in all links, included in the optimal solution, these graphs clearly indicate where capacity improvement and vulnerability reduction are needed in order to reach a higher resilience value. Since pipeline capacity issues imply physical limitation to deliver energy, improvement in the involved links are required. Once such physical restrictions have

been addressed, resilience values are directly related to the strategic management decisions about risk acceptance.

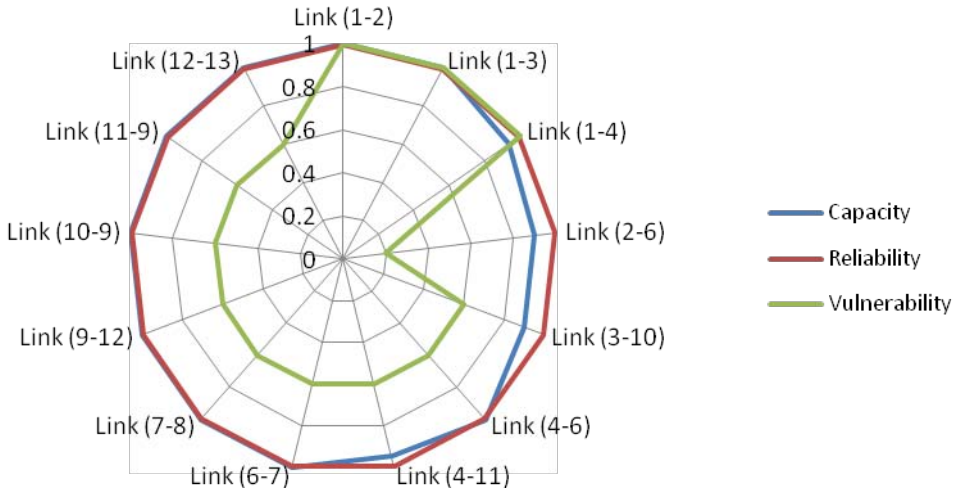


Figure 34. Resilience Configuration in Scenario 5

No issues were found regarding recovery capability, because this model still meets theoretical performances in that area and hence maximum value of resilience was reached for this attribute. However link's inherent reliability (Rs) configuration needs to be improved and vulnerability reduction is required. Since Vd=Vc for the trunk links, no vulnerability issues were found in theses links. Since pipeline capacity configuration is coincident with Scenario 3, improvement is needed for the same four links (1-4; 2-6; 3-10 and 4-11).

Reliability configuration, representing inherent reliability (Rs) and recover capability (Rr) contribute to power network resilience as a parallel system (Rp), reliability issues can be addressed in two possible ways:

1. Improving inherent reliability within the links (Rs), or

2. Reducing variability or time to recover for the recover capability (Rr) (assumed to be lognormal distributed).

Finally, the excess of energy modeled in this scenario (balanced by node #5) represents real world situation. Currently there is no way to store such energy; it is normally used for instance, to generate potential energy to run hydraulic turbines when demand increases.

Scenario 6

The main characteristic in this scenario is the use of more conservative values to represent inherent reliability and recovery capability. In this case, these variables are considered as fixed, and hence, resilience improvement should be addressed by improving pipeline capacity and reducing vulnerabilities. To do so, the objective function was modified by changing the values of design reliability (Rd) by the modeled actual values (Rp as function of Rs and Rr). Additionally, inherent reliability at link 2-6 was reduced from $Rs_{(2-6)}$=0.8574, to $Rs_{(2-6)=}$0.4219, that is approximately 50%. Consequently more conservative values of network's resilience were modeled. Likewise, energy supply is increased causing a excess of supply within the model. Following values were used:

1. Supply-demand configuration: Total supply was set as 1,100,000 MW while total demand was set 915,000 MW. Consequently $\sum S > \sum D$.
2. Links characteristics:
    a. Inherent reliability (Rs) was reduced from 0.9703 (0.95x0.95x0.95 = 0.9703) to 0.8574 (0.95x0.95x0.95 = 0.8574) for all links except link

2-6, whose value was reduced in a higher amount ($Rs_{(2-6)=}$ 0.75x0.75x0.75 = 0.4219).

b. Recovery capability (Rr) at each link is set with the same value (Rr=0.955) for design as well as for actual values in the model. So, there are no issues regarding to this attribute.

c. Hence, resulting resilience value at each link (Rp) was obtained as a parallel system (Rs, Rr). Solving this parallel system in each link, the overall reliability was obtained as Rp = 0.99358 for all links, except for link 2-6 whose value was $Rp_{(2-6)}$=0.97397.

d. Designed reliability (Rd: goal). Same value of designed reliability was set for all links (Rd=0.998663). Not considered for optimal solution calculation but for resilience estimation.

3. Vulnerability in the power network: same as in Scenario 5:

    a. Current vulnerability values (Vc) were set as follows:

        i. Vc=3 for Links 1-2; 1-3 and 1-4 (trunk links).

        ii. Vc=15 for Link 2-6 (longer link and highest vulnerability).

        iii. Vc=5 for all others links in the network.

    b. Designed vulnerability (Vd=goal) was set as Vd=3 (acceptable without review, according to MIL-STD 883D).

4. Pipeline capacity: Same as Scenario 2. An efficiency coefficient (α= 0.9) was applied to the pipeline capacity configuration, reducing the design capacity:

    a. Capacity at the trunk links ➔ 315,000 MW.

    b. Capacity at the secondary links ➔ 180,000 MW.

5. Distance between nodes or links length. All distance values were set equal to 100 miles, except link 2-6 (200 miles).

Results

Numerical results are summarized as follows:

1. Total network resilience → R = 0.8601
2. Objective function value (OF) → 48.86
3. Number of used links → 15
4. Total pipeline length → 1600 miles.

The relevant reduction in Rp in link 2-6 reduced the amount of energy to be delivered from 200 MW (Scenario 5) to only 45 MW for current scenario.

This scenario resulted in the lowest resilience value among all modeled scenarios as a consequence of pipeline capacity restrictions as well as vulnerabilities and reliabilities issues introduced for this scenario. Table 12 shows the resilience configuration for each link.

Table 12. Resilience Values throughout the Network for Scenario 6

Links		Resilience components (Sc.6)		
#	(i - j)	$R_{(Capacity)}$	$R_{(Reliability)}$	$R_{(Vulnerability)}$
1	(1-2)	1.000	0.995	1.000
2	(1-3)	1.000	0.995	1.000
3	(1-4)	0.900	0.995	1.000
4	(2-4)	1.000	0.995	0.600
5	(2-6)	1.000	0.975	0.200
6	(3-10)	0.900	0.995	0.600
7	(4-6)	0.900	0.995	0.600
8	(4-11)	0.900	0.995	0.600
9	(6-7)	1.000	0.995	0.600
10	(7-8)	1.000	0.995	0.600
11	(9-8)	1.000	0.995	0.600
12	(9-12)	1.000	0.995	0.600
13	(10-9)	1.000	0.995	0.600
14	(11-9)	1.000	0.995	0.600
15	(12-13)	1.000	0.995	0.600

Figures 35 and 36 show how pipeline capacity and vulnerability impact the overall resilience of the power network. Additionally, although reliability improvements are suggested for this scenario (for those links that were selected for the optimal solution path), the optimal solution was addressed considering Rp as unchangeable. Nevertheless, the impact of reliability issues is almost imperceptible despite the low value for inherent reliability in link 2-6 ($Rs_{(2-6)}$=0.4219 (Figure 36). This is because the recovery capability (Rr) is combined in a parallel system with link inherent reliability (Rs) resulting in overall reliability (Rp) that is still high (Rp=0.97397). This is relevant to improve resilience through recovery capability (Rr) instead of improving three hard elements within the link (source-node, arc and destination-node), which are serially related.

Figures 35 and 36 show the high value of vulnerability in the link 2-6 as well as how capacity restrictions affect the power network resilience.

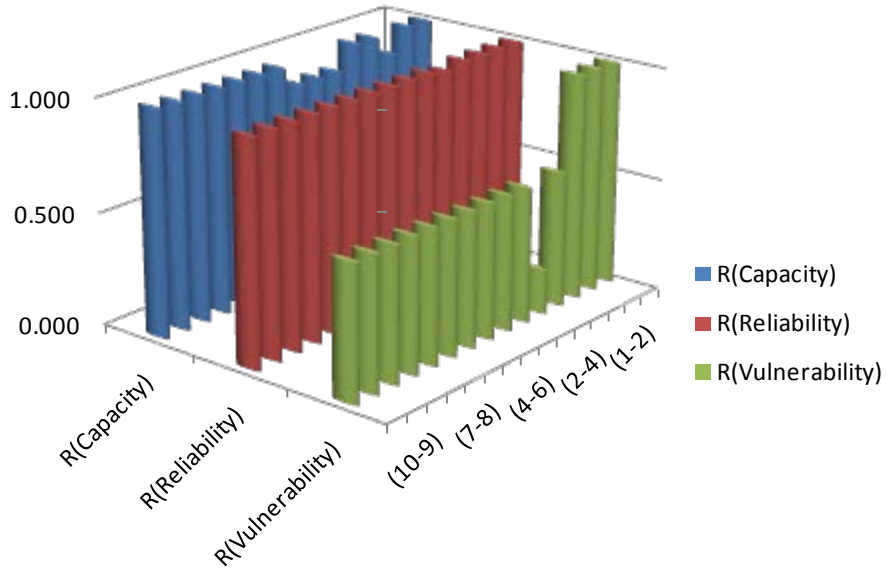


Figure 35. Resilience Components in Scenario 6

Figure 36 shows how each resilience issue (pipeline capacity, vulnerability and links inherent reliability (Rs)) affect grid resilience. Link 2-6 is the most vulnerable within the grid. Reduced inherent reliability (Rs) and the high vulnerability value in link 2-6 force the use of an alternate path to supply the energy at all nodes.

Considering that reliability improvement was assumed as no feasible (criterion), these graphs clearly indicate where capacity improvement and vulnerability reduction are needed in order to reach higher resilience values. Pipeline capacity issues imply physical limitation for energy delivery. Improvement in the involved links is required.

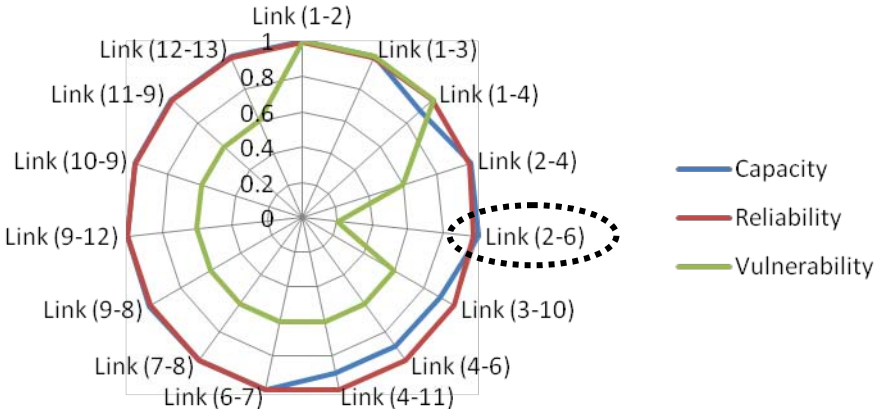


Figure 36. Resilience Configuration in Scenario 6

This scenario meets theoretical performances, no issues were found regarding recovery capability (Rr) performance. However inherent link reliability configuration should be improved and vulnerability reduction is required. Since Vd=Vc for the trunk links, no vulnerability issues were found in theses links. As occurred in scenarios 3 and 5, vulnerability reduction is needed in link 2-6. Additionally, pipeline capacity improvement is needed in the links 1-4; 3-10, 4-6 and 4-11.

In the same way, the optimal solution's path (architecture) was affected by the reliability values. Vulnerability configuration would affect potential optimal solution if grid attributes were considered within the objective function.

Finally, the excess of energy modeled in this scenario (balanced by node #5) represents a situation of the real world. Currently there is no way to store such energy, it is normally used to generate potential energy to run hydraulic turbines when demand increases, and peaks in demands stress the power network.

Answers to the Research Questions

According to the aforementioned concepts and scenario analysis's results, we answer the research questions presented in Chapter I, what in turn present an affordable answer for the overall problem regarding the quantitative assessment of resilience in power grids.

1. How can be resilience defined for power grids?

    - As stated in Chapter II, in defining resilience, it is necessary to focus on the functions or performance that a system is designed to fulfill, and not the individual components of the system or network under study. This holistic standpoint recognizes the complexity involved in resilient systems. Therefore, the following definition is presented for resilience in power grids: **Resilience in power grids is defined as their capability to cope with adversity arising from intentional and unintentional threats and to recover in a timely manner to an acceptable level (new equilibrium) of performance after have been stressed.** Additionally, since vulnerability has been closely related to intentional attacks, its minimization should be addressed through security allocation.

2. What attributes are relevant to a resilient power grid behavior? Are they quantifiable?

    - Based on previous researches and criteria found in Chapter II, the following attributes were identified as relevant to a resilient power grid behavior:

        a. Reliability.

        b. Timely recover capability (Also defined as "rapidity").

        c. Vulnerability.

        d. Pipeline capacity.

    - Since management requires variables to be measured, relevant attributes were identified as actual drivers of resilience in power grids. Additionally, their measurements were parameterized for resilience assessment in power grids as a particular case of SCM.

3. How should attributes involved in power grids performance be embedded within a resilience assessment model, in order to have a quantitative (objective) and comparable measurement?

    - Chapters II, III and IV present theoretical support and implementation process for resilience assessment through model development. The parameterization of resilience drivers was the mean to integrate, originally heterogeneous variables into a unique homogenous index (R) for alternate scenario analysis.

4. Does a Linear Programming Model provide quantifiable information to support decision making processes with respect to resilience in power grids?

    - From previous researches as well as from the specific theory regarding Linear Programming, it was found LPM as a valid quantitative tool to address resilience assessment in networked systems. Likewise, it showed to be useful also for resilience assessment in power networks as a particular case of SCM.

5. What is the necessary data to solve a model of the problem under study?

    - The necessary data to solve a model are:

        a. Design or desired values (goal) for power grid infrastructure's reliability (Given for each link).
        b. Design or desired value of (goal) probability for Time to Recover when a link goes down.
        c. Design or acceptable values (goal) for power grids's vulnerability, coded according to the MIL-STD-882D.
        d. Design or desired value (goal) for electricity transmission capacity (analog to pipeline capacity).
        e. Current values for the previous variables.

Summary

Current resilient assessment model merges a broad power network's characteristics that let the managers not only learn from the past (reliability) but also to prevent critical damages to the grid (identified through its vulnerability configuration) throughout a more accurate and efficient security allocation.

Pipeline capacity has been included into the model as a constraint to ensure feasibility. It also has played an active role in the tradeoff between finding a feasible optimal solution in terms of resilience and shortest feasible path. Results are consistent in that they show a direct relationship between high values of resilience and shortest path for optimal solution. Although distances between nodes are not directly considered in the resilience assessment model, such measures are actually embedded in vulnerability assessment process and constitute useful information for strategic decision makers.

Likewise, sensitivity analysis was addressed in order to study of the impact that changes in one or more resilience attributes embedded within the model have on overall network resilience. As expected, it showed that the design (model) is more sensitive to vulnerability and pipeline capacity issues than reliability issues within the network (between nodes). This is a consequence of the virtual parallel system that keep high values of reliability by combining both, actual reliability within each link and the recovery capability. Therefore, resource allocation can be more efficiently improved in two complementary ways:

1. Focusing effort on those links belonging to the optimal solution configuration (path).

2. Maximizing the security allocation effort on those links or nodes that show undesirable or unacceptable vulnerability levels, base on the MIL-STD 882D.

However, model flexibility lets decision makers to fix grid's variables such reliability, reduced pipeline capacity or vulnerabilities within the model in order to find optimal solutions that withstand with such restrictions. As result, optimal solutions will include the referred restrictions as constraints, and improvement requirements will be focused only on those variables or characteristics that decision makers are willing or able to effectively address.

Finally, answer to the research questions were presented, what in turn gives a comprehensive response to the overall problem referred in the first chapter.

V. **Conclusions**

Introduction

This chapter presents the summary, potential limitations of the developed model (to assess power networks' resilience), and possible areas of interest are also presented.

As presented in Chapter II, typical transmission line capacities are a function of the line voltage, number and size of the wires, and the distance over which the power is being transmitted (links). Since results in this work have consistently shown a direct relationship between high values of resilience and shortest path for optimal solution, such optimal power network configurations are considered as leading actual power grids capability improvement.

Research Summary

This thesis was developed upon the strategic importance that power grids, as critical infrastructure have for the US.

It was found that power grids's basic characteristics are shared with the Supply Chain Management and other areas of expertise as well. Hence, cross-functional analysis was conducted including theoretical research about resilience's scope in different fields. Then, common attributes shared by resilient systems were identified and power grids were considered as a particular case of Supply Chain Management. Therefore, a resilience model was proposed in order to develop a decision tool to assess power grids' resilience, toward the strategic energy management.

Since model development requires specific frame to ensure validity, assumptions and limitations were presented, including those for specific scenario analysis.

Although networked systems, like SCM, are vulnerable to intentional as well as unintentional threats, power networks' functionality constitutes a cornerstone for networked critical infrastructures.

Chapter III covered the theoretical foundations for the methodology used for model development and Chapter IV included the results interpretation, answers for the research questions and preliminary conclusions.

Managerial Implications

This work lets decision makers bring heterogeneous attributes from power grids into a more quantifiable and comparable arena. This allows easy comparison of alternate scenarios in terms of resilience during the decision making process. Ultimately, more objective decisions will support strategic power grids management as a particular critical infrastructure.

Resilience has been found to be function of Reliability, Recovery capability, Vulnerability and Pipeline Capacity, embedded within the power grids (R=***f*** [Reliability, Recovery Capability, Vulnerability, Pipeline capacity]). This perspective is considered to be more accurate and better representative for power grids than merely considering the risk related to trees falling over power grids (Hoffman, 2008).

This work is beneficial for the implementation of the GAO's recommendations of developing a mechanism to track Defense Critical Infrastructure Program risk management decisions and responses intended to address electrical power–related risks and vulnerabilities to DoD's most critical assets. In particular, the US Air Force will be able to improve its effective contribution to the DHS's goals, in addressing not only risks

and vulnerabilities assessment of electrical power infrastructure but also in finding alternate solutions (GAO, 2009:3).

Moreover, this work constitutes an effective tool for rational security allocation in the most critical links in the network (improving efficiency), in order to reduce vulnerability. Additionally, since resilience can be measured by the functionality of the system as presented by MCEER, the following four common attributes of disaster resilience (as defined by MCEER), can be assessed by the model presented in this work: Robustness through Reliability, Redundancy and Rapidity through parallel systems within the network (Recovery capability), Resourcefulness is directly related to the use of the model as a tool in order to identify and prioritize issues and to take managerial decisions for resources allocation.

Since most of critical infrastructure is currently owned by private sector, information sharing between public sector and private companies arises as a critical point for successful power networks management. Supply chain intelligence, concept coined in the logistics arena, is the environment needed to conduct this strategic information sharing toward the needed resilience improvement.

Theoretical or design values for grid's attributes are used in the model to set each of the goals (design values) which are used to compare current measures in the networks.

When such goals are reached, unitary values of resilience are obtained. Besides, working with design values of performance (reliability, recovery capability, vulnerability, pipeline capacity), the manager is confident about feasibility of the solutions emerging from the model's results.

Actual data from failure occurrences as well as Time To Repair (TTR) will be useful to develop empirical distribution of Recovery Capability leading to more accurate information and hence reliable results from the model.

This work lets decision makers improve overall performance through reliability improvement as well as rational security allocation and pipeline capacity improvements at the more strategic links based on optimal solutions.

Additionally, the model lets decision makers to fix grid's variables such as reliability, reduced pipeline capacity or vulnerabilities within the model in order to find optimal solutions with no changes in the fixed variables. Under these circumstances, optimal solution will include the referred restrictions as constraints, and improvement requirements will be focused on those variables or characteristics that decision makers are willing or able to address. Logically, not all variables regarding resilience attributes can be fixed simultaneously and tradeoffs are always a decision maker's challenge. Moreover, as generalized network problem, the model allows different units for pipeline capacity.

Since the DoD has recognized that the most critical assets are vulnerable to electrical power disruptions, but also the lack sufficient information to determine the full extent of their vulnerability (GAO, 2009:22), this work provides to the DoD an effective tool to accomplish its responsibilities regarding the four strategic goals in supporting the path to the future sustainable energy:

1. Maintain or enhance operational effectiveness by reducing total force energy demands.
2. Increase energy security through strategic resilience.

3. Enhance operational and business effectiveness by institutionalizing energy considerations and solutions in DoD planning & business processes.
4. Information Technology (IT) will play a major role in the near future when smart grids are implemented based on cyber platforms.

Reliability and Recovery Capability

Since recovery capability leads to an actual resilient behavior within the power networks, links resilience can be improved through a virtual parallel design, where two elements are combined to improve resilience at a favorable cost-benefit ratio.

A principle of improving resilience through redundancy was applied, in the model by using a virtual redundancy in each link (recovery capability) what allows reliability improvement throughout the entire network.

By combining inherent reliability (Rs) with recovery capability (Rr) within each link (as a virtual redundant component), a more resilient network is developed with the benefits summarized by Sheffi in his book ("*Resilience through redundancy*"; Sheffi, 2005:171). While reliability is related to the hardware and the likelihood of occurrence of accidental (unintentional) disruptions, recovery capability represents the timely recovery needed when an unexpected power disruption occurs. The main advantage of this design is that more resilient parallel systems are designed without actual physical redundancy. Consequently major reduction of cost and effort are associated to this resilient design improvement. Additionally, while physical infrastructure within power networks need to be replicated for alternate electricity flows (one way versus two ways flow), recovery capability (Rr) design works as a two ways component as shown in Appendix D.

Considering that reliability issues hardly can be significantly improved in the short run, resilience improvement can be addressed throughout strategic teams (team works) to ensure timely recovery after a disruption (reduced Time To Recover).

Vulnerability

Critical power infrastructure has been proven to be a high vulnerable target for sabotages and terrorist attacks. Vulnerability assessment is identified as a critical component for resilient behavior. In addition, vulnerability assessment lets managers make a more rational decision concerning budgeting of security allocation.

Vulnerability is considered as integrated through the entire network instead of a specific or standalone point value. This contributes to solve the DoD concern about vulnerability extent throughout power grids that seriously degrade critical national security capabilities (DoD, 2008).

Resilience improvement can be efficiently addressed throughout strategic teams to ensure timely recovery after a disruption, vulnerability reduction plays a significant role in the overall power grids resilience.

Path's Length and Pipeline Capacity Implications

Resilience implications related to distances between nodes (link's length) are included as a critical factor for vulnerability assessment. However, since optimal solutions account for the shortest path for a given scenario, this solution will also contribute to the pipeline capacity maximization. This is because conceptual studies to examine point to point transmission are performed using typical transmission line capacities that are a function of the distance over which the power is being transmitted.

Applicability to Other Fields

Resilience metric developed in this work brings to the logistic arena not only a more quantitative tool but also a common and comparable metric to assess alternate scenarios in terms of resilience. This work presents a quantitative tool to assess resilient behavior not only in power grids but also in other key business process involving supply chain management, like manufacturing and distribution capabilities.

While long term investments are needed to further enhance and build resilient power grid infrastructures for the future, it is imperative to become better prepared to leverage current capabilities to minimize the impact of catastrophes, crises and terrorist attacks. A similar approach could be utilized to determine optimal paths for evacuation routing, determining the best paths for emergency vehicles, the best allocation of resources for rebuilding bridges and the optimal order for bringing key infrastructure assets back online. Once the capabilities and tools have been put in place, decision makers and operational entities have the power to make rapid and adaptive decisions to maximize the use of their scarce resources. The ability to make key informed decisions in an agile real time environment is a critical function to effectively instill critical infrastructure resilience and preparedness in the future.

Limitations

The main limitation of this work is the lack of real world data for the modeled scenarios. The data used in the model is notional as real world data was unavailable due to political and security concerns.

However, this research developed a linear programming tool based in a common software package, Excel ® that enhances the decision making process in terms of resilience.

While this tool is not intended to design power networks but to assess actual performance in a more measurable and comparable way in order to support strategic decision making process, it is also important to recognize that attributes involved in actual power grid resilience are not linearly related to each other.

Areas of Further Research

Since the model developed in this work included one source (node 1), further developments are needed to include more complex scenarios like several sources of supply. In such scenarios, models could include attributes related to green sources as resilience indicator. Recall that coal is the most used element in fueling US power networks, accounting also for the higher contribution of Carbon Dioxide emissions related to all other sectors (e.g. transportation activity in Figure 3).

This consideration will contribute to the sustainability of future power grids designs because this characteristic is not an end state to be reached; rather it is a major characteristic of complex, dynamic and evolving systems.

Final Conclusion

The goal in this work was to develop a quantitative method to assess resilience in power grids based on the synergic interaction among critical attributes within such networks. While risk assessment procedures deal with actual and potential weaknesses and threats, experience shows that disruptions will occurs. So, resilient systems designs

imply not only proactive actions toward known or predictable threats, but also reactive preparedness to face contingencies. This standpoint recognizes the holistic characteristics of the challenge on hand.

Critical components in resilience were identified and their interaction is noted using electrical system power grid as the implementation testbed. This work represents an actual means to quantify resilience in a manageable way. The linear program developed in this research highlights the January 2006; Homeland Security Advisory Council (HSAC) recommendations to the DHS Secretary that resilience should be adopted as the top-level national goal for dealing with the nation's critical infrastructure.

Two concepts portrayed by the Homeland Security Advisory Council (CITF, 2006:25) are coincident with conclusions drawn in this work:

1. While long term investments are needed to further enhance and build resilient infrastructures for the future, it is imperative that the nation become better prepared to leverage current capabilities to minimize the impact of catastrophes and crises.
2. Once the capabilities and tools have been put in place, decision makers and operational entities have the power to make rapid and adaptive decisions to maximize the use of their scarce resources.

Strategic energy management and the role that critical infrastructures play for nation's security is worth the needed effort toward effective resilience assessment and improvement as well.

Finally, the ability to make key informed decisions in an agile real time environment is not only an actual endeavor in progress but also a critical function to effectively instill national resilience and preparedness in the future.

Appendix A: Department of Homeland Security – Target capabilities

Source: *McGill and Ayyub. 2009*

Appendix B: Literature Review. Attributes that Drive Resilience in Systems and Organizations

38 literature references and the 45 attributes

Number	Factor	1 MCEER	2 Bruneau and Tierney	3 Pres. Decis. Dir./NSC-63	4 Executive Order 13123	5 DoD - ESSP (2008)	6 EO 13423, 2007/sec. 2	7 ICTF, 2006 (DHS)	8 N. Lavenson (Woods, 2009)	9 Ulieru, 2007	10 Peter Farley, 2004	11 SHEFFI, 2005	12 U.S.G.A.O. 2009	13 DoD, The Smart Grid, 2008	14 Fiksel, 2003/5334	15 Fiksel, 2006	16 Omer, 2009	17 Physyos (Eng)	18 Giles, 2006:13-16, 29	19 Invase, Stress-Strain Curve	20 Industrial & Organiz. Safety	21 www.bookrags.com	22 Hollnagel & others, 2008	23 Christopher & Peck, 2004	24 George Mason University, '07	25 Bush & Grayson, 2009	26 SSE, 2009	27 Hoffman, 2008:8	28 Anderies, 2004	29 Husdal, 2004	30 Husdal, 2009	31 Rice & Caniato, 2008	32 Pettit, 2008	33 Hamel/Valikangas, 2003	34 Bruneau and Tierney, 2007	35 Schafer & others, 2007	36 The Economist, 2004	37 Ramanathan & Lac, 2009	38 King and Zobel, 2008	TOTAL	TOTAL %
1	Robustness & Reduced consequences	2	1														1			1	1		1			1	1	1	1	1	1							1	14	6.76%
2	Redundancy	1	1																				1			1		1				1							1	6	2.90%
3	Resourcefulnes	1	1																							1		1				1		1					1	7	3.38%
4	Rapidity&Reduced TimeToRecover	2	1	1				2				1					1					2	2			1	1	1					1			1	1	1	20	9.66%
5	Flexibility		1														1				1		3			1			1	1	1					1			10	4.83%
6	Adaptability		1												2	1	1	1			1	2	2			1	1	1							1	1			16	7.73%
7	Infrequent disruptions &Reliability	1		1				1														1						1										1	6	2.90%
8	minimum neg. effects			1																					1														2	0.97%
9	Sustainability (GHG); Environment			1	1	1	1							1	1																								6	2.90%
10	Sustainability (Long lasting)				1										1	1															1								4	1.93%
11	Sustainability (Nonrenew. Res.)				1		1							1																									3	1.45%
12	Security					1		1			1	1																										1		5	2.42%
13	Metrics for assessment and procedures needed					1					1		2				1	1		1					1	1			1							1	1		1		13	6.28%
14	Scicence & Technology (Knowledge to improve Resil.)					1																		1												1				3	1.45%
15	energy self-sufficiency					1																																		1	0.48%
16	Reactive vs Proactive measures							1	1	1	1											1																		5	2.42%
17	Mitigate & recover from stress							1				2	1				1	1						2	1	1														10	4.83%
18	Long distances issues in nets					1																																		1	0.48%
19	Cyber-vulnerabilities					1				1		1																												3	1.45%
20	Natural disasters; wheather conditions											1					1											1									1			4	1.93%
21	Terrorism attacks									1		1																												2	0.97%
22	predictability								1			1						1			1	1			1															6	2.90%
23	Safety - Accidents likelihood								1	1														1														1		4	1.93%
24	Risk/Vunerability issues (assessed or not)								1				1				1					1		1				1	1											7	3.38%
25	Human factor									1							1																								2	0.97%
26	Systems' complexity (Networks)									1					1									1																3	1.45%
27	Near misses & Incidents investigation											1																												1	0.48%
28	Cross function, Participation, proper comunication											1												1																2	0.97%
29	New (different) equilibrium after stress (Learning process)																1		1					2	1	2			1					1			1			10	4.83%
30	Resistant & withstand							1														2																		3	1.45%
31	Diversity														1																										1	0.48%
32	efficiency														2																										2	0.97%
33	Cohesion														2																										2	0.97%
34	simplicity (of design)														1																										1	0.48%
35	Descentralization							1							1																										2	0.97%
36	Forecasting influence																							2							1									3	1.45%
37	Brittleness																							1																1	0.48%
38	Ability to absorb Stress or negative change																												1											1	0.48%
39	Quality + Availability + Functioanlity	1						1																1					1							2		1	1	8	3.86%
40	Interoperativity																												1									1		2	0.97%
41	Maintenability																																					1		1	0.48%
42	Information Technology																																						1	1	0.48%
43	Capacity (pipeline capacity)																1																								1	0.48%
44	Laws/Legislation																												1											1	0.48%
45	Finantial issues																												1											1	0.48%
	TOTAL	8	6	4	3	7	2	9	4	6	3	9	5	2	12	2	10	4	1	2	6	8	22	4	5	4	4	12	1	3	3	3	1	2	4	4	4	6	5	207	100.00%

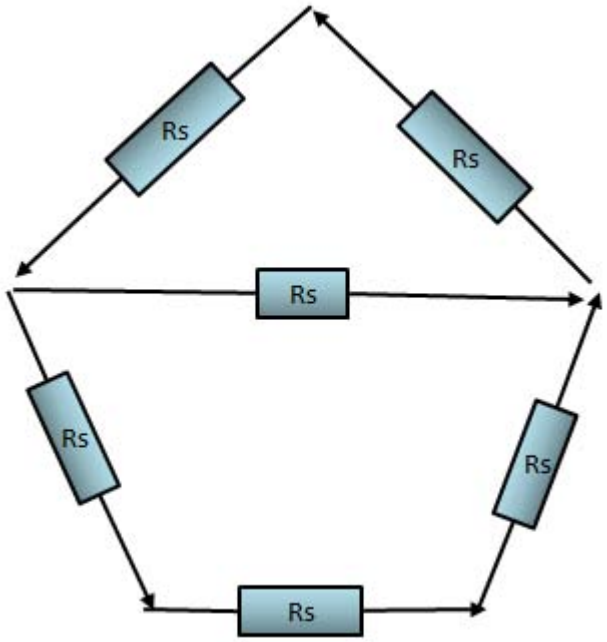
Appendix C: Attributes that Drive Resilience in Systems and Organizations

Aggregated Attributes

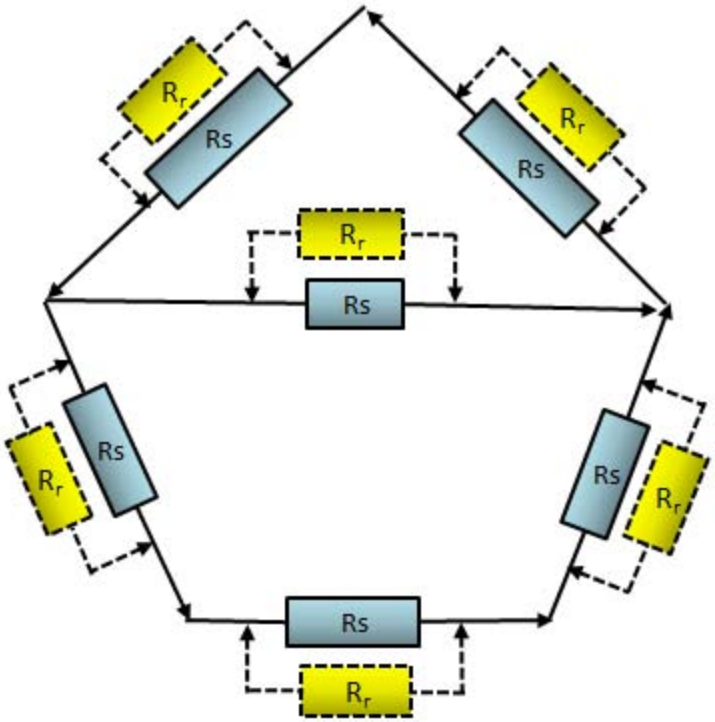
Literature Review Number		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38		
Rows aggregation Number	Aggregated Factors	MCEER	Bruneau and Tierney	Pres. Decis. Dir./NSC-63	Executive Order 13123	DoD - ESSP (2008)	EO 13423, 2007 sec. 2	CITF, 2006 (DHS)	N. Levenson (Woods, 2008)	Uliieru, 2007	Peter Flanlay, 2004	SHEFFI, 2005	U.S.G.A.O. 2009	DoD, The Smart Grid, 2008	Fiksel, 2003/6334	Fiksel, 2006	Omer, 2009	Physyck (Eng)	Ujles, 2008 13-16, 69	Invasee, Stress-Strain Curve	Industrial & Organiz. Safety	www.bookrags.com	Holnagel & others, 2008	Christopher & Peck, 2004	George Mason University, '07	Bush & Grayson, 2009	SSE, 2009	Hoffman, 2006:8	Anderies, 2004	Husdal, 2004	Husdal, 2009	Rice & Caniato, 2008	Petit, 2008	Hamel/Valikangas, 2003	Bruneau and Tierney, 2007	Schafer & others, 2007	The Economist, 2004	Ramanathan & Lac, 2009	King and Zobel, 2008	Aggregated values	Aggregated values as %
4+17+41+29	Rapidity&Reduced TimeToRecover+ Mitigate and recover from stress+Maintenability+ New (differ.) equilibrium after stress	2	1	1				2					1				1					2	2			1	1	1						1	1		1	1	1	41	19.81%
2+7+10+22+36 +39	Infrequent disruptions &Reliability+ Sust(Long Lasting)+Predictability+ Forecasting+Availability-Quality-Functionality	1		1				1														1						1										1		33	15.94%
5+6+38	Flexibility + Adaptability+Ability to Absorb Stress-Neg.Changes		1														1				1		3						1	1	1					1			27	13.04%
1+30+37+8	Robustness & Reduced consequences+ Resistant+Brittless+ Min. neg. effects	2	1														1			1	1		1			1	1	1	1	1	1								1	20	9.66%
12+24+19+21	Security+ Risks & Vulnerarability issues+Cyber-Vulnerab.+ Terrorist Attack					1		1			1	1																										1		17	8.21%
13	Metrics for assessment and procedures needed					1					1		2				1	1		1				1	1			1						1	1		1			13	6.28%
20+23+25+27	Natural disasters; wheather cond.+ Safety-Accid.+ Incid+ Human Factors(No-Intent.)									1							1											1									1			11	5.31%
9+11	Sustainability (GHG); Environment+ No-renew. Rwsources			1	1	1	1							1	1																									9	4.35%
3+15	Resourcefulnes+ Energy-Self-sufficiency	1	1																							1		1				1		1					1	8	3.86%
16	Reactive vs Proactive measures							1	1	1	1										1																				5	2.42%
26+34	Systems' complexity (Networks)+ Simplicity od design									1					1								1																		4	1.93%
14	Science & Technology (Knowledge to Improve Resil.)					1																	1													1					3	1.45%
28	Cross function, Participation, proper comunication											1											1																		2	0.97%
32	Efficiency														2																										2	0.97%
33	Cohesion														2																										2	0.97%
35	Descentralization							1							1																										2	0.97%
40	Interoperativity																											1										1			2	0.97%
18	Long distances issues in nets					1																																			1	0.48%
31	Diversity														1																										1	0.48%
42	Information Technology																																							1	1	0.48%
43	Capacity (pipeline capacity)																1																									1	0.48%
44	Laws/Legislation																											1													1	0.48%
45	Finantial issues																											1													1	0.48%
	TOTAL	8	6	4	3	7	2	9	4	6	3	9	5	2	11	2	10	4	1	2	6	8	22	4	5	4	4	13	1	3	3	3	1	2	4	4	4	7	5	207	100.00%

Appendix D: POWER NETWORK MODEL – Virtual Redundancy

Virtual Parallel design: Physical infrastructure reliability within each link (Rs) plus and Recovery Capability (Rr)



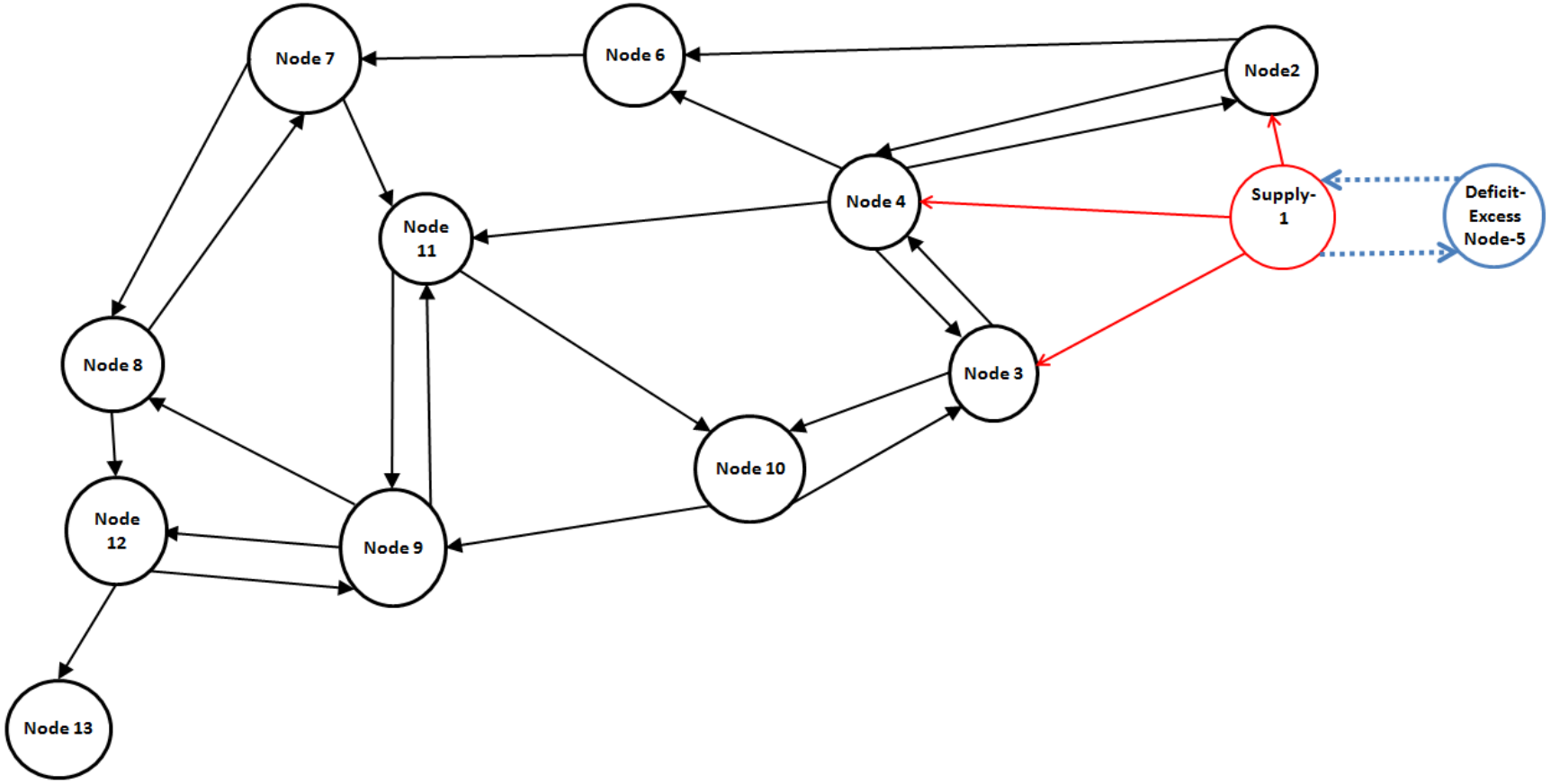
a. Physical network with inherent reliability within each link (Rs)



b. Physical network with both, inherent reliability within each link (Rs) and virtual parallel reliability (Rr)

Appendix E: POWER NETWORK MODEL - Lay-out

13 Nodes: 1 Source, 11 Demands and 1 Dummy node; 27 arcs

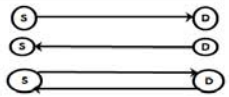


Appendix F: Power Network Model. Spreadsheet – Part 1/3

	Connectivity between nodes				Serial Components Reliability (Rs)				f (t)	Rs+Rr-Rs*Rr					Connectivity between nodes			
arc number	From (Supply or Node) MW		To (Node) MW		Source Node (1)	Arc (2)	Destination Node (3)	Serial Reliability (Rs) (1x2x3)	Time to Recover Probab. (Rr)	Parallel (composed) Reliability at each Link Rp=f(Rs,Rr)	Failure Probability (1-Rp)	Design (Max.) Reliability (Rd)	Failure Probab. Design (1-Rd)	Reliability allocation needed to reach max. performance	From (Supply or Node) MW		To (Node/supply) MW	
1	1	N1-Supply	2	N2-D	0.99	0.99	0.99	0.9703	0.9550	0.998663	0.001337	0.998663	0.001337	0.000000	1	N1-Supply	2	N2-D
2	1	N1-Supply	3	N3-D	0.99	0.99	0.99	0.9703	0.9550	0.998663	0.001337	0.998663	0.001337	0.000000	1	N1-Supply	3	N3-D
3	1	N1-Supply	4	N4-D	0.99	0.99	0.99	0.9703	0.9550	0.998663	0.001337	0.998663	0.001337	0.000000	1	N1-Supply	4	N4-D
4	1	N1-Supply	5	Dummy node	0.99	0.99	0.99	0.9703	0.9550	0.998663	0.001337	0.998663	0.001337	unused Link	1	N1-Supply	5	Dummy node
5	2	N2-D	4	N4-D	0.99	0.99	0.99	0.9703	0.9550	0.998663	0.001337	0.998663	0.001337	unused Link	2	N2-D	4	N4-D
6	2	N2-D	6	N6-D	0.99	0.99	0.99	0.9703	0.9550	0.998663	0.001337	0.998663	0.001337	0.000000	2	N2-D	6	N6-D
7	3	N3-D	4	N4-D	0.99	0.99	0.99	0.9703	0.9550	0.998663	0.001337	0.998663	0.001337	unused Link	3	N3-D	4	N4-D
8	3	N3-D	10	N10-D	0.99	0.99	0.99	0.9703	0.9550	0.998663	0.001337	0.998663	0.001337	0.000000	3	N3-D	#	N10-D
9	4	N4-D	2	N2-D	0.99	0.99	0.99	0.9703	0.9550	0.998663	0.001337	0.998663	0.001337	unused Link	4	N4-D	2	N2-D
10	4	N4-D	3	N3-D	0.99	0.99	0.99	0.9703	0.9550	0.998663	0.001337	0.998663	0.001337	unused Link	4	N4-D	3	N3-D
11	4	N4-D	6	N6-D	0.99	0.99	0.99	0.9703	0.9550	0.998663	0.001337	0.998663	0.001337	unused Link	4	N4-D	6	N6-D
12	4	N4-D	11	N11-D	0.99	0.99	0.99	0.9703	0.9550	0.998663	0.001337	0.998663	0.001337	0.000000	4	N4-D	#	N11-D
13	5	Dummy node	1	N1-Supply	0.99	0.99	0.99	0.9703	0.9550	0.998663	0.001337	0.998663	0.001337	unused Link	5	Dummy node	1	N1-Supply
14	6	N6-D	7	N7-D	0.99	0.99	0.99	0.9703	0.9550	0.998663	0.001337	0.998663	0.001337	0.000000	6	N6-D	7	N7-D
15	7	N7-D	8	N8-D	0.99	0.99	0.99	0.9703	0.9550	0.998663	0.001337	0.998663	0.001337	0.000000	7	N7-D	8	N8-D
16	7	N7-D	11	N11-D	0.99	0.99	0.99	0.9703	0.9550	0.998663	0.001337	0.998663	0.001337	unused Link	7	N7-D	#	N11-D
17	8	N8-D	7	N7-D	0.99	0.99	0.99	0.9703	0.9550	0.998663	0.001337	0.998663	0.001337	unused Link	8	N8-D	7	N7-D
18	8	N8-D	12	N12-D	0.99	0.99	0.99	0.9703	0.9550	0.998663	0.001337	0.998663	0.001337	unused Link	8	N8-D	#	N12-D
19	9	N9-D	8	N8-D	0.99	0.99	0.99	0.9703	0.9550	0.998663	0.001337	0.998663	0.001337	unused Link	9	N9-D	8	N8-D
20	9	N9-D	11	N11-D	0.99	0.99	0.99	0.9703	0.9550	0.998663	0.001337	0.998663	0.001337	unused Link	9	N9-D	#	N11-D
21	9	N9-D	12	N12-D	0.99	0.99	0.99	0.9703	0.9550	0.998663	0.001337	0.998663	0.001337	0.000000	9	N9-D	#	N12-D
22	10	N10-D	3	N3-D	0.99	0.99	0.99	0.9703	0.9550	0.998663	0.001337	0.998663	0.001337	unused Link	10	N10-D	3	N3-D
23	10	N10-D	9	N9-D	0.99	0.99	0.99	0.9703	0.9550	0.998663	0.001337	0.998663	0.001337	0.000000	10	N10-D	9	N9-D
24	11	N11-D	9	N9-D	0.99	0.99	0.99	0.9703	0.9550	0.998663	0.001337	0.998663	0.001337	unused Link	11	N11-D	9	N9-D
25	11	N11-D	10	N10-D	0.99	0.99	0.99	0.9703	0.9550	0.998663	0.001337	0.998663	0.001337	unused Link	11	N11-D	#	N10-D
26	12	N12-D	9	N9-D	0.99	0.99	0.99	0.9703	0.9550	0.998663	0.001337	0.998663	0.001337	unused Link	12	N12-D	9	N9-D
27	12	N12-D	13	N13-D	0.99	0.99	0.99	0.9703	0.9550	0.998663	0.001337	0.998663	0.001337	0.000000	12	N12-D	#	N13-D

Module: Connectivity

Link: Set of "Source node" + "Arc" ("pipeline" piece) + "Destination node".



Module: Reliability and Recovery capability

1) System Reliability and Recovery capability design (Rd)
2) Actual system relaibility and recovery capability values
3) Overall Reliability (inlcuding recovery capability) improvement needed for optimal soution feasibility

Optimal Solution (Min OF) is estimated based on best possible performance. So, Reliability allocation needs are identified based on the difference between actual Reliability (Rc) and Designed Reliability (Rd) at each Link.

Design Reliability = Rs + Rr - (Rs*Rr)

Link:

Rs=R(Source Node) x R(Arc) x R(Destination Node)

R(Source Node) =	0.99
R(Arc) =	0.99
R(DestinationNode)=	0.99
Rs=	**0.970299**

Recovery Probability (Lognormal distribution based)

Rr= 1-[Lognormdistr(t,mean,StdDev)]

t: Time to recover after disruption =	5
mean: ussually time to recover =	5
StdDev: Stardard Deviation =	2
Rr=	**0.9550**

System Reliability Design:

Rd = *f*(Rs,Rr) Rd = Rs + Rr - (Rs * Rr) ; (parallel)

Rd =	0.99866313

Appendix G: Power Network Model. Spreadsheet - Part 2/3

Constraints										
Delivery Qd [MW]	Constraint	Design (Max.) pipeline capacity (UL)	Effc. Coef. (α)	Link Capac. Reduction (%)	Actual (reduced) pipeline capacity	Restricted Delivery (If actual capacity applies)	Surplus (+) or Deficit (-) of delivery at link	Desired (Min) Vulnerability (MIL-STD 882C) (Goal -> Vd ≤)	Current (Actual) Vulnerability (MIL-STD 882C) Vc	Amount of Vulneravility to reduce at link
290.00	≤	350	0.90	10.00%	315	290.00	25	3	3	0
290.00	≤	350	0.90	10.00%	315	290.00	25	3	3	0
335.00	≤	350	0.90	10.00%	315	315.00	-20	3	3	0
185.00	≤	350	0.90	10.00%	315	185.00	130	N/A	N/A	N/A
0.00	≤	200	0.90	10.00%	180	0.00	Unused Link	3	3	Unused-Link
200.00	≤	200	0.90	10.00%	180	180.00	-20	3	15	12
0.00	≤	200	0.90	10.00%	180	0.00	Unused Link	3	5	Unused-Link
200.00	≤	200	0.90	10.00%	180	180.00	-20	3	5	2
0.00	≤	200	0.90	10.00%	180	0.00	Unused Link	3	5	Unused-Link
0.00	≤	200	0.90	10.00%	180	0.00	Unused Link	3	5	Unused-Link
55.00	≤	200	0.90	10.00%	180	55.00	125	3	5	2
190.00	≤	200	0.90	10.00%	180	180.00	-10	3	5	2
0.00	≤	200	0.90	10.00%	180	0.00	Unused Link	N/A	N/A	N/A
165.00	≤	200	0.90	10.00%	180	165.00	15	3	5	2
80.00	≤	200	0.90	10.00%	180	80.00	100	3	5	2
0.00	≤	200	0.90	10.00%	180	0.00	Unused Link	3	5	Unused-Link
0.00	≤	200	0.90	10.00%	180	0.00	Unused Link	3	5	Unused-Link
0.00	≤	200	0.90	10.00%	180	0.00	Unused Link	3	5	Unused-Link
0.00	≤	200	0.90	10.00%	180	0.00	Unused Link	3	5	Unused-Link
0.00	≤	200	0.90	10.00%	180	0.00	Unused Link	3	5	Unused-Link
150.00	≤	200	0.90	10.00%	180	150.00	30	3	5	2
0.00	≤	200	0.90	10.00%	180	0.00	Unused Link	3	5	Unused-Link
120.00	≤	200	0.90	10.00%	180	120.00	60	3	5	2
110.00	≤	200	0.90	10.00%	180	110.00	70	3	5	2
0.00	≤	200	0.90	10.00%	180	0.00	Unused Link	3	5	Unused-Link
0.00	≤	200	0.90	10.00%	180	0.00	Unused Link	3	5	Unused-Link
75.00	≤	200	0.90	10.00%	180	75.00	105	3	5	2

Module: System Pipeline capacity Design (Upper Limit - UL):

Design Capacity: Given for each link (Maximun and hence, theoretical value).

Reduction Coefficient (α): To adjust the theoretical capacity to current one.

Link:

System Pipeline capacity Design (Upper Limit - UL):

Trunk Link: From Supply Node

Secondary Links: connecting other than supply nodes whitin the network

Trunk Link (Pipeline capacity - UL) =	350
Secondary Links (Pipeline capac.- UL) =	200

Pipeline capacity also drives potential outages (When equal to zero) simulation within power grid.

Failure probability and Vulnerability are proportional to the amount of energy delivered through each path (link).

The lognormal is useful for modeling failures, but is more commonly used to model maintenance time: Blanchard (1992):"maintenance time for complex sys is lognormal in the majority of cases".

Module: System Vulnerability Design (Vd)

Based on **MIL-STD 882C.**

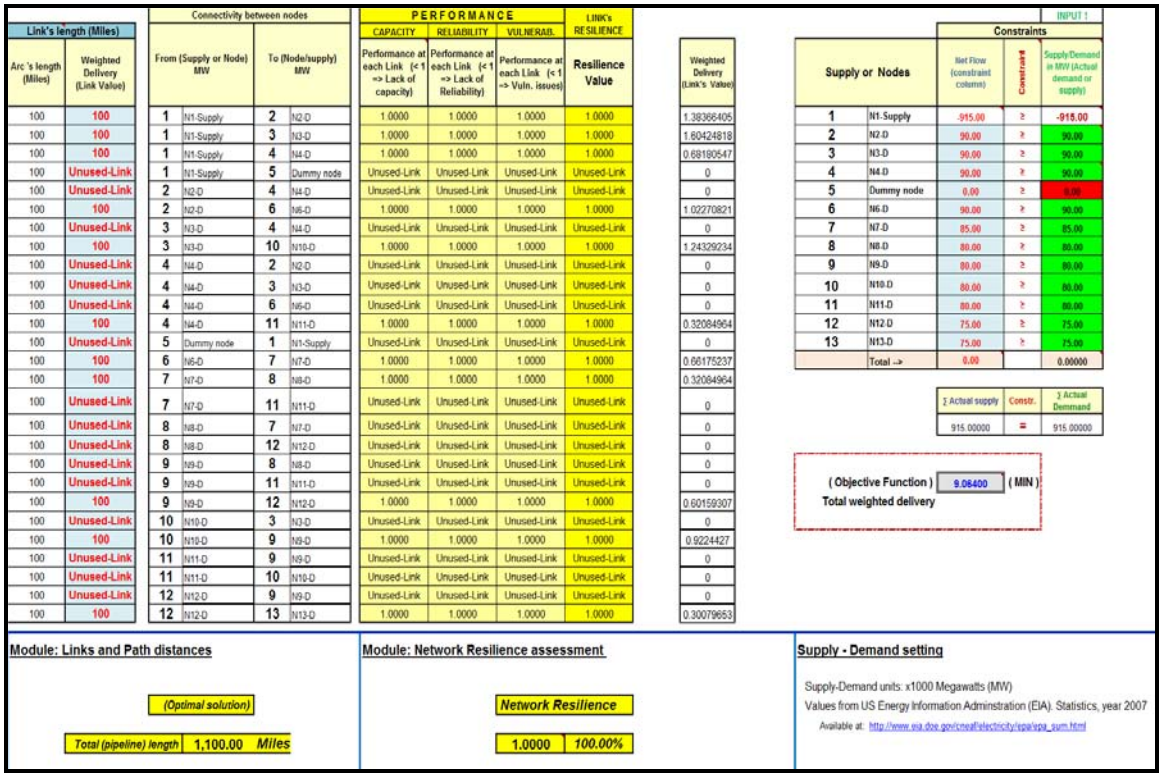
Vulnerability Values are assigned to each link according to the following criteria regarding to potential damages:

Acceptability	Value
Acceptable without review	1 - 3
Acceptable with Review	4 - 11
Undesirable (Strat. Decision needed)	12 - 15
Unacceptable	16 - 20

Trunk Link (Vulnerability Goal) =	3
Secondary Links (Vulnerabi. Goal) =	3

Criteria: "Less is better"

Appendix H: Power Network Model. Spreadsheet - Part 3/3



Link's length (Miles)		Connectivity between nodes				PERFORMANCE			LINK's RESILIENCE		INPUT ↑			
						CAPACITY	RELIABILITY	VULNERABIL				Constraints		
Arc 's length (Miles)	Weighted Delivery (Link Value)	From (Supply or Node) MW		To (Node/supply) MW		Performance at each Link (< 1 => Lack of capacity)	Performance at each Link (< 1 => Lack of Reliability)	Performance at each Link (< 1 => Vuln. issues)	Resilience Value	Weighted Delivery (Link's Value)	Supply or Nodes		Net Flow (constraint column)	Constraint	Supply/Demand in MW (Actual demand or supply)
100	100	1	N1-Supply	2	N2-D	1.0000	1.0000	1.0000	1.0000	1.38366405	1	N1-Supply	-915.00	≥	-915.00
100	100	1	N1-Supply	3	N3-D	1.0000	1.0000	1.0000	1.0000	1.60424818	2	N2-D	90.00	≥	90.00
100	100	1	N1-Supply	4	N4-D	1.0000	1.0000	1.0000	1.0000	0.68180547	3	N3-D	90.00	≥	90.00
100	Unused-Link	1	N1-Supply	5	Dummy node	Unused-Link	Unused-Link	Unused-Link	Unused-Link	0	4	N4-D	90.00	≥	90.00
100	Unused-Link	2	N2-D	4	N4-D	Unused-Link	Unused-Link	Unused-Link	Unused-Link	0	5	Dummy node	0.00	≥	0.00
100	100	2	N2-D	6	N6-D	1.0000	1.0000	1.0000	1.0000	1.02270821	6	N6-D	90.00	≥	90.00
100	Unused-Link	3	N3-D	4	N4-D	Unused-Link	Unused-Link	Unused-Link	Unused-Link	0	7	N7-D	85.00	≥	85.00
100	100	3	N3-D	10	N10-D	1.0000	1.0000	1.0000	1.0000	1.24329234	8	N8-D	80.00	≥	80.00
100	Unused-Link	4	N4-D	2	N2-D	Unused-Link	Unused-Link	Unused-Link	Unused-Link	0	9	N9-D	80.00	≥	80.00
100	Unused-Link	4	N4-D	3	N3-D	Unused-Link	Unused-Link	Unused-Link	Unused-Link	0	10	N10-D	80.00	≥	80.00
100	Unused-Link	4	N4-D	6	N6-D	Unused-Link	Unused-Link	Unused-Link	Unused-Link	0	11	N11-D	80.00	≥	80.00
100	100	4	N4-D	11	N11-D	1.0000	1.0000	1.0000	1.0000	0.32084964	12	N12-D	75.00	≥	75.00
100	Unused-Link	5	Dummy node	1	N1-Supply	Unused-Link	Unused-Link	Unused-Link	Unused-Link	0	13	N13-D	75.00	≥	75.00
100	100	6	N6-D	7	N7-D	1.0000	1.0000	1.0000	1.0000	0.66175237		Total -->	0.00		0.00000
100	100	7	N7-D	8	N8-D	1.0000	1.0000	1.0000	1.0000	0.32084964					
100	Unused-Link	7	N7-D	11	N11-D	Unused-Link	Unused-Link	Unused-Link	Unused-Link	0			∑ Actual supply	Constr.	∑ Actual Demand
100	Unused-Link	8	N8-D	7	N7-D	Unused-Link	Unused-Link	Unused-Link	Unused-Link	0			915.00000	=	915.00000
100	Unused-Link	8	N8-D	12	N12-D	Unused-Link	Unused-Link	Unused-Link	Unused-Link	0					
100	Unused-Link	9	N9-D	8	N8-D	Unused-Link	Unused-Link	Unused-Link	Unused-Link	0					
100	Unused-Link	9	N9-D	11	N11-D	Unused-Link	Unused-Link	Unused-Link	Unused-Link	0					
100	100	9	N9-D	12	N12-D	1.0000	1.0000	1.0000	1.0000	0.60159307					
100	Unused-Link	10	N10-D	3	N3-D	Unused-Link	Unused-Link	Unused-Link	Unused-Link	0					
100	100	10	N10-D	9	N9-D	1.0000	1.0000	1.0000	1.0000	0.9224427					
100	Unused-Link	11	N11-D	9	N9-D	Unused-Link	Unused-Link	Unused-Link	Unused-Link	0					
100	Unused-Link	11	N11-D	10	N10-D	Unused-Link	Unused-Link	Unused-Link	Unused-Link	0					
100	Unused-Link	12	N12-D	9	N9-D	Unused-Link	Unused-Link	Unused-Link	Unused-Link	0					
100	100	12	N12-D	13	N13-D	1.0000	1.0000	1.0000	1.0000	0.30079653					

(Objective Function) 9.06400 (MIN)
Total weighted delivery

Module: Links and Path distances

(Optimal solution)

Total (pipeline) length 1,100.00 *Miles*

Module: Network Resilience assessment

Network Resilience

1.0000 *100.00%*

Supply - Demand setting

Supply-Demand units: x1000 Megawatts (MW)
Values from US Energy Information Adminstration (EIA). Statistics, year 2007
Available at: http://www.eia.doe.gov/cneaf/electricity/epa/epa_sum.html

Appendix I: *Blue Dart* Submission Form

First Name: _Gabriel _____ Last Name: _Montoya_____

Rank (Military, AD, etc.): _Lt. Col._____ Designator #_AFIT/ENS/10-08_

Student Involved in Research for Blue Dart:_Lt. Col. Gabriel A. Montoya_____
_____

Position/Title: _Student_____

Phone Number: _937-6090853____ E-mail: gabriel_montoya@yahoo.com

School/Organization: _AFIT_____

Status: [X] Student [ ] Faculty [ ] Staff [ ] Other

Optimal Media Outlet (optional): _____

Optimal Time of Publication (optional): _____

General Category / Classification:

[ ] core values	[ ] command	[ ] strategy
[ ] war on terror	[ ] culture & language	[ ] leadership & ethics
[ ] warfighting	[ ] international security	[ ] doctrine

[X] other (specify): _Resilience assessment in networked systems_____

Suggested Headline: Assessing resilience in power grids as a particular case of Supply Chain Management

Keywords: _ Resilience, Resilience assessment, Networked system assessment, Power grids, Supply chain management assessment

Blue Dart

Electrical power grids represent not only a critical infrastructure for the nation's economy and development, but also a strategic component in strategic planning environment.

In 2006, the US Department of Defense (DoD) was responsible for 80% of the energy used by the US Government and almost 1% of the nation's total energy use (Ryan, 2008).

On the other hand, technology development, quality of life improvements and military operations have required the US to use more energy than expected. The current trend is a 2% annual increment in US electricity consumption. This trend demands strategic decisions in order to be able to reach goals in a more sustainable and secure environment (Peltier, 2006:70).

Since current geopolitical environment has changed traditional beliefs, the focus of this work is not only about commercial grids but electricity supply as a whole. DoD has traditionally assumed that commercial electrical power grids are highly reliable and subject to only infrequent (generally weather-related), short-term disruptions. However, current threats are complex, long lasting and dangerous as well, ranging from natural disasters and accidents to intentional attacks on electrical power grids. Accidents include failures related to material, hardware and software systems as well as unintentional human-being errors. These networks have been found to be particularly relevant in supplying energy to accomplish the overall critical infrastructure's missions (GAO, 2009:1-2).

This work develops a theoretical research about resilience's scope in different fields in order to look for common attributes shared by resilient systems. In this context, power grids are considered as a particular case of Supply Chain Management.

Common attributes that drive resilience have been found ranging from resilience in ecology and psychology to supply chain environments. Among the more than 200 individual references to resilience drivers and management issues that have been found, most of them share common concepts. Consequently, the original 45 attributes extracted from the 38 different publications were grouped into a relative few classes in such a way they showed consistent meaning in actual resilience drivers.

Therefore, these classes (attributes) enable strategic decision makers to successfully assess resilience in systems and organizations, where Supply Chain Management represents a particular environment of challenge.

On the other hand, although it was found that some of the literature disregards reduced time to recover after disruption or stress as critical resilient behavior, rapidity was also presented by practitioners as necessary to enable efficient systems to reduce unnecessary and expensive robustness as well as physical redundancy. Moreover, desirable recovery processes take resilient systems to an acceptable level of performance rather than to the same situation existing before the stress or disruption. This attribute was presented as desirable rather of overprotecting (securing) systems that makes them more fragile and hence less flexible to withstand unexpected stress.

While resilience is proactive in positioning a system to survive and thrive given known and unknown challenges, security, as generally practiced, provides specific protection against identified or projected risks or circumstances (George Mason University, 2007:105). As a result, excess of security can become a disadvantage.

It was shown that power grids are, in essence, a supply network where essential components can be identified: suppliers, customers, commodity to be delivered and

infrastructure to conduct the transportation (shipment). Therefore a specific definition of resilience was proposed for power grids and a resilience model was proposed in order to develop a decision tool to assess power grid resilience to contribute to the strategic energy management.

In methodological matters, lineal programming models have been used for performance assessment, including availability in networked systems. Meanwhile, resilient behavior was identified as related to several variables or attributes, where the highest frequencies were found for reduced time to recover, reliability, pipeline capacity and vulnerability. Pipeline capacity was identified as a physical constraint for power grids resilience.

On the other hand, the standard MIL-STD 882D was also presented as a quantitative tool for vulnerability classification.

In order to embed these heterogeneous variables into the model, parameterization of resilience drivers were developed. A principle of improving resilience through redundancy was applied in the model by using a virtual redundancy in each link which allows reliability improvement throughout the entire network. A unique index (ρ) integrates the resilience complexity to facilitate alternate scenarios analysis toward strategic decision making. Decision makers are enabled to improve overall power grid performance through reliability development as well as security allocation at the more strategic links identified by the optimal solutions. Moreover, this tool lets decision makers fix grid variables such as reliability, reduced pipeline capacity, or vulnerabilities within the model in order to find optimal solutions that withstand disruptions.

Finally, the model constitutes an effective tool not only for efficient reliability improvement but also for rational security allocation in the most critical links within the network. Additionally, this work contributes to the federal government mandates accomplishment, intended to address electrical power-related risks and vulnerabilities.

The views expressed in this article are those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the US Government.

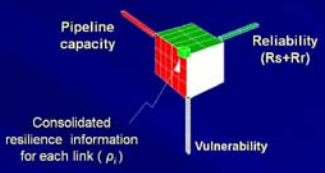
Appendix J: Quad Chart

Assessing resilience in power grids as a particular case of Supply Chain Management

Lt. Col. Gabriel A. Montoya (AAF)
Advisor: Major Daniel D. Mattioda (USAF)

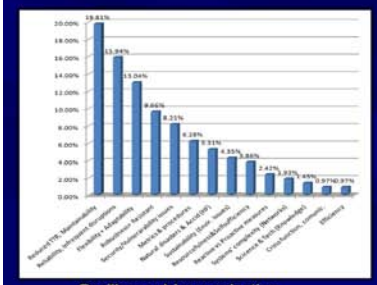
DEPARTMENT OF OPERATIONAL SCIENCES
AIR OFRCE INSTITUTE OF TECHNOLOGY

The Problem: What attributes define resilience in power grids, and what metrics will enable effective strategic management?



United States Power Grid Interconnections (Hoffman, 2008)

Network: 13 Nodes: 1 supplier, 2 artificial, 11 demmands 27 arcs



Resilience drivers selection
Frequency distribution (%) of aggregated resilience drivers, found through the literature (The 14 most relevant).

❑Resilience in power grids is defined as the capability to cope with adversity arising from intentional & unintentional threats, and to recover in a timely manner to an acceptable level (new equilibrium) of performance after have been stressed

SEVERITY CATEGORY / FREQUENCY	CATAS-TROPHIC	CRITICAL	MARGI-NAL	NEGLIGI-BLE
FREQUENT	20	18	14	8
PROBABLE	19	16	12	5
OCASIONAL	17	15	10	3
REMOTE	13	11	7	2
IMPROBABLE	9	6	4	1

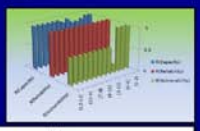
Vulnerability assessment; Adapted from MIL-STD 883D

Mathematical formulation

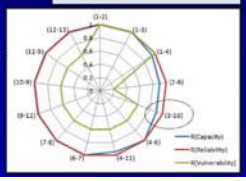
❑*Objective Function* → *Minimize*
- *Failure probability [P(f) = 1- R]*
- *Vulnerability*
- *Energy flow*

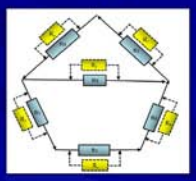
(MIN); $\sum (Q_{[i]} \times P(\text{failure})_{[i]} \times \text{Vulnerability}_{[i]} + \sum Q_{[i,r]} \times P(\text{failure})_{[i,r]} \times \text{Vulnerability}_{[i,r]})$; for all i, j

❑*Constraints*
- *Pipeline capacity* $Q_{ij} \le C_{ij}$; for all i, j
- *∑Demand = ∑Supply* $Q_{ij} \le C_{ji}$; for all i, j
- *No negativity* $\sum Qd = \sum Qs$



Complex scenario assessment
- *∑ Qs > ∑ Qd*
- *Reliability: Rd > Rp*
- *Pipeline capacity reduced → α=0.9*
- *Vulnerability: Vd (all links)=3*
  Vc(1-2, 1-3, 1-4) = 3; Vc(2-6) = 15; Vc(others) = 5
- *Overall resilience: ρ = 0.8775*
- *# of selected links = 13*
- *Pipeline capacity issues were identified*
- *Vulnerability issues (worst at link 2-6)*
- *Reliability issues → minimized by parallel design*
- *Excess of supply → node # 5 = 185 MW*





Virtual redundancy (hybrid design):
Physical (inherent) reliability within each link (Rs) and virtual parallel reliability (Rr)

Findings & conclusions

- ❑Resilience has been found to be function of Reliability, Recovery capability, Vulnerability and Pipeline Capacity
- ❑*H*eterogeneous attributes from power grids were embedded into a quantifiable and comparable resilience index (ρ)
- ❑Performance can be improved through reliability as well as rational security allocation and pipeline capacity improvements at the more strategic links based on optimal solutions
- ❑Shortest paths for a given scenario (optimal solution) contribute to the pipeline capacity maximization
- ❑This quantitative tool can assess resilient behavior in power grids and other key business process involving supply chain management, like manufacturing and distribution capabilities
- ❑Additionally, contribute to Federal mandates accomplishment regarding critical infrastructures management

Bibliography

AEP (American Electric Power). 2010. Available at http://www.aep.com/

Anderies, J.and others. *A framework to analyze the robustness of social-ecological systems from an institutional perspective*. Ecology and Society 9(1): 18. 2004.

Bochman, Andy. *The Smart Grid Security Blog*. Available at: http://smartgridsecurity.blogspot.com/. NOV-17-2009

Bookrags. *http://www.bookrags.com*. Accessed on 11-11-2009.

Bruneau and Tierney. *Conceptualizing and Measuring Resilience: A Key to Disaster Loss Reduction*. TR News May-June: 14. 2007.

Bush and Grayson. *The Critical Infrastructure Resilience Study Working Group*. National Infrastructure Advisory Council- NIAC. July, 2009.

Christopher and Peck. *Building the Resilient Supply Chain.* The International Journal of Logistics Management; Vol.15. 2005.

CISCO. *Microsoft Exchange 2007-End-to-End Messaging Infrastructure Solution*. Available at: http://www.ciscointernethome.com/en/US/docs/solutions/. 2008

CITF (Critical Infrastructure Task Force). Report of the critical infrastructure task force. Homeland Security Advisory Council. January 2006.

DoD. *Energy Strategic Security Plan*. October 2008.

DoD. MIL-STD 882D: Standard Practice for System safety. 2000

DoE. *The Smart Grid: An Introduction*. 2008.

Ebeling, Charles. An Introduction to Reliability and Maintainability Engineering. Waveland Press, Inc. 2005.

Economist, the. *Building the energy internet.* London; Vol. 370. 2004

EIA. *Electric Power Annual with data form 2007*. Available at: http://www.eia.doe.gov/). Accessed on 01-07-2010.

EIA. *US energy-related Carbon Dioxide. Emissions by sector; 1990-2007. http://www.eia.doe.gov/oiaf/1605/ggrpt/carbon.html#emissions. 11-11-2009.*

EIA. *Short-Term Energy Outlook*. http://www.eia.doe.gov/emeu/. 11-05-2009.

Evans and Lindsay. *The Management and Control of Quality*. South-western – Thomson Learning. 2001.

Fiskel, Joseph. *Designing Resilient, Sustainable Systems*. Environ. Sci. Technol. 37, 5330-5339. 2003.

Fiksel, Joseph. *Sustainability and resilience: toward a systems approach*. Sustainability: Science, Practice, & Policy, Vol. 2, No. 2, pp. 1-8. 2006.

Foster, Thomas. *Managing Quality. An integrative approach*. Prentice Hall. 2001

GAO (US Government Accountability Office). *Defense Critical Infrastructure*. Report to Congressional Committees. OCT-2009.

George Mason University. *Critical Thinking: Moving from Infrastructure Protection to Infrastructure Resilience*. 2007.

Haeussler Jr, Paul Richard and Wood Richard. *Introductory Mathematical Analysis for Business, Economics and the Life and Social Sciences*. Pearson; Prentice Hall; 11e. 2005

Hamel and Välikangas. *The quest for resilience*. Harvard Business School Publishing Corporation. 2003.

Hertzberg, Richard. *Deformation and Fracture Mechanics of Engineering Materials*. John Wiley & Sons, INC. 1996.

Hinkle, Trotter and Osgood. *The Integration of Reliability Centered Maintenance with a Structural Integrity Program*. Journal of the Reliability Information Center. Volume 17. Second quarter, 2009.

Hoffman, Jason and Roshanak Nilchiani. *Assessing Resilience in the US National Energy Infrastructure*. SSE. Fall 2008

Hollnagel and others; *Resilience Engineering; Concepts and Precepts*. Ashgate. 2008

Husdal, Jan. *De-confusing SCRM: robustness, resilience, flexibility and agility*. http://www.husdal.com/2009/05/26/robustness-resilience-flexibility-agility/#ixzz0XX0XreR2. OCT-30-2009

Husdal, Jan. *Flexibility and robustness as options to reduce risk and uncertainty. Unpublished working paper*. Molde University College, Molde, Norway. 2004

ICF Consluting. *The Economic Cost of the Blackout, an issue paper on the Northeastern* Blackout August 2003. http://www.solarstorms.org/ICFBlackout2003.pdf. Accessed nov-11-2009.

IEEE. *Transactions on Power Apparatus and Systems*. Vol.PAS-98, 1979.

Invsee. *Stress-Strain Curve for Brittle Material*. http://invsee.asu.edu/srinivas/brittle/. 11-11-2009.

Jacques David. *Introduction to Systems Engineering Process and Design*. AFIT; CH 13 class. 2009

Jiles, David. *Introduction to the Principles of Materials Evaluation*. CRC Press. 2008

Keyof metals. http://steel.keytometals.com/default.aspx?ID=CheckArticle&NM=41. Accessed on 11-11-2009

King and Zobel. *Applying the R4 Framework of Resilience: Information Technology Disaster Risk Management at Northrop Grumman*. 2008. Available at http://www.sedsi.org/Proceedings/2008/proc/p071010036.pdf

Leenders, Michiel and others. Purchasing and Supply Management. McGraw-Hill-Irwin. 2006.

Masten, A. *The development of competence in favorable and unfavorable environments*. American Psychologist. 1998.

MCEER (Multidisciplinary Center for Earthquake Engineering Research). MCEER's *Resilience Framework.* University at Buffalo; NY. Available at: http://mceer.buffalo.edu/research/resilience/. 2009.

MCEER (Multidisciplinary Center for Earthquake Engineering Research). *From Earthquake Engineering to Extreme Events*. University at Buffalo; NY. December, 2008.

McGill and Ayyub. Regional Capabilities Performance Assessment for Homeland Security; IEEE. June,2009.

Moteff and Parfomak. *Critical Infrastructure and Key Assets: Definition and Identification*. CRS Report for Congress. Order Code RL32631. October, 2004

NERC (North American Electric Reliability Corporation). *Understanding the power grids*. Accessed on FEB-7-2010. Available at http://www.nerc.com/page.php?cid=1|15

Omer and others. *Measuring the Resilience of the Global Internet Infrastructure System.* IEEE SysCon 2009. 3rd Annual IEEE International Systems Conference. 2009.

Peltier, Robert; *Preventive Maintenance; New York*. Vol 150; Iss.8. October 2006.

Peter Fairley. The Unruly Power Grid. IEEE Spectrum. August 2004

Pettit, Timothy and others. *Can you Measure your Supply Chain Resilience?*. Journal: Supply Chain & Logistics Association Canada. Summer 2008.

Ragsdale, Cliff T. *Spreadsheet Modeling & Decision Analysis 5e*. Thompson South-western. 2008

Ramanathan and Lac. Towards a Resilience Benchmarking for Home Gateways. Orange Labs. 2009.

Rice and Caniato. *Building a secure and resilient supply chain. http://www.husdal.com/2008/06/11/building-a-secure-and-resilient-supply-chain/.* 2008.

Schafer and others. *Towards a decision engine for self-remediating resilient networks.* Lancaster University-UK; NEC Laboratories Europe-Germany; University of Kansas- USA. 2007. Available at: http://www.ittc.ku.edu/resilinets/papers/

Sheffi, Yossi. *The Resilient Enterprise.* Massachusetts Institute of Technology. 2005.

SSE (School of Systems & Enterprise*). Complex infrastructure systems resilience and sustainability*. Center for Complex Adaptive Sociotechnological Systems. Nov-2009. Available at: http://www.socio-technical.org/

Ulieru, Michaela. *Design for Resilience of Networked Critical Infrastructures*. University of New Brunswick. Canada. 2007.

Umstattd, Ryan. *Future energy efficiency improvements within the US department of Defense: Incentives and barriers. 2008*

USAF. *United States Air Force Infrastructure Energy Strategic Plan USAFIESP*. 2008

USG.A.O. (US Government Accountability Office). *Defense Critical Infrastructure, Report to Congressional Committees. OCT-2009.*

US Geological Survey. USGS website. http://www.usgs.gov/hazards/

US President. *Presidential Decision Directive/NSC-63*. May 22. 1998.

US President. *Executive Order # 13123*. June 1999.

US President. *Executive Order # 13423*. January 2007.

USPGS&U (United States of America Power Grid Status and Updates). US Power Grids. Status and Updates. www.dieselserviceandsupply.com/ US_power_grid.aspx; 10/21/2009

Vita

Lt. Col. Gabriel Alejandro Montoya graduated as officer form the Argentine Air Force Academy in 1989. He is an aeronautical engineer graduated from the Argentine Air Force Institute of Technology in 1992. He also got his post degree Specialization in Safety at the University of Buenos Aires (Argentina), in 2006.

He has had several assignements as Maintenance Oficcer in aircraft maintenance squadrons. In 2005 he graduated as Staff Officer at the Argentine Airt Force War College.

He was assigned to the Materiel Command Staff (Planning Department) until he entered the Graduate Scholl of Engineering and Management, Air Force Institute of Technology in August 2008. Upon graduation he will be assigned to the Materiel Command (Head Quarter) in Buenos Aires, Argentina.

REPORT DOCUMENTATION PAGE	Form Approved OMB No. 074-0188

1. REPORT DATE (DD-MM-YYYY)	**2. REPORT TYPE**	**3. DATES COVERED**
25 - March - 2010	Master's Thesis	Sept 2010-March 2010

4. TITLE AND SUBTITLE

ASSESSING RESILIENCE IN POWER GRIDS AS A PARTICULAR CASE OF SUPPLY CHAIN MANAGEMENT

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Gabriel Alejandro Montoya, Lt. Col., Argentine Air Force

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)
AIR Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 Hobson Way - WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER
AFIT/LSCM/ENS/10-08

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(S)

INTENTIONNALY LEFT BLANK

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION AVAILABILITY STATEMENT
APPROVED FOR PUBLIC RELEASE, DISTRIBUTION UNLIMITED

13. SUPPLEMENTARY NOTES

14 ABSTRACT

Electrical power grids represent a critical infrastructure for a nation as well as strategically important. Literature review identified that power grids share basic characteristics with Supply Chain Management. This thesis presents a linear programming model to assess power grid resilience as a particular case of Supply Chain Management. Since resilient behavior is not an individual or specific system's attribute but a holistic phenomenon based on the synergic interaction within complex systems, resilience drivers in power grids were identified. Resilience is a function of Reliability, Recovery Capability, Vulnerability and Pipeline Capacity. In order to embed heterogeneous variables into the model, parameterization of resilience drivers were developed. A principle of improving resilience through redundancy was applied in the model by using a virtual redundancy in each link which allows reliability improvement throughout the entire network. Vulnerability was addressed through the standard MIL-STD 882D, and mitigated through security allocation. A unique index (R) integrates the resilience complexity to facilitate alternate scenarios analysis toward strategic decision making. Decision makers are enabled to improve overall power grid performance through reliability development as well as security allocation at the more strategic links identified by the optimal solutions. Moreover, this tool lets decision makers fix grid variables such as reliability, reduced pipeline capacity, or vulnerabilities within the model in order to find optimal solutions that withstand disruptions. The model constitutes an effective tool not only for efficient reliability improvement but also for rational security allocation in the most critical links within the network. Finally, this work contributes to the federal government mandates accomplishment, intended to address electrical power-related risks and vulnerabilities.

15 SUBJECT TERMS

16 SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONS. PERSON**
REPORT	**ABSTRACT**	**THIS PAGE**			**19b. TELEPHONE NUMBER (include area code)**
U	**U**	**U**	**UU**	185	**Daniel Mattioda; Maj; USAF; PhD**

Standard Form 298 (Rev:8-98)
Prescribed by ANSI Std Z39-18