Int. J. Disaster Risk Sci. 2013, 4 (4): 159–168
doi:10.1007/s13753-013-0017-7

ARTICLE

Antifragility Analysis and Measurement Framework for Systems of Systems

John Johnson and Adrian V. Gheorghe*

Engineering Management and Systems Engineering Department, Old Dominion University, Norfolk, VA 23529, USA

Abstract The twenty-first century is defined by the social and technical hazards we face. A hazardous situation is a condition, or event, that threatens the well-being of people, organizations, societies, environments, and property. The most extreme of the hazards are considered X-Events and are an exogenous source of extreme stress to a system. X-Events can also be the unintended outputs of a system with both positive (serendipitous) and negative (catastrophic) consequences. Systems can vary in their ability to withstand these stress events. This ability exists on a continuum of fragility that ranges from fragile (degrading with stress), to robust (unchanged by stress), to antifragile (improving with stress). The state of the art does not include a method for analyzing or measuring fragility. Given that "what we measure we will improve," the absence of a measurement approach limits the effectiveness of governance in making our systems less fragile and more robust if not antifragile. The authors present an antifragile system simulation model, and propose a framework for analyzing and measuring antifragility based on system of systems concepts. The framework reduces a multidimensional concept of fragility into a two-dimensional continuous interval scale.

Keywords complex adaptive systems engineering, extreme events, governance, smart grids, system of systems, X-Events

1 Introduction

Systems meet vital needs in our society by providing capabilities that are not possible by discrete components. These capabilities are manifested in a host of ways that include but are definitely not limited to: human activities; physical products; informational products; mechanical functions; logical decisions. Designing systems to meet these demands is the purpose of systems engineering. Traditional systems engineering (SE) is a discipline for solving problems that typically conforms to a certain set of assumptions. These assumptions often include: fully understood set of defined requirements; a single governance body for the development and configuration of the system; the relationship between the system and the external environment are defined and managed by machine interface specifications. The output of systems engineering is an engineered system. These systems are composed of multiple components with specific functionality, assembled in a hierarchal form and grouped into modules that perform functions. The systems functions are a sum of the functions of its components and modules (Blanchard and Fabrycky 2006). For the class of problems and systems that do not conform to these assumptions, another approach is required. Complex adaptive systems engineering (CASE), complexity engineering, and system of system engineering (SOSE) are names for the variation on traditional systems engineering that addresses the nature of complex systems and problems. These disciplines offer a platform that addresses technical systems and environments, where traditional SE assumptions do not hold (White 2009). Though there is some variation in the approaches, they are all based on complexity theory and share some common attributers.

The environment in which systems operate presents a variety of hazards (that is, stressors). Hazards can compromise the functions of the systems and jeopardize the successful completion of their missions. When characterizing systems in terms of their stress implications, there are several approaches to consider: risk, reliability, vulnerability, and resiliency. System analysis based on these methods are used to improve system designs; compare and select systems; identify systems that are in jeopardy more or less than others; and develop strategies and policies for governance given the hazards in our society. The general assumption in all of these methods is that the stressful events or hazards will result in negative system outcomes.

Antifragility is an approach that is not based on these assumptions; it considers the possibility that some systems might actually get better with stress (Taleb 2012). The authors' motivations are to explore methods for analyzing engineered systems in the context of the hazards they face. A framework is offered with a potential application for analyzing and measuring antifragility based on complex adaptive systems theories. The framework reduces a multidimensional concept of fragility into a two-dimensional, continuous interval scale. The authors present a systems dynamic model, as well as definitions of antifragility attributes in systems. In

* Corresponding author. E-mail: AGheorgh@odu.edu

section 2, a brief literature review and definitions of current approaches are presented for analyzing systems and how they respond to hazards (that is, stress). Antifragile systems are defined in section 3 through a discussion of complex adaptive systems (CAS), examples of antifragile systems, and observations from a simulation model of an antifragile system developed by the authors. Section 4 introduces a conceptual framework for analyzing hazards and systems based on systems engineering concepts and the authors' model for antifragility. The article concludes with observations and opportunities for additional study.

2 Analyzing Systems and Hazards

In the most basic form, a system is naively accepted to be a collection of interconnected parts. By this definition almost everything is a system of some sort. A more engineering focused definition includes the concept for an ensemble of autonomous elements, achieving a higher level functionality by leveraging their shared information, feedbacks, and interactions while performing their respective roles (Zadeh 1969; Sokolowski and Banks 2010; Buede 2011; INCOSE 2011). The elements of a system can include hardware, software, people, processes, policies, tools, doctrine, and virtually anything that is required to be transformed into desired outputs.

2.1 Hazards and Stressors

When systems are performing their intended purpose or otherwise functioning correctly, they are in an intended state. When systems are not functioning correctly they are in an unintended state. A state can be unintended and known (that is, predicable failure states). It can also be unintended and previously unknown (failure states or serendipitous state). Stressors are those forces outside of the specified operating conditions and constraints that threaten to move a system from an intended to an unintended state (Turner et al. 2003; Chrousos 2009).

The stress created by these forces can originate from internal interaction between system components, like heat caused by friction between moving parts or pressure gradually building up in a water line. Stress can also be the result of external hazards. A hazard is a physical condition, or event, that threatens the well-being of people, organizations, societies, environments, and/or property. Extreme hazards are those that potentially have catastrophic consequences and are generally not reducible to cause-effect relationships, which make them irreducible. These are the hazards that do not fit normal distributions. Their history of severity and frequency is not an indicator of their future behavior. These are the unknown unknowns, Black Swans, or X-Events (Taleb 2010, 2012; Casti 2012). X-Events can also be the unintended output of a system with both positive (serendipitous) and negative (catastrophic) consequences. System of systems (SOS) and complex adaptive systems (CAS), in particular, are designed with hazards in mind and are intended to have the ability to defend against stressors and hazards (X-Events). Analytical frameworks are required in order to assess this ability in systems as well as their propensity to produce X-Events.

2.2 Current Assessment Approaches

The threat that hazards pose varies in degree of impact and uncertainty of occurrence: for example, driving without a seatbelt, smoking, high-cholesterol diets, spending beyond ones means; under resourcing projects; and ignoring preventive maintenance. This is a pretty eclectic group of hazards. They span the spectrum of personal injury, financial loss, personal inconvenience, and even death, with low to almost certain occurrence. The impact and uncertainty of occurrence posed by a hazard is an exogenous point of view and is focused on the hazard rather than the system that experiences it. What are the chances that a hazard will occur and if it does, how will it impact the system? These questions are addressed in the framework of risk analysis. How does the system (people, property, and/or environment) respond when a hazard (that is, stress) is experienced? There are both exogenous and endogenous considerations to this question. The answer can be determined by the characteristics of the system and its environment: reliability, vulnerability, and resiliency (Table 1).

3 Complex Adaptive Systems

When the outputs of a system are predictable and can be explained or reduced to the behaviors of its micro level components, then the system is resultant. However, when the system has unexpected outputs and the behavior is not explainable by its components, the system is emergent (Goldstein 1999; Bar-Yam 2004). Emergence is both a characteristic and a phenomenon in complex systems. As a characteristic, emergence is the same as irreducibility, that is, the inability to transfer knowledge, methods, causations, or explanations about the macro system to its micro system components, and vice versa (Menzies 1988; Christen and Franklin 2002). As a phenomenon, emergence is an interesting and unpredicted pattern, behavior or otherwise state of the system (Holland 2012).

3.1 Adaptive Systems

In a dynamic environment, a host of things are always changing: conditions, constraints, threats, opportunities, technology, knowledge, requirements, and so on. The ability to make internal adjustments in response to, or in anticipation of, external environmental changes, is the essence of being adaptive. In less complex systems, these changes take place based on pre-established rules in the system that allows

Table 1. Hazard response characteristics of systems

Characteristic	Definition	Considerations
Risk Analysis	A process of identifying potential hazards based on severity of consequence and likelihood of occurrence (McNeil, Frey, and Embrechts 2005). The intent is to sort potential hazards (that is, risk) and prioritize them for action based on objective criteria. One method is to grade likelihood and consequence on a scale of 1–5 (Simpleman et al. 2003; PMI 2008).	Exogenous
Vulnerability	The openness of a system to lose its design functions or the degree to which a system, subsystem, or component is in situations where it is exposed to those specific hazards that would be harmful or damaging to the system (Dowdney et al. 1995; Turner et al. 2003; Adger 2006; Gheorghe and Vamanu 2004).	Exogenous
Reliability	Determines the probability that a system will remain in an intended or non-failure state while operating (Dowdney et al. 1995; Johansson and Hassel 2010; Defense Acquisition University 2012). Systems are reliable to the extent that they are able to continue functioning and producing desired outcomes even when operating conditions are at the extremes of their specified limits (Kececioglu 1991; Kundur et al. 2004).	Endogenous
Resiliency	The ability of a system to quickly return to its intended or non-failure state (Kjeldsen and Rosbjerg 2004; Laprie 2008) or the capacity of a system to absorb stress (Gheorghe and Muresan 2011; Gheorghe 2013). The key element of resiliency is not the ability to withstand stress by remaining unchanged, but rather the ability to bounce back to a desired state after experiencing a stressor.	Endogenous

the component (or agent) to anticipate the consequences of particular actions. The structure of the rules are typically "if condition then action." Based on these rules, the agents in an adaptive system autonomously analyze the environment and make adjustments, and respond within the constraints of their established rules (Lansing 2003). Complex adaptive systems (CAS) are not only responsive to environment dynamics; they have the ability to learn from experiences (Geli-Mann 1994). Learning is distinguished from merely adapting based on environmental experiences to predefined structures based on internal rule sets. Learning goes further by forming new emergent structures that were previously unknown. CAS self-organize and display Darwinism or natural selection type behaviors like those of biological systems (Holland 1992; Brandon 2010). The complex adaptive system applies artificial (or natural) intelligence to adjust its schema and may apply a revised set of rules to future environmental experiences. These adjusts over time allow CAS to improve as they experience hazards and stress over time.

3.2 An Alternative Framework

How systems respond to X-Events as stressors, or how they produce X-Events as unintended outputs, can alternatively be characterized on a continuum that ranges from fragile (degrading with stress), to robust (unchanged by stress), to antifragile (improving with stress) (Taleb 2012).

3.2.1 Robustness

Systems have to perform their functions over a range of environmental conditions. These conditions include varying levels of stress from a variety of stressors. Robustness is the ability of a system (or characteristic of a system) to remain in a desired state over a range (magnitude and duration) of stress (Stelling et al. 2004; Kriete 2013). The broader the range of stress and the more stable the system (or particular attribute of the system), the more it is considered to be robust. The lack of sensitivity or the increased tolerance to stress makes a system more robust than systems that are sensitive or less tolerant to stress. Arguably, the concepts of robustness and reliability are very similar. However, there is a critical difference. Reliability is remaining unchanged within specified limits while robustness is remaining unchanged outside of specified limits (Laprie 2008). To be robust is to withstand stress due to X-Events.

3.2.2 Fragility

While robust systems (or system characteristics) remain unchanged by stress and continue to function, stress can easily cause a fragile system (or system characteristics) to fail (Allen and Hoekstra 1993). Like robustness and reliability, fragility and vulnerability are similar, but have critical differences. Vulnerable systems fail because of their degree of exposure to stress of a specific nature, while fragile systems fail because they are easily broken regardless of the nature of stress they are exposed to. Vulnerability is an exogenous matter of susceptibility while fragility is an endogenous matter of weakness.

3.2.3 Antifragile

In some cases, not only do some systems develop the ability to withstand stress but they actually get better as they are exposed to stress or they produce serendipitous outputs; hence the term "antifragile" (Taleb 2012). Taleb argues that to some extent a system's ability to withstand stress is a function of intended exposures to smaller stress events. Regular exposure to smaller doses of stress can strengthen a system and protect it from X-Events (or extreme stress). This is an endogenous characteristic but unlike any of the other concepts previously mentioned.

3.3 Antifragile Examples

Most of us are familiar with the Greek mythological creature Hydra and her many heads. When Hercules attempted to kill the monster by cutting off its head, two would grow in its place (Linebaugh and Rediker 1990). This may be the ultimate example of antifragility as there were no limits to the expanding generation of Hydra's heads. This section presents several real world antifragile examples. Though not a comprehensive list, the examples demonstrate that antifragility is more than a mythical concept.

3.3.1 Living Systems

We can look to the field of biology for real life versions of Hydra. Danchin, Binder, and Noria (2011) describe how after attempts to destroy life, many new forms evolve. Living systems possess the characteristic of "novelty creation." When confronted with stress (that is, attempts to destroy them), they form previously unknown strains and structures. In other words they are emergent. Living systems use information management to enable successive generations to get stronger by learning from metadata about the stressors (antibiotics, antivirals, and so on.) experienced by previous generations.

Consider forest fires. Forest fires destroy trees, but they also enable trees and other desirable vegetation to flourish (Certini 2005). The overgrowth of ground cover plants can prevent the germination of seeds from trees and ultimately stop their growth. Excessive overgrowth also is a source of fuel for more intense fires which not only destroy more trees but cause damage to the soil. Forest fires help the growth of trees by removing ground cover so seeds can germinate, and by removing excessive fuel so the fires will not grow stronger and do more damage.

3.3.2 Industry and Technology

Airplane crashes can be tragic events. However, these crashes are "the fuel" for continuous improvement in aviation. The Aviation Safety Information Analysis and Sharing (ASIAS) system connects over 131 databases of aviation safety incidents (Duquette 2013). Though in more recent years there has been very modest improvement, the aviation industry has successfully used data about failures to improve flight safety by 139 times over the last sixty years (Graham 2010; Pasztor 2013). In contrast to its information systems (safety data, traffic control, and so on) which are highly coupled, the aviation industry's components (planes, pilots, airports, airlines companies, and so on) are loosely coupled. This means the safety of one flight is not directly dependent on another flight and the failures do not ripple through the system. This allows one flight to tragically crash and the other flights to benefit from the postcrash analysis. Under these conditions, a short-term increase in aviation accidents can lead to greater overall safety in the industry.

Netflix is well known for being an inexpensive source for online movies. However, they are also pioneers in the area of antifragile internet based systems. This may not be the official title of their effort, but it is an appropriate fit. Netflix created "Chaos Monkey," a software application that intentionally generates real system outages with the intent that engineers will fix small outages and apply lessons learned to prevent larger outages in their video streaming business (Bennett and Tseitlin 2012). They also use the approach as a form of Hormesis and natural selection to weed out weak components and subsystems. Their original efforts were limited to small sectors of their network, but have expanded to include city-wide outages. Netflix is currently experimenting with "Chaos Gorilla" which will take down entire states. Netflix is applying the principle of supplying small amounts of stress to build up resistance against future stressors that could be catastrophic to their network.

3.4 The Antifragility Model

Based on the examples and definitions previously discussed, a model of an antifragile system can be constructed. Using the stock and flow structure from systems dynamic modeling (Sterman 2000), the authors represent antifragile systems in Figure 1 and simulation output of the model in Figure 2.

3.4.1 Model Description

System stress is generically represented by the boxed variable (that is, a stock) "stress." Stress is increased by the variable "change in stress." From the definitions and examples discussed, stress has an impact on "system performance." The positive impact of stress does not exist in perpetuity; there are limits before the impact will turn negative. System performance is also a stock variable and is increased by the variable "increase in performance" when the impact from stress is positive and decreased by the variable "decrease in performance" when the impact from stress is negative. System performance can represent the entire system or particular

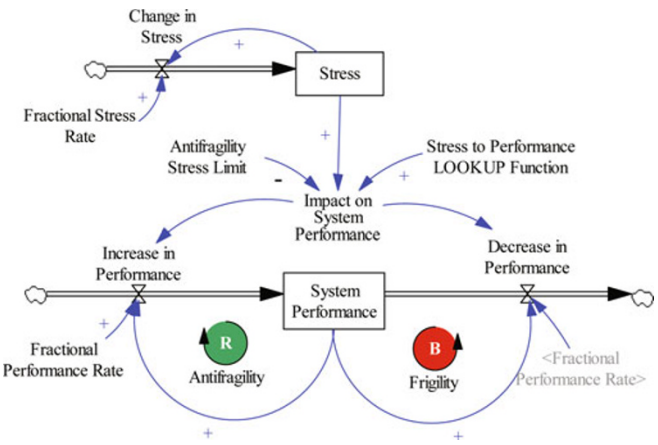

Figure 1. System dynamic model of antifragility

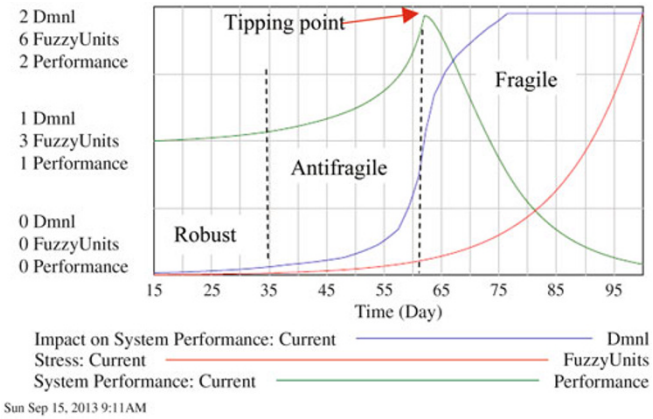

Figure 2. Antifragile system dynamic simulation

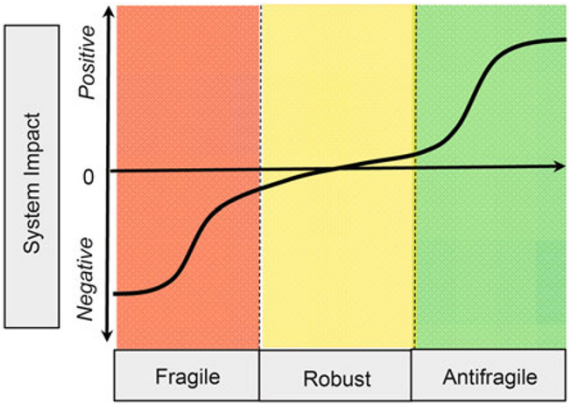

Figure 3. Antifragility curve

attributes of the system. The other variables in the model are necessary for the structure and simulation of the model.

The most important characteristic of the model is its reinforcing and balancing loops. The green circle with the clockwise arrow represents the system's tendency to be antifragile: as the rate of change in system performance is increased by stress, it causes the stock of performance to grow which in turn increases the rate of change in performance and causes even more performance growth. Performance would continue to grow indefinitely if it were not for the balancing loop (the red circle with the counterclockwise arrow). The balancing loop has the opposite effect on system performance and represents the system's tendency to be fragile: the rate of decreasing performance is increased by the negative impact of stress and causes the stock of performance to decline. Since the rate of decline is a function of the existing performance level, the rate of decline is initially high but declines as level of performance gets lower. Performance continues to decline but at ever decreasing rates as the level approaches zero.

3.4.2 Simulation Results

There are three variables represented in Figure 2: impact of stress on system performance (blue line); stress level (red line); and system performance (green line). Running a simulation of the model, several observations can be made that further support the definition of an antifragile system. When the slope of the three variables is relatively flat, the system is in a robust state. It is remaining unchanged by stress. As the slopes begin to increase the system moves into an antifragile state. During this phase, performance increases beyond the system's initial level. As observed in the examples presented, there is a limit to system improvement caused by stress. Once the stress level reaches a "tipping point" the slope of the impact variable starts to decrease and the system enters a fragile state. During this phase the impact of stress is negative, the system's performance continues to decline and approaches zero (complete failure).

3.5 The Antifragility Curve

The relationship between the impacts of stress on system performance can be expressed graphically as seen in Figure 3.

When the system is in the Robust zone, all outcomes are known and intended. The system is functioning according to its design and the stakeholder's expectations. As the curve moves to the regions left of Robust and into the Fragile zone, forces from stressors eventually overcome the system and it rapidly declines into a failure state. All outcomes in the fragile zone are unintended but may include known failure states as well as previously unknown failure states (or X-Events). All outcomes to the right of Robust are positive outcomes that were previously unknown (or positive X-Events).

4 Assessing Antifragility in Complex Adaptive Systems

In order to determine where a system fits on the antifragility curve, a set of analytical criteria must be identified. For each criterion, given the strategies, policies, and design of the system, the question is: how will the system respond to an X-Event or other stressor?

4.1 Analytical Criteria

Complex systems can be characterized by a set of common attributes that they tend to possess. Analyzing systems in terms of these attributes can provide insight into how the system will respond to stressors. Several concepts are presented on which to base the analysis of complex systems in terms of their response to stress (or X-Events). In their books *X-Events: The Collapse of Everything* and *Antifragile: Things that Gain from Disorder*, Casti (2012) and Taleb (2012) discuss system attributes based on theories of system responses to X-Events. Jackson and Ferris (2012) offer a list of criteria based on domain expert analysis of 10 case studies on system of system

Table 2. Antifragility analytical criteria

Attribute	Theory
Entropy	Systems tend to increase in complexity over time. In doing so they lose the ability to use information to transform inputs into desired outputs; the number of potential system states relative to known system states increase (that is, disorder grows); and X-Events emerge (Chakrabarti and De 2000; Atkins 2003; Bradnick 2008).
Emergence	The relationship between the outputs of a system at the macro level and the actions of the micro level components in the system is either resultant or emergent (Goldstein 1999). When system outputs can be directly traced to activities or functions of its components and there are cause-effect relationships between micro level component activity and macro level results, then the system output is said to be resultant. However, when no such traceability can be constructed, the output is said to be emergent and X-Events are produced (Menzies 1988; Christen and Franklin 2002).
Efficiency vs. Risk	Efficiencies are gained at the expense of increased potential for harm due to stress. For example, redundant components may reduce the potential for system failure, but at the expense of more resources without more functionality or output. Less redundant systems designs are more efficient but are more fragile.
Balancing Constraints vs. Freedom	The optimum condition for a system is a balance of constraints and degrees of freedom. A system that is too open (that is, high degrees of freedom, minimum constraints, maximum interactions and dependencies with other systems, and so on) has increased exposure to X-Events.
Coupling (Loose/Tight)	Failures can reverberate through tightly coupled (that is, linked) systems increasing in amplitude and potentially leading to catastrophic failure. The greater the degree of coupling between systems and system components, the more fragile the system becomes.
Requisite Variety	There are regulators in a SOS that attempt to control the outcome and behaviors of the agents in the system. When the number of regulators is insufficient relative to the number of agents, the behavior of the system becomes unpredictable and extreme hazardous events emerge. In other words, a gap in complexity of the systems and its agents or subsystems causes X-Events to occur.
Stress Starvation	Withholding stress from systems or attempting to reduce uncertainty in them can cause weakness, fragility, and expose them to hazardous X-Events. Applying regular and controlled stress to a system can increase its robustness and potentially lead to antifragility.
Redundancy	Having duplicate components that are required for a function or duplicate functions to meet the same objective, are to create excess system capacity and are effective hazard defenses. This is good for building robustness to a degree, but falls short when it is based on estimates from historical worse case events. When X-Events reoccur, they can do so with an impact that is more or less than the historical levels. Redundancy tends to stabilize systems and make them more robust (that is, less fragile but not antifragile).
Non-Monotonicity	Learning from mistakes can be an effective defense against stressors. Mistakes and failures can lead to new information. As new information becomes available it defeats previous thinking, which can result in new practices and approaches (Augusto and Simari 2001; Nute 2003; Goverrtori and Terenziani 2007). In this case, stressors can actually cause the system to improve.
Absorption	Systems shall have design margins that can encompass (that is, absorb) the magnitude and duration of the potential stress it may encounter and continue in an intended state. The greater the absorption, the greater the robustness and the less the fragility. Absorption does not increase antifragility.

interventions intended to improve a system's ability to survive a threat. These theories and related system complexity theories are summarized in Table 2.

4.2 Evaluating Systems

Systems are evaluated based on systems attributes that are of interest to its stakeholders: strategies, policies, governance structure, components, subsystems, processes, and so on. Questions are framed about a system in terms of how the system would respond to stress and answered based on the criteria in Table 2. The question should require a quantitative response on an interval scale. Many methods can be used to collect and aggregate responses. For example, the inventory of questions can be answered by subject matter experts or stakeholder focus groups, and the responses aggregated using Delphi methods (Ishikawa et al. 1993; Rowe and Wright 2001) and quantified using fuzzy logic (Zadeh 1975; Klir and Yuan 1995). For example, Likert type questions could be posed for one or more system attributes:

A. The system performance will improve if it experiences stress
- Strongly disagree (1)
- Somewhat disagree (2)
- Somewhat agree (3)
- Agree (4)
- Strongly agree (5)

B. If the system experiences stress, it will
- Significantly degrade (1)
- Moderately degrade (2)
- Remain the same (3)
- Moderately improve (4)
- Significantly improve (5)

The specific questions are less important than the format in which they are framed. The interval responses maintain order and distance. Having responses on an interval scale is most important to be able to aggregate responses for each criterion (and multiple responders if necessary), apply statistics, and draw inferences (see Section 5).

5 Smart Grid Example

The smart grid electrical power system and space weather hazard are used here to demonstrate the application of the antifragility analysis framework.

5.1 Applying Antifragility Analysis

The electric power grid refers to a system that performs four major operations for electricity: generation, transmission, distribution, and control (Kappenman 2001; Fang et al. 2011). The basic system consists of a power generation plant, power transmission substations, power distribution substations, and power consumers (commercial, residential, and industrial) (Gheorghe and Muresan 2011; Gao et al. 2012). Space weather is solar induced disturbances as meteorological phenomenon (Gold 1959; Kane 2006). The electric currents produced by space weather storms have the most potential for damage to electrical power grids. These powerful currents have the potential to penetrate almost any natural or man-made structure: power lines, stone, rock, metal, and brick, for example (Fry 2012).

5.1.1 Implications of Space Weather on Smart Grid Development

Space weather is episodic, with long periods of calm between storms followed by rare periods of extreme events that can have catastrophic impacts on technology (Hapgood 2011). The major classes of power system failures that can have space weather implications are: voltage collapse, frequency collapse, loss of synchronism, large power swings, and cascade of overloads (Singh 2012). Smart grid technologies improve the efficiency and performance of electrical power systems. However, these technologies are still vulnerable to space weather events, as much or possibly more so than the basic power grid. Smart grids are complex adaptive systems that are highly interconnected and dependent upon communication systems (wireless networking and internet). The dependencies among artifacts expose them to the risk of cascading failures (Bar-Yam 2005; DeWeck, Roos, and Magee 2012). Even if geomagnetically-induced currents (GICs) or electromagnetic energy from solar flares only made localized contact with the power grid, the interdependencies of the smart grid can lead to broad cascading failures. Space weather is inevitable and cannot be prevented. It is not a question of if, but when a space storm will occur. Even though the storm cannot be avoided, societies can take defensive measures to mitigate the risk. An effective defense plan for smart grid systems against space weather must address the speed and breadth of the space storm event as well as the interdependent nature of the power system artifacts. Important aspects of an effective defense plan include (Singh 2012; RAE 2013):

- Intelligent Electronic Devices (IEDs)—High-speed protective relays, and programmable logic controllers (PLCs) can shut down segments of the power grid tens of milliseconds to protect the system from cascading failures.
- Wide Area Monitoring Protection and Control (WAMPAC)—Rather than local protection of individual equipment (transformer, generator, line, and so on), the WAMPAC strategy attempts to protect the whole power system. WAMPAC uses Wide Area Measurement Systems (WAMS) to monitor the system and identify opportunities for proactive interventions, and Wide Area Control (WAC) to implement automated actions to minimize the spread of negative events in the system.
- Temporary interconnectivity—Create paths in the power grid that can be proactively disconnected if there is a threat of a solar storm.
- More robust components—Advanced materials help make transformers, transmission lines, and circuits resistant to spikes in electromagnetic currents and high-voltage strikes.
- Modeling and simulation (M&S)—M&S can be an effective tool to better understand the risk, and to test potential grid modifications.
- Weather event forecasting—Much like the terrestrial weather forecasting system, implementing forecasting for space weather could provide early warning of impending storms. This will allow suppliers, businesses, and individuals to be better prepared for a space weather X-Event: increasing power reserves, staging spare components, and relocating critical systems to unthreatened sections of the grid.

5.1.2 Antifragility Analysis of Smart Grid Power Systems

The antifragility analysis of smart electrical grids in the United States is summarized in the following section. For demonstration purposes, following expert discussions, a scale from −10 to 10 is used to represent fragility, robustness, and antifragility: $-10 \leq$ fragility < -3; $-3 \leq$ robustness ≤ 3; $3 <$ antifragility ≤ 10. The results represent a hypothetical survey of domain experts: red where the assessment finds exposure to an X-Event will cause the system to degrade (that is, system is fragile); yellow where there is no expected impact (that is, the system is robust); and green where the findings suggest the system may actually improve (that is, the system is antifragile). The antifragility measurement is an average of the impact score for each criterion: Average (entropy, emergence, efficiency vs. risk, balancing constraints vs. freedom, coupling, requisite variety, stress starvation, redundancy, non-monotonicity, absorption) = Fragility Score.

5.2 Summary

The application of the antifragility analysis framework to the U.S. smart power grid is summarized in Table 3 and Figure 4.

Table 3. Summary of the U.S. smart power grid system analysis

Attribute	Analysis	Impact
Entropy	Efficiency of information in the power grid system declines as the interconnectedness and the number of components increase. Given the growing interconnectedness, the increasing demand curve for power and the entrance of new suppliers as a result of deregulation there appear to be indications of growing entropy. Therefore, a space weather X-Event will likely still cause the system to degrade.	−8
Emergence	Significant efforts are being made to increase the system's robustness through component improvements. These attempts are not likely to work as space weather is complex and not reducible to a predicable vector for which component design criteria can be established. Consequently, a space weather X-Event will likely cause the system to degrade.	−7
Efficiency vs. Risk	Reducing power usage far below the capacity of the system would create power reserves that could be transferred to damaged areas of the grid in the event of a power interruption. However, the trend in the power industry is in the other direction toward: greater capacity consumption, reductions in safety margins, increased efficiencies, and therefore increased risk. A space weather X-Event will likely cause the system to degrade.	−7
Balancing Constraints vs. Freedom	Regulations promote safety in the power grid system by controlling who can distribute power, and standards for how power is distributed. As the industry moves toward greater deregulation there will be more distributors, fewer controls on standards for use, and greater opportunities for dangerous practices that make it easier to break the system. These practices make the system more fragile. A space weather X-Event will likely cause the system to degrade.	−6
Coupling	Integration of internet technologies is increasing the coupling of components and agents in power grid systems. However, temporary interconnectivity and the implementation of Intelligent Electronic Devices (IEDs) are among the strategies to lessen the likelihood that cascading failures will occur. A space weather X-Event will likely have little to no impact on the system.	−1
Requisite Variety	Privatization of the utility industry through deregulation is increasing the variety of suppliers in the power grid system and decreasing the variety for the U.S. government as a controlling body. This puts the system at risk of not having enough controls to keep the power grid system stable. A space weather X-Event will likely cause the system to degrade.	−7
Stress Starvation	There is no evidence that e.g. the United States has a practice of intentionally exposing its power grid system to regular and sustained stress in an effort to build its resilience. In fact, our technologies are intended to reduce uncertainty and make the system less exposed to stress. A space weather X-Event will likely cause the system to degrade.	−8
Redundancy	Technology has been used to create multiple paths to transport power, and process information. If one subsystem fails, power can be diverted to or from another source. However, the redundancies are only good if the X-Event does not exceed the excess capacity they create. A space weather X-Event will likely have little to no impact on the system.	−1
Non-Monotonicity (Learning from Mistakes)	The transparency created by the openness of U.S. society creates an opportunity for society to learn from its mistakes. The free market economy creates motivation to learn from past mistakes and create profitable business opportunities. Innovations are created based on these mistakes and the prospects of profiting from innovation. A space weather X-Event will ultimately have a positive impact on the system.	+4
Absorption	Advanced materials in smart grid power systems help make transformers, transmission lines, and circuits more resistant to spikes in electromagnetic currents. The components allow the design margins to be increased, which improves the system's ability to withstand stress form space weather. A space weather X-Event will likely have no impact on the system.	−2

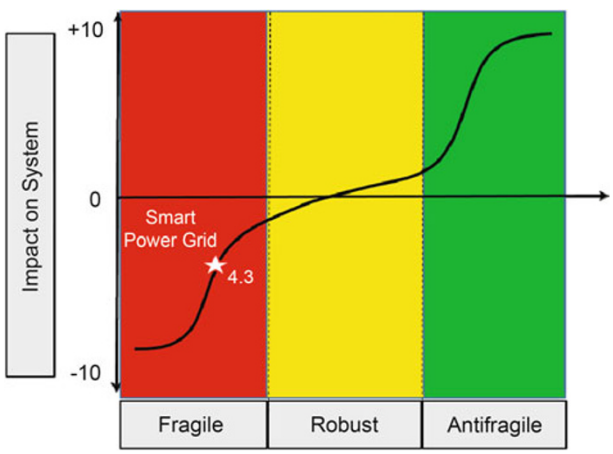

Figure 4. Smart power grid antifragility analysis for e.g. the United States

For six of the ten analytical criteria (or 60%), it was determined that a space weather X-Event would have a negative impact on the U.S. smart power grid. There was only one case of antifragility, and three cases of robustness. The average score on the antifragility analysis was −4.3. Based on this result, we can conclude that the space weather defense plan and smart grid technology, in general, are not having the intended effect of reducing the threat of space weather. In terms of the fragility continuum, U.S. power grid systems would be considered fragile and would degrade with exposure to the stress of a space weather X-Event.

6 Conclusion

The antifragility analysis framework has the potential to provide new insight about systems and system characteristics

in terms of their ability to withstand or improve when they experience stress. The antifragile simulation model demonstrates the antifragile concept. However, the model assumes first order relationships between stress and system performance when in fact the relationships might be of higher orders. The model can be improved by formally defining these relationships. More work also needs to be done to define the standards for selecting the evaluation criteria, and methods for aggregating evaluation results. Though the antifragility evaluation has been presented as a two-dimensional analysis, in reality a multidimensional construct may be more appropriate. The authors are investigating the application of multiattribute decision-making and evidential reasoning as potential methods to address the issues of aggregation and representation of multidimensional considerations.

References

Adger, W. N. 2006. Vulnerability. *Global Environmental Change* 16 (3): 268–281.

Allen, T. F. H., and T. W. Hoekstra. 1993. Toward a Definition of Sustainability. In: *Sustainable Ecological Systems: Implementing an Ecological Approach to Land Management*, edited by W. W. Covington and L. F. Debano, 98–107. Rocky Mountain Forest and Range Experiment Station, Fort Collins, Colorado.

Atkins, P. 2003. *Galileo's Finger: The Ten Great Ideas of Science*. Oxford: Oxford University Press.

Augusto, J. C., and G. R. Simari. 2001. Temporal Defeasible Reasoning. *Knowledge and Information Systems* 3 (3): 287–318.

Bar-Yam, Y. 2004. A Mathematical Theory of Strong Emergence Using Multiscale Variety. *Complexity* 9 (6): 15–24.

Bar-Yam, Y. 2005. *Making Things Work: Solving Complex Problems in a Complex World*. Cambridge, MA: Knowledge Press.

Bennett, C., and A. Tseitlin. 2012. Netflix: Chaos Monkey Released into the Wild. Netflix Tech Blog.

Blanchard, B. S., and W. J. Fabrycky. 2006. *Systems Engineering and Analysis*, 5th Edition. Upper Saddle River, NJ: Pearson/Prentice Hall Prentice International Series in Industrial and Systems Engineering.

Bradnick, D. 2008. A Pentecostal Perspective on Entropy, Emergent Systems, and Eschatology. *Zygon: The Journal of Religion and Science* 43 (4): 925– 942.

Brandon, R. 2010. Natural Selection. In: *Stanford Encyclopedia of Philosophy*, Fall 2010 Edition, edited by E. N. Zalta. http://plato.stanford.edu/archives/fall2010/entries/natural-selection/.

Buede, D. M. 2011. *The Engineering Design of Systems: Models and Methods*. Wiley Series in Systems Engineering and Management (Vol. 55). Hoboken, NJ: John Wiley & Sons.

Casti, J. L. 2012. *X-Events: The Collapse of Everything*. New York: HarperCollins.

Certini, G. 2005. Effects of Fire on Properties of Forest Soils: A Review. *Oecologia* 143 (1): 1–10.

Chakrabarti, C. G., and K. De. 2000. Boltzmann-Gibbs Entropy: Axiomatic Characterization and Application. *International Journal of Mathematics and Mathematical Sciences* 23 (4): 243–251.

Christen, M., and L. R. Franklin. 2002. The Concept of Emergence in Complexity Science: Finding Coherence between Theory and Practice. *Proceedings of the Complex Systems Summer School*, 4. Santa Fe, New Mexico.

Chrousos, G. P. 2009. Stress and Disorders of the Stress System. *Nature Reviews Endocrinology* 5 (7): 374–381.

Danchin, A., P. M. Binder, and S. Noria. 2011. Antifragility and Tinkering in Biology (and in Business) Flexibility Provides an Efficient Epigenetic Way to Manage Risk. *Genes* 2 (4): 998–1016.

Defense Acquisition University. 2012. Glossary of Defense Acquisition Acronyms and Terms: Reliability Key System Attribute (KSA). https://dap.dau.mil/glossary/pages/2555.aspx.

DeWeck, O. L., D. Roos, and C. L. Magee. 2012. *Engineering Systems: Meeting Human Needs in a Complex Technological World*. Cambridge: MIT Press.

Dowdney, L., L. Woodward, A. Pickles, and D. Skuse. 1995. The Body Image Perception and Attitude Scale for Children: Reliability in Growth Retarded and Community Comparison Subjects. *International Journal of Methods in Psychiatric Research* 5 (1): 29–40.

Duquette, A. 2013. U.S. Aviation Industry, FAA Share Safety Information with NTSB to Help Prevent Accidents. http://aireform.com/news-clips-folder-2/u-s-aviation-industry-faa-share-safety-information-with-ntsb-to-help-prevent-accidents-faa-news-release/.

Fang, X., S. Misra, G. Xue, and D. Yang. 2011. Smart Grid – The New and Improved Power Grid: A Survey. *Communications Surveys & Tutorials*, IEEE 14 (4): 944–980.

Fry, E. K. 2012. The Risks and Impacts of Space Weather: Policy Recommendations and Initiatives. *Space Policy* 28 (3): 180–184.

Gao, J., Y. Xiao, J. Liu, W. Liang, and C. L. Chen. 2012. A Survey of Communication/Networking in Smart Grids. *Future Generation Computer Systems* 28 (2): 391–404.

Geli-Mann, M. 1994. Complex Adaptive Systems. In: *Complexity: Metaphors, Models and Reality*, edited by M. Geli-Mann and J. A. Hawkins, 17–45. Reading, MA: Addison-Wesley.

Gheorghe, A. V. 2013. Lecture Notes. Engineering Management and Systems Engineering Department, Old Dominion Uiversity, Norfolk, VA.

Gheorghe, A. V., and L. Muresan, eds. 2011. *Energy Security: International and Local Issues, Theoretical Perspectives, and Critical Energy Infrastructures*. London: Springer.

Gheorghe, A. V., and D. V. Vamanu. 2004. Towards QVA – Quantitative Vulnerability Assessment: A Generic Practical Model. *Journal of Risk Research* 7 (6): 613–628.

Gold, T. 1959. Plasma and Magnetic Fields in the Solar System. *Journal of Geophysical Research* 64 (11): 1665–1674.

Goldstein, J. 1999. Emergence As a Construct: History and Issues. *Emergence* 1 (1): 49–72.

Governtori, G., and P. Terenziani. 2007. Temporal Extensions to Defeasible Logic. In: *AI 2007: Advances in Artificial Intelligence*, edited by M. A. Orgun and J. Thornton, 476–485. Berlin: Springer.

Graham, N. 2010. Aviation Safety: Making a Safe System Even Safer. Air Navigation Bureau, International Civil Aviation Organization. http://www.icao.int/Newsroom/Presentation%20Slides/Streaming%20video%20message%20-%20Aviation%20Safety.pdf.

Hapgood, M. A. 2011. Towards a Scientific Understanding of the Risk from Extreme Space Weather. *Advances in Space Research* 47 (12): 2059–2072.

Holland, J. H. 1992. Complex Adaptive Systems. *Daedalus* 121 (1): 17–30.

Holland, O. T. 2012. *Partitioning Method for Emergent Behavior Systems Modeled by Agent-Based Simulations*. Old Dominion University. ProQuest Dissertations and Theses, 283. http://search.proquest.com/docview/1283121663?accountid=12967.

INCOSE (International Council on Systems Engineering). 2011. *Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities*. INCOSE-TP-2003-002-03.2. 1. INCOSE.

Ishikawa, A., M. Amagasa, T. Shiga, G. Tomizawa, R. Tatsuta, and H. Mieno. 1993. The Max-Min Delphi Method and Fuzzy Delphi Method Via Fuzzy Integration. *Fuzzy Sets and Systems* 55 (3): 241–253.

Jackson, S., and T. L. Ferris. 2012. Resilience Principles for Engineered Systems. *Systems Engineering* 16 (2): 152–164.

Johansson, J., and H. Hassel. 2010. An Approach for Modelling Interdependent Infrastructures in the Context of Vulnerability Analysis. *Reliability Engineering & System Safety* 95 (12): 1335–1344.

Kane, R. P. 2006. The Idea of Space Weather – A Historical Perspective. *Advances in Space Research* 37 (6): 1261–1264.

Kappenman, J. G. 2001. An Introduction to Power Grid Impacts and Vulnerabilities from Space Weather. In: *Space Storms and Space Weather Hazards*, edited by I. A. Daglis, 335–361. Springer.

Kececioglu, D. 1991. *Reliability Engineering Handbook: Volume I*. Englewood Cliffs, NJ: Prentice Hall.

Kjeldsen, T. R., and D. Rosbjerg. 2004. Choice of Reliability, Resilience and Vulnerability Estimators for Risk Assessments of Water Resources Systems (Choix d'estimateurs de fiabilité, de résilience et de vulnérabilité pour les analyses de risque de systèmes de ressources en eau). *Hydrological Sciences Journal* 49 (5): 755–767 (in French).

Klir, G. J., and B. Yuan. 1995. *Fuzzy Sets and Fuzzy Logic*. Upper Saddle River, NJ: Prentice Hall.

Kriete, A. 2013. Robustness and Aging – A Systems-Level Perspective. *Biosystems* 112 (1): 37–48.

Kundur, P., J. Paserba, V. Ajjarapu, G. Andersson, A. Bose, C. Canizares, and V. Vittal. 2004. Definition and Classification of Power System Stability. IEEE/CIGRE Joint Task Force on Stability Terms and Definitions. *IEEE Transactions on Power Systems* 19 (3): 1387–1401.

Lansing, J. S. 2003. Complex Adaptive Systems. *Annual Review of Anthropology* 32 (1): 183–204.

Laprie, J. C. 2008. From Dependability to Resilience. 38th IEEE/IFIP International Conference on Dependable Systems and Networks, Anchorage, Alaska, USA, June 2008.

Linebaugh, P., and M. Rediker. 1990. The Many-Headed Hydra: Sailors, Slaves, and the Atlantic Working Class in the Eighteenth Century. *Journal of Historical Sociology* 3 (3): 225–252.

McNeil, A. J., R. Frey, and P. Embrechts. 2005. *Quantitative Risk Management: Concepts, Techniques, and Tools*. Princeton, NJ: Princeton University Press.

Menzies, P. 1988. Against Causal Reductionism. *Mind* 97 (388): 551–574.

Nute, D. 2003. Defeasible Logic. In: *Web Knowledge Management and Decision Support*, Lecture Notes in Computer Science, Vol. 2543, edited by O. Bartenstein, U. Geske, M. Hannebauer, and O. Yoshie, 151–169. London: Springer.

Pasztor, A. 2013. NTSB Report Highlights Safety Gains Across U.S. Commercial Aviation. *Wall Street Journal*. http://online.wsj.com/article/SB10001424127887324522504578654920889235036.html.

PMI (Project Management Institute). 2008. *A Guide to the Project Management Body of Knowledge: PMBOK® Guide*. Newtown Square, PA.

RAE (Royal Academy of Engineering). 2013. *Extreme Space Weather: Impacts on Engineered Systems and Infrastructure*. London: Royal Academy of Engineering. http://www.raeng.org.uk/news/publications/list/reports/space_weather_full_report_final.pdf.

Rowe, G., and G. Wright. 2001. Expert Opinions in Forecasting: The Role of the Delphi Technique. In: *Principles of Forecasting*, edited by J. Armstrong, 125–144. Norwell, MA: Kluwer Academic Press.

Simpleman, L., P. McMahon, B. Bahnmaier, K. Evans, and J. Lloyd. 2003. *Risk Management Guide for DOD Acquisition* (Version 2.0). Defense Acquisition University, Ft. Belvoir, VA.

Singh, A. 2012. Smart Grid Wide Area Monitoring, Protection and Control. *International Journal of Engineering Research and Applications* 2 (6): 553–584.

Sokolowski, J., and C. M. Banks, eds. 2010. *Modeling and Simulation Fundamentals: Theoretical Underpinnings and Practical Domains*. Hoboken: Wiley.

Stelling, J., U. Sauer, Z. Szallasi, F. J. Doyle III, and J. Doyle. 2004. Robustness of Cellular Functions. *Cell* 118 (6): 675–685.

Sterman, J. 2000. *Business Dynamics: Systems Thinking for a Complex World*. New York: McGraw-Hill.

Taleb, N. N. 2010. *The Black Swan: The Impact of the Highly Improbable Fragility*. New York: Random House Digital.

Taleb, N. N. 2012. *Antifragile: Things that Gain from Disorder*. New York: Random House Digital.

Turner, B. L., R. E. Kasperson, P. A. Matson, J. J. McCarthy, R. W. Corell, L. Christensen, N. Eckleyg, J. X. Kasperson, et al. 2003. A Framework for Vulnerability Analysis in Sustainability Science. *Proceedings of the National Academy of Sciences* 100 (14): 8074–8079.

White, B. E. 2009. Complex Adaptive Systems Engineering (CASE). In: *Proceeding of Systems IEEE Xplore Conference*, 3rd Annual IEEE, 70–75.

Zadeh, L. A. 1969. The Concepts of System, Aggregate, and State in System Theory. In: *System Theory*, edited by L. A. Zadeh and E. Polak, 3–42. New York: McGraw-Hill.

Zadeh, L. A. 1975. The Concept of a Linguistic Variable and Its Application to Approximate Reasoning – I. *Information Sciences* 8 (3): 199–249.